Cisco Meeting Server

Cisco Meeting Server リリース 3.7

単一分割サーバ導入ガイド

2024 年 4 月 25 日

Cisco Systems, Inc. www.cisco.com

目次

変更履歴

バージョン	変更
2023 年 10 月 12 日	複数のインターフェイスの参照を削除
2023 年 6 月 6 日	アップグレードプロセスの手順を更新。
2023 年 3 月 16 日	バージョン 3.7 に更新しました。
2022 年 8 月 23 日	バージョン 3.6 用に更新しました。
2022 年 6 月 2 日	TURN サーバーの単一 NIC 構成に関する情報を更新しました。NIC 要件を参照してください。
2022 年 8 月 20 日	バージョン 3.5 用に更新しました。
2022 年 3 月 1 日	Call Bridge クラスタの検証中に実行される証明書名の検証に関するドキュメントを更新しました
2021 年 12 月 15 日	バージョン 3.4 用に更新されました。
2021 年 8 月 24 日	バージョン 3.3 用に更新されました。
2021 年 8 月 25 日	ガイドの一部のセクションを、より包括的にするために再構成し、書き直しました。このバージョンには、いくつかのバグ修正が含まれています。
2021 年 6 月 2 日	TURN サーバーのポートとループバック インターフェイスに関する情報を更新しました。
2021 年 5 月 19 日	Web アプリの通話キャパシティと中規模 OVA Expressway の推奨事項に関するドキュメントを更新。
2021 年 4 月 21 日	ポート範囲の詳細に関する TURN サーバーの接続と Meeting Server のコンポーネント使用のセクションを更新。
2021 年 4 月 8 日	バージョン 3.2 で更新。 Cisco Meeting Server プラットフォームによるコールキャパシティを更新。
2020 年 3 月 15 日	Meeting Server の短期的なログイン情報が完全にサポートされる機能としてドキュメントを更新。
2020 年 12 月 2 日	軽微な修正。
2020 年 11 月 30 日	3.1 の新しいバージョン。たとえば、 Cisco Meeting Server の Web Edge 情報を追加。 シングルサインオン情報を追加。
2020 年 10 月 7 日	軽微な修正。
2020 年 9 月 2 日	レコーダー/ストリーマの VM の最小要件を 4 vCPU コアに明確化する軽微な編集。
2020 年 8 月 17 日	3.0 の新しいバージョン。 3.0 リリースノートに記載されている廃止コンポーネントを削除。

1 はじめに

Cisco Meeting Server ソフトウェアは、Cisco ユニファイド コンピューティング サーバー（UCS）テクノロジーに基づく特定のサーバー、または仕様に基づく VM サーバーにホストできます。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 以降では、X シリーズサーバをサポートしません。

このガイドは、分散型サーバーの展開として展開された Meeting Server について説明します。この展開では拡張性や復元力に関する要因は考慮されません。サーバーは、多数のコンポーネントで構成されています（図 1 を参照）。

注：Meeting Server 3.0 では、Cisco Meeting Management 3.0（またはそれ以降）を使用するための必須の要件が導入されました。Meeting Management では、製品登録と、スマートライセンスのサポートに関連するスマートアカウント（セットアップされている場合）とのやり取りを処理します。スマートライセンスの詳細については、スマートライセンスのセクションを参照してください。

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アクセスできる場合、単一の結合された Meeting Server 展開により、SIP と Web アプリの両方の参加者が会議に参加できます。この展開は、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ある場合に機能します。

ネットワーク境界の外にいる可能性のある参加者へのサポートが必要な場合は、NAT およびファイアウォールのルールによる制限を克服するために追加のコンポーネントが必要になるため、**分割サーバー展開**と呼ばれるものが必要です。

Meeting Server は、この外部接続に対処するための 3 つの一般的な戦略をサポートしています。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、そして Meeting Server Edge 展開モデルです。

- 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 テクノロジーと、Web アプリ参加者向けの TURN Server 機能を備えた Web プロキシを提供します。Cisco Expressway は、Core インスタンスと Edge インスタンスにさまざまな展開オプションを提供し、通話と会議のセキュリティエンクレーブにまたがるように意図的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エッジ戦略を提供します。
- サードパーティの SIP ファイアウォール トラバーサル ソリューションが利用可能であり、セッション ボーダー コントローラなど、SIP 通話のネットワーク境界をトラバースするための他のテクノロジーを提供します。このようなテクノロジーについては、このガイドでは特に取り上げていません。

- Meeting Server Edge 展開モデルは、Core ロールと Edge ロールに分割された複数の Meeting Server インスタンスを使用して、ネットワークの外部からの Web アプリ参加者の接続を可能にします。Meeting Server Edge 展開の価値は、ネットワークの外部からの Web アプリ参加者に、Cisco Expressway でサポートされているキャパシティを超える大容量接続を提供することです。Meeting Server Edge 導入モデルは、SIP ファイアウォールのトラバーサルのニーズに対処していません。SIP 通話のトラバーサルのニーズは、Cisco Expressway または他の SIP 通話テクノロジーを使用して個別に対処する必要があります。一般的な Meeting Server Edge 展開では、SIP Calling に Cisco Expressway を使用し、Web アプリケーション参加者に Meeting Server Edge インスタンスを使用します。

展開モデルの選択は、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 トラバーサル用に Cisco Expressway ソリューションを展開することをお勧めします。Web アプリケーション接続の場合、Expressway（大規模 OVA または CE1200）は、中規模の Web アプリケーションスケール要件（つまり、800 コール以下）の展開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 Web アプリケーションスケール要件（すなわち 200 コール以下）の展開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 Web アプリケーションスケールが必要な展開では、Meeting Server Edge が推奨される展開モデルです。

注：Meeting Server Edge の展開では、このガイドで説明されているキャパシティと機能をサポートするために Web Bridge 3 を使用する必要があります。このガイドに従うには、Web Bridge 2 を使用する既存の展開を Web Bridge 3 に移行する必要があります。

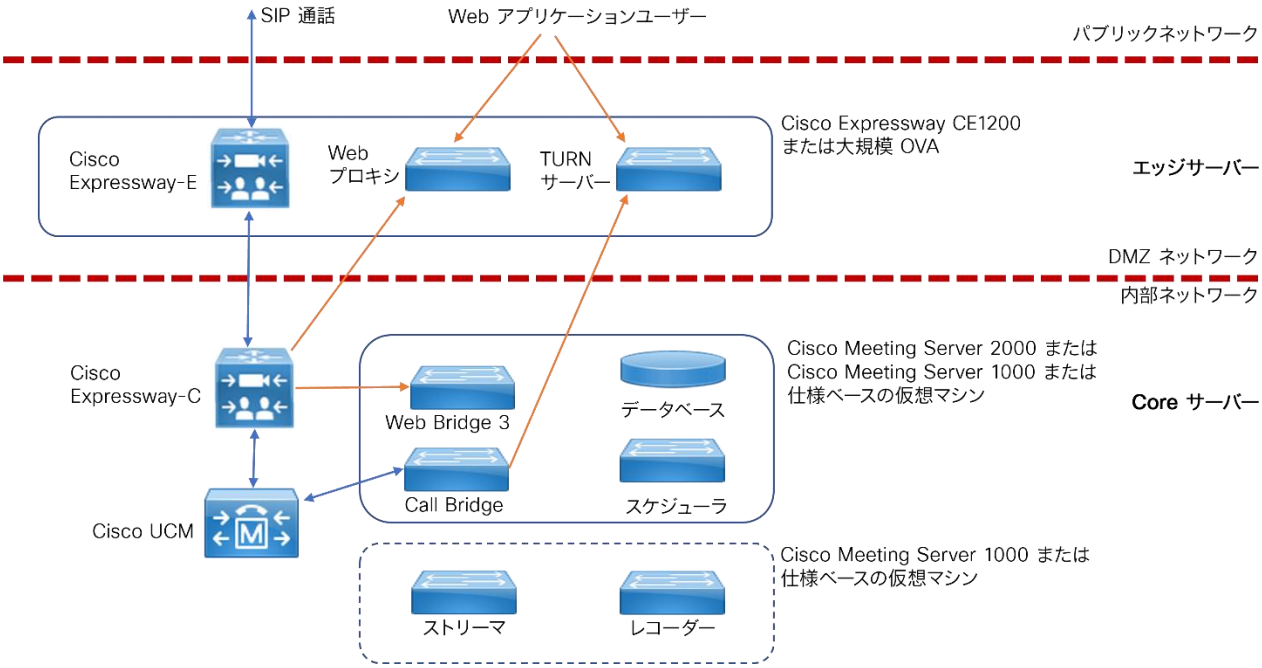
これらの展開は、役割が複数のサーバーに分割されているため、分割型サーバー展開と呼ばれます。Edge ロールは、ネットワークのパブリックアクセス可能な部分に存在して、組織外の接続をサポートします。Core ロールは、外部から直接アクセスすることなく、内部ネットワークで動作します。各ロールは、さらに専門的なタスクに分割される場合があります。たとえば、Meeting Server レコーダーおよびストリーマの役割は、Core に展開されるオプション機能ですが、メインの Meeting Server とは別のサーバーに展開されます。

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

- 図 1 は、Edge で SIP と Web アプリの両方の接続を提供する Cisco Expressway を示しており、Core に Meeting Server があり、Call Bridge、Web Bridge、およびその他の Meeting Server サービスを提供しています。
- 図 2 は、DMZ の Meeting Server が Meeting Server Edge インスタンスとして提供する TURN サービスと Web Bridge 3 機能を示しています。

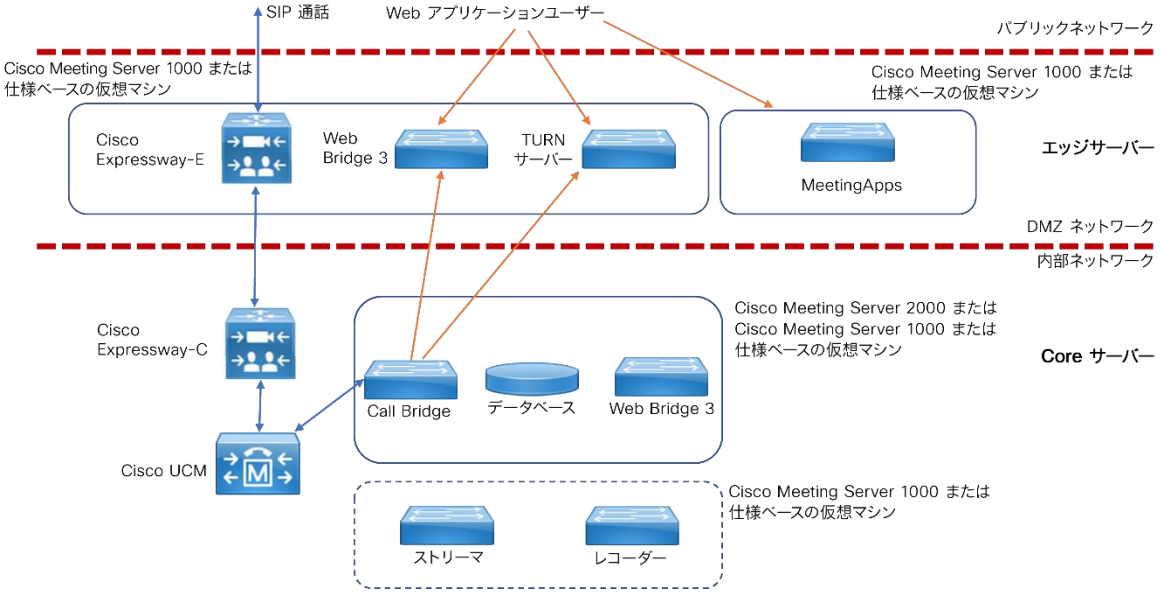
  注：Web Bridge 3 は Edge サーバーに移動しますが、内部参加者のために Core で引き続き運用することもできます。

図 1：TURN サービスを提供する Cisco Expressway での分散型サーバー展開



Edge サーバーとして使用する場合、Meeting Server は必要最小限のサービスのみで構成され、表面積を減らしてセキュリティ態勢を向上させます。Edge インスタンスは、Web アプリユーザーがインターネットから到達できるようにするために必要なサービス、つまり Web Bridge と TURN 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、TURN はメディアにファイアウォール トラバーサル テクノロジーを提供します。Edge はこれらの拡張機能を Core に提供しますが、他のすべてはコアネットワークで運用され、一般に公開されることはありません。

図 2：Meeting Server Edge を使用した分割型サーバー展開



1.1 Meeting Server 展開での Edge デバイスとしての Cisco Expressway-E の使用

Expressway（Large OVA または CE1200）は、中規模の Web アプリの規模要件（つまり 800 コール以下）の展開に推奨されるソリューションです。Expressway（中規模 OVA）は、小規模の Web アプリの規模要件（つまり 200 コール以下）の展開に推奨されるソリューションです。ただし、Web アプリの規模を大きくする必要がある導入の場合は、バージョン 3.1 から、必要なソリューションとして Cisco Meeting Server Web Edge を推奨します。

Cisco Expresswayソフトウェアの Edge 機能は、Cisco Expressway-E を Meeting Server の展開環境でエッジデバイスとして使用できるようにするために開発されました。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 Web アプリを使用して Meeting Server 会議に参加する外部参加者をサポートするリバース Web プロキシ、Web 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 エンドポイントへの登録や、内部呼制御プラットフォーム（Cisco Unified Communications Manager または Cisco Expressway-C）への登録のプロキシとして使用できます。

注意：Expressway ユーザ向けの重要事項
Web Bridge 3 と Web アプリを導入する場合は、Expressway バージョン X12.6 以降を使用する必要があります。それより前のバージョンの Expressway は、Web Bridge 3 ではサポートされていません。

注：Cisco Expressway-E は、オンプレミス Microsoft インフラストラクチャと Meeting Server の間では使用できません。オンプレミスの Microsoft インフラストラクチャと Meeting Server を使用した展開では、Meeting Server は Microsoft Edge サーバを使用して、Microsoft のコールを組織に出入りさせる必要があります。

注: オンプレミス Meeting Server とオンプレミス Microsoft Skype for Business インフラストラクチャ間でデュアルホーム会議を設定している場合、Meeting Server は Skype for Business Edge の TURN サービスを自動的に使用します。

次の表 1 では、これらの機能を実行するための Cisco Expressway-E の設定を説明する構成ドキュメントを示しています。 表 2 では、リリースごとの機能を紹介しています。

表 1：Meeting Server の Edge デバイスとしての Cisco Expressway に関するドキュメント

Edge の機能	このガイドに関する設定
リモートブラウザベースの Meeting Server Web アプリの接続	Cisco Meeting Server 用の Cisco Expressway Web プロキシ 導入ガイド
リモート処理 Lync/Skype for Business クライアントへの接続	Cisco Meeting Server 用の Cisco Expressway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に対するプロキシ登録	Cisco Expressway-E および Expressway-C 基本設定（X12.6）

表 2: Expressway Edge でサポートされた Meeting Server

Cisco Expressway-E バージョン	Edge の機能	Meeting Server バージョン
X 12.6	Cisco Meeting Server Web アプリをサポートしています。Cisco Meeting Server （X12.6）用の Cisco Expressway Web プロキシ を参照してください。	2.9 以降

1.2 コアネットワークの Meeting Server での Cisco Expressway-C の使用方法

ネットワークの Edge で Cisco Expressway-E を導入することに加えて、Cisco Expressway-C は、Meeting Server を使用してコアネットワークに導入できます。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展開されている場合、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 では次の機能を提供します。

- SIP レジストラ
- h.323 ゲートキーパー
- Meeting Server ノード間で会議をロードバランシングするように設定された Call Bridge グループを使用した Meeting Server 展開での呼制御。

表 3：Meeting Server の Edge デバイスとしての Cisco Expressway に関する追加のドキュメント

機能	このガイドに関する設定
クラスタ化された Meeting Server の負荷を分散するためのコール制御デバイス	Cisco Meeting Server 間の Cisco Meeting Server のコールのロードバランシング
SIP レジストラ	Cisco Expressway-E および Expressway-C 基本設定（X12.6）
H.323 ゲートキーパー	Cisco Expressway-E および Expressway-C 基本設定（X12.6）

1.2.1 Cisco Expressway H.323 ゲートウェイコンポーネントの使用

Cisco Meeting Server と Cisco Expressway 全体で単一の 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。Cisco Expressway では、より成熟した H.323 ゲートウェイコンポーネントに移行することが推奨されています。

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 を呼び出すときに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 展開での Edge デバイスとしての Meeting Server の使用

Meeting Server Edge の設計では、外部の参加者が到達できる場所に Meeting Server の 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に配置できます。このサーバーは信頼できないトラフィックにさらされるため、重要なサービスのみが有効になります。推奨される展開は、必要なトラフィックのみを許可する選択的なルールを使用して、NAT またはファイアウォールの背後にある DMZ に Edge インスタンスを展開することです。DMZ の Edge サーバーは、コアに展開された Call Bridge サーバーから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してアクセス制御することをお勧めします。

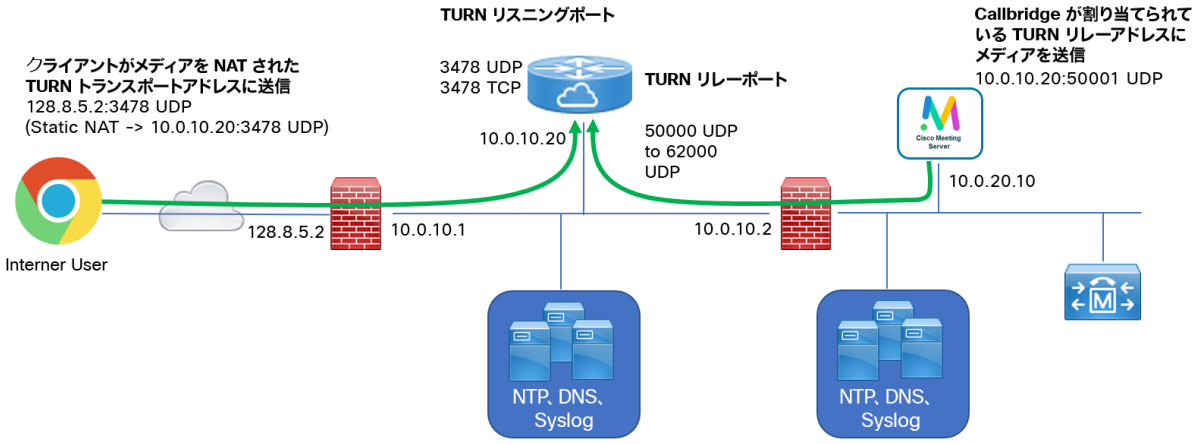
Web アプリクライアントの接続は、TLS を使用して Call Bridge を Web Bridge C2W インターフェイスにアウトバウンド接続させ、Web Bridge 機能のために Core と Edge の間に安全な制御チャネルを確立することによって実現します。外部ブラウザクライアントは、HTTPS を使用して Edge の Web Bridge に接続します。

外部 Web 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 サーバーを介した TURN リレーセットアップを使用して処理されます。Web Bridge に接続して検証された後、Web 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それら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。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相互にトラフィックを送信できることを検証し、結果のリレーにより、両当事者がネットワーク境界を越えてメディアを送受信できるようになります。

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、Meeting Server Edge の公開されたコールキャパシティを実現するために Edge サーバーに必要な展開哲学です。他の組み合わせまたはシナリオでは、メディア接続が確立される可能性がありますが、キャパシティが減少し、メディアルーティングが最適化されない可能性があるため、お勧めしません。

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



注意：Edge Meeting Server は DMZ 内にある必要があります。信頼レベルやセキュリティエンクレーブが異なるネットワークに直接接続しないでください。TURN サーバーがリレーのロールを実行するために必要なインターフェイスは 1 つだけです。

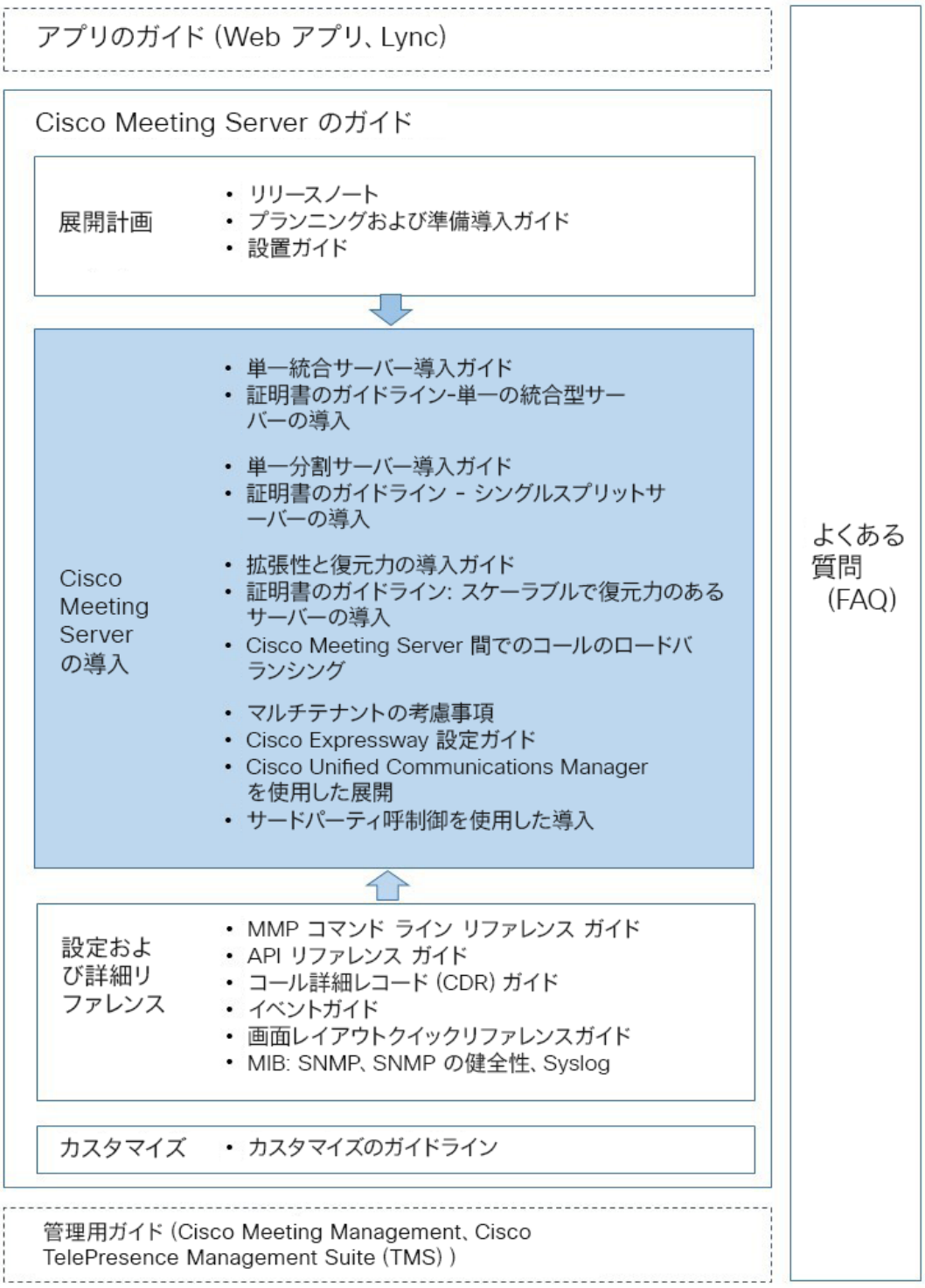
1.4 本ガイドの使用方法

この導入ガイドは、サーバー向けの適切な設置ガイドに続くもので、インストール手順が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、適切な証明書ガイドラインと一緒に読み、組み合わせて使用される必要があります。

この導入ガイドと証明書ガイドラインに加えて、以下の図に示す参考資料は Cisco Meeting Server のマニュアルページからアクセスできます。

注：本ガイドでは、「coSpace」という用語を「スペース」と呼んでいます。

図 4：Meeting Server を網羅したガイドの概要



注：Cisco のユーザマニュアルで使用するアドレス範囲は、RFC 5737 に定義されており、文書化用として明示的に予約されています。Meeting Server ユーザの IP アドレスは、特に明記しない限り、ネットワークでルーティング可能な正しい IP アドレスで置き換える必要があります。

1.4.1 コマンド

このドキュメントでは、コマンドは黒文字で示されており、表示どおりに入力する必要があります。ただし、山括弧 <> で囲まれているパラメータについては、適切な値に置き換えてください。サンプルは青文字で示されており、導入環境に合わせて変更する必要があります。

1.5 Meeting Server の構成

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）で構成されます。MMP は、低レベル ブートストラッピングと、そのコマンドライン インターフェイスによる構成に使用されます。たとえば、MMP は Web Bridge、データベースクラスタリングなど、さまざまなコンポーネントに使用されています。
- アプリケーションは、MMP プラットフォーム上で実行されます。必要に応じて、Call Bridge の Web 管理インターフェイスまたはアプリケーション プログラミング インターフェイス（API）から、アプリケーションレベルの管理（コールとメディアの管理）を行います。API はトランスポートメカニズムとして HTTPS を使用し、展開環境で使用可能なアクティブコールとスペースの非常に大きな数を管理するために、拡張性をもって設計されています。

  バージョン 2.9 から、アプリケーションレベルの管理はすべて Call Bridge の Web 管理インターフェイス経由で、単一の Meeting Server とクラスタ化された Meeting Server の両方で実行できます。

1.5.1 MMP および API インターフェイス

表 4：異なる Meeting Server プラットフォーム上で MMP と API 用に構成されたネットワーク インターフェイス

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 での Serial over LAN（SoL）接続。 注：MMP にアクセスする前に、ファブリック インターコネクト 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。これは仮想接続で、ファブリック インターコネクト モジュールのポート 1 に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ます。 注：Cisco Meeting Server 2000 プラットフォームでは、複数のインターフェイス、つまり「ipv4 b| c	d」の設定はサポートされていません。
Cisco Meeting Server 1000 およびその他の仮想化された展開	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、任意の A-D イーサネット インターフェイスで実行するように構成できます。

1.5.2 Meeting Server の構成を容易にする新しいツール

管理者が Meeting Server を構成および展開するには、次のツールを使用できます。

- 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、または基本インストールの開始点となる、Cisco Meeting Server の簡単なインストールの作成を簡略化します。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。これは Meeting Management と統合されており、Meeting Management UI から使用できます。
- Cisco Meeting Server Web アプリのユーザを Cisco Meeting Management を介してプロビジョニング（バージョン 2.9 から利用可能）。
- Meeting Server Web インターフェイスを介した API アクセス。Meeting Server Web 管理インターフェイスの[**設定**（Configuration）]タブで Meeting Server API にアクセスできます（バージョン 2.9 から利用可能）。このガイドのいくつかの例は、API メソッド POST および PUT の使用から、Web インターフェイスを介した API アクセスの使用に変更されました。

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して、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開始点として単一の Cisco Meeting Server の簡単なインストールの作成を簡略化します。このツールでは、『Cisco Meeting Server Single Server Simplified Deployment guide（Cisco Meeting Server シングル サーバ シンプル導入ガイド）』に記載されている導入のベスト プラクティスに基づいて、Meeting Server を設定します。バージョン 3.3 以降、このツールは Meeting Management と統合され、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なく、設定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。インストールアシスタントは、ミーティング管理 UI から実行できます。クライアントコンピュータ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、Meeting Server の設定手順については、『Meeting Management 設置ガイド』を参照してください。

インストールアシスタントは、コールを発信および受信できる SIP MCU として Meeting Server を構成します。必要に応じて、Cisco Meeting Server の Web アプリケーションを有効にできます。

インストール アシスタントは、空で未設定の Meeting Server 上で使用することを目的としています。これは、Meeting Server の管理ツールではありません。また、既存の Meeting Server のインストールを再設定することもできません。このツールは、Meeting Server 仮想マシンのみを構成するために作成されています。これは、Cisco Meeting Server 2000 プラットフォームでは使用できません。

Cisco Meeting Management を使用した Cisco Meeting Server Web アプリユーザのプロビジョニング

Cisco Meeting Management は Meeting Server または Meeting Server クラスタに接続されており、Meeting Server API を使用するのではなく、LDAP で認証される Cisco Meeting Server Web アプリユーザをプロビジョニングする機能を提供します。この機能では、管理者が Web アプリユーザが自分のスペースを作成するために使用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 サーバーを Meeting Server クラスタに接続する方法、ユーザーインポートを追加する方法、スペーステンプレートを作成する方法、変更を確認してコミットし、最後に LDAP 同期を実行する方法については、『管理者向け Cisco Meeting Management ユーザーガイド』を参照してください。

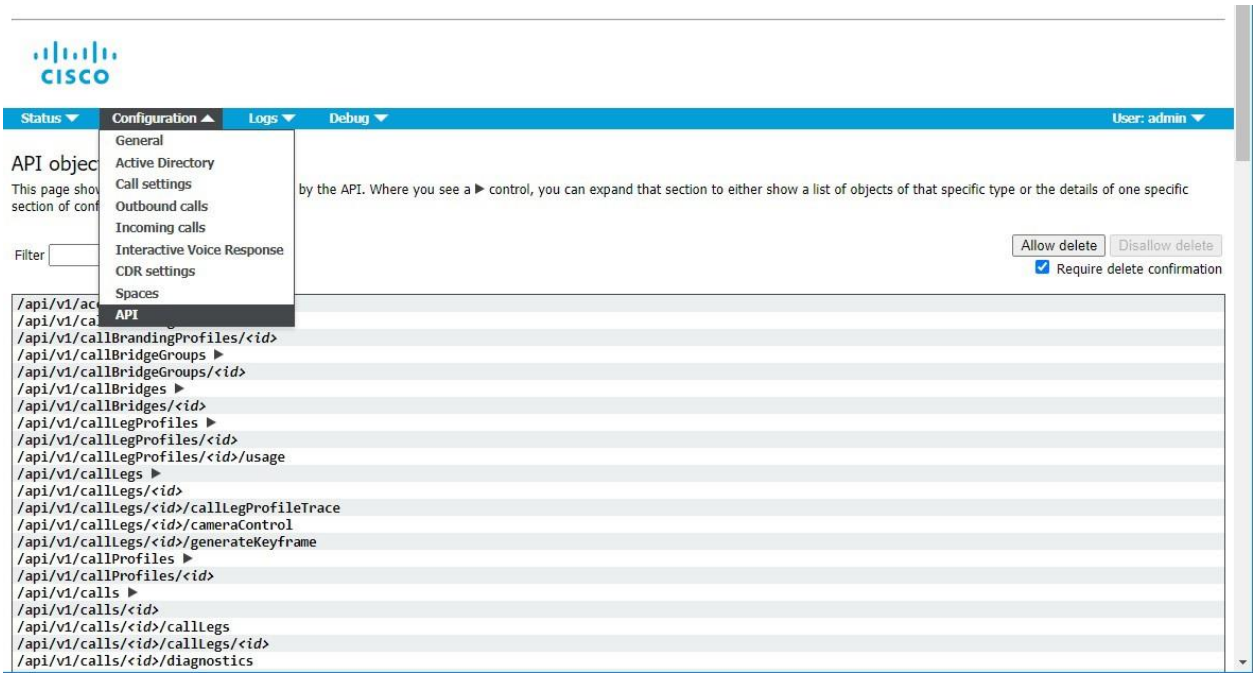
Web インターフェイスでの API アクセス

バージョン 2.9 では、サードパーティ製アプリケーションを必要とせずに Call Bridge API の使用を簡素化するために、Call Bridge API 用のユーザーインターフェイスが導入されました。このインターフェイスには、Meeting Server Web インターフェイスの [設定（Configuration）] タブからアクセスできます（図 5 を参照）。

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ではサポートされていません。スケジューラ API へのアクセスを参照してください。

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のように、MMP を使用して Meeting Server の構成設定および認証を実行する必要があります。詳細については、『MMP Command Reference Guide（MMP コマンド リファレンス ガイド）』を参照してください。

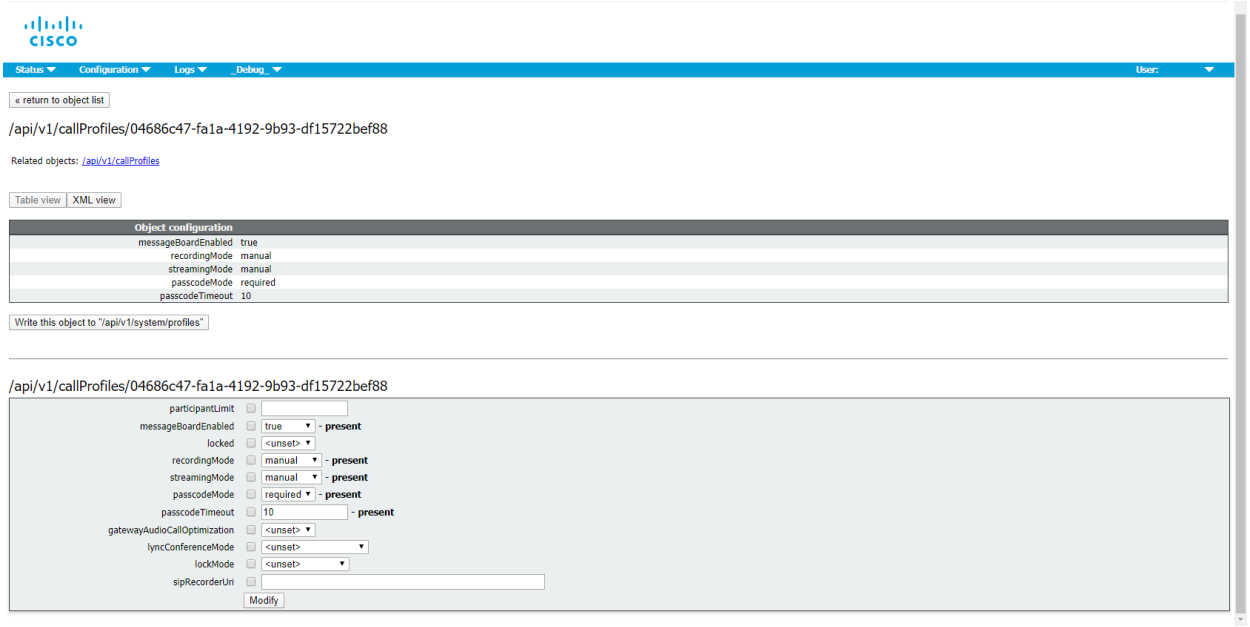
図 5：Meeting Server Web インターフェイスを介した Call Bridge API へのアクセス



注：設定済みの API オブジェクトを削除する場合は、画面右側にある [削除を許可（Allow delete）] を選択します。デフォルトでは削除は許可されておらず、意図しない削除を防止するために [削除の確認を要求（Require delete confirmation）] がオンになっています。

Web インターフェイスから API を使用することで、より視覚的な Meeting Server の設定方法が提供され、API の操作が簡単になります。たとえば、callProfiles の構成は、図 6 に示したチェックボックスとフィールドを使用して指定できます。

図 6：Web インターフェイスでの API アクセスを使用した callProfiles の構成



1.6 Meeting Server 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 製品によるライセンス管理を必要とし、Cisco スマートライセンスをサポートします。3.4 リリース以降、スマートライセンスは Meeting Server に必須です。3.4 リリース以降、従来のライセンスのサポートは廃止されました。スマートライセンス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により 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、代替のライセンスオプションについてシスコアカウントチームにお問い合わせください。

この章では、ライセンス機能、スマートライセンス、およびスマートアカウントとバーチャル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 ライセンスが必要な機能

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）
- 録音またはストリーミング
- 会議参加者のスナップショット

機能ライセンスの他にユーザ ライセンスも購入する必要があります。ユーザ ライセンスには次の異なる 2 種類があります。

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

詳細については、「Multiparty ライセンス」を参照してください。

注：Cisco Meeting Management では、ライセンスがなくても 90 日間はフル機能をトライアルモードで使用できます。

1.6.2 スマートライセンス

Meeting Server のバージョン 3.0 では、Cisco Meeting Management バージョン 3.0 以降を使用した Cisco Meeting Server でのスマートライセンスのサポートが導入されています。今回のソフトウェア 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スへの移行により、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 でも、他のシスコ製品におけるソフトウェアライセンスの方法と同様に Cisco スマートアカウントを利用します。これは、組織全体でライセンスの表示、格納、管理ができる一元的なリポジトリです。

注：Cisco スマートライセンスクラウド証明書は 2023 年 2 月に更新されます。更新後、スマートライセンスクラウドとの直接通信、またはオンプレミスの Cisco Smart Software Manager (SSM) を介した通信はすべて影響を受けます。2023 年 2 月までに Meeting Management 3.6 にアップグレードすることをお勧めします。SLR/PLR のお客様は、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のために、Meeting Management 3.6 にアップグレードする必要もあります。

すべての新規ライセンス購入で引き続き PAK コードが提供されます。すべてのライセンスは Meeting Management が同期するスマートアカウントで利用可能になるため、この PAK コードは参照用に保持されます。

詳細について、またスマートアカウントを作成するには、 https://software.cisco.com にアクセスして、[スマートライセンス（Smart Licensing）] を選択してください。

3.0 より前のバージョンからの Meeting Server ライセンスの変更は次のとおりです。

- バージョン 3.0 では Cisco Meeting Management バージョン 3.0 以降が必須です。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）とのやり取りを処理することができます。
- スマートアカウントに存在する 1 セットの Meeting Server ライセンスを使用して、複数のクラスタにライセンスを付与できるようになり、3.0 より前のバージョンでのように個々の 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す。

- スマート ライセンスを使用した Meeting Management では、クラスタあたりいくつの Call Bridge が使用されているかをトラッキングできるため、R-CMS-K9 アクティベーション ライセンスは不要になります。
- 既存のライセンスがない新規の展開の場合は、次のようになります。
    - 新規購入のライセンスはデフォルトでスマート対応になっておりスマート アカウントが必要な場合があります。Meeting Management にライセンスの詳細情報を入力すると、スマート アカウントで保有されているライセンスに対してライセンスの詳細情報が検証されます。
- 各 Call Bridge にローカルのライセンス ファイルがある既存の環境の場合は、次のようになります。
    - 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することができます。
- SMP Plus と PMP Plus のライセンス使用状況が合算され、ある特定の 1 日の使用数が超過であるかどうか判別されます（いずれかのライセンスが超過した場合、その日は終日、使用数が使用権を超えていると見なされます）。他の機能のライセンス（録音やカスタム レイアウトなど）は個別に評価され、（スマート アカウントにライセンスが存在する前提で）Meeting Management を通じて有効化されます。

注：「ライセンスの超過」という表現は、ライセンスの使用数が使用権を超えている状態を表します。

注：3.0 のすべての展開で Meeting Management が必須であるため、大規模なカスタマー展開の場合は、アクティブな Meeting Management を使用せずに、新規ライセンス専用モードで Meeting Management を展開できます。

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。これにより、部門別などの任意の指定でライセンスを整理できます。Meeting Server と Meeting Management でスマート バーチャル アカウントを使用する場合の重要な注意事項を以下に示します。

- 単一の Meeting Management に対する Meeting Server クラスタを、それぞれ 1 つのユーザ定義のスマート バーチャル アカウントにリンクする必要があります。
- 各バーチャル アカウントは、スマート ライセンスを処理するように設定された 単一の Meeting Management サーバにのみ接続できます。
- 1 つの Meeting Management のみをスマートに構成します。スマートライセンス用に重複する 2 つ目の Meeting Management を構成**しない**ことを推奨します。ライセンス使用数の二重カウントが発生します。
- PMP Plus、SMP Plus、録音/ストリーミングのライセンスは、単一の Meeting Management インスタンスと単一のバーチャルアカウント内でのスマートライセンスを使用している複数のクラスタで共有できます。
- ACU ライセンスは、Meeting Management ライセンスダッシュボードでは使用できません。ACU は 3.0 以降ではサポートされていません。

ライセンスの詳細については、「ライセンスに関する追加情報」を参照してください。

2 展開に関する一般的な概念

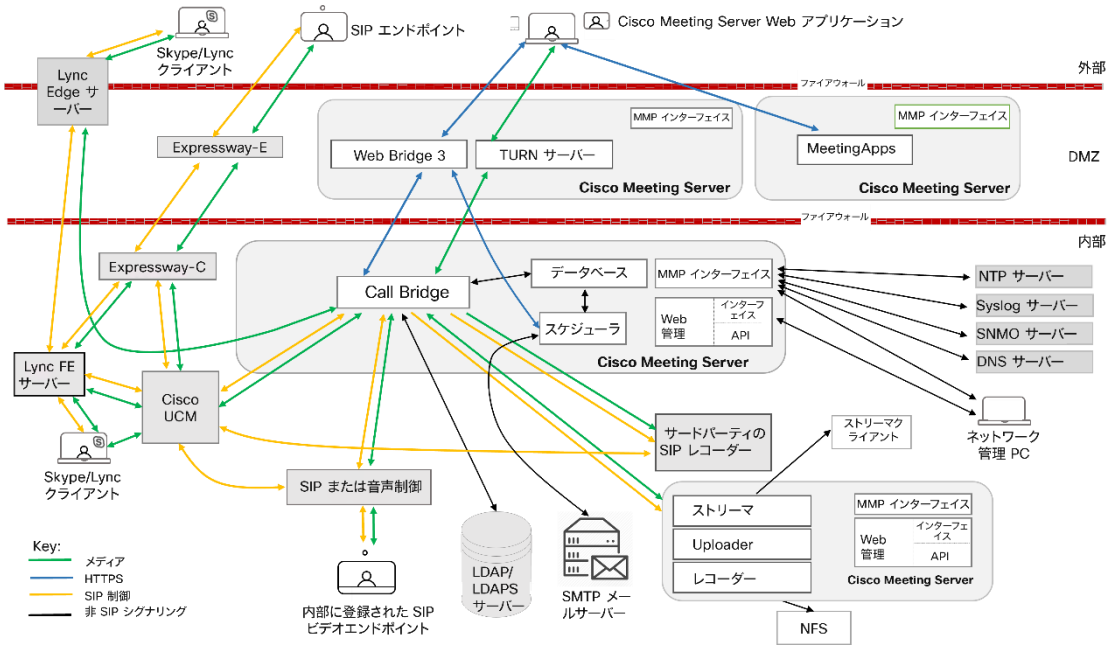
この章では、分散型サーバー展開に Meeting Server を展開する場合の一般的な概念の概要を説明します。図 7 は、DMZ の VM Meeting Server 上で TURN サーバーと Web Bridge 3 コンポーネントが有効になっている一般的な展開を示しています。

注：コアサーバとエッジサーバはどちらも、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（Large OVA または CE1200）は、中規模の Web アプリの規模要件（つまり 800 コール以下）の展開に推奨されるソリューションです。Expressway（中規模 OVA）は、小規模の Web アプリの規模要件（つまり 200 コール以下）の展開に推奨されるソリューションです。ただし、Web アプリの規模を大きくする必要がある導入の場合は、バージョン 3.1 から、必要なソリューションとして Cisco Meeting Server Web Edge を推奨します。

リモートワークの需要が高まり、Web アプリケーションの規模を拡大する必要性が高まっていることから、この Web アプリケーションの規模拡大のためのエッジサポートを提供するため、Cisco Meeting Server バージョン 3.1 が開発およびテストされています。 図 7 は、Meeting Server Web Edge ソリューションを導入して、Web アプリケーションの規模を拡大するために展開を最適化する方法の例を示しています。

図 7：分割型サーバ展開で TURN サーバコンポーネントを使用する Meeting Server 展開例



注：

- Meeting Server には、録音機能とストリーミング機能が備わっています。機能を評価する目的でのみ、Call Bridge と同じサーバーでレコーダ/ストリーマを有効にします。有効化すると、通話が開始されてから 15 分後に接続が切断されます。通常の展開では、Call Bridge に対して別のサーバのレコーダー/ストリーマを有効にします。レコーダーとストリーマを同じ Meeting Server に展開する場合、両方の使用に合わせてサーバをサイズ調整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 管理者は、Meeting Server を構成する Web ベースのインターフェイスです。

Meeting Server の設置ガイドで説明されているとおり、HTTPS アクセス用の Web 管理インターフェイスを構成した後、Web ブラウザにサーバのホスト名または IP アドレスを入力して、Web 管理インターフェイスのログイン画面にアクセスします。Web 管理インターフェイスからアクセス可能な構成の詳細については、「Web 管理インターフェイス：構成 メニューのオプション」を参照してください。バージョン 2.9 から、Web 管理インターフェイスの[設定（Configuration）]タブから API にアクセスできます。

Web 管理は、Meeting Server の管理者用 Web ページを提供するだけでなく、Meeting Server の REST API のインターフェイスも提供します。REST API には、Postman や Chrome Poster などの従来の REST ツールを使用してアクセスできます。バージョン 2.9 以降、Web 管理インターフェイスには、管理者が追加のツール/ソフトウェアなしで Meeting Server API を操作できるようにする API Explorer インターフェイスが含まれています。API リファレンスガイドは、こちらから参照できます。

2.2 Call Bridge

Call Bridge は、会議の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 AVMCU にホストされている会議に参加できます。Call Bridge による音声ストリームやビデオストリームの交換により、参加者はお互いの声を聞き、姿を見ることができます。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の最近のアクティビティなど、スペースに関する情報を格納するデータベースの読み取りと書き込みを行います。分散型の展開では、データベースはメインのコアインスタンス上で実行されている Call Bridge によって自動的に作成および管理され、ライセンスや構成は不要です。

2.4 Web Bridge 3

Web Bridge 3 は、参加者がブラウザベースの Cisco Web アプリケーション クライアントを使用して会議に参加できるようにするための Meeting Server コンポーネントです。Web Bridge 3 は、Cisco Meeting Server Web アプリケーションの参加者に Web 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。バージョン 3.0 では、元の Web Bridge 2 コンポーネントと WebRTC 用 Cisco ミーティング アプリケーションが削除されました。デスクトップ版および iOS 版 Cisco ミーティング アプリケーションもサポート終了となり、Cisco Meeting Server Web アプリに置き換えられました。

注：Web アプリケーションを使用しない場合は、Web Bridge 3 を展開する必要はありません。

Web アプリケーションを使用している場合（Web Bridge 3 を展開している場合）、Web アプリケーションに関連する機能のリリース時期および解決済みの問題の詳細については、『Cisco Meeting Server web app Important Information』（Cisco Meeting Server Web アプリケーション重要事項）を参照してください。Web アプリケーションに関連するすべての情報は、この別個のドキュメントに記載され、Meeting Server のリリースノートには含まれません。

重要事項ガイドでは、以下のことを説明しています。

- Web アプリケーションの新機能または変更された機能、および Web アプリケーションに関連する修正済みの問題と未解決の問題の詳細を、その機能または修正が利用可能な Meeting Server のバージョンとともに示しています。
- Web アプリケーションに影響するブラウザの今後の変更、および影響を受ける Web アプリケーションのバージョンと推奨される回避策。

注：Web Bridge 2 から Web Bridge 3 への自動アップグレードによる移行はありません。バージョン 2.9 の Web Bridge 3 をすでに展開している場合は、Web 管理または /webBridges/<webbridge id> の設定から引き継がれないため、アップグレード後に設定を確認する必要があります。

2.5 TURN サーバー

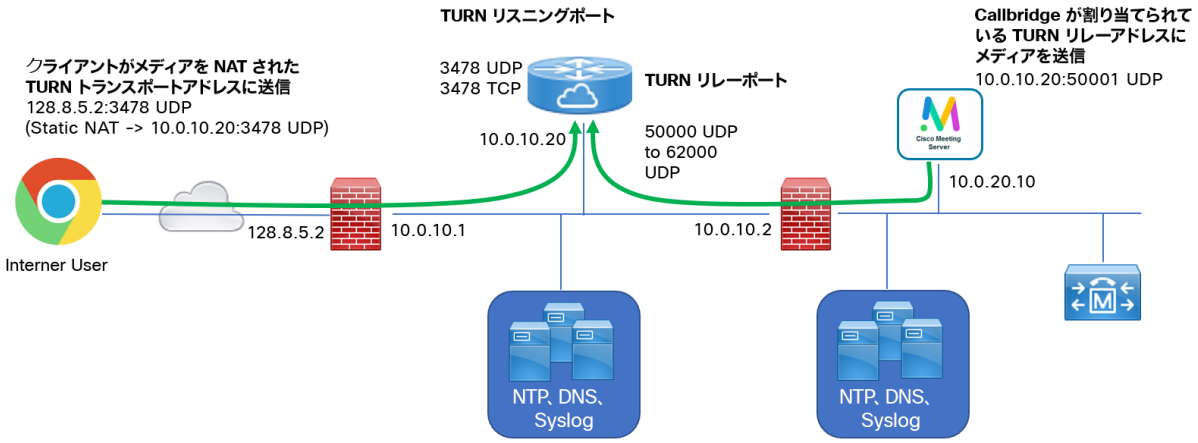
TURN サーバーは、ファイアウォール トラバーサル技術を提供し、ファイアウォールまたは NAT の内側での Meeting Server の展開を可能にします。TURN サーバーは TURN リレーを提供し、ファイアウォールまたは NAT テクノロジーのために Web アプリユーザーが Call Bridge との直接ルートを持たない場合に、メディアを交換できるようにします。TURN サーバーの使用にライセンスは不要です。

TURN サーバーの役割は、Meeting Server Edge 展開シナリオで Meeting Server を使用して提供できます。Web Bridge プロキシに Cisco Expressway を使用している場合は、Expressway によって提供できます。Meeting Server の展開では、TURN サーバーは Web 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 コールは、TURN を使用しません。

TURN サーバーは、コールの両側から到達できるリレーポイントを提供することにより、メディアをエンドツーエンドで直接送信できないコールに対してファイアウォール トラバーサルを提供します。コールのセットアップ中に、Web アプリクライアントはリッスンポートで TURN サーバーに接続し、認証を行い、リレーの割り当てを要求します。TURN サーバーは、TURN サーバーがこのクライアントに転送する必要のあるメディアをリッスンする別のポート番号を割り当てることによって、このクライアントに固有のリレー トランスポート アドレスを割り当てます。リレーアドレスはリモート側に渡され、クライアント向けに意図されたメディアをこのリレーアドレスに送信されるよう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 サーバーは、コールのリモート側に到達するためにメディアを送信できるリモート側のソースアドレスを学習します。この交換により、両側から到達できるポイントが確立され、TURN サーバーは割り当てられたリレーに基づいてトラフィックを双方向に選択的に転送します。

Web アプリクライアントは TURN リスニングポートに接続し、リモート側（Call Bridge）はリレーポートに接続します。TURN に接続してリレーを要求するように Call Bridge を設定する（ロールを逆にする）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、その必要はありません。

図 8：TURN サーバーリレーの例



デフォルトで、TURN サーバーはポート 3478 で UDP をリッスンします。これは STUN トラフィックの業界標準であり、TURN サーバー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 サーバーは、UDP STUN/TURN トラフィックをブロックする可能性のあるネットワーク上にあるクライアントに対応するために、TCP ベースの接続を 2 番目のポートでリッスンすることもできます。この TCP ポートは通常、ポート 443 を使用して許可された HTTPS トラフィックをシャドーイング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 サーバーは内部的にトラフィックを UDP にインターワークし、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 を有効化する Meeting Server の設定オプションは「tls」という名前ですが、TURN TLS は Meeting Server や Web アプリケーションでは使用されません。Web アプリケーションは 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合流点として機能します。

2.6 Meeting Server Edge

Meeting Server Edge または CMS Edge は、DMZ または外部ネットワークに展開され、外部 Web アプリ参加者の連絡ポイントとなる限定された役割の 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。サービスが制限された Meeting Server インスタンスが DMZ または外部ネットワークに 1 つまたは複数展開され、「エッジ」ロールになり、内部ネットワークに展開された Meeting Server インスタンス（「コア」）と連携して動作します。CMS エッジでは、 Web Bridge 3 と TURN サービスのみが有効になっている必要があります。これは、Cisco Expressway を外部 Web アプリ参加者用のプロキシおよび TURN サーバーとして使用する代わりに、高キャパシティ用に使用できる展開シナリオです。Meeting Server Edge 展開モデルは、SIP ファイアウォールのトラバーサルのニーズに対処していません。SIP 通話のトラバーサルのニーズは、Cisco Expressway または他の SIP 通話テクノロジーを使用して個別に対処する必要があります。典型的な Meeting Server Edge 展開では、SIP 通話に Cisco Expressway を使用し、Cisco Web アプリ参加者に Meeting Server Edge 機能を使用します。

2.7 会議の録画

3.0 以前は、Meeting Server の内部レコーダコンポーネント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 サーバーが削除されています。バージョン 3.0 では、SIP ベースの新しい内部レコーダーおよびストリーマが導入されています。

この新しい内部レコーダーおよびストリーマコンポーネントと、サードパーティの SIP レコーダーへのダイヤルアウトはすべて、SIP URI を使用して設定されます。このため、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 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、ミーティングの録音と、録音をネットワーク 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。

ミーティングの録音の詳細については、セクション 11 を参照してください。

2.7.1 録音のライセンスキー

録音には 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、既存の録画ライセンスでストリーミングが可能になります。ライセンス要件については、シスコのセールス担当者またはパートナーにお問い合わせください。

2.8 会議のストリーミング

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、スペースに保持されているミーティングをストリーミングする機能を、スペース上に構成された RTMP URL に追加します。

この RTMP URL をリッスンするように外部ストリーミングサーバを構成する必要があります。外部ストリーミング サーバは、ユーザにライブ ストリーミングを提供することも、後で再生するためにライブ ストリームを録画することもできます。

注：ストリーマコンポーネントは RTMP 標準規格をサポートしており、同様に RTMP 標準規格をサポートしているサードパーティ製ストリーミングサーバーで使用できます。Vbrick は、公式にサポートされている外部ストリーミングサーバです。ただし、他のサーバもテスト済みです。

バージョン 3.1 は、内部 SIP ストリームアプリケーションの RTMP サポートを RTMPS に拡張します –TLS 接続を使用した基本的な RTMP です。これまでは、ストリームと RTMP サーバ間のすべてのトラフィックが暗号化されていませんでしたが、3.1 RTMPS がサポートされることで、このトラフィックを暗号化できます。

既存の **`tls`** MMP コマンドが拡張され、オプションで RTMPS 用 の TLS 信頼 の構成が許可されます。この手順はオプションですが、推奨しています。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 ストリーミング用のライセンスキー

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 つのレコーディングライセンスは 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、既存のレコーディングライセンスでは、ストリーミングが可能です。ライセンス要件については、Cisco のセールス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のローカルでのホスティング

Meeting Server 上で、1 セットのブランディングファイルをローカルで保持できます。これらのローカルにホストされているブランディングファイルは、Meeting Server が動作すると Call Bridge と Web Bridge で使用でき、Web サーバーの問題によるカスタマイズ適用の際の遅延のリスクを排除できます。画像と音声のプロンプトによって、Meeting Server ソフトウェアに組み込まれた同等のファイルが置き換えられます。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。ローカルにホストされているブランディングファイルは、Web サーバ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。

これらのローカルにホストされているファイルは、新しいバージョンのファイルをアップロードして Call Bridge と Web Bridge を再起動するだけで変更できます。ローカルにホストされているファイルを削除すると、Call Bridge と Web Bridge の再起動後に、Meeting Server がビルトイン (米国英語) ブランディングファイルの使用に戻ります。これにより、Web サーバはブランディングファイルを提供するように設定されていません。

注:ブランディングファイルの複数のセットを使用するには、外部 Web サーバを使用する必要があります。

ローカルでのブランディングファイルのホスティングの詳細については、『Cisco Meeting Server の カスタマイズのガイドライン』を参照してください。

2.10 画面上のメッセージング

Meeting Server は、Meeting Server でホストされたミーティングの参加者に対して、画面に表示されるテキストメッセージを表示する機能を提供します。一度に表示できるメッセージは 1 つのみです。API を使用すると、メッセージの表示時間を設定したり、新しいメッセージが構成されるまで永続的に表示したりできます。API オブジェクト **`/calls`** には、**`messageText`**、**`messagePosition`** および **`messageDuration`** パラメータを使用します。

SIP エンドポイントと Lync/Skype for Business クライアントのユーザーに対して、ビデオペインに画面に表示されるテキストメッセージが表示されます。ビデオペイン内のメッセージの位置は、上、中央、下から選択できます。

また、画面上のメッセージングは、CE8.3 エンドポイントなどの展開環境で ActiveControl を使用している他のデバイスや、クラスタ内ではなく、コール中の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 Servers は、独自のメカニズムを使用した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 では、SIP Call Control、Voice Call Control、Lync Front End（FE）サーバーなど、1 つ以上の SIP トランクをセットアップする必要があります。相互運用性を確保するために Web Bridge サービスが必要な Meeting Server にコールをルーティングするには、これらのデバイスのコール ルーティング構成を変更する必要があります。

2.12 Lync および Skype for Business のサポート

2.12.1 Lync と 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 サーバまたは Lync 2010/2013 サーバーに接続された Lync 2010 クライアントと 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 は商業用の Skype 2019 をサポートしています。

Meeting Server は、次を使用します。

- 最大で 1080p の、2010 Lync Windows クライアントと 2011 Lync Mac クライアントを持つ、RTV コーデック トランスコーディング。
- 2013 Lync Windows クライアントと Skype for Business クライアントを持つ、H.264 コーデック。

クライアントバージョンが複数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 2010/2013 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、ミーティングに参加している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 クライアントと Skype for Business クライアントも、RDP ストリームによりコンテンツを受信し、それをメイン 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（つまりコールを、SIP ビデオエンドポイント ドメイン内の接続先を指定して Call Bridge にルーティングする）ように構成された、信頼できる SIP トランクが必要です。

SIP コール制御は、SIP ビデオエンドポイントが Lync/Skype for Business クライアントを呼び出せるように、コールの宛先を Lync/Skype for Business クライアントドメインから Call Bridge に構成変更してルーティングすることが必要です。

ダイヤルプランは、Lync/Skype for Business コールを、それら 2 つのドメイン間で双方向にルーティングします。

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

デュアルホーム会議機能により、Meeting Server と Lync AVMCU との通信方法が向上します。これにより、Lync/Skype for Business と Cisco Meeting Server Web アプリの両方のユーザーに対する会議エクスペリエンスが向上します。 付録 E では、デュアルホーム会議のエクスペリエンスについて説明します。

2.12.2 デュアルホーム会議のサポート

デュアルホーム会議では、会議ルックアップのため、Meeting Server の Lync Edge サーバ設定に Lync Edge の設定を構成する必要があります。Meeting Server 展開を使用するオンプレミス Lync 展開または Lync フェデレーション展開がすでにある場合は、Meeting Server 上で追加の構成は必要ありません。これが新しい展開の場合は、Lync Edge サーバを使用するために 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する機能については、以下を参照してください。

- Lync 参加者の会議エクスペリエンスの向上に関する FAQ。
- RDP サポートに関する FAQ。
- 複数のビデオエンコーダサポートに関する FAQ。

2.13 Web Scheduler

スケジューラは、エンドユーザーが Web アプリを介してミーティングをスケジュールするための Meeting Server コンポーネントです。これは、VM 展開上の Meeting Server 1000、Meeting Server 2000、および Meeting Server でサポートされています。仕様準拠の 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の 4 GB の RAM が必要です。Meeting Server 1000 および Meeting Server 2000 には、追加の RAM 要件はありません。スケジューラは、SMTP 電子メールサーバーの設定を介した電子メール通知の送信をサポートします。電子メールサーバー設定の詳細については、『Cisco Meeting Server 設置ガイド』を参照してください。

1 つのスケジューラで 150,000 の会議をサポートします。回復力を提供するために 2 つまたは 3 つのスケジューラを追加できますが、キャパシティは 150,000 のスケジュールされた会議のままです。スケジュールされたミーティングデータは Meeting Server データベースに保存され、クラスタ化されたデータベースとシングル ボックス データベースの両方の展開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 Web アプリ UI のスケジューラ

- 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場合、会議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 Web アプリ ユーザに表示されます。スケジューラが有効になっていない場合、Web アプリのユーザには、会議をスケジュールするためのユーザインターフェイスが表示されません。
- 管理者が Call Bridge/Web Bridges API を介して Web Bridge を追加、削除、または変更しても、スケジューラはそれらの変更を自動的に認識しません。したがって、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しない理由で停止するのではなく、意図的に無効にされていることを認識しません。スケジューラが管理者によって意図的に無効にされている場合は、Web Bridge を再起動して、スケジューリング 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、またはその他の問題が原因で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（使用可能な場合）。そうしないと、Web アプリのユーザにエラーが表示されます。

2.14 MeetingApps

ファイル共有をサポートするために、MeetingApps と呼ばれる新しいサービスが導入されました。MeetingApp は、他のサービスを使用せずに、スタンドアロンの Meeting Server ノードで構成する必要があります。参加者が外部ネットワーク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適宜構成できます。

注：MeetingApps サービスは、Meeting Server 2000 では構成できません。MeetingApp は、仕様ベースの Meeting Server の仮想化展開でのみ構成することをお勧めします。ただし、Meeting Server 2000 または Meeting Server 1000 を、VM 展開上の Meeting Apps とともに Call Bridge または Web Bridge として使用できます。

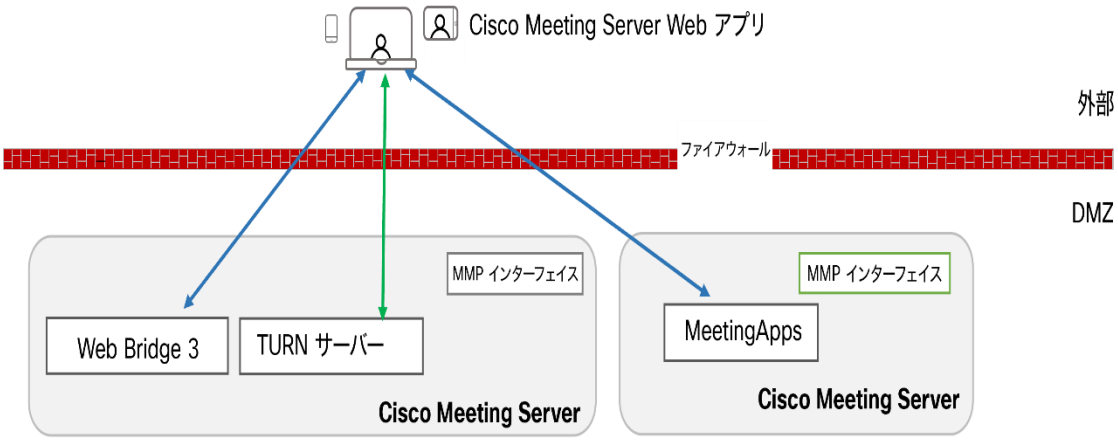
内部および外部ネットワークから参加する Web アプリ参加者がいる会議でファイル共有を有効にするには、MeetingApp を DMZ ネットワークに展開する必要があります。MeetingApp には、パブリックアクセス可能な IP アドレスが割り当てられている必要があり、パブリックアクセスのためにファイアウォールポートが DMZ で開かれている必要があります。

ファイル共有が内部で Web アプリ会議に参加する参加者のみに制限されている場合、MeetingApp はデータセンターのどこにでも展開できます。

MeetingApps は、MMP コマンド **`meetingapps`** を使用して、Meeting Server の VM 展開で構成できます。

MeetingApps のファイル保存容量は、特定の時点で約 20 GB です。最初のファイルが共有されてから 12 時間以内にファイル保存容量がなくなると、会議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。

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



会議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には、環境内の Web Bridge が MeetingApp と通信するように設定されている必要があります。

MeetingApp の構成中に、MeetingApp と Web Bridge 間の安全な通信を確保するための秘密鍵が生成されます。MMP コマンド **`webbridge3 meetingsapps add`** を使用して Web Bridge を構成するには、MeetingApps ホスト名、ポート番号、および生成された秘密鍵を提供する必要があります。Web アプリケーションユーザーがログインするたびに、Web Bridge は MeetingApps に要求を送信してユーザーを認証します。

詳細については、「MeetingApp の設定」を参照してください。

3 前提条件

3.1 Meeting Server 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する必要があるネットワーク構成の変更について説明します。これらの項目の一部は事前に構成できます。

3.1.1 DNS 構成

Meeting Server には、複数の DNS SRV と 1 件のレコードが必要です。完全なリストについては 付録 A を参照してください。ただし、特定のレコードについては他の場所でも説明されています。

3.1.2 セキュリティ証明書

TLS を使用するサービス用の X.509 証明書とキーを生成してインストールする必要があります。TLS を使用するサービスは、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。

分散型展開の『証明書ガイドライン』には、証明書に関するバックグラウンド情報と手順の両方が含まれています。このガイドラインには、Meeting Server の MMP コマンドを使用した自己署名証明書の生成方法も含まれます。これらの証明書は、ラボで構成をテストする場合に役立ちます。ただし、実稼働環境では、認証局（CA）によって署名された証明書の使用を**強く推奨**します。

このガイドで証明書に関して以前に説明した手順は削除され、『証明書ガイドライン』に記載された単一の手順に置き換えされています。

注：証明書に自己署名して使用すると、サービスが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。このメッセージを回避するには、証明書を再発行して、信頼できる CA によって署名してもらいます。コンポーネントへのパブリック アクセスを予定しているのでない限り、これは内部 CA でもかまいません。

3.1.3 ファイアウォール構成

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

3.1.4 Syslog サーバー

Meeting Server は Syslog レコードを作成します。このレコードはローカルに保存され、リモートの場所に送信することもできます。これらのレコードは、Meeting Server の内部ログページでの使用よりも詳細なロギングが含まれているため、トラブルシューティングに役立ちます。内部 Syslog メッセージは SFTP によりダウンロードできます。ただし、リモート Syslog サーバーにデバッグ情報を送信するようにホストサーバー（Edge および Core）を構成することを推奨します。どちらの Meeting Server も同じ Syslog サーバーを使用する必要があります。Syslog サーバーをトラブルシューティングに使用する場合は、両方の Meeting Server のログを確認してください。

注：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 を使用するように構成されていることを確認してください。

Syslog サーバを定義するには、各 Meeting Server で以下の手順に従います。

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. 以下を入力して、Syslog サーバを有効にします。
   ```
   syslog enable
   ```
4. オプションで、監査ログを Syslog サーバに送信する場合は、以下の手順に従います。

   （監査ログ機能は、構成変更と重要な低レベル イベントを記録します。たとえば、Web 管理インターフェイスまたは API からダイヤルプランまたはスペースの構成に加えられた変更は、このログファイル内で追跡され、変更を加えたユーザーの名前とそれぞれの送信元 IP アドレスおよび SSH ポートでタグ付けされます。これにより、特に同時進行のセッションで、イベントの送信元を識別できます。このファイルは SFTP を使用しても入手できます。）

   a. ユーザを監査ロールで作成します。
      ```
      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 アカウントで再度ログインします。
   c. 次のコマンドを入力します（このコマンドは、監査ロールを持つユーザ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 ファイルは時間内に上書きされますが、**`syslog rotate <filename>`** と **`syslog audit rotate <filename>`** コマンドを使用して、システムログファイルと監査ログファイルを恒久的に保存できます。これらのファイルは SFTP によりダウンロードすることもできます。『MMP Command Reference』を参照してください。

3.1.5 ネットワーク タイム プロトコル サーバ

Meeting Server コンポーネント間で時間を同期する 1 つ以上の Network Time Protocol（NTP）サーバーを構成します。

注：時刻の共通ビューを共有することが重要で、これには複数の理由があります。証明書の有効性を確認する場合や、反射攻撃を防ぐために必要です。また、これによってログ内の時刻の一貫性も保証されます。

各 Meeting Server で、次の手順を実行します。

1. 必要であれば、MMP に SSH でログインします。
2. NTP サーバーをセットアップするには、次のように入力します。

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

構成済みの NTP サーバーの状態を調べるには、 **`ntp status`** と入力します。

`ntp` コマンドの一覧については、『MMP コマンドリファレンス』 を参照してください。

3.1.6 コール詳細レコードのサポート

Meeting Server では、サーバー側で接続される新しい SIP 接続や、アクティブ化または非アクティブ化されたコールなど、重要なコール関連イベントに関するコール詳細レコード（CDR）が内部で生成されます。この 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構成できます。Meeting Server でレコードを長期間保存する規定や、Meeting Server 上の CDR を参照する方法はありません。

1 つの分散型サーバー展開のコアサーバーは、最大 4 台の CDR 受信者をサポートし、Meeting Management などのさまざまな管理ツール、または復元力を高くするために Meeting Management の複数のインスタンスを展開できます。

CDR レシーバとしての Meeting Management の設定の詳細については、『Cisco Meeting Management 管理者ガイド』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 を構成できます。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）] に移動し、CDR レシーバの URI を入力します。API を使用し、CDR 受信者の URI を使用してコア Meeting Server を構成する方法の詳細は『コール詳細レコードガイド』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ます。

1. 必要であれば、MMP に SSH でログインします。
2. 次のように入力します。
   ```
   hostname <name>
   hostname london1
   hostname mybox.example.com
   ```
3. 次のように入力します。
   ```
   Reboot
   ```

注：このコマンドを実行した後は、再起動が必要です。

3.1.8 その他の要件

- ユーザをインポートするには、LDAP サーバにアクセスします。これには Microsoft Active Directory（AD）サーバまたは OpenLDAP サーバを使用できます。

  ユーザーが Web アプリケーションを利用して Meeting Server に接続する場合は、LDAP サーバーが必要です。ユーザ アカウントは、LDAP サーバからインポートされます。[LDAP 設定（LDAP configuration）] の説明に従って、LDAP からフィールドをインポートすることで、ユーザ名を作成できます。パスワードは Meeting Server にキャッシュされません。パスワードは LDAP サーバー上で安全に一元管理されます。Web アプリを認証すると、LDAP サーバに対してコールが実行されます。
- Call Bridge 上でホストされるコールにアクセスするために使用するダイヤル プランの決定。ダイヤルプランは環境によって異なります。つまり、Lync、SIP（音声を含む）、または Web アプリケーションコールのうちどのタイプのコールを行うかどうかによります。このダイヤルプランを導入する手順については、第 6 章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、必要に応じて、Lync クライアント、SIP エンドポイント、SIP 電話機、Web アプリなど、1 つ以上のソリューションにアクセスします。
- SIP コール制御プラットフォームへのアクセス（SIP コールを実行する場合）。 第 7 章と第 8 章では、Cisco VCS に 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構成の変更について説明しています。Cisco Unified Communications Manager（CUCM）、Avaya CM および Polycom DMA への SIP トランクの設定に関する情報は、『コール制御を使用した Cisco Meeting Server 展開ガイド』を参照してください。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できます。
- Meeting Server を音声展開と統合する場合、Meeting Server は PBX に接続されている Voice Call Control 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 環境に導入する場合は、Lync Front End（FE）サーバーにアクセスして、そこでダイヤルプランの構成変更を行います。必要な変更は、このドキュメントで説明しています。

3.1.9 仮想化された展開に関する具体的な前提条件

- 『Cisco Meeting Server 仮想化展開の設置ガイド』で指定されているリソースに準拠したホストサーバー。

3.2 Meeting Server Edge ハードウェア構成

Meeting Server Edge のロールは、単一のサーバーまたは複数のサーバーとして展開できます。選択は、外部の Web アプリからの参加者に必要な同時通話キャパシティによって決まります。外部 Web アプリケーションからの参加者の割合が高いことが予想される場合、Edge サーバーを展開して、そのキャパシティをコアの Call Bridge キャパシティ以上にすることをお勧めします。Edge キャパシティを余分に増やしても、コア Call Bridge 展開がサポートする数よりも多くの参加者が接続できるようにはなりません。Edge は、参加者に Web Bridge と TURN のキャパシティを提供します。コアは、引き続き Web アプリ参加者に Call Bridge キャパシティを提供する必要があります。

3.2.1 エッジ サーバーの構成

エッジサーバーロールでは、2 つの仮想マシンハードウェア構成がサポートされています。これらの構成は、サポートされる最小ハードウェア要件とそれらがサポートする容量を定義します。

「小規模」の Edge サーバー

サポートされている Cisco ハードウェアについて次の仕様の Cisco Meeting Server VM 1 台

- 4 GB RAM
- 4 vCPU
- 1Gbps ネットワークインターフェイス

「大規模」の Edge サーバー

サポートされている Cisco ハードウェアについて次の仕様の Cisco Meeting Server VM 1 台

- メモリ 8 GB
- 16 vCPU
- 10Gbps ネットワークインターフェイス

推奨されるプロセッサの仕様：

2.5GHz 以上で実行されている Intel Xeon E5 2600 などのプロセッサ仕様を推奨します。1 つの vCPU から 1 つの物理 CPU をお勧めします。

NIC 要件：

Cisco は、TURN サーバーに単一の NIC 設定を使用したスプリット サーバー展開をテストおよび検証しました。したがって、バージョン 3.0 からは、1 つのインターフェイスでのみ TURN Server のリッスンポートを設定することをお勧めします。

共存のサポート：

エッジサーバーは他の VM と同じ場所に常駐することができます。ただし、4 つの vCPUVM ごとに 1 Gbps の NIC 要件があり、16 の vCPU ごとに 10 Gbps の NIC 要件があります。VM ホストには、すべてのアプリケーションに十分な NIC 容量が必要です。

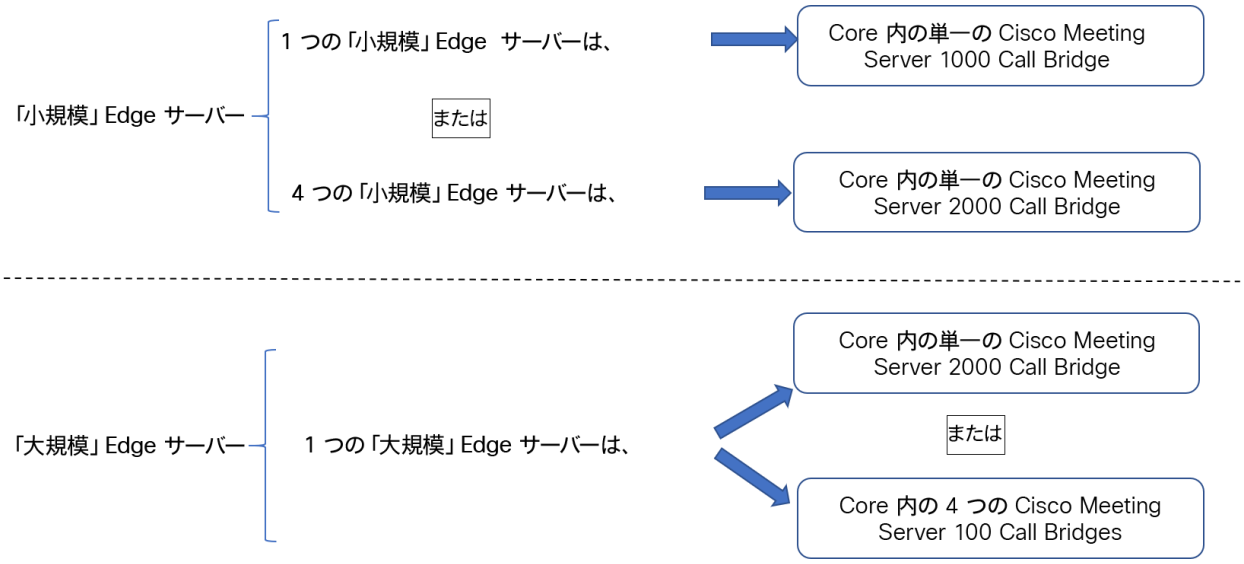
注：

- Meeting Server 1000 M4 ハードウェアは、1Gbps NIC をサポートします。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 Edge インスタンスとしては適していません。

表 5：エッジサーバー Web アプリのコールキャパシティ

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

2 つのエッジサーバー構成は、Call Bridge に Cisco Meeting Server アプライアンスを使用するときに、エッジキャパシティを Core Call Bridge キャパシティに簡単に一致させる機能を提供します。



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エッジサーバーのハードウェア構成を確認して、必要なエッジサーバーの数を決定します。

3.2.2 導入に関する考慮事項

- 同じ Call Bridge または Call Bridge グループを処理するすべてのエッジサーバーの容量を同じにすることをお勧めします。つまり、4 つの vCPU すべて、または 16 の vCPU すべてを、両方を組み合わせて使用するのではなく、同じ容量にすることをお勧めします。
- スケーラブルまたは復元力のある展開にするためには、Call Bridge グループを設定することをお勧めします。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容易にし、TURN サーバーを Call Bridge で適切に地理的に配置するのに役立ちます。
- Web アプリが SIP スケールと一致する（クラスタごとに最大 24 のコールブリッジ）、複数のエッジサーバがサポートされます。ただし、Call Bridge グループは、グループごとに最大 10 台のエッジサーバをサポートします。10 台を超える Edge サーバーが必要なスケーラブルまたは回復力のある展開のためには、複数の Call Bridge グループが必要です。
- Meeting Server Web Edge ソリューションをサポートするため、新しい MMP コマンド **`turn high-capacity-mode (enable|disable)`** が導入され、TURN の拡張性モードが有効になります。この設定はデフォルトでイネーブルになっています。

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 Edge の設計では、外部の参加者がアクセスできる 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に配置できます。推奨される展開は、必要なトラフィックのみを許可する選択的なルールを使用して、NAT またはファイアウォールの背後にある DMZ に Edge インスタンスを展開することです。DMZ の Edge サーバーは、コアに展開された Call Bridge サーバーから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してアクセス制御することをお勧めします。

Web アプリクライアントの接続は、TLS を使用して Web Bridge C2W インターフェイスに発信接続し、Web Bridge 機能のコアとエッジの間に制御チャネルを確立することで、Call Bridge を実現します。外部クライアントは、HTTPS を使用して Web Bridge リスニングポートに接続します。

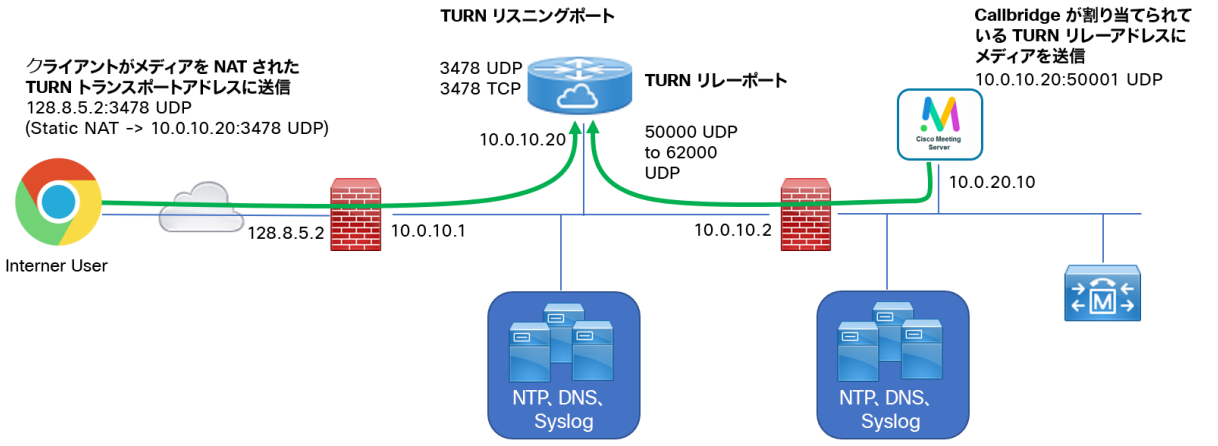
外部 Web アプリクライアントのメディアトラフィックは、TURN サーバーをリレーとして使用して処理されます。認証された Web クライアントは、TURN サーバーのリスニングポートに接続し、TURN サーバーのインターフェイスでリレー トランスポートアドレスが割り当てられるように要求します。ICE を使用して、クライアントと Call Bridge は、このリレーを介して相互にトラフィックを送信できるか、また最適なルートであるかどうかを検証します。Call Bridge は、割り当てられたリレー アドレスにメディアを送信できます。このアドレスは、TURN サーバーによって外部クライアントに送信（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 サーバーの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て Call Bridge に戻されます。UDP ベースのメディアは、ファイアウォールで対称 UDP トラフィックを発信元の接続に戻すことによってコアの Call Bridge に到達できます。

注：バージョン 3.0 以降、TURN Server のリスニングポートを単一のインターフェイスで構成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、公開されているコールキャパシティを実現するために Edge サーバーに必要な展開モデルです。他の組み合わせまたはシナリオでは、メディア接続が確立される可能性がありますが、キャパシティが減少し、メディアルーティングが最適化されない可能性があるため、お勧めしません。

Meeting Server Edge の推奨される展開では、外部 Web アプリケーションの参加者が、UDP 経由の TURN と、UDP 経由で TURN リレーに接続する Call Bridge を使用して、Edge インスタンスに接続できます。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。制限付きの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、TURN を独自のインターフェイスに移動して TCP 443 経由の TURN をサポートするために 2 番目の DMZ インターフェイスを追加するオプションのシナリオについても説明します。他のネットワークパスとサービス構成の組み合わせも技術的に実現可能ですが、他のセキュリティリスクやキャパシティへの影響を引き起こす可能性があるため、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本書から除外されています。

図 9：UDP を使用した TURN のサンプル図



3.3.2 ネットワーク プランニング

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について概説します。使用されている名称は、ネットワークにインターネット、DMZ、イントラネットの 3 つのセキュリティレベルがあることを前提としています。概説されているシナリオには、複数の会議サーバーインスタンスと TCP フォールバックが含まれています。接続先は、そのロールに基づいてラベル付けされ、また環境内の複数のアドレスに対応付けられている場合があります。

3.3.2.1 DMZ からインターネットへの境界

デフォルトでは、DMZ は、承認されたトラフィックとサービスについてのみインターネットからの着信接続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 から受け入れる必要があります。

注：DMZ ネットワークは、NAT されているか、パブリックインターネットから直接ルーティング可能です。この例では、DMZ が NAT されていると想定しています。

Web アプリをサポートするには、ファイアウォールは、Web Bridge 3 サービスをホストする Meeting Server Edge サーバーのポート 443 へのインターネットからの着信 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 を有効にして、HTTP 接続を試みるユーザーが自動的に HTTPS にリダイレクトされるようにすることができます。参加者は、通話に HTTP を使用できません。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可能性のあるファイアウォールの内側にいる可能性があるため、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 上の 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 を有効にすると、TURN サーバーは TCP 3478 および指定されたポートでもリッスンします。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ースでリッスンするサーバー上に 2 番目の DMZ IP インターフェイスが必要です。

注：DMZ が NAT されており、複数の Edge サーバーを使用している場合は、各 Edge サーバーの NAT 構成で個別の IP が必要です。これは、それぞれが 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	方向	送信元 IP	送信元プロトコル：ポート	標的のIP	送信先プロトコル：ポート
クライアントブラウザ HTTPS	着信	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	Any	TCP {未予約}	{WB3}	TCP 80
クライアント STUN/TURN	着信	Any	UDP {未予約}	{TURN}	UDP 3478
クライアント STUN/TURN TCP	着信	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	Any	TCP {未予約}	{TURN}	TCP 443
対称リターン TURN トラフィック（通常は自動）	発信	{TURN}	UDP {3478}	Any	UDP {未予約}

注：

- {WB3} = Web Bridge 3 サーバーがリッスンしているインターフェイスの IP リスト
- {TURN} = TURN サーバーがリッスンしているインターフェイスの IP リスト
- TURN TCP 443 はオプションの展開です。443 で TURN TCP を有効にする必要があり、Web Bridge 3 にすでに TCP ポート 443 を使用している場合は、それらが別のインターフェイスにあるかどうかに関係なく、新しい Meeting Server Edge サーバーを展開する必要があります。

- 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トラフィックまたはリターン UDP トラフィックを許可する必要があります
- 複数の TURN サーバーを使用する場合、各 TURN サーバー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ります。

3.3.2.3 イントラネットから DMZ への境界

デフォルトでは、ファイアウォールは、イントラネットを保護するために、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 接続を許可しないようにする必要があります。また、Meeting Server Edge サーバーからイントラネットへの UDP パケットの送信も、パケットがすでに（そして最近）イントラネットから Edge ボックスに同じアドレス/ポートのペアリングで送信されてない限り許可してはなりません。 つまり、<DMZ IP>：50342 から <Intranet IP>：50131 への UDP パケットは、以前に <Intranet IP>：50131 から <DMZ IP>：50342 へのパケットがあった場合を除き、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 リスニングポート上の Meeting Server Edge 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 からの着信 UDP パケット（つまり、送信元 <任意のコアの <any core callbridge IP>：< 32,768 ～ 65,535 > から接続先<Edge CMS IP>：< 50,000 ～ 62,000 >）を許可する必要があります。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。

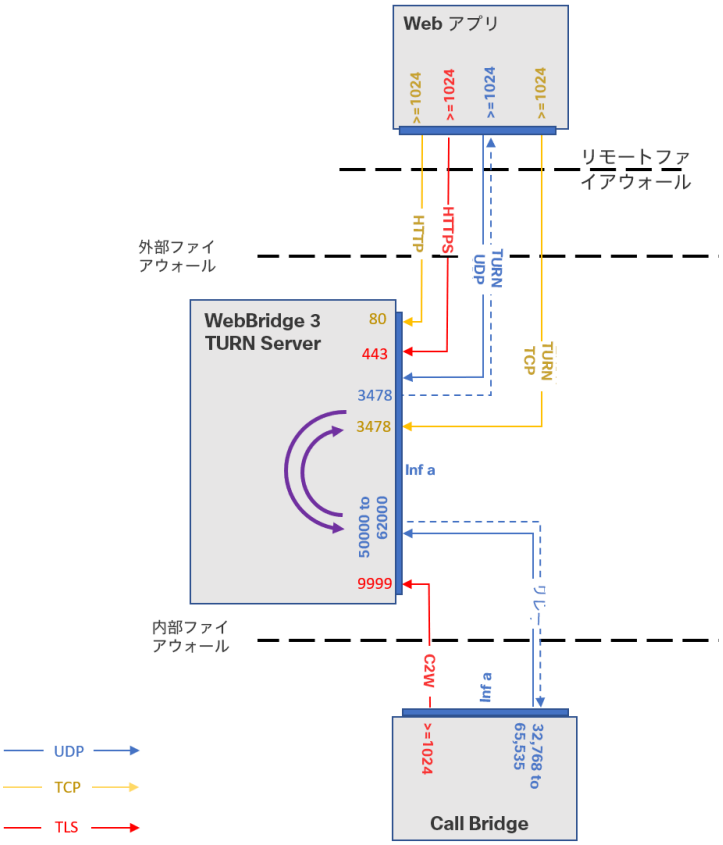
コアの Call Bridge を Meeting Server Edge ノードと直接ルーティングできることが望ましいですが、コアの Meeting Server は DMZ サービスに対して NAT の背後にあり、外部クライアントによって割り当てられた TURN リレーを引き続き使用できます。コアの Meeting Server は、TURN リスニングポートに接続する必要はありません。これは、外部クライアントによるリレーセットアップが双方にとって十分であるためです。NAT を使用している場合、Call Bridge へのトラフィックは、ICE 接続テストでピア再帰候補と見なされます。

説明	方向	送信元 IP	送信元プロトコル：ポート	標的のIP	送信先プロトコル：ポート
Meeting Server C2W インターフェイス	発信	{Call Bridge IP}	TCP {未予約}	{WB3}	Web Bridge 3 C2W リスニングポート。たとえば、webbridge3 c2w listen 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 IP}	UDP {32,768 ～ 65,535}	{TURN}	UDP {50,000～62,000}
対称リターン TURN トラフィック（通常は自動）	着信	{TURN}	UDP {50,000～62,000}	{Call Bridge IP}	UDP {32,768 ～ 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 = コア内の Call Bridge サーバーの IP リスト
- 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対称/リターン UDP トラフィックを許可する必要があります
- TURN サーバーのリスニングポートは、1 つのインターフェイスで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 Web アプリ



3.3.2.4 管理およびプラットフォームのトラフィック

わかりやすくするために、これまで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説明しませんでした。このセクションでは、管理とプラットフォームの要件について個別に説明します。DMZ ネットワークのインフラストラクチャ サービスと運用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ではなく、Edge Meeting Server インスタンスに関連する用語で説明します。これらの概念を環境の詳細に適用してください。

Meeting Server が TLS と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、SFTP と SSH を使用して、Meeting Server ソフトウェアを構成および更新する必要もあります。集中ログの Syslog は任意ですが、強くお勧めします。これらのサービスは、既知の送信元にトラフィックを制限するなどの一般的なセキュリティ慣行に準拠しながら、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構成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	方向	送信元 IP	送信元プロトコル：ポート	標的のIP	送信先プロトコル：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 {未予約}	{DNS サーバー}	UDP 53
Syslog	着信	{WB3} または {TURN}	TCP {未予約}	{Syslog サーバー}	TCP 514*
アプリ管理（SSH、SFTP）	着信	{イントラネット/管理 IP}	TCP {未予約}	{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 接続先ポートは設定可能
- 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 の接続先へのアウトバウンド接続が必要になる場合があります。
- ここでは、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の管理に使用される可能性のあるその他のサーバー管理技術については記載されていません。

3.3.3 Meeting Server Web Edge の展開

次の手順は、Meeting Server Web Edge を導入する方法の概要を示しています。

1. MMP を使用して Meeting Server エッジ上で TURN サーバを設定します。
2. MMP を使用して Meeting Server エッジに 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、Web 管理ユーザーインターフェイスの[設定（Configuration）] > [API]で callBridge パラメータを /api/v1/turnServers と /api/v1/webBridges に追加し、Web Bridge 3 の証明書要件を確認します）。

4. 接続が正しく機能していることを確認します。これを行うには、Web アプリケーションのアドレスからログインして手動でテストするか、Web 管理インターフェイスの[**ステータス**（Status）] > [全般（General）]で障害状態と最近のエラーと警告を確認します。（Web Bridge 3/TURN 接続失敗メッセージは表示されないことに注意してください。）
5. ファイアウォールの設定を次のように追加します。
    a. Call Bridge は、TCP 接続 WebBridge 3 c2w 接続ポートに接続できる開く必要があります（API の「c2w://address:port」、つまり /api/v1/webBridges の url フィールドで指定されているとおり）。
    b. Meeting Server エッジの TURN リレーポートは 50000～62000 であるため、Call Bridge が UDP 上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 Web アプリクライアントは、UDP 3478 上の TURN サーバーに到達できる必要があります。TCPへのフォールバックは可能ですが、 ポートは「turn tls」<port> 設定に依存するため、 その場合、ポートも開く必要があります。

4 MMP の構成

Meeting Server のコンポーネントは、MMP を使用して構成されます。各 Meeting Server インスタンスには設定が必要です。

4.1 MMP および Web 管理インターフェイスのユーザアカウントの作成と管理

『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する必要があります。ユーザーアカウントを作成した場合は、次のセクションに進んでください。Web 管理インターフェイスへのアクセスにも、同じアカウントを使用します。

（これらの MMP 管理者ユーザーアカウントがない場合は、お使いの展開に適した設置ガイドに詳細が示された緊急管理者リカバリ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と他の役割を持つユーザーアカウントの設定を含む、MMP コマンドの全範囲については、『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 ソフトウェアのアップグレード

Cisco Meeting Server 2000 および Cisco Meeting Server 1000 は、出荷時に利用可能な最新のソフトウェアリリースを搭載しますが、最新の製品ではない場合があります。同様に、ソフトウェアをダウンロードしてから日が経っている場合は、新しいバージョンが利用可能になっていることがあるため、シスコの Web サイトで確認することをお勧めします。その場合は最新バージョンにアップグレードしてください。

次の手順は、すべてのタイプの展開に適用されます。

1. Meeting Server 上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 でログインし、
   `version`
2. Meeting Server をアップグレードする前に、次の手順を実行します。
   a. 各サーバー上の現在の構成のバックアップを取ります。ローカルサーバーにバックアップを安全に保存します。詳細については、『MMP Command Reference Guide（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た自動バックアップファイルを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、すべてのコール（SIP とクライアント）が動作し、障害状態がリスト表示されないことを確認します。

d. クラスタ化されたデータベースを展開している場合は、Meeting Server をアップグレードする前に、**database cluster remove** コマンドを使用してすべてのノードのクラスタ化を解除します。

3. アップグレードするには、最初にCisco の Web 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、Web ページの右側の列にリストされている適切な Meeting Server タイプをクリックし、ダウンロードリンクに表示される指示に従います。
4. SFTP クライアントを使用して、新しいソフトウェアイメージを Meeting Server の MMP にアップロードします。例：

   ```
   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. コアサーバをアップグレードし、SSH 経由で MMP に接続し、次の内容を入力します。

   upgrade

   サーバが再起動し、Web 管理インターフェイスが使用可能になるまで、約 10 ~ 12 分間待機します。
6. アップグレードが成功したことを確認するには、各サーバの MMP に SSH を入力し、ログインして次のコマンドを入力します。

   version
7. Edge サーバ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 展開のアップグレードが完了します。次に、以下の確認を行います。

- ダイヤルプランが無傷であること。
- Web 管理インターフェイスおよびログファイルに障害状態が報告されていないこと。

アップグレードする前にノードのクラスタ化を解除した場合は、MMP コマンドを使用してそれらをクラスタリングし直してください。

SIP および Web アプリケーションを使用して接続できることを確認します（サポートされている場合は Web Bridge 3 も同様）。

ロールバック手順に関する注意：サーバーをアップグレードした後に予期しないことが発生し、ダウングレードする場合は、前のバージョンのソフトウェアリリースをアップロードし、**upgrade** と入力します。その後、各サーバー上で MMP コマンド **factory_reset app** を使用します。サーバーが工場出荷時の状態にリセットして再起動したら、**backup rollback <name>** コマンドを使用して、各サーバー上の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 リスニングインターフェイスの構成

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、および Skype Front End（FE）サーバーなどのピアとの TLS 接続や Web Bridge の C2W 接続を確立するために使用するキーと証明書のペアを必要とします。ピア SIP プロキシに TLS が必要な場合（Skype for Business など）、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 Lync のコールは、Cisco Expressway を使用してローカルのファイアウォールを通過する場合があるため、Call Bridge と Cisco Expressway 間で信頼を構成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 and/or Microsoft Infrastructure (Expressway X8.9.2)』、または X8.10 を実行している場合は『Cisco Meeting Server 版Cisco Expressway Web プロキシ（X8.10）』と『 Cisco Expressway セッション 分類導入ガイド（X8.10）』を参照してください。

コマンド **callbridge listen <interface>** を使用して、リスニングインターフェイス（A、B、C、D から選択）を設定できます。デフォルトの推奨事項は、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です。

1. 『証明書 ガイドライン』の説明に従って、Call Bridge 証明書を作成およびアップロードします。
2. MMP にサインインして、Call Bridge がインターフェイス a 上でリッスンするように構成します。

   ```
   callbridge listen a
   ```

   注：Call Bridge では、直接通信する必要のある SIP 参加者または SIP プロキシとの間に NAT を存在させることができません。Call Bridge を Cisco Expressway などのファイアウォール トラバーサル ソリューションと組み合わせることで、ファイアウォール トラバーサルまたは NAT の問題に対処できますが、Call Bridge と SIP プロキシ間の NAT をトラバーサルすることはできません。

   ---

3. 次のコマンドを使用して、Call Bridge が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
   ```
   コマンド全体と、CA により提供された証明書バンドルの使用については、証明書のガイドラインで説明されています。
4. 変更を適用するには、Call Bridge インターフェイスを再起動します。

   ```
   callbridge restart
   ```

4.4 HTTPS アクセス用 Web 管理画面インターフェイスの構成

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

Web Admin インターフェイスは、Call Bridge のユーザ インターフェイスです。Web Admin インターフェイスの証明書は、（いずれかの設置ガイドに従って）セットアップ済みのはずです。セットアップされていない場合は、ここでセットアップします。

1. インストールは、Web 管理画面インターフェイスがインターフェイス A でポート 443 を使用するように自動的にセットアップします。ただし、Web Bridge でも TCP ポート 443 は使用されます。Web 管理インターフェイスと Web Bridge の両方で同じインターフェイスを使用する場合、MMP コマンド **webadmin listen <interface> <port>**を使用して、Web 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ます。 例：

   webadmin listen a 445
2. Web 管理インターフェイスにアクセスできることをテストするには、同等の情報を Web ブラウザに入力します。**https://meetingserver.example.com:445**

   アクセスに成功した場合は次のセクションに進みます。
3. Web Admin インターフェイスにアクセスできない場合は、次のようにします。

   a. MMP にサインインし、以下を入力して、出力を確認します。

      webadmin

      出力の最終行は、 「**webadmin running**」 となっているはずです。

   b. そうでない場合は、Web Admin インターフェイスに構成上の問題があります。以下を入力して、有効化していることを確認します。

      webadmin enable

   c. **webadmin** コマンドの出力には、インストール済み証明書（webadmin.key や webadmin.crt など）の名前も表示されます。

      注：これらは、前にアップロードした証明書と同じ名前にする必要があります。

      例として示した名前であると想定した場合、次のように入力します。

      pki match webadmin.key webadmin.crt

      これによりキーと証明書が一致していることを確認します。

   d. それでも問題が発生する場合は、『証明書のガイドライン』に説明されている手順に従って 、問題のトラブルシューティングを行います。

4.5 Edge サーバーインスタンスのステージング

外部 Web アプリケーション参加者の Edge として Meeting Server を使用する場合は、このセクションを完了します。Call Bridge に直接アクセスできない Web 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、このセクションは省略できます。

Meeting Server Edge インスタンスは、セキュリティリスクを最小限に抑えるために必要最小限のサービスでのみ構成する必要があります。Edge サーバーインスタンスがその役割を実行するには、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、ルックアップを実行し、TLS 操作に必要な正確な時間を維持できるように、NTP クライアントと DNS クライアントも構成する必要があります。任意ですが、中央管理サーバーにログを送信するように syslog を構成することをお勧めします。展開手順では、標準の TURN UDP 構成と、TCP 443 を使用したオプションの TURN 構成の両方を説明します。

Web Bridge と TURN を設定する前に、Edge のすべての Meeting Server インスタンスを、プラットフォームに関連する設置ガイドに従って展開し、以下を完了しておく必要があります。

- サーバー MMP インターフェイス（コンソールまたは SSH）へのアクセスのセットアップ
- ネットワークインターフェイスの IP 情報の構成
- サーバー上の DNS クライアントの構成
- サーバー上の NTP クライアントの構成
- Syslog の構成（必要な場合）

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 の構成

Web Bridge 3 は、ブラウザベースの Cisco Meeting Server Web アプリの使用を可能にするために使用されます。展開で Web アプリケーションの使用を有効にしない場合は、Web Bridge サービスは必要ないため、このセクションをスキップできます。

- 内部ネットワークから Web 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。
- プロキシとして Cisco Expressway を使用し、Web アプリケーションに TURN サーバーを使用している場合、Web Bridge は Core のメインの Meeting Server インスタンスで設定する必要があり、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 Bridge を Edge だけで実行するか、Edge とメインの内部の Meeting Server インスタンスの両方で実行するかを選択できます。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 Web アプリを使用できます。Edge Meeting Server モデルを使用した展開で推奨されるのは、DMZ と内部サーバーインスタンスの両方で Web Bridge を実行することです。このセクションの手順を完了して、Edge インスタンスで Web Bridge を構成し、Core でメインの Meeting Server インスタンスを構成します。

注：Core と Edge の両方で Web Bridge を実行するには、クライアントが同じ Web Bridge のホスト名を内部インスタンスまたは Edge インスタンスに適切に解決する必要があります。これは通常、DNS サーバーがクライアントの所在地に基づいて名前をアドレスに解決する「スプリット DNS」と呼ばれます。

注意：Expressway ユーザ向けの重要事項
Web Bridge 3 と Web アプリケーションを導入する場合は、Expressway バージョン X12.6 以降を使用する必要があります。それより前のバージョンの Expressway は、Web Bridge 3 でサポートされていません。

注：Web アプリの詳細については、『Cisco Meeting Server Web アプリケーションの重要 事項』を参照してください。

4.6.1 Web Bridge 3 の構成に役立つ情報

Web アプリケーションを使用できるように Web Bridge 3 を設定するために役立つ情報を以下に示します。

- 「Call Bridge to Web Bridge」（C2W）プロトコルは、callbridge と webbridge3 の間のリンクです。これは、Call Bridge から Web Bridge への発信接続であり、それらの間に制御チャネルを確立します。証明書は、C2W 接続を認証および保護するために使用されます。C2W は、Call Bridge - Web Bridge トラフィック専用であり、ユーザーまたは他のサービスによって使用されません。
- C2W リスニングポートは、**`webbridge3 c2w listen`** を使用して Web Bridge サーバーで定義され、Call Bridge が HTTPS 接続を使用して Web Bridge に接続できるようにします。使用するポート番号のデフォルト値は設定されていませんが、このガイドでは例として 9999 を使用します。この接続は、証明書を使用してセキュリティで保護する必要があります。
- C2W ポートは Call Bridge からのみ到達可能であればよいため、外部からアクセスできないように保護することをお勧めします。

- Call Bridge は、動作するように設定されている各 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）。
- Web アプリクライアントには、Web Bridge に到達するための単一のアドレスがあるため、複数の Web Bridge が使用されている場合は、DNS またはロードバランサ ソリューションを使用して、共有名を使用可能な Web Bridge インスタンスに送信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、両側が検証のための証明書を提示する必要があります。Call Bridge は **`callbridge certs`** を使用して設定された証明書を使用し、Web Bridge は **`webbridge3 c2w certs`** コマンドを使用して設定された証明書を使用します。
- Web Bridge は、Web Bridge の C2W 信頼ストアに含まれる、または **`webbridge3 c2w trust`** によって設定された信頼ストアの証明書によって署名された Call Bridge およびスケジューラの証明書を信頼します。この Web Bridge に接続する Call Bridge 証明書を含むバンドルを使用して、特定の証明書の一致のみが許可されるようにすることをお勧めします（証明書ピン留め）。
- Call Bridge は、Call Bridge の C2W 信頼ストアにある Web Bridge の証明書、または **`callbridge trust c2w`** によって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。この Call Bridge が接続する Web Bridge 証明書を含むバンドルを使用して、特定の証明書の一致のみが許可されるようにすることをお勧めします（証明書ピン留め）。
- スケジューラは、スケジューラの C2W 信頼ストアにある、またはコマンド **`scheduler c2w certs <key-file> <crt-fullchain-file>`**によって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、それらの使用法を有効にして、Call Bridge と Web Bridge 間の相互 TLS 認証交換を許可する必要があります。拡張キー使用法が証明書で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ている必要があり、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ている必要があります。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見なされます。
- C2W 接続は内部サービス間のみであるため、パブリック認証局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 Bridge 3 を登録するために使用された c2w:// の URL で使用されている FQDN または IP アドレスに一致する必要があります。これが一致しない場合、Call Bridge は Web Bridge が提示した証明書を拒否し、TLS ネゴシエーションを失敗させるため、Web Bridge との接続が失敗します。

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。（IP アドレスを含む証明書は、パブリック CA では署名できません。）C2W アドレスで IP アドレスを使用する場合は、C2W 接続が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 リスニング インターフェイスに使用される証明書は、クライアントが接続するときに証明書の警告が表示されないようにするために、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。クライアントが Web Bridge に到達するために使用する FQDN は、クライアントが接続するときに証明書の警告が表示されないようにするために、証明書の CN または SAN リストに含まれている必要があります。
- 証明書に関する一般的な情報については、展開環境に応じた 証明書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 Web アプリケーション クライアントをサポートしている場合は、Web Bridge サービスを Core Meeting Server インスタンスで有効にする必要があります。Meeting Server Edge 展開を使用する場合、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 Core Meeting Server インスタンスで実行できます。

Web Bridge 3 が実行される各 Meeting Server インスタンスで次の手順を実行します。

1. MMP に SSH でログインします。
2. 次のコマンドを使用して、Web Bridge が Web サーバーに使用するインターフェイスとポートを構成します。
   webbridge3 https listen <interface>:<port>.
   最初のインターフェイスとポート 443 を使用することをお勧めします。例：
   webbridge3 https listen a:443
3. コマンド **webbridge3 https certs<key file> <full certificate chain file>** を使用して、Web Bridge が Web サーバーに使用する HTTPS 証明書とキー ペアを設定します。
   このコマンドでは、証明書を完全な証明書チェーンとして定義する必要があります。つまり、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です。例：
   webbridge3 https certs wb3-https.key wb3-https-fullchain.crt
4. 次の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構成します。
   webbridge3 c2w listen <interface>:<port>.
   最初のインターフェイスと、例で使用されているデフォルトのポート 9999 を使用することをお勧めします。例：
   webbridge3 c2w listen a:9999

5. コマンド **webbridge3 c2w certs** で C2W 接続証明書を設定します 。
   <key file> <full certificate chain file>。
   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 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。この FAQ 「How do I configure connection certificates for use with Web Bridge 3?（Web Bridge 3 で使用する接続証明書を構成するにはどうすればよいですか?）」にも追加情報が記載されています。

6. Web Bridge 3 C2W 信頼ストアは、この Web Bridge への接続を許可される Call Bridge 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。制御を最大化するために、署名機関の証明書ではなく、バンドル内の個々の Call Bridge 証明書を使用することをお勧めします（証明書ピン留め）。コマンド **webbridge3 c2w trust <certificate bundle>** を使用して Web Bridge の c2w 信頼バンドルを設定します。例：
   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を向上するために推奨されます。
   webbridge3 http-redirect enable
8. Web Bridge サービスを有効化します。
   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、使用される証明書またはキーペアが各インスタンスで正しいことを確認します。

4.6.3 C2W 接続を使用するための Call Bridge の構成

C2W は、Call Bridge インスタンスと Web Bridge インスタンス間の制御インターフェイスであり、Web Bridge が展開されている場合は、Call Bridge でこのインターフェイスを構成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 Web Bridge C2W 証明書、または Web Bridge 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。制御を最大化するために、署名機関の証明書ではなく、バンドル内の個々の Web Bridge C2W 証明書を使用することをお勧めします (証明書のピン留め)。

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 は、Call Bridge リスニングインターフェイスの設定で実行された手順からの証明書で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構成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の設定の手順を繰り返します。Call Bridge は、C2W 機能の証明書を使用して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 信頼ストアを設定します。例：

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

   注：スコープによって制限されない限り、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。

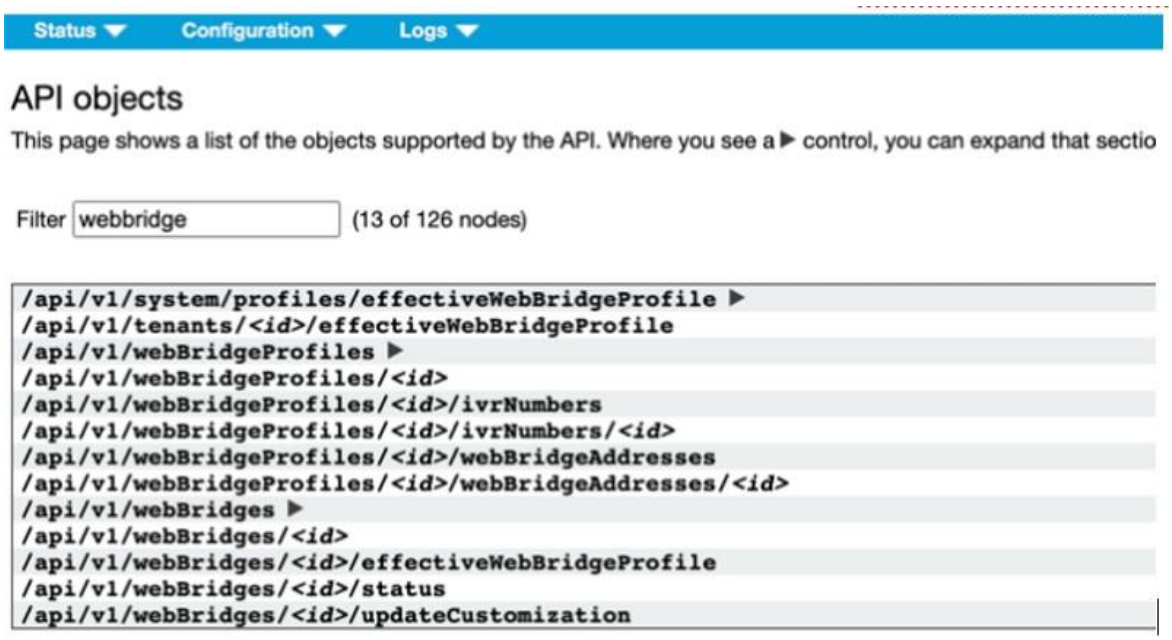
4. Call Bridge を再起動します。

   ```
   callbridge restart
   ```

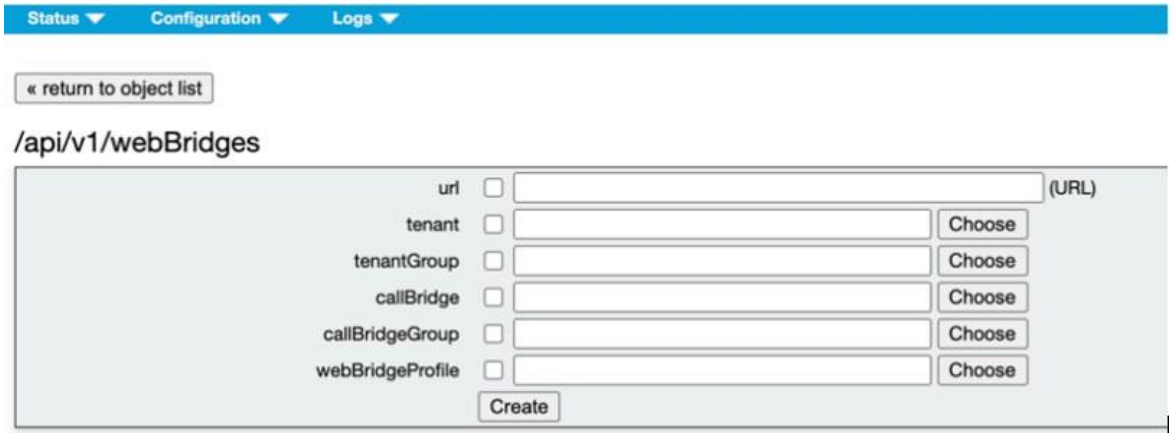
4.6.4 Web Bridge アドレスでの Call Bridge の構成

Meeting Server API で Web Bridge エントリを作成することにより、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 Web 管理インターフェィスで 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 Web 管理インターフェイスにログインし、[設定（Configuration）] > [API] を選択します。
2. 次に示すように、フィルタ入力ボックスに **webBridges** と入力し、リストビューをフィルタ処理します。



3. 結果のリストから **/api/v1/webBridges** 行を見つけ、► アイコンをクリックして展開します。
4. [新規作成（Create new）]をクリックして新しい Web Bridge オブジェクトを作成すると、パラメータフィールドが次のように表示されます。



5. *c2w://<Web Bridge FQDN>:<c2w port>* の形式を使用して、Web Bridge の C2W インターフェースの FQDN アドレスを追加して URL フィールドに入力します。例：

   c2w://cmsedge1.company.com:9999

   注：ここで入力する FQDN は、CN であるか、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 SAN 名のリストに含まれている必要があり、Web Bridge の C2W インターフェイスの IP に解決される必要があります。 IP アドレスは、C2W 証明書に証明書の SAN または CN に IP アドレスがある場合にのみ使用できます。

   ---

6. [作成（Create）]をクリックして、新しい Web Bridge エントリを保存します。

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

4.7 TURN サーバーの構成

TURN サーバーは、Call Bridge に直接到達できない Web 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。

- 展開で Web アプリクライアントを使用していない場合は、このセクションを省略できます。
- Web プロキシおよび TURN プロバイダーとして Cisco Expressway を使用している場合は、TURN サーバーおよび Call Bridge 設定の構成手順について、このセクションの代わりに『Cisco Expressway Web Proxy for Cisco Meeting Server (X12.6)』を使用してください。

- Meeting Server Edge 展開を使用している場合は、各 Edge インスタンスで TURN サーバーを設定する必要があります。このセクションの手順を実行して、TURN サービスを設定します。

次のセクションを完了して、TURN サーバーを設定し、それを Call Bridge に追加します。

4.7.1 TURN サービスの有効化

1. MMP に SSH でログインします。
2. TURN サーバーの短期間のログイン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ログイン情報では、以前に使用されていた静的な TURN サーバーのログイン情報よりもセキュリティが大幅に向上します。TURN 資格情報は、TURN サーバーでリレーを要求できるユーザーを制御するために使用され、TURN サーバーの使用を許可するために、コールのセットアップ中に Web アプリクライアントに自動的に提供されます。Meeting Server Edge を使用するすべての展開で、短期間の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、短期間の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 サーバーの短期資格情報機能の共有秘密とレルムを設定します。

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

   この 2 つの値は任意の文字列にすることができ、パスワードのように扱う必要があります。これらの値は、Call Bridge の設定で TURN サーバーを定義するときにも必要になります。例：

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

   注意：TURN サーバーのパスワードと資格情報は一意である必要があります。管理者のユーザ名やパスワードを再使用しないでください。

   ---

4. TURN サーバー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 の内側にある場合は、次のコマンドを使用して、TURN サーバーにマッピングするパブリック IP アドレスを TURN サーバーに通知します。

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

   TURN サーバーがルーティング可能なパブリック IP アドレスを使用している場合は、この手順を省略してください。例：

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

5. コマンド **turn listen <interface allowed list>** を実行して、TURN サーバーが特定のインターフェイス上でリッスンを実行するように構成します。Web Bridge とともに最初のインターフェィス「a」でリッスンするように TURN を構成する必要があります。例：

   ```
   turn listen a
   ```

6. 3478 で TURN TCP を有効にする場合は、TURN サーバーが使用する TCP ポートを **turn tls <port|none>** コマンドを
   使用して設定します。例：

   ```
   turn tls  3478
   ```

   この例では、TCP 3478 ポートを使用していると想定しています。TURN TCP を有効にしない場合は、この手順を省略してください。

7. TURN TCP を有効にする場合は、使用する証明書とキーのペアで TURN サーバーを構成する必要があります。証明書は、Web Bridge で使用するものと同じ CA により署名される必要があります。TURN TCP を有効にしない場合は、この手順を省略できます。次のコマンドで TURN サーバー証明書を設定します：**turn certs <key file> <certificate file> <ca cert>.**
   例：

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

   注：TURN サーバーに使用される証明書は、Web Bridge 3 証明書などの既存の証明書にすることができます。

   ---

8. TURN サービスを有効化します。

   ```
   turn enable
   ```

複数の Edge Server インスタンスを使用する場合は、Edge Meeting Server インスタンスごとに上記の TURN 構成手順を繰り返し、使用される証明書/キーペアが各インスタンスで正しいことを確認します。

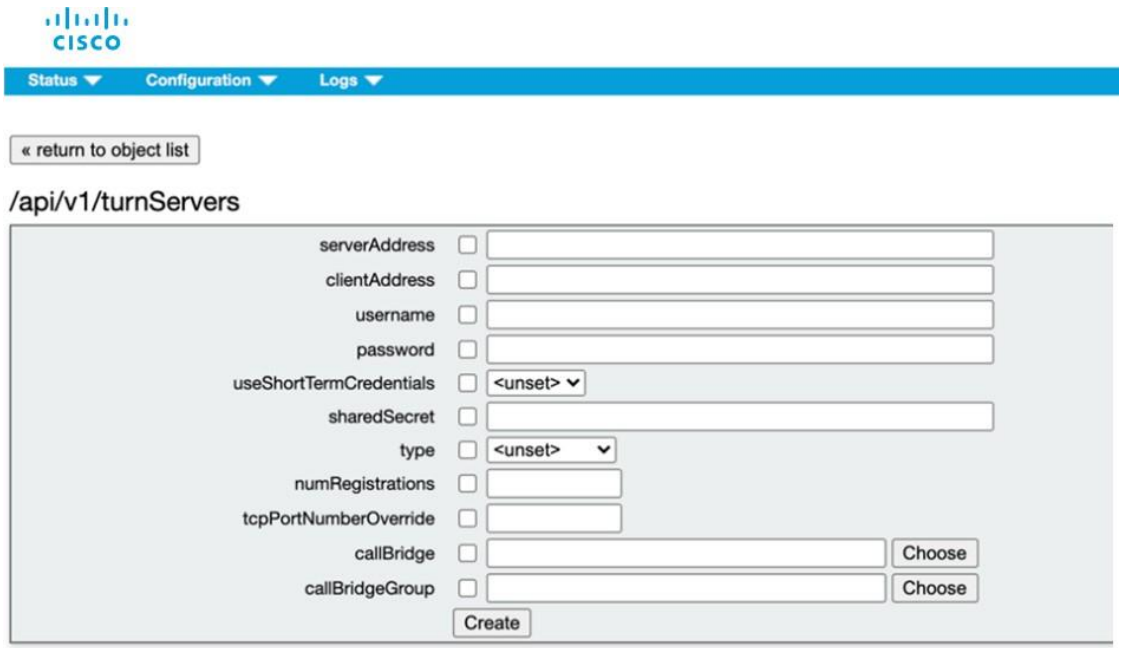
4.7.2 TURN アドレスを使用した Call Bridge の設定

使用する使用可能な TURN サーバーの詳細を使用して Call Bridge を設定する必要があります。これらの TURN 構成は、Web アプリの参加者と Skype for Business の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。

Call Bridge には、Meeting Server API で各 TURN サーバーの turnServers エントリを作成して、使用できる TURN サーバーに通知する必要があります。このガイドでは、Meeting Server の Web 管理インターフェイスで 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 Web 管理インターフェイスにログインし、[設定（Configuration）] > [API] を選択します。
2. 次に示すように、フィルタ入力ボックスに turn と入力し、リストビューをフィルタ処理します。

3. 結果のリストから /api/v1/turnServers 行を見つけ、▶ アイコンをクリックして展開します。
4. [新規作成（Create new）] をクリックして新しい turnServer オブジェクトを作成すると、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 サーバーについて次のフィールドを入力します。

   serverAddress - Call Bridge が TURN サーバー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 サーバーの 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 サーバーに接続しようとしないようにダミーアドレスを提供します - 例：nothing.local

   clientAddress - 外部クライアントが TURN サーバー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 の場合は、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間の資格情報を使用するように TURN サーバーを設定した場合は、true に設定します（推奨）。

   sharedSecret - 前のセクションのステップ 3 で TURN サーバーを構成したときに使用した sharedSecret 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「standard」になり、クライアントに UDP 3478 を使用し、TCP 443 でフォールバックして TURN サーバーに接続するように指示します。Meeting Server Web Edge を展開する場合、このパラメータを「cms」に設定する必要があります。

   tcpPortNumberOverride - 443 以外のポートで TURN TCP を構成した場合は、turn tls コマンドで構成され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 サーバーに接続できないというステータスが生成される可能性があります。これは既知の問題ですが、展開には影響しません。

   ---

6. [作成（Create）]をクリックして、新しい TURN サーバーエントリを保存します。

複数の TURN サーバーがある場合は、上記の手順を繰り返して、TURN サーバーインスタンスごとに TURN サーバーオブジェクトを作成します。

4.8 MeetingApp の構成

Meeting Server 管理者は、MeetingApps を構成する前に、ファイル共有やアンケートなどの Web アプリケーション機能を有効にする必要があります。サインインしている Web アプリユーザーのみが、会議でファイルを共有およびダウンロードできます。。スタンドアロンの Meeting Server で MeetingApps サービスを構成することをお勧めします。

構成の手順は、次のとおりです。

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

   meetingapps https listen <interface> <port>

   注：
   - 構成されたポートは、MeetingApp を展開する場所に応じて、内部ネットワークと外部ネットワークの両方から到達可能である必要があります。
   - MeetingApp の到達可能性のトラブルシューティングには、API **https://hostname/IP address:port/api/ping** を使用できます。

   ---

3. 次のコマンドを使用して、MeetingApp の証明書キーペアを設定します。

   meetingapps https certs <key-file> <crt-fullchain-file>

   注：公的に信頼された署名証明書を使用することを強くお勧めします。内部 CA 署名付き証明書の使用を計画している場合は、CSR の生成と証明書の検証について、『*Cisco Meeting Server リリース 証明書ガイドライン*』を参照してください。

   ---

4. 次の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、後で Web Bridge を構成します。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 を新しい鍵で構成する必要があります。
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 を構成する前に、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. セットアップ内のすべての Web Bridge は、会議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ために、MeetingApp と通信する必要があります。次のコマンドを使用して MeetingApp に接続するように Web Bridge を構成します。

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

   Meeting Server 管理者は、MeetingApps の **hostname** と、**meetingapps gensecret** コマンドを使用して前に生成した秘密鍵を提供する必要があります。
8. 次のコマンドを使用して、すべての Web Bridgeを有効にします。

   webbridge3 enable

4.9 MMP ユーザー用 LDAP 認証

新しい **ldap** オプションが **user add** MMP コマンドに追加され、LDAP サーバー、ディレクトリ検索パラメータ、TLS 設定の詳細を構成し、LDAP 認証を有効化または無効化できるようになりました。Meeting Server の展開中、LDAP ユーザーアカウントを持つ管理者および Web アプリケーションユーザーは、LDAP 認証を使用して Web 管理インターフェイス、SSH、SFTP、シリアルコンソールにログインできます。LDAP 認証に失敗した場合、ユーザーのログインは拒否されます。

注：共通アクセス カード（CAC）展開の場合、CAC 認証は LDAP 認証とローカル認証の両方よりも優先されます。

この機能は、LDAP を介した MMP ユーザーのインポート、または既存のローカルユーザーの LDAP 認証ユーザーへの切り替えをサポートしていません。管理者は、MMP コマンド **user add** を使用して各ユーザーを手動で追加することにより、LDAP ユーザーを事前に構成する必要があります。ログイン名がローカルユーザーと 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ために、新しいオプション [**ldap**] がコマンドに追加されました。

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

注：Meeting Server API は、LDAP 認証によるユーザへのアクセスをサポートしていません。

---

ldap オプションを使用して追加されたユーザーの認証は、LDAP サーバーによって行われます。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のルックアップのみで実行されます。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 サーバーが使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 ユーザはログインできません。バックアップとして、少なくとも 1 人のローカル管理者ユーザを常に MMP で設定しておくことをお勧めします。

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、およびポートを使用して、Microsoft AD LDAP サーバーまたは Open LDAP サーバーの構成をサポートします。この LDAP サーバーは、Web アプリのユーザー認証に使用されるものと同じにすることができます。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を確認してください。また、Meeting Server 用に個別に設定する必要があります。

詳細については、『MMP Command Reference Guide（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 設定

ユーザーが Web アプリを使用して Meeting Server に接続する場合は、LDAP サーバーが必要です（現在の Microsoft Active Directory、OpenLDAP、または Oracle Internet Directory LDAP3。以下の注を参照）。Meeting Server は、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。

ユーザ名は、LDAP からフィールドをインポートして作成できます。これについては、このセクションで説明しています。パスワードは Meeting Server にキャッシュされません。Web アプリの認証時に LDAP サーバにコールが送信されるため、パスワードは LDAP サーバ上で中央に安全に管理されます。

注：LDAP/AD 同期用に Meeting Server を構成する場合、LDAP/AD の属性を受け入れるフィールドには、大文字と小文字を区別するフォーマットで属性を入力する必要があります。たとえば、ユーザー名マッピングで属性 userPrincipalName を使用する場合は、次のようになります。$userPrincipalName$ の場合、同期は成功しますが、$UserPrincipalName$ の場合は同期が失敗します。各 LDAP 属性が正しい大文字や小文字で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）をサポートしています。これは、Web 管理インターフェイスではなく、API を介して構成する必要があります。Meeting Server を構成して Oracle Internet Directory をサポートするには、Meeting Server は、LDAP 同期中の検索操作で LDAP ページ結果コントロールを使用しません。**`/ldapServers`** への POST または**`/ldapServers/<ldap server id>`** への PUT で、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

LDAP を使用して Meeting Server を設定するのは、環境を設定するのに強力で拡張性の高い方法です。LDAP 構造内で組織のコール要件を定義することで、Meeting Server で必要となる構成の量を最小限に抑えることができます。

サーバでは、フィルタ、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、ユーザをたとえば以下のようなグループに分けることができます。

- 人事部の全員
- 等級 11 以上の従業員
- 職位 = 「取締役」
- 姓の最初の文字が「B」である人

5.2 Meeting Server の構成

このセクションの例では、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（この場合は Active Directory）を設定する方法について説明します。ただし、Meeting Server は API を介して設定できる複数の LDAP サーバをサポートしています。『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 のクラスタを構成する場合、最も簡単なメソッドは API を使用する方法です。Web 管理インターフェイスを介して複数の Call Bridge を構成する場合は、それぞれが同じ構成である必要があります。

注：Web 管理インターフェイスでは、1 つの LDAP サーバのみを構成できます。

Active Directory で動作する Meeting Server を設定するには、次の手順を実行します。

1. Web 管理インターフェイスにサインインし、[設定（Configuration）] > [Active Directory] に移動します。

2. 最初のセクションで、LDAP サーバへの接続を以下のように構成します。

   - アドレス = これは LDAP サーバのホスト名または IP アドレス
   - Port = 通常は 636
   - Username = 登録済みユーザの識別名（DN）。この目的のために、専用のユーザを作成できます。
   - パスワード = 使用しているユーザ名のパスワード
   - セキュアな接続 = セキュアな接続の場合は、このチェックボックスをオンにします。例：

```
Address: ldap.example.com
Port:     636
Username: cn=Fred Bloggs,cn=Users,OU=Sales,dc=YourCompany,dc=com
Password: password
```

注：ユーザ名とパスワードのログイン情報で必要な権限の詳細については、 付録 F を参照してください。

注：Meeting Server はセキュアな LDAP をサポートしています。デフォルトでは、LDAP サーバーはセキュア通信の場合はポート 636 で稼働し、非セキュア通信の場合にはポート 389 で稼働します。Meeting Server は両方をサポートしますが、636 を使用することを推奨します。安全な通信を行うには、セキュア通信（上記の説明を参照）を選択する必要があることに注意してください。ポート 636 のみを使用するだけでは不十分です。

注：LDAP サーバがセキュアな接続で設定されている場合、MMP で **tls ldap** コマンドを使用して TLS 証明書の検証が構成されるまで、接続は完全にセキュアではありません。

3. インポートするユーザの制御に使用するインポート設定を入力します。

- Base Distinguished Name = ユーザーのインポート元にする LDAP ツリー内のノードです。ユーザをインポートするベース DN には、以下のような設定が最適です。

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

- Filter = ユーザーの LDAP レコード内の属性値が満たす必要があるフィルタ式です。[フィルタ（Filter）] フィールドのシンタックスについては、rfc4515 に記載されています。

  ユーザーをメインデータベースにインポートする場合のルールは、「電子メールアドレスを持つすべてのユーザーをインポート」などにするのが妥当です。次のフィルタで表現できます。

```
mail=*
```

  テスト目的で、指定されたユーザー（fred.blogg など）と、メールアドレスが「test」で始まるテストユーザー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*))
```

  指定されたユーザー（fred.blogg など）とは別にすべてのユーザーをインポートする場合、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には、memberOf 属性をフィルタ処理できます。例：

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

  これは、APAC グループのメンバーであるグループとユーザの両方をインポートします。ユーザを制限（およびグループを省略）するには、以下を使用します。

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

  拡張可能一致ルール（LDAP_MATCHING_RULE_IN_CHAIN / 1.2.840.113556.1.4.1941）を使用すると、メンバーシップ階層（指定したグループの下）の任意のグループのメンバーシップをフィルタ処理できます。たとえば、以下のようにします。

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

LDAP のセットアップに適応できるその他の良い例には、次があります。

! で定義されたユーザーを除くすべての人とユーザーを追加するフィルタ。

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

上記と同じものを（krbtgt ユーザーは除く）、sAMAccountName がある場合にのみ追加するフィルタ。

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

上記と同じものを（krbtgt ユーザーを含む）、sAMAccountName があ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グローバルカタログクエリ（=cn=xxxxx で示されます）

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

4. フィールド マッピング式をセットアップします。

   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を、対応する LDAP レコードのフィールド値からどのように作成するのかを制御します。現在、この方法で以下のフィールドに値が取り込まれます。

   - 表示名
   - ユーザ名
   - スペース名
   - スペースの URI のユーザ パート（つまり、ドメイン名なしの URI）
   - スペースの 2 次 URI のユーザ パート（オプションであるスペースの代替 URI）
   - スペース コール ID（WebRTC クライアント ゲスト コールで使用するスペースの固有 ID）

   次のように、フィールドマッピング式にはリテラルテキストと LDAP フィールド値を混ぜた値を含めることができます。

   ```
   $<LDAP field name>$
   ```

式の例：

```
$sAMAccountName$@example.com
```

生成結果：

```
fred@example.com
```

詳細については、「LDAP フィールドマッピングの詳細」を参照してください。

注：インポートされた各ユーザーは、[設定（Configuration）]>[Active Directory]の[フィールドマッピング式（Field Mapping Expressions）]セクションにある JID フィールドを使用して作成された、一意のユーザー ID（JID）を持っている必要があります。有効な JID を作成するために、JID フィールドマッピング式で使用されるすべての LDAP 属性が、インポートされる各 LDAP レコード内に表示されている必要があります。表示されている属性を持つレコードのみをインポートするには、JID フィールドマッピング式で使用される各属性に対して、[インポート設定（Import Settings）]の下の[フィルタ（Filter）]フィールドに、「&」（AND）を使用してプレゼンスフィルタ（<attribute name>=*）の形式のもの）を組み込むことを推奨します。

たとえば、JID フィールドマッピング式が **`$sAMAccountName$@company.com`** だとして、グループ cn=Sales、cn=Users、dc=company、dc=com のメンバーであるユーザーをインポートする場合、適切なインポートフィルタは次のとおりになります。

```
(&(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**（Sync now）] を選択するか、適切な API コールを使用して同期をアクティブにします（『Cisco Meeting Server API リファレンスガイド』を参照）。

   注：LDAP サーバのエントリが変更された場合は、手動で再同期する必要があります。

   ---

6. [ステータス（Status）] > [ユーザ（Users）] にアクセスして、同期の結果を表示します。

LDAP からインポートする場合は、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（Configuration）] > [Active Directory] に移動します。[社内ディレクトリの設定（Corporate Directory Settings）] セクションで[検索をSearcher OUに制限（Restrict Search to Searcher OU）]を選択し、ユーザーアカウントの OU 内 でのみ検索を有効にします。

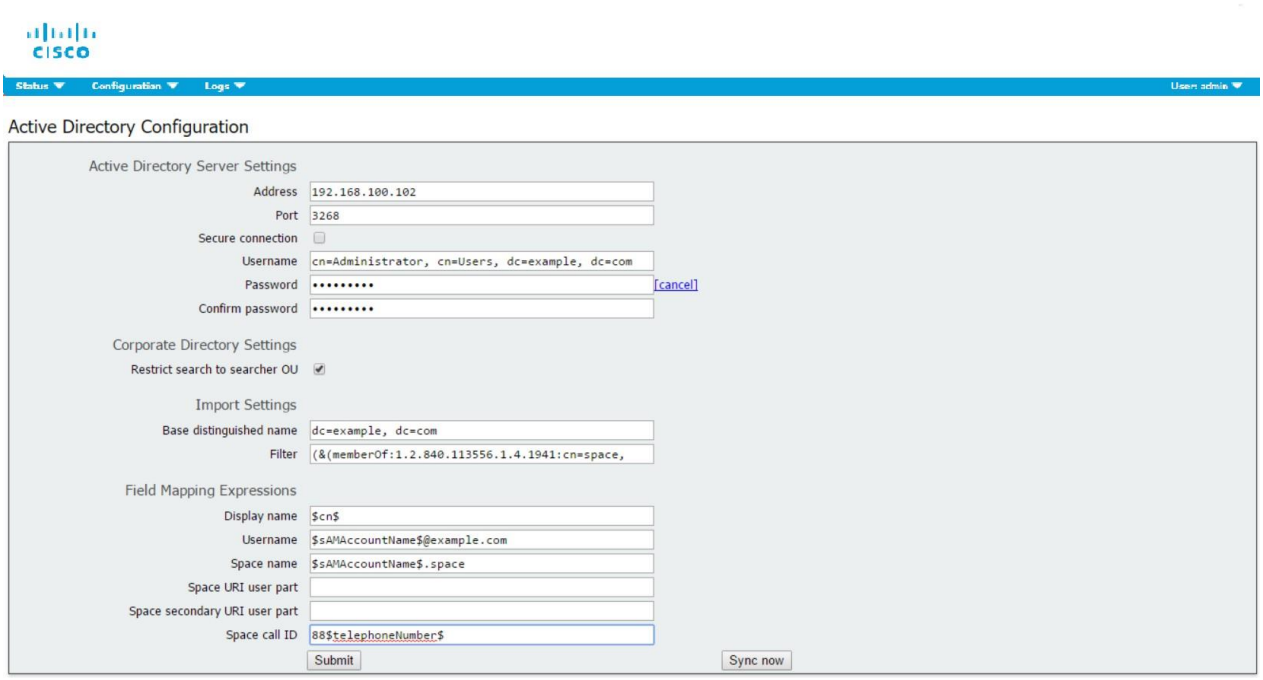
5.3 例

この例では、スペースを、ユーザの特定のグループと、正規の電話番号の前にプレフィックス 88 を付けたそのスペースのコール ID に指定します。

1. LDAP 構造内に「space」というグループを作成し、必要なメンバーをそのグループに指定します。

2. 次のフィルタを使用して、拡張一致ルール（LDAP_MATCHING_RULE_ IN_CHAIN / 1.2.840.113556.1.4.1941）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. その後、次のディレクトリ内の特定のユーザを同期します。

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

[ステータス（Status）] > [ユーザ（Users）] ページ上で表示できる次のスペースを作成します。

名前	ユーザ名
Fred Blogs	**fred.blogs@example.com**

[設定（Configuration）] > [スペース（space）] ページで次のスペースが表示できます。

名前	URI user part
fred.blogs	**fred.blogs.space**

5.4 メンバー以外のすべてのユーザスペースへのアクセスに関するパスコード保護の強化

スペースは、LDAP 同期を介して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。デフォルトでは、**nonMemberAccess** は **true** に設定されています。既存の動作は変更されず、スペースにアクセスするためのパスコードは不要で、メンバー以外のユーザーは作成されたスペースにアクセスできます。

nonMemberAccess を **false** にすると、すべてのユーザースペースへのメンバー以外のユーザーのアクセスについて、パスワード保護を強制することができます。

メンバーがメンバー以外のユーザのアクセスを構成し、LDAP 同期の一部としてパスコードを設定するには、次を実行します。

- リクエストパラメータ **nonMemberAccess** を **/ldapSources** に POST または **/ldapSources/ <ldap source id>** に PUT して、**false** に設定します。
- **nonMemberAccess** 設定を取得するには、 **/ldapSources/<ldap source id>** で GET を使用します。

注：バージョン 2.4（このパラメータが導入されたバージョン）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

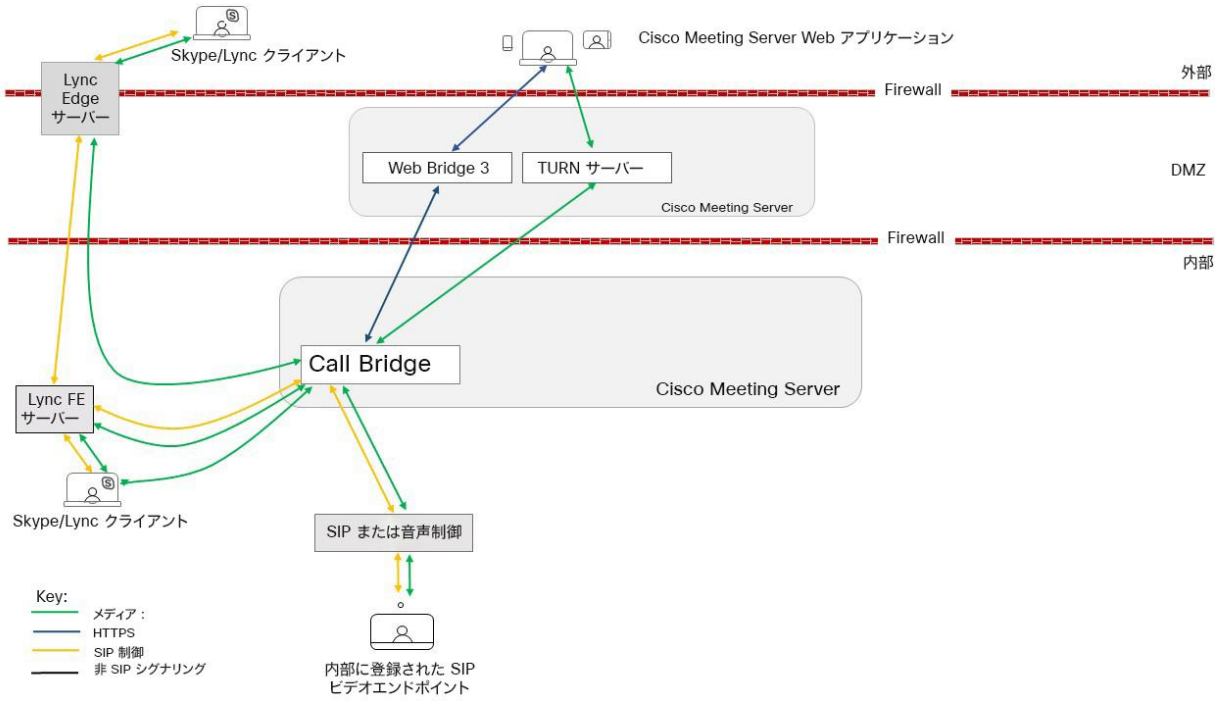
6.1 はじめに

Meeting Server を SIP、Lync、および音声環境に統合するには、SIP コール制御、Lync FE サーバー、音声コール制御から Meeting Server への接続を設定する必要があります。Meeting Server が必要なコールを正しくルーティングするには、これらのデバイスのコールルーティング構成の変更が必要です。

図 11 は、SIP ビデオエンドポイント、Lync クライアント、IP フォンが混在する企業へ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、および Lync クライアントと IP フォン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 というドメイン上で構成し、Lync クライアントは example.com というドメイン上で構成します。この例は、必要に応じて調整する必要があります。

図 11：ダイヤルプラン構成の展開例



上の図に示すように、Lync FE サーバには、Meeting Server への信頼された SIP トランクが必要です。SIP トランクは、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 アプリユーザ、SIP ビデオエンドポイントへルーティングするように構成されます。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、このトランクを経由して、Lync FE サーバから Meeting Server にルーティングする必要があります。

注：Office 365 または別の組織内のオンプレミスの Lync 展開への接続は、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には、example.com ドメイン（Lync クライアントの場合）と meetingserver.example.com（スペースおよび Web アプリの場合）にコールを Meeting Server にルーティングするため、SIP トランクをセットアップする必要があります。

Meeting Server では、ドメイン example.com を持つコールを Lync FE サーバーおよびサブドメイン vc.example.com と SIP コール制御プラットフォームにルーティングするダイヤルプランが必要です。

次のセクションでは、Meeting Server の Web 管理インターフェイスにある 2 つの構成ページについて説明し、Meeting Server が着信コールと発信コールを処理する方法を決定します。

この章に続いて、 第 7 章と 第 8 章では、トータルソリューションの構成に関する手順を説明します。

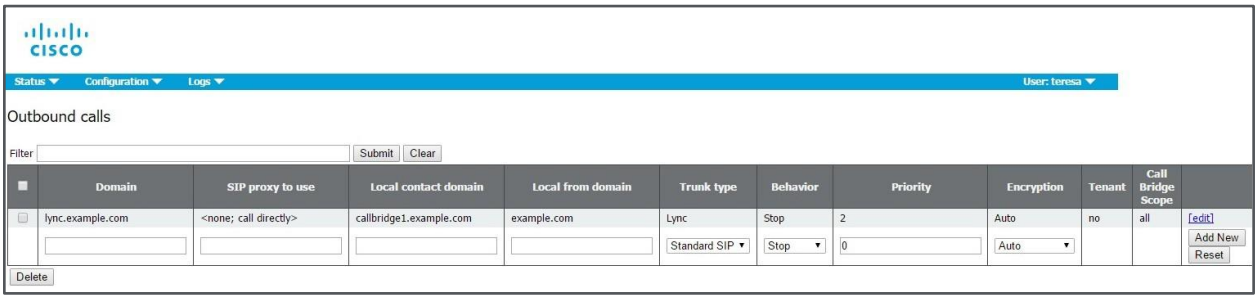
6.2 コールを処理する Web 管理インターフェイスの構成ページ

このセクションでは、Meeting Server が各コールの処理方法を決定するために使用する Web 管理インターフェイスの構成ページについて説明します。

Web 管理インターフェイスの[発信コール（Outbound calls）]と[着信コール（Incoming calls）]の 2 つの構成ページで、Meeting Server の着信コールと発信コールの動作を制御します。[発信コール（Outbound Calls）]ページは、発信コールの処理方法を制御します。[着信コール（Incoming calls）]ページは、着信コールが拒否されるかどうかを決定します。着信コールが拒否されず、マッチングされて転送される場合には、その転送方法に関する情報が必要になります。[着信コール（Incoming calls）] ページには、マッチング/拒否の構成用と転送動作用の 2 つのテーブルがあります。

6.2.1 発信コールページ

[発信コール（Outbound Calls）] ページでは、複数のダイヤルプランルールで構成された適切なダイヤルプランを構成できます。ダイヤル変換を発信コールに適用して発信コール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（Domain）]：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（「example.com」など）または「ワイルドカード」（「*.com」など）のいずれか。

[使用する SIPプロキシ（SIP proxy to use）]：ダイヤルプランの各エントリ/ルールは、発信コールのドメインと一致し（以下を参照）、使用する SIP プロキシ（またはダイレクトコールかどうか）を決定します。

[ローカル連絡先ドメイン（Local contact domain）]：このダイヤルプランルールを使用してコールの 連絡先 URI に使用されるドメインです。

注意：Lync を使用している場合、ローカル連絡先ドメインを使用することを推奨します。Lync を使用していない場合、SIP コールフローで予期しない問題を回避するために、[ローカル連絡先ドメイン（Local contact domain）] フィールドを空白のままにすることを推奨します。

注意：各 Lync ドメインについて、発信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います。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発信ルールを作成できます。

ドメインからのローカル：コールが発信元 ID/発信者 ID として 使用するドメイン。

トランクタイプ：通常、CiscoExpressway、Avaya Manager、または Lync サーバなどのサードパーティ SIP 制御デバイスにコールをルーティングするルールを設定します。したがって、現在設定できる SIP トランクには、標準 SIP、Avaya、および Lync の 3 種類があります。

注：Meeting Server では、Avaya PBX を使用する場合が一般的です。音声専用のコールです。ただし、Meeting Server は、Avaya 製品との相互運用性にこの制限を課すわけではありません（ビデオもサポートしている場合があります）。そのため、「avaya」のタイプのコールは、コールが音声専用であるわけではありません。

[動作（Behavior）]と[優先順位（Priority）]：ダイヤルプランルールが優先順位の値の順序で試行されます。ルールが一致するが、コールを実行できない場合、他の優先順位の低いルールを試行できます。ルールに STOP の動作がある場合、それ以降のルールは使用されません。

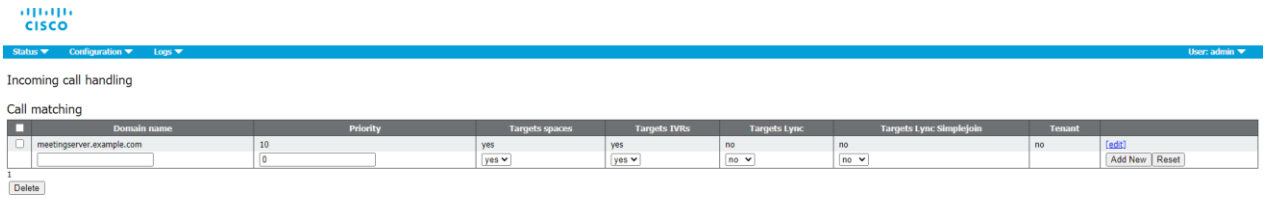
[暗号化（Encryption）]：[自動（Auto）]、[暗号化（Encrypted）]、[非暗号化（Unencrypted）]から選択します。

注意：デフォルトの[暗号化（Encryption）]動作モードは[自動（Auto）]です。LS 接続試行が失敗した場合に Call Bridge がこれらの接続に暗号化されていない TCP を使用しようとするのを防ぐために、すべての「Lync」発信ダイヤルルールが[暗号化（Encryption）]モードに明示的に設定されている必要があります。

6.2.2 着信コールページ：コールの照合

[着信コール（Incoming Call）] ページの 1 番上のテーブルは、[コールマッチング（Call Matching）] テーブルです。[コールマッチング（Call Matching）] テーブルで定義されるルールは、Meeting Server が着信 SIP コールを処理する方法を規定します。どのドメインの Meeting Server にルーティングされたコールでも、IVR、Web アプリユーザー、またはそのサーバー上の事前設定済みスペースの一致についてテストできます。

次に示すコールマッチングルールの例では、**meetingserver.example.com** ドメインに着信するすべてのコールについて、Web アプリユーザーとスペースの両方とのマッチングを試行します。



たとえば、着信コールが **name.space@meetingserver.example.com** 宛てで、**name.space** というスペースが構成されている場合、コールはその名前のスペースにルーティングされます。

着信コールに必要なドメインごとにルールを作成することを推奨します。コール制御ソリューションの中には、ドメインがサーバの 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、優先順位の高いドメインがメインドメインになる必要があります。IP アドレスとホスト名ルールの優先順位は低くなります。

優先順位値の高いルールが最初に一致します。複数のルールの優先順位が同じ場合は、ドメインのアルファベット順に照合が行われます。

1 つのルールが実行された後は、コールに対するリストのそれ以降ルールは無視されます。

すべてのコールマッチングルールに失敗した場合は、次のセクションの説明に従って次の表（コール転送）が使用されます。

注意点：

- スペースまたはユーザ（あるいはその両方）のマッチングは、@ の前の URI 部分に対してのみ行われます。
- スペースにマッチする優先順位の高いルールが、招待テキストの URI に使用されます。最も優先順位の高いルールは、個々の IP アドレスやホスト名のためではなく、展開全体のためであることが想定されます。
- ルールでは[ドメイン（Domain）]フィールドを空白のままにしないでください。空白のままにすると、Call Bridge がコールを拒否します。
- [Call matching] テーブル内のどのルールも、すべてのドメインとのマッチングが行われることはありません。

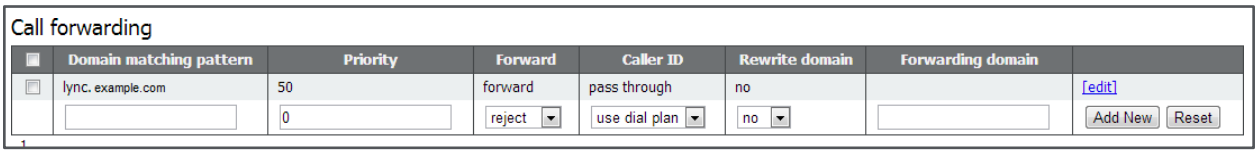
6.2.3 コール転送

着信コールがコールマッチングテーブル内のどのルールにも一致しない場合、コール転送テーブルに従ってコールが処理されます。この表では、コールを完全に拒否するか、ブリッジモードでコールを転送するか（Lync 会議への転換など）を決定するルールを持つことができます。ルールを定義することで、コールを転送するかどうかを決定します。特定のコールを「捕捉」して、拒否することが適切という場合もあります。

ルールは重複できます。ドメインマッチングパターンにはワイルドカード（exa*.com など）を含めることができますが、すべての一致として「*」を使用しないでください。使用した場合、コールループが作成されます。[優先順位（Priority）]の値を使用して、ルールを順序付けします。番号の大きいルールが最初に試行されます。

転送されるコールの場合は、[転送ドメイン（Forwarding domain）] を使用して接続先ドメインを書き換えることができます。新しいコールは、指定したドメイン宛に作成されます。[発信者 ID（Caller ID）] 設定を使用すると、転送されたコールが元の発信者の ID を保持するか、新しい発信者 ID を生成できます。[パススルー（pass through）] を選択すると、発信者の ID が保持されます。または、[ダイヤルプランを使用（use dial plan）] で、コールルーティング構成に従って新しい発信者 ID を生成します。

以下のコール転送ルールの例では、ドメイン lync.example.com コールを転送し、ルーティングはコールルーティングルールによって決定されます。



着信コールは、コールマッチングテーブル内のルールと一致しない場合や、コール転送テーブル内のドメインマッチングパターンと一致しない場合は終了します。

6.3 ダイヤル変換

ダイヤル変換は、発信ルールが適用される前に発信コールに適用されます。ダイヤル変換が適用されると、変換された番号に発信ダイヤルプランルールが適用されます。ダイヤル変換は発信コールにのみ影響しますが、ゲートウェイコールには影響しません。

変換には次の 3 つの段階があります。

- 「タイプ」が適用され、変換に適用するプリプロセスのタイプを定義します。
  - Raw：1 つのコンポーネントを生成します - $1
  - ストリップ：点、ダッシュ、スペースを削除し、1 つのコンポーネントを生成します - $1
  - Phone：国際電話番号への変換に使用します。 2 つのコンポーネント $1国コードと $2番号を生成します

注：電話 URI は、有効な国際ダイヤルコード（たとえば英国の場合は 44、米国では 1 など）で始まり、その地域の電話番号に対する正しい数字の桁数が続く場合に、純粋な数字文字列（オプションで「+」のプレフィックス付き）として認識されます。

- コンポーネントは正規表現を使用して一致し、ルールが有効かどうかを確認します
- 定義された変換に従ってコンポーネントから出力文字列が作成されます

例

例	タイプ	一致	変革
米国の番号の場合は、直接「vcs1」を使用します	電話	($1/01/)	$2@vcs1
英国の番号の場合は、プレフィックスを追加して「vcs2」を使用します。	電話	($1/44/)	90044$2@vcs2
7 で始まる英国の番号の場合は、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	($1/44/)($2/^7/)	90044$2{}123@mobilevcs
認識できない全桁の文字列の場合は、サフィックスとして「@vcs3」を使用します	除去	($1/(\d){6,}/)	$1@vcs3
+ を 00 に置き換えます	除去	($1/\+(\d)+/)	$1{/\+/00/}
英数字の正規表現（たとえば (.*)@example.com）を \1.endpoint@vc.example.com に置き換えます	未加工	($1/(.*) @example.com/)	$1{/@example.com$/ .endpoint@vc.example.com/}

1 台の Meeting Server に対して、Web 管理インターフェイスの [設定（Configuration）] > [発信コール（Outbound Calls）] ページを使用して、ダイヤルする番号の変換方法を制御します。一致式が指定されると、正規表現によって、指定された変換式が適用されるかどうかを決定します。

たとえば、以下のスクリーンショットのダイヤルプランでは、発信「+1」（米国）コールが 1 つの Call Bridge を使用し、+44（英国）コールが別の Call Bridge を使用できるようになります。

7 ダイヤルプラン設定：SIP エンドポイント

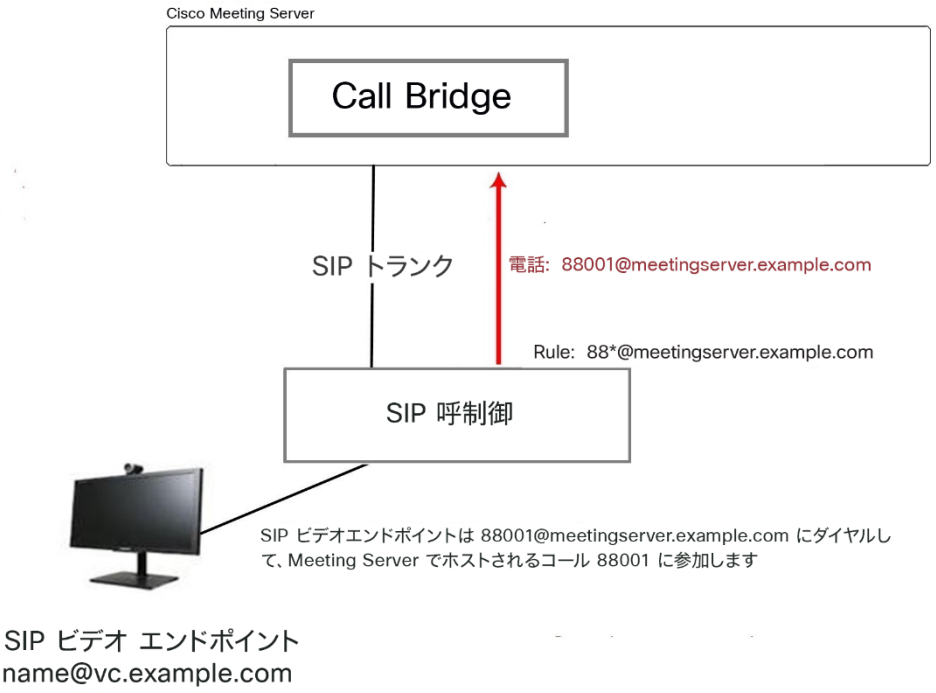
7.1 はじめに

この章では、SIP ビデオエンドポイントが Meeting Server でホストされている会議にダイヤルインできるようにするための構成について説明します。指定された順序で手順を実行し、必要に応じて例を適用します。

7.2 Meeting Server でホストされたミーティングをダイヤルする SIP ビデオエンドポイント

この最初の手順では、コール制御デバイスと Meeting Server の構成を考慮して、SIP ビデオエンドポイントを Meeting Server でホストされているミーティングに送信します。

図 12：Meeting Server でホストされたコールを呼び出す SIP ビデオエンドポイントの例



7.2.1 SIP コール制御の構成

この例では、SIP コール制御は Cisco VCS と仮定しますが、他のコール制御デバイスでも同様の手順が必要です。たとえば Cisco Unified Communications Manager を使用する場合、『Cisco Unified Communications Manager を使用した Cisco Meeting Server の導入ガイド』を参照してください。

1. 管理者として VCS にサインインします。
2. Meeting Server へのコールをルーティングするゾーンを設定します
   a. [VCS 設定（VCS Configuration）] > [ゾーン（Zones）] > [新規（New）] に移動します。
   b. 以下のように指定してゾーンを作成します。
      - H.323 Mode = Off
      - SIP Mode = On
      - SIP Port = 5060（TLS を使用している場合は 5061）
      - SIP Transport = 必要に応じて TCP または TLS
      - SIP Accept Proxied Registrations = Allow
      - Authentication Policy = 認証済みとして処理
      - SIP Authentication Trust Mode = Off
      - Peer 1 Address = Call Bridge の IP アドレス
3. Meeting Server にコールをルーティングする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 エンドポイント上のコールを Meeting Server のミーティングにルーティングする場合は、次の手順を実行します。
   a. [VCS 設定（VCS Configuration）] > [ダイヤルプラン（Dial Plan）] > [検索ルール（Search rules）] と移動します
   b. ルールに適切な名前（「**Meeting Server に EP をルーティング**」など）を付けます。
   c. 次の設定を行います。
      - Source = Any
      - Request Must Be Authenticated = No
      - Mode = Alias pattern match
      - Pattern Type = Regex
      - Pattern String = **.*@meetingserver.example.com**
      - Pattern Behavior = Leave
      - On Successful Match = Stop
      - Target = Meeting Server に作成したゾーン。

7.2.2 Meeting Server の構成

1. Meeting Server の Web 管理インターフェイスにサインインします。
2. Meeting Server に、エンドポイントがダイヤルできるよう、次のスペースを作成します。
   a. [設定（Configuration）] > [スペース（space）] に移動します

b. スペースを、以下を指定して追加します。
   - 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ます。

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。『API リファレンスガイド』を参照してください。

---

3. Meeting Server への着信コールに対する着信ダイヤルプランルールを追加します。
   a. [設定（Configuration）]>[着信コール（Inbound Calls）]に移動して、次の詳細を含む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**
      - Targets spaces = **yes**
      - Targets IVRs = **yes**
      - （オプション）Targets users = **yes**
      - Targets Lync = **yes** 注：これは後のセクション 8.1.2 で必要です

注：Web Admin インターフェイスの[着信コール（Inbound calls）]ページの詳細については、セクション 6.2.2 を参照してください。

---

4. VCS を介した SIP エンドポイントへの発信コールに対する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）]に移動して、次の詳細を含むダイヤルプランルールを追加します。
      - [ドメイン（Domain）]=<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 =

注：ローカル連絡先ドメインフィールドは、Lync にトランクを設定しない限り空白のままにします（セクション 8.1.2 のとおり）。

      - ドメインからのローカル = <FQDN of the Meeting Server>
      - トランクタイプ = **標準 SIP**。

注：Web Admin インターフェイスの [発信コール（Outbound calls）] ページの詳細については、セクションを参照してください。

SIP ビデオエンドポイントは、Meeting Server でホストされているコール 88001 にダイヤルできるようになりました。これを行うには、**88001@meetingserver.example.com** にダイヤルすることで、Meeting Server は SIP エンドポイントにコールアウトできます。第 8 章で Lync のダイヤルプランを作成する前に、次の点を検討してください。

- メディア暗号化設定を構成する場合は、セクション 7.3 を参照します。
- Cisco CTS エンドポイントの TIP サポートを有効にする場合は、セクション 7.4 を参照します。
- 自動音声応答（IVR）を構成する場合は、セクション 7.5を参照します。

7.3 SIP コールのメディア暗号化

Meeting Server は、Meeting Server との間で行われた Lync コールを含む、SIP 接続用のメディア暗号化をサポートしています。これは、Web 管理 インターフェイスの [設定（Configuration）] > [コール設定（Call settings）] ページで構成できます。

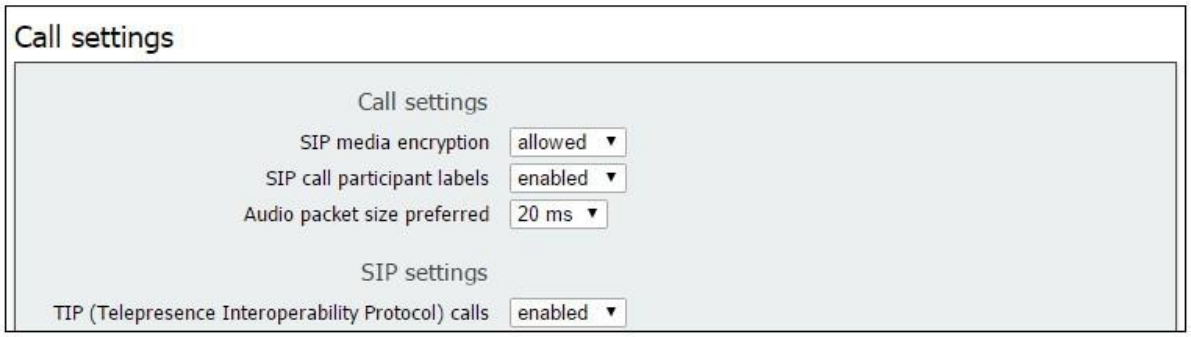
1. Web 管理インターフェイスにサインインし、[設定（Configuration）] > [コール設定（Call settings）] に移動します
2. 適切な [SIP メディア暗号化（SIP media encryption）] 設定（[許可（allowed）]、[必須（required）]、または [無効（disabled）]）を選択します。
3. SIP、CMA（Web アプリ）、またはサーバの反射的な帯域幅の設定を変更します。
4. すでに進行中の SIP コールにこれらの変更を適用する場合は、ページの最後にある[アクティブな通話に適用（Apply to Active Calls）]ボタンをクリックします。これらの変更を今後の SIP コールに適用する場合は[送信（Submit）]ボタンをクリックします。

注：Web 管理インターフェイスの[SIP 暗号化（SIP Encryption）]フィールドの[設定（Configuration）]>[発信コール（Outbound Calls）]ページでは、各発信コールルールに対して SIP 制御の暗号化動作を設定できます。これにより、制御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に TLS 制御接続を使用できます。API を介して動作を設定することもできます。

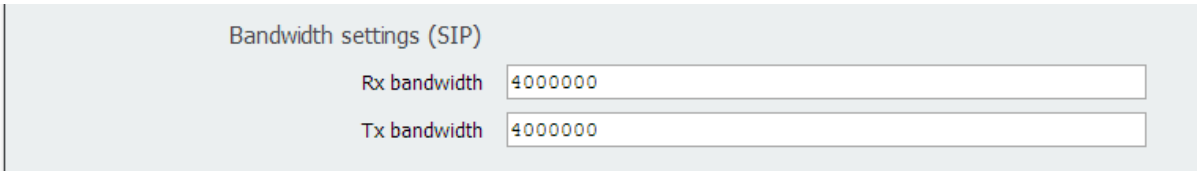
7.4 TIP サポートの有効化

Cisco CTS 製品などのエンドポイントを使用する場合は、TIP プロトコル サポートを選択する必要があります。これを有効にするには、以下のようにします。

1. Web 管理インターフェイスで [構成（Configuration）] > [コール設定（Call settings）] の順に選択します。[SIP 設定（SIP Settings）] セクションで、TIP（Telepresence 互換性プロトコル）を [有効（enabled）] に設定します。



2. [SIP Bandwidth Settings] をどちらも、4000000 以上に設定します。



3. [送信（Submit）] をクリックします。

7.5 IVR 構成

自動音声応答（IVR）を構成して、事前設定されたコールに手動でルーティングすることができます。着信コールは IVR にルーティングできます。そこで発信者は事前に録画された音声メッセージで、コールの ID 番号または参加を希望するスペースを入力するように案内されます。ビデオ参加者には、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、ユーザは適切なコールまたはスペースにルーティングされます。または、コールまたはスペースに PIN が割り当てられている場合は、PIN の入力を求めるプロンプトが表示されます。（発信者は、誤ったコール ID を 3 回入力してしまうと切断されます）。

IVR を使用する予定であれば、以下の手順に従います。

1. Web 管理インターフェイスにサインインし、[設定（Configuration）] > [全般（General）] に移動します。

2. [IVR] セクションで、次を設定します。
   - IVR numeric ID = <numeric call ID that users call to reach the IVR>
   - スケジュールされた Lync 会議にIDを使用して参加 = ポリシーに応じて「許可されていない」または「許可」を入力します。
3. [構成（Configuration）] > [着信コール（Incoming Calls）] の順に選択して、Target IVRs = "yes" と設定し、着信コールを IVR に一致させます。
4. 前の手順で設定した番号へのコールが Meeting Server にルーティングされるよう、SIP コール制御で適切なルーティングを構成します。

7.6 次のステップ

第 8 章の手順に従って、Meeting Server と Lync の展開を統合するダイヤルプランを構成します。

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

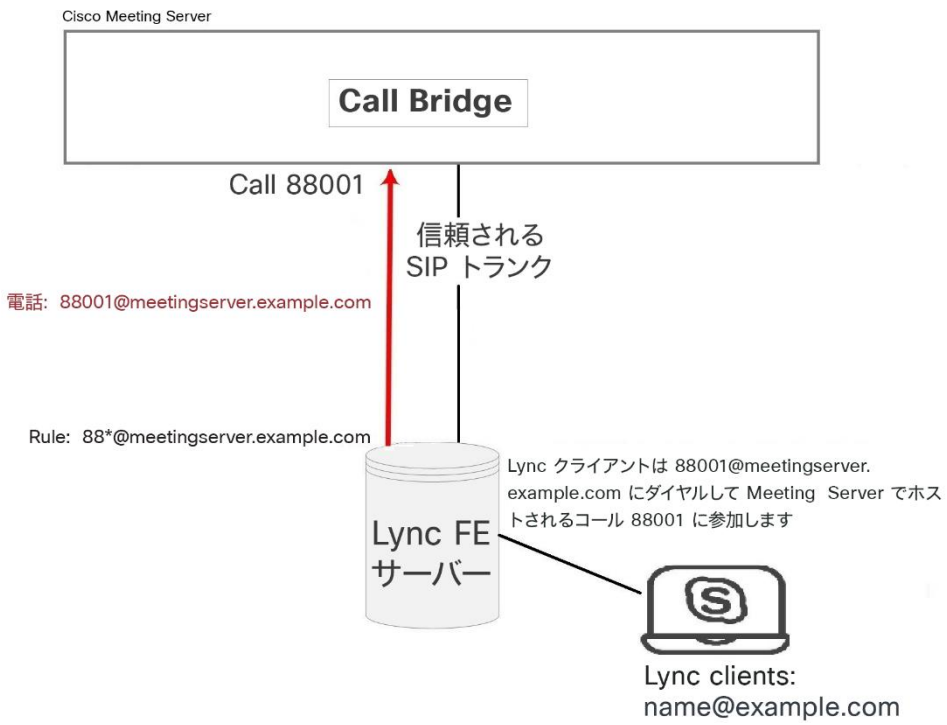
この章を通じて、Microsoft Lync への言及は、Microsoft Skype for Business を意味します。

注：Call Bridge と Lync Edge を統合するには、Call Bridge に独自のログインアカウントが必要です。Call Bridge との間の各 Lync コールに対して、サーバは、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。そのコールが接続解除されるまで、そのリソースは Lync の観点から「使用中」と見なされます。Lync は、ユーザアカウントごとに最大 12 件の TURN 割り当てを許可します。したがって、登録 1 件について、可能なコールは 12 件のみです。

8.1 Meeting Server 上のコールにダイヤルする Lync クライアント

このセクションでは、Lync エンドポイントが Meeting Server でホストされている会議に参加するために必要な構成の詳細を説明します。ここでは、 セクション 7.2 で使用されているのと同じ電話番号/URI を使用していますが、例は必要に応じて調整してください。

図 13：Meeting Server でホストされたミーティングに発信する Lync クライアントの例



8.1.1 Lync Front End（FE）サーバの構成

注意：このセクションでは 、Lync FE サーバーと Meeting Server 間の静的ルートの設定例を示します。これは単なるガイドラインであり、ユーザーが従う明示的な手順を示すものではありません。Cisco では、サーバの構成に同等の情報を導入する最良の方法について、ローカルの Lync サーバ管理者に助言を求めるよう、強く推奨します。

注：Lync FE サーバーから静的ルートを構成する前に、『証明書ガイドライン』に記載されているとおり、Lync FE サーバーによって信頼される証明書が Meeting Server にインストールされていることを確認します。

Lync クライアントから Meeting Server に発信されたコールを Meeting Server にルーティングするには、Meeting Server に向けた Lync 静的ルートを追加します。これには、Meeting Server を Lync FE サーバの信頼できるアプリケーションとして設定し、静的ルートを追加する必要があります。

1. Lync Server 管理シェルを開きます。
2. Meeting Server を信頼できるアプリケーションとして含める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
   ```

   次のように置き換えます。

   - **fqdn.meetingserver.com** を Meeting Server の FQDN と置き換えます。アイデンティティは Call Bridge の証明書で指定されている CN である必要があります。
   - **fqdn.lyncserver.com** を Lync FE サーバーまたは FE プールの FQDN に置き換えます。
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 -Port 5061
   ```

   次のように置き換えます。

   - **meetingserver-application** を任意の名前で置き換えます。
   - **fqdn.meetingserver.com** を Meeting Server の FQDN で置き換えます。
4. Meeting Server と Lync FE サーバ間に静的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
   ```

   次のように置き換えます。

- **fqdn.meetingserver.com** を Meeting Server のユーザーの FQDN で置き換えます。
- **meetingserver.example.com** を すべての Meeting Server コールに使用されるドメインと一致する URI で置き換えます。

5. 既存の静的ルートの集合に新しい静的ルートを追加します
   Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$x}
6. オンプレミスの場合、HTTPのデフォルトは8090、HTTPSのデフォルトは8181です。静的ルートを有効にする前に、Lync コールのデフォルトの画面の解像度をデフォルトの 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、次の方法を使用します。
   Set-CsMediaConfiguration -MaxVideoRateAllowed Hd720p15M
7. 新しい静的ルートを有効にします。
   Enable-CsTopology

注：ユーザーはログアウトして再度ログインし、新しい HD720p 設定を更新する必要がある場合があります。その他の設定はすべて自動的に実行され、数分で動作するようになります。

8.1.2 Meeting Server 上でのダイヤルプランルールの追加

1. Meeting Server の Web 管理インターフェイスにサインインし、[構成（Configuration）] > [発信コール（Outbound Calls）] に移動します。
2. 発信コールテーブルの下部に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）] フィールドに、Lync に送信する必要があるコールに対して一致する Lync ドメインを入力します。例：**example.com**
   b. [使用する SIP プロキシ（SIP Proxy to Use）] フィールドに、コールの送信先であ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白のままにしておくと、サーバーは **次** を使用して、呼び出し先ドメインの **DNS SRV** ルックアップを実行します。
        _sipinternaltls._tcp.<yourlyncdomain>.com
      - 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、サーバーは最初に、定義されたドメインの DNS SRV ルックアップを **_sipinternaltls._tcp.<サーバーアドレス>.com** を使用して実行し、SRV ルックアップが解決しない場合は入力されたホストの 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）] フィールドに、Meeting Server の FQDN を入力します。例：
      meetingserver.example.com

注：このフィールドを設定する必要がある場合は、Lync にトランクを設定する場合のみです。設定しない場合は、空白のままにする必要があります。

d. [ドメインからのローカル（Local From Domain）]フィールドに、コールの発信者を表示するドメイン（発信者 ID）を入力します（例：**meetingserver.example.com**）。

注：[ドメインからのローカル（Local From Domain）]を空白のままにした場合、発信者 ID で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）]として入力されたドメインになります。

e. [トランクタイプ（Trunk Type）] フィールドには、**Lync** を選択します。

f. [動作（Behavior）] フィールドには、このルールに失敗してコールが接続された場合に次の発信ダイヤルプランルールを試行するかどうかによって、[停止（stop）] または [続行（continue）]を選択します。

g. [優先順位（Priority）] フィールドで、優先順位レベルを割り当て、ダイヤルプランルールを適用する順序を決定します。より高い優先順位の値があるルールが最初に適用されます。

h. [暗号化（Encryption）] フィールドには、このルールを介したコールで暗号化された SIP 制御トラフィックが強制されるかどうかによって、[自動（Auto）]、[暗号化（Encrypted）]、または [非暗号化（Unencrypted）] を選択します。

i. [新規追加（Add New）] を選択します。

注：テナントおよび Call Bridge の範囲は API を通じてのみ設定できます。

終了後、Lync 環境から Meeting Server、Meeting Server から Lync にコールできるようになります。

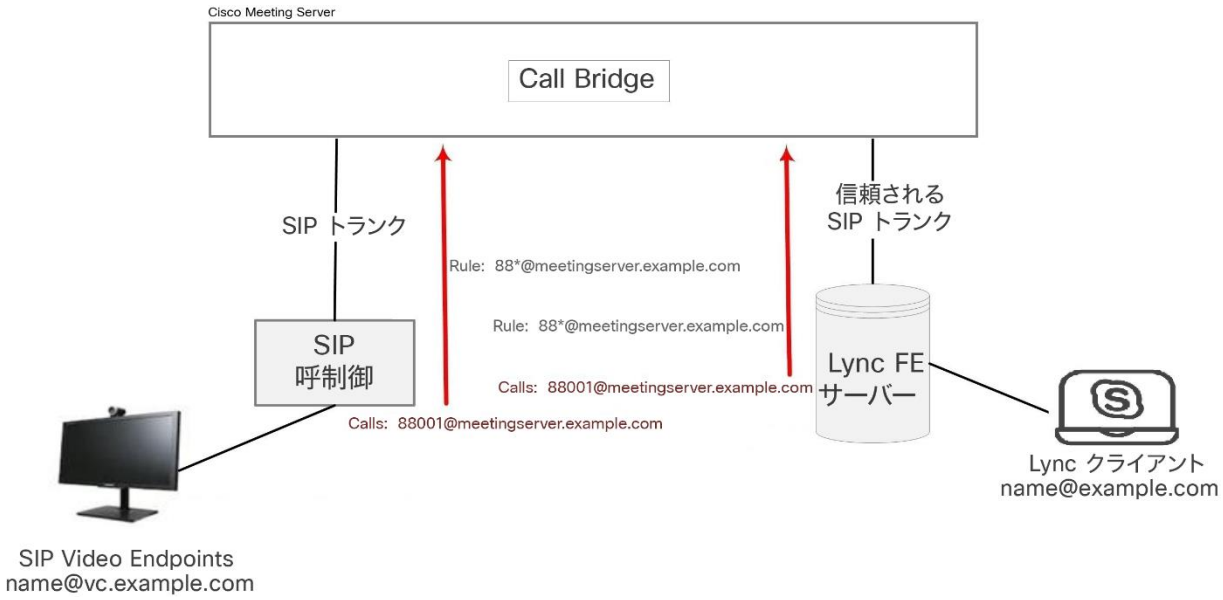
この例では、Lync クライアントは、Meeting Server でホストされているコール 88001 に、88001@example.com をダイヤルすることでダイヤルインできるようになります。

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 の手順を導入します。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 を導入します。

次に、SIP ビデオエンドポイントユーザと Lync クライアントユーザの両方は、
<call_id>@meetingserver.example.com

図 14：Meeting Server でホストされた会議に発信する SIP ビデオエンドポイントと Lync クライアントの例

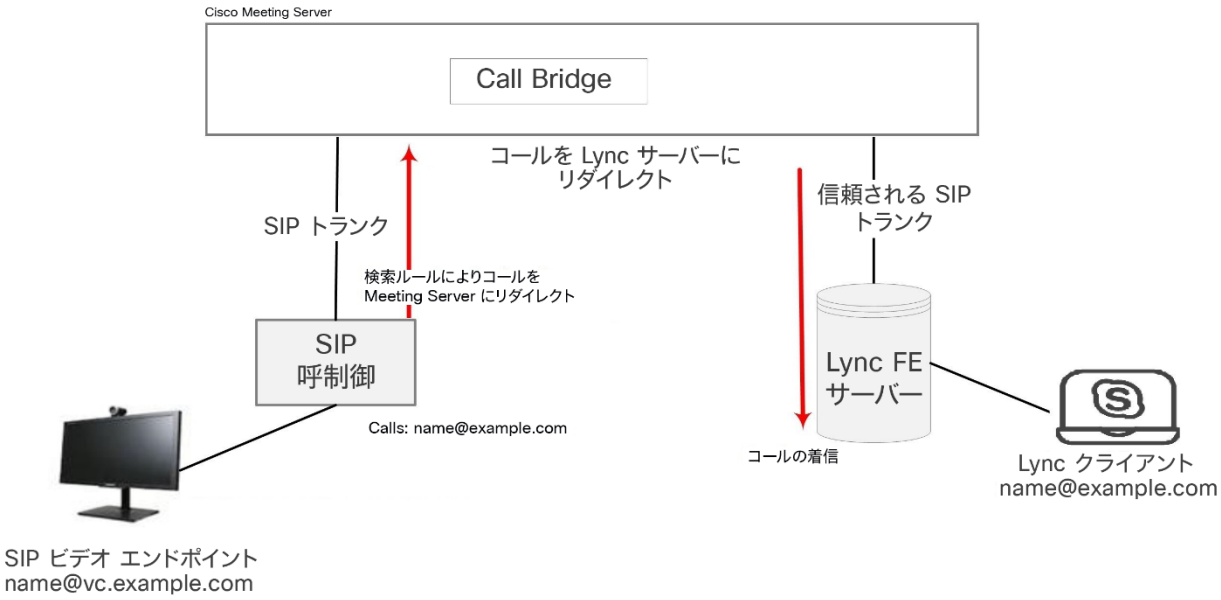


8.3 Lync クライアントと SIP ビデオエンドポイント間でのコールの追加

このセクションでは、2 つのダイヤルプラン構成セクション（セクション 7.2 と セクション 8.1）で説明されている構成の完了を前提としています。この例は、Lync と SIP のビデオエンドポイントが、ビデオと音声をトランスコーディングするゲートウェイとして Meeting Server を使用して、コール中に互いに通話することができるよう展開します（以下の図を参照）。

注：[発信コール（Outbound Calls）] ページは、以前に Meeting Server から Cisco VCS に SIP トランクを設定するために使用されています。Lync と SIP 環境の間を「ポイント対ポイントブリッジ」として機能するように Meeting Server を構成するには、このセクションの説明に従ってコール転送を構成する必要があります。また、Meeting Server から、Lync FE サーバ、Cisco VCS、Avaya CM、または Polycom DMA などの使用している他の SIP コール制御デバイスに SIP トランクを設定する必要があります。

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



この例では、以下のようになっています。

- Lync ユーザーは、**<name>@vc.example.com** をダイヤルして、SIP ビデオエンドポイント（たとえば **meetingroom1@vc.example.com**）とコールをセットアップできます。
- SIP ビデオエンドポイントは、**<name>@example.com** をダイヤルして、Lync エンドポイント（たとえば **roberta.smith@example.com**）とコールをセットアップできます。

例は必要に応じて調整してください。

8.3.1 Lync Front End サーバの構成

Lync クライアントが SIP ビデオ エンドポイントを呼び出せるようにするには、以下のようにします。

- Meeting Server 宛ての Lync 静的ルートを追加して、**@vc.example.com** へのコールをリダイレクトします。 セクション 8.1 で指定された Lync 静的ルートを作成する手順に従います。

Lync クライアントコールを SIP ビデオエンドポイントにルーティングします。

8.3.2 VCS の構成

SIP ビデオエンドポイントが Lync クライアントを呼び出せるようにするには、以下のようにします。

- VCS（SIP コール制御デバイス）に検索ルールを追加し、サフィックス **@example.com** を使用して Meeting Server にコールをルーティングします。

これにより、SIP ビデオエンドポイントコールが Lync クライアントにルーティングされます。

8.3.3 Meeting Server の構成

Meeting Server に 2 つの転送ルールを作成し、一方は SIP エンドポイントにコールを転送し、もう一方は Lync クライアントにコールを転送します。次に、2 つの発信ダイヤルプランルールを作成し、1 つは発信コールを SIP エンドポイントにルーティングし、もう 1 つは発信コールを Lync クライアントにルーティングします。

1. Web 管理インターフェイスにサインインし、[設定（Configuration）] > [着信コール（Incoming Calls）] に移動します。
2. [コール転送（Call forwarding）] セクション で、次の 2 つの新しいルールを作成します。
   a. 着信を vc.example.com に転送するコール転送ルールを作成します
      - [ドメインマッチングパターン（Domain matching pattern）] = **`vc.exa*.com`**
        ワイルドカードはドメインマッチングパターンの任意の部分で許可されますが、すべての一致として「*」を使用しないでください。使用した場合、コールループが作成されます。
      - [優先順位（Priority）] = <number> 任意の値を受け入れ可能です（他に転送ルールが設定されていない場合は 0 を含みます）。ルールが常に使用されていることを確認するには、その優先順位を設定したルールの中で最も高く設定します。

        （ルールは優先度順に処理され、優先度が最も高いものが最初に実行されます。2 つのドメインマッチングパターンが接続先ドメインと一致する場合、優先順位が高いルールが使用されます。
      - [転送（Forward）] = **`forward`**

        (「拒否」を選択すると、ドメインマッチングパターンと一致するコールは転送されませんが、終了します。）
      - [発信者ID（Caller ID）] = **`use dial plan`** 発信ダイヤルプランのドメインを使用します。
      - [ドメインの書き換え（Rewrite Domain）] = **`no`**
        コールは、コールされたドメインを使用して転送されます。

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

   b. 着信を example.com に転送するコール転送ルールを作成します
      - [ドメインマッチングパターン（Domain matching pattern）] = **`exa*.com`**
      - 優先順位：<number>

- [転送（Forward）] = **forward**
- [発信者 ID（Caller ID）] = **use dial plan**
- [ドメインの書き換え（Rewrite Domain）] = **no**
- [新規追加（Add new）] をクリックします。

3. [設定（Configuration）] >[発信コール（Outbound calls）] ページに移動し、次の 2 つの新しいルールを作成します。
   a. SIP エンドポイント用のドメイン vc.example.com に対するコール用のダイヤルプランを作成します。これは、セクション 7.2.2 の手順 4 の繰り返しです。
      - [ドメイン（Domain）]フィールドに、SIP エンドポイントに送信する必要があるコールに対して一致する SIP ドメインを入力します。例：**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 =

        注：ローカル連絡先ドメインフィールドは空白のままにする必要があります。

      - ドメインからのローカル = <FQDN of the Meeting Server>
      - トランクタイプ = **標準 SIP**。
      - [新規追加（Add New）] を選択します。
   b. Lync クライアントに対するドメイン example.com に対するコールの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）] フィールドに、Lync に送信する必要があるコールに対して一致する Lync ドメインを入力します。例：**example.com**
      - [使用する SIP プロキシ（SIP Proxy to Use）] フィールドに、コールの送信先であ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白のままにしておくと、サーバーは **次** を使用して、呼び出し先ドメインの **DNS SRV** ルックアップを実行します。**_sipinternaltls._tcp.<yourlyncdomain>.com**
        - 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、サーバーは最初に、定義されたドメインの DNS SRV ルックアップを **_sipinternaltls._tcp.<yourlyncdomain>.com** を使用して実行し、SRV ルックアップが解決しない場合は入力されたホストの 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）] フィールドに、Meeting Server の FQDN を入力します。例：**meetingserver.example.com**

注：このフィールドを設定する必要がある場合は、Lync にトランクを設定する場合のみです。設定しない場合は、空白のままにする必要があります。

- [ドメインからのローカル（Local From Domain）] フィールドに、コールの発信者を表示するドメイン（発信者 ID）を入力します。これは Call Bridge の FQDN です（**meetingserver.example.com** など）

  注：[ドメインからのローカル（Local From Domain）]を空白のままにした場合、発信者 ID で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）]として入力されたドメインになります。

- [トランクタイプ（Trunk Type）] フィールドには、**Lync** を選択します。
- [動作（Behavior）] フィールドには、このルールに失敗してコールが接続された場合に次の発信ダイヤルプランルールを試行するかどうかによって、[停止（stop）] または [続行（continue）]を選択します。
- [優先順位（Priority）]フィールドで、優先順位レベルを割り当て、ダイヤルプランルールを適用する順序を決定します。より高い優先順位の値があるルールが最初に適用されます。
- [暗号化（Encryption）] フィールドには、このルールを介したコールで暗号化された SIP 制御トラフィックが強制されるかどうかによって、[自動（Auto）]、[暗号化（Encrypted）]、または [非暗号化（Unencrypted）] を選択します。
- [新規追加（Add New）] を選択します。

SIP ビデオエンドポイントは、**<name>@example.com** をダイヤルして Lync クライアントにコールできるようになります。また、Lync クライアントは **<endpoint>@vc.example.com** をダイヤルして SIP ビデオエンドポイントをコールできるようになります。

8.4 WEB アプリと SIP および Lync クライアントの統合

注：Web アプリのユーザは、Lync ミーティングにコールアウトすることはできません。

Web アプリを使用するように Meeting Server を構成する手順については、「LDAP 設定」のセクションを参照してください。

同じ LDAP 構成を使用して Lync アカウントと Web 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、目的の Lync クライアントではなく Web アプリクライアントを呼び出しているユーザに問題が発生する可能性があります。こうした問題が発生するのを防ぐため、コールマッチングとコール転送に関するルールを設定します。以下に説明します。

たとえば、Meeting Server 上にアカウント **fred@example.com**、Lync FE サーバー上に **fred@lync.example.com** アカウントが作成されていると仮定します。Meeting Server にコールが到達して、コールマッチングルールが構成されていない場合、Meeting Server はドメインを無視し、そのコールは Meeting Server の **fred@example.com** アカウントに送信されます。Meeting Server は、ローカルにユーザー「fred」がいるかどうかを確認し、**fred@xxxx** の「**xxxx**」は無視します。

解決策は、コールマッチングルールを [着信コール（Incoming Calls）] ページに構成してローカル Web アプリユーザーのドメインと一致させ、コール転送ルールを構成して Lync クライアントにコールを転送します。コールマッチングルールとして、[ドメイン名（Domain name）] 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名前に設定します（**example.com** など）。[コール転送（Call forwarding）]セクションで、[ドメインマッチングパターン（Domain matching pattern）]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（**lync.example.com** など）。**fred@example.com** へのコールは、Web アプリユーザーに到達しますが、**fred@lync.example.com** へのコールは Fred 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 サーバーを使用した NAT トラバーサルの場合は、このセクションの構成手順に従って Meeting Server の Lync Edge 設定を構成します。これは、 デュアルホーム 会議をサポートするために必要です。または、Lync Edge が Meeting Server ではなく、Lync コールの TURN/ICE ロールを実行する場合に必要です。

8.5.1 Lync Edge コールフロー

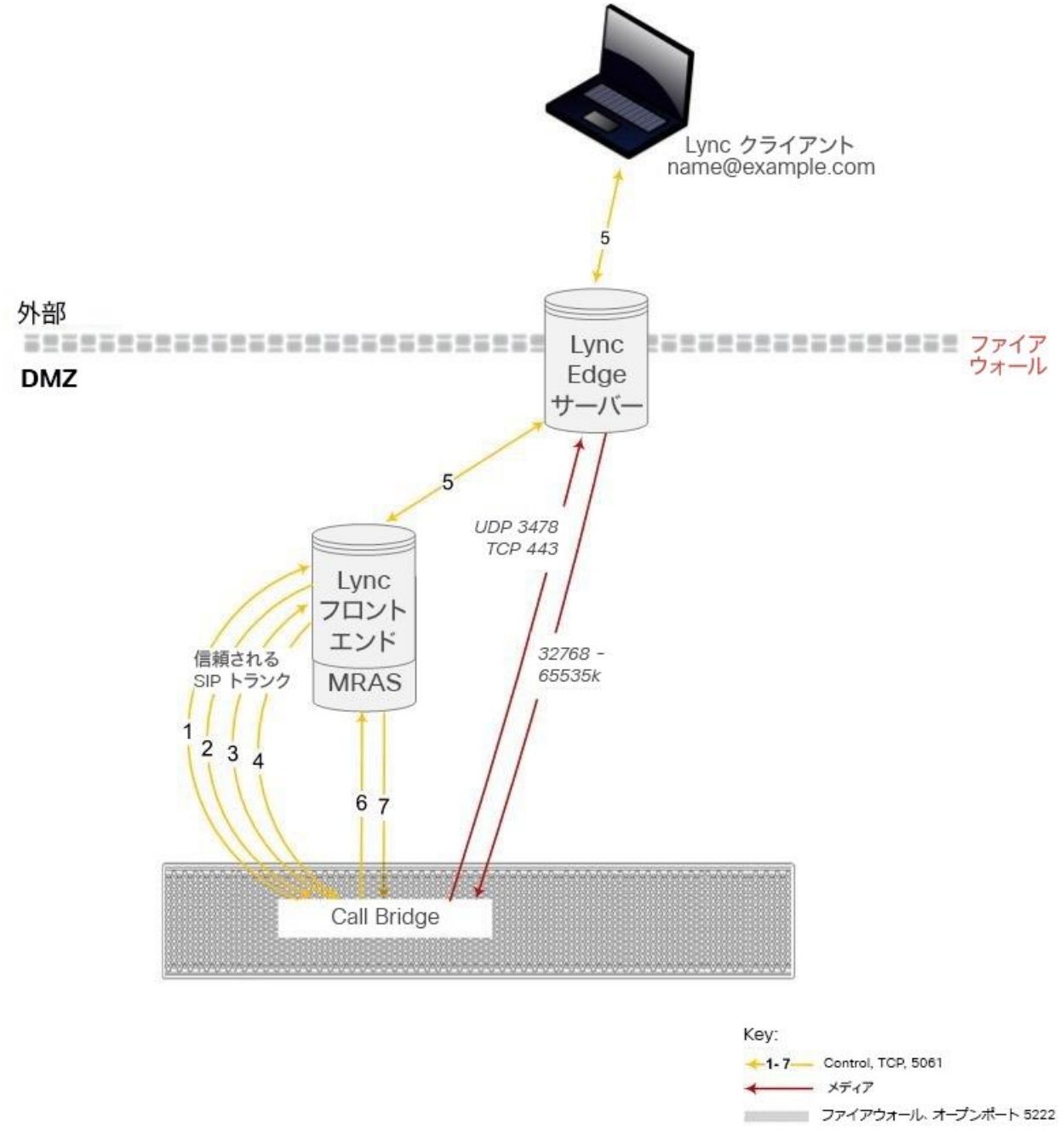
Meeting Server から Lync Edge サーバーへのコールを確立するには、次の手順を実行します（下の図 16 を参照）。

1. Call Bridge は、Lync FE サーバに対して「登録」SIP コールを行います。
2. 「登録」が承認されます。
3. Call Bridge は、Lync FE サーバに「サービス」を送信します。
4. FE サーバは、メディアリレー認証サーバ（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 クライアントは着信コールを開始します。
6. Call Bridge は、Lync FE サーバに「サービス」メッセージを送信して、Lync Edge MRAS サービスを使用するための MRAS のログイン情報を要求します
7. Lync FE サーバは、Call Bridge が使用するログイン情報、および UDP ポートと 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、STUN メッセージを Lync Edge サーバに直接送信します。
9. コールメディアは、UDP ポート 3478 で Call Bridge と Lync Edge の TURN サーバーとの間を直接フローし、上記の一時範囲内にあるポートで Lync Edge サーバーから Call Bridge に戻ります。

したがって、Call Bridge と Lync Edge サーバーのメディア間に、ファイアウォールで UDP 3478 発信と 32768-65535 着信のポートを開く必要があります。

図 16：Lync Edge サーバーへの Call Bridge のコールフロー



8.5.2 Lync Edge を使用する Meeting Server の構成

Lync Edge サーバを使用するには、Meeting Server の Web 管理インターフェイスにログインし、[設定（Configuration）] > [全般（General）] に移動し、Lync Edge 設定を構成します。（Lync Edge サーバが設定されている場合、Lync コールに対して TURN/ICE のロールを担います。そのため、あるレベルでは上記の TURN サーバ設定に代わる方法になります）。

また、Meeting Server と Lync Server Edge 構成を設定するには、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。

Lync Edge サーバを使用するために Meeting Server を設定するには、次の手順を実行します。

1. 適切な DNS レコードが設定されていることを確認します。分散型サーバータイプの展開に必要な DNS レコードのリストについては、 付録 1 を参照してください。

2. LDAP ディレクトリ内に新規ユーザを作成します（通常使用しているディレクトリで他のユーザを作成するのと同じ手順です）。たとえば、firstname = "edge"、second name = "user" などと指定します。

3. Lync FE サーバのユーザ マネージャにログインし、前の手順で作成したユーザから Lync クライアント ユーザを作成します。これは、他のユーザが Lync を使用できるようにする場合と同じ手順で実行します。上記の例の名前を使用すると、**edge.user@lync.example.com** という Lync クライアントユーザを作成します

4. Meeting Server の Web 管理インターフェイスにサインインし、[設定（Configuration）] > [全般（General）] 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ホスト名）を入力して、Lync Edge 設定を構成します。ユーザ名には、前の手順で作成した Lync クライアント ユーザ名を入力します。

5. 必要であれば、[Number of Registrations] フィールドに入力します。

   このフィールドは、1 台の登録デバイスに対して実行される同時コール数を制限する Lync Edge サーバの機能よりも優先されます。1 より大きな数を入力すると、Call Bridge によってその登録数が増え、Lync Edge Server を介して Meeting Server が可能な同時コールの数が増加します。

   1 より大きい数字を入力すると、数字が Lync Edge ユーザ名の末尾に追加され、最終的なユーザ名に登録されます。たとえば、ユーザー名が edge.user@lync.example.com と設定されており、[登録数（Number of Registrations）]を 3 に設定すると、Edge サーバーで使用できるように以下のユーザーを Lync 環境内に作成する必要があります。

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

これにより管理上のいくらかのオーバーヘッドが求められることになりますが、前述の Lync Edge サーバの制限に起因するものです。

登録数は空白のままにして、登録を **edge.user@lync.example.com** の 1 件のみ行います。

注：Lync FE サーバーは Call Bridge を信頼しているので、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 Edge の構成に関する注意点：

- Meeting Server は、Lync Edge サーバーを介してメディアが届く外部 Lync クライアントから、Lync コンテンツ（RDP で提供されたプレゼンテーション）をサポートします。また、スペース（URI）は、お気に入りにスペースがある Lync クライアントがスペースのステータスを確認できるよう、現在スペースにいる参加者の数に基づいてビジーまたは使用可能とレポートを返します。
- Lync AVMCU を使用している場合は、Lync FE サーバに登録するために、Lync エッジ設定を構成する必要があります。
- Web アプリは、Lync Edge サーバーが構成されている場合でも、引き続き Meeting Server TURN サーバーを使用します。
- Lync Edge サーバが構成されていれば、Lync のすべてのコールは、ICE 候補の収集と外部メディア サーバの接続にそのサーバを使用します。Lync Edge サーバーが構成されていないが、展開環境で Cisco Expressway が構成されている場合、Lync のコールは Expressway で構成された TURN サーバーによって処理されます。
- 通常の Lync Edge 導入環境では、Lync Edge サーバの内部インターフェイスには、規定のデフォルト ゲートウェイはありません。規定のデフォルト ゲートウェイがあるのは、外部インターフェイスのみです。Call Bridge インターフェイスが、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は、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、静的および永続的なネットワークルートを Lync Edge サーバーに定義する必要があります。Lync Edge サーバーにスタティックで持続的なネットワーク ルートを追加するには、CMD を開き、以下のコマンドを発行して、例のデータを独自の 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 のサブネット全体をゲートウェイ 10.255.106.1 経由でルーティングできる、ネットワークルートが追加されます。ここで 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ゲートウェイです。

  このルートを追加しない場合、Meeting Server から Lync Edge サーバーに送信される STUN パケットはすべて応答しなくなり、コールが失敗することになります。

8.6 Lync ダイレクトフェデレーション

Meeting Server は、NAT からの関与がないパブリック IP アドレスに Call Bridge を置くことによって、Microsoft Lync とのダイレクトフェデレーションをサポートしています。これにより、Meeting Server から任意の Lync ドメインに直接コールを行い、その逆もできます。

着信コールを許可するには、以下を行う必要があります。

1. Meeting Server の FQDN に宛てた 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 が必要であり、NAT はこのシナリオではサポートされないので、この手順が必要になります。

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. 以下に準拠した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. 証明書には CN としての FQDN が必要です。または SAN のリストがある証明書を使用する場合は、その FQDN が SAN のリスト内にもあることを確認します。注：証明書に SAN のリストが含まれている場合、Lync は CN フィールドを無視して、SAN のリストのみを使用します。

    b. 証明書は、パブリック CA により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）を使用してください。CA の詳細および Meeting Server と Lync 間の統合のサポートについては、Lync アドバイザーにお問い合わせください。

    ---

    c. 証明書バンドルには、信頼チェーンを確立できるように、ルート CA の証明書、およびチェーン内のすべての中間証明書が順番どおりに含まれている必要があります。

    注：証明書の詳細については、『Cisco Meeting Server 証明書ガイドライン』の「概要」を参照してください。

    ---

    d. 付録 B で言及されている適切なファイアウォール ポート（TCP 5061、UDP 3478、UDP 32768-65535、TCP 32768-65535 など）を開きます。

Meeting Server からの発信コールの場合は、次の手順を実行します。

1. 発信ダイヤルルールを作成し、[ドメイン（Domain）] フィールドと [SIPプロキシ（SIP proxy）] フィールドを空白のままにし、[トランク（Trunk）] のタイプを Lync に設定します。また、適切な[ローカル連絡先ドメイン（Local contact domain）]と[ドメインからのローカル（Local from domain）]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々のドメインを指定する場合は、Lync 側で構成されているすべてのドメインが追加されていることを確認します。使用中のドメインは、Lync Server トポロジビルダーツールから読み取ることができます。追加のドメインが後で Lync に追加される場合は、これらのドメインを発信ダイヤルプランルールにも追加する必要がありますので、注意してください。

8.7 スケジュールされた Lync ミーティングへの直接発信と IVR 経由のコール

Lync の展開前の前提条件：この機能には、電話ダイヤルイン機能がすでに有効になっている Lync 展開が動作している必要があります。Lync の展開には、1 つ以上のオンプレミス Lync FE サーバーを構成する必要があります。

注：Lync の展開が外部の Lync または Skype for Business をサポートしていない場合でも、オンプレミスの Lync FE サーバーを構成する必要があります。

Meeting Server は、Lync コール ID を使用してコールに参加し、WebRTC または SIP エンドポイントからスケジュールされた Lync ミーティングへのコールをサポートしています。Cisco Meeting アプリのユーザは、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、会議ルックアップ用に Meeting Server に 1 つ以上の Lync FE サーバを構成する必要があります。1 つのサーバの構成は、Web Admin インターフェイスで [設定（Configuration）] > [全般（General）] と進み、[Lync Edge settings] の下で行うことができます。1 つ以上のサーバの構成は、API で行うことができます（サーバを「lyncEdge」タイプの TURN サーバとして作成します）。これを行う方法については、「Lync Edge を使用する Meeting Server の構成」を参照してください。プールに複数の FE サーバがある場合は、このプール FQDN をサーバ アドレスとして使用します。

注：Lync のミーティングの解像度には、Meeting Server は、発信ルールではなく、_sipinternaltls._tcp.lync-domain ドメインの Lync ミーティング ID と 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<DNS RR>** を使用します。dns app コマンドの使用の詳細については、『MMP コマンドライン リファレンス』を参照してください。分散型の展開に必要な DNS レコードのリストについては、付録を参照してください。

Lync FE サーバーを構成し、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タスクシーケンス

順序	タスク	Web Admin インターフェイスを使用	API を使用
1	Lync 会議 ID を入力できるように Call Bridge IVR を設定する。	Web Admin インターフェイスを使用して IVR をセットアップした場合は、次のようにします。 [IVR] セクションで [設定（Configuration）] > [全般（General）] に移動し、[スケジュールされた Lync 会議にIDを使用して参加（Joining scheduled Lync conferences by ID）] を [許可（allowed）] に設定します	API を使用して IVR をセットアップした場合は、次のようにします。 構成された IVR に対して **resolveLyncConferenceIds** を true に設定します。
2	標準の SIP システムからの Lync 会議 ID への直接ダイヤルを許可する。注：既存の設定されたドメインを拡張して、Lync 会議へのアクセスを許可するか、この目的で新しいドメインを作成することができます。	[設定（Configuration）] > [着信コール（Incoming calls）] に移動し、1 つ以上の構成されたコールマッチングドメインについて、[ターゲット Lync（Targets Lync）] を yes に設定します。	Set **resolveToLyncConferences** を **true** に設定します。
3	Web Bridge コール参加インターフェイスで Lync 会議 ID を入力できるようにする。	Web Admin インターフェイスから Web Bridge をセットアップ済みの場合は、以下のようにします。 Web bridge 設定セクションで [設定（Configuration）] > [全般（General）] に移動して、[スケジュールされたLync会議にIDを使用して参加（Joining scheduled Lync conferences by ID）]が [許可（allowed）] に設定されていることを確認します。	API から Web Bridge をセットアップ済みの場合は、以下のようにします。 Web Bridge で **resolveLyncConferenceId** を **true** に設定します

コールが Lync 会議 ID に照合される場合、Call Bridge はまずコール ID がスペースに適用されないことを確認します。適用されない場合には、Call Bridge はそのコール ID を構成し、ID を解決できるサーバーとしてアドバタイズする Lync Front End サーバーを特定します。Call Bridge は、調査中のそのコール ID が Lync 会議に対応するかどうかを判別するために Lync Front End サーバーに照会します。対応する場合には、ルックアップが成功したと見なされ、そのコールは Lync コールに参加します。コール ID が Lync 会議に対応しているとして認識されない場合は、それ以降の Lync FE サーバは照会されません。

注：異なる Lync 展開環境内にある複数の Lync FE サーバーの設定を追加すると、予期しない結果が生じる場合があります。たとえば、異なる Lync 展開環境で複数の Lync 会議が同じコール ID を使用する場合、ルックアップに対して複数の Lync FE サーバがプラスに応答する場合があります。その場合には、「最初の」成功した Lync 解像度が使用されます。

注：Meeting Server から Lync ミーティングに接続する各参加者は、Lync AVMCU での参加者の競合を回避するために、固有の「from:」SIP アドレスを設定する必要があります。PSTN ゲートウェイを経由して接続する電話参加者は、一般的な発信者 ID 情報によって参加者の競合が発生するリスクが高くなります。すべての電話参加者が、Meeting Server のデュアルホームゲートウェイではなく、Lync PSTN 会議/仲介サーバーを介して Lync ミーティングに接続してください。

スケジュール済み Lync ミーティング用に送信された出席依頼のテキストをカスタマイズして、ユーザが Meeting Server を介して参加できるよう、必要な詳細を含めることができます。その詳細は、カスタム フッター セクションに記入してください。たとえば、「SIP/H.323 エンドポイントの場合は、join@example.com をコールして、上記の会議 ID を入力することで参加できます。WebRTC の場合は、join.example.com に移動し、上記の会議 ID を入力してください。」この中の URI は、上記で設定されたものと一致している必要があります。詳細については、Microsoft のマニュアル 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 会議に接続するための Call Bridge モードの選択

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

同じ Call Bridge 上のコールを 1 つの会議に統合する場合は、**`dualHomeCallBridge`** に設定します。Call Bridge で 1 回の会議を行うことができ、Call Bridge は AVMCU 会議にコールアウトします。

コールを 1 つの会議に統合しない場合は、**`gateway`** に設定します。各 SIP 参加者は、それぞれ独自の会議に参加し、AVMCU 会議に関連付けられたコールアウトを行います。

注：デュアルホーム会議を無効にするには、**`lyncConferenceMode`** を **`gateway`** に設定します。

9 Office 365 OBTP スケジュール機能搭載のデュアル ホーム エクスペリエンス

9.1 概要

「Office 365 OBTP （ワンボタン機能）スケジュール機能を使用したデュアル ホーム エクスペリエンス」により、参加者は OBTP をサポートするシスコエンドポイントを使用して Office 365 会議に参加できます。

ホストは、Microsoft Outlook と Skype for Business プラグインを使用してミーティングのスケジュールを設定し、参加者と会議室（OBTP 対応エンドポイントを含む）とミーティングする場所を追加します。

OBTP 対応エンドポイントを使用して会議に参加するには、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参加できます。Skype for Business のクライアントは通常通り、リンクをクリックしてミーティングに参加します。

注：Office 365 を使用する場合、招待された OBTP が有効なエンドポイントまたは Office 365 を搭載した Skype for Business のクライアントのみが Lync 会議に参加できます。Cisco のエンドポイントは、Meeting Server IVR を介して手動で会議に参加することはできません。これは、オンプレミスの Lync 展開の主な違いです。これにより、どのCisco エンドポイントでも Meeting Server IVR を介して手動で参加できます。

注：「Office 365 OBTP（ワンボタン機能）スケジュール機能搭載のデュアルホーム エクスペリエンス」はバージョン 2.2 以降でサポートされています。Cisco TMS 15.5 および Cisco TMS XE 5.5 以降が必要です。

9.2 構成

注：この機能では、Office 365 に接続するために、Call Bridge がパブリックインターネットに接続されている必要があります。発信トラフィックのためにファイアウォールで TCP ポート 443 を開く必要があります。

Office 365 会議に参加するこの方法を設定するには、Meeting Server の Web 管理インターフェイスにサインインして [構成（Configuration）] > [着信コール（Incoming calls）] に移動し、着信コールに対してコールマッチングルールを構成して [ターゲット Lync シンプルジョイン（Targets Lync Simplejoin）] フィールドを **`true`** に設定します。これは、Office 365 の招待で送信された Lync Simple Meet URL を解決する方法を Meeting Server に通知します。

会議だけでなく参加者にコールする機能を持たせるには、既存の発信ダイヤルプランルールを使用して発信コール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 会議中のエクスペリエンス

「OBTP スケジュール機能を使用した 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、コンテンツ共有を備える「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 によって決定された、使い慣れた会議中のエクスペリエンスが提供されます。OBTP が有効なエンドポイントを使用する参加者には、Meeting Server によって決定されるビデオ会議のエクスペリエンスが提供されます。参加者全員に、統合された参加者リストが表示されます。

注：クライアントに対する制御は会議全体で動作しません。また、何らかの異常な動作を引き起こす場合があります。たとえば、Skype for Business のクライアントが Meeting Server に接続されているエンドポイントをミュートした場合、エンドポイントはミュートになりますが、ミュート済みと言う通知はエンドポイントに送信されません。エンドポイント自体はミュートを解除できません。Skype for Business のクライアントが 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にしてからミュートを解除すると、すべてのエンドポイントはミュートされた状態のままになります。

注：ミュートや参加者の削除などの ActiveControl 機能は、ローカル Call Bridge の参加者にのみ影響を与え、Lync AVMCU には影響を与えません。

---

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を説明します。これにより、Web アプリのビデオコールやミーティングを使用できます。

Web アプリケーションをテストする場合は、最初の Meeting Server の構成が完了した後、いつでも提供される順序で、セクション 10.2 の手順に従ってください。Web 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：展開環境で Cisco Expressway Web プロキシが Web Bridge に接続する必要がある場合、Web Bridge 証明書の SAN フィールドに、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ます。含まれていない場合、接続は失敗します。たとえば、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、この FQDN の A レコードが存在する必要があります。また、Web Bridge 証明書の SAN フィールドに join.example.com が含まれている必要があります。

10.1 Web Bridge 3 の接続

表 7 に、Web アプリの接続に使用されるポートを示します。 セクション 10.1.1 では、Web アプリと Meeting Server のコンポーネント間のコールフローについて説明します。

図 17：Web アプリケーションポートの使用方法

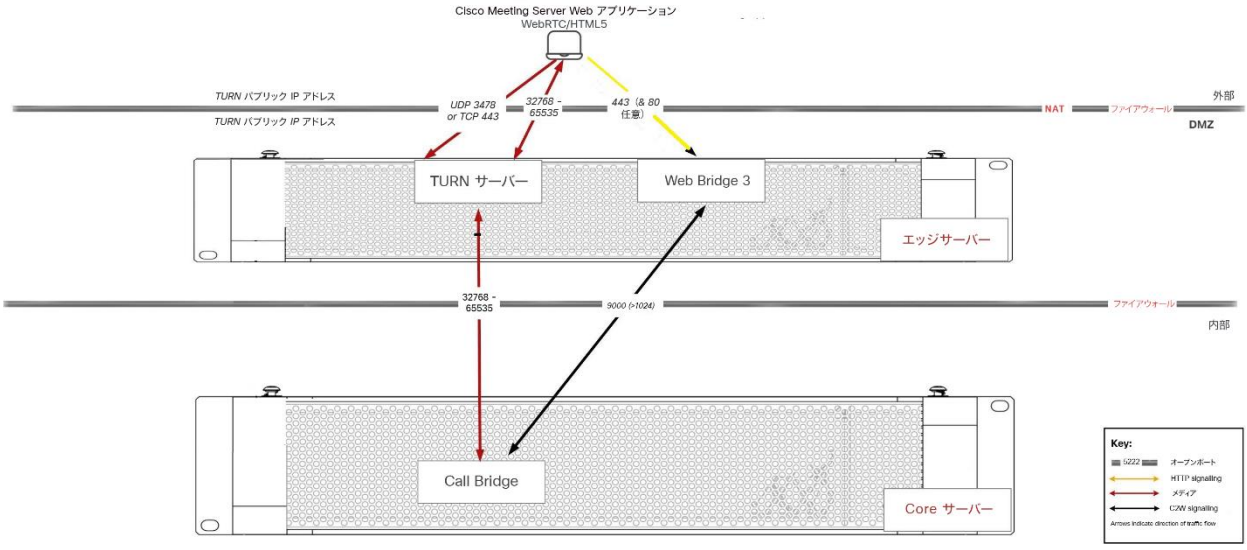


表 7：Web アプリ接続に必要なポート

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	コンポーネントを基準にしたトラフィックの方向	その他の情報
Web Bridge 3	Web アプリケーション	443（注 1）	TCP（HTTPS）	着信	
Web Bridge 3	Web アプリケーション	80	TCP（HTTP）	着信	
Call Bridge	Web Bridge 3				開く接続先ポート：ユーザが設定可能です。トラフィックタイプ：TCP（C2W）方向：発信

注 1：接続先ポートは、Web Bridge 3 の 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、Web アプリと Meeting Server のコンポーネント間のコールフローについて説明します。

1. Web ブラウザで HTTPS 接続が開きます。
2. [ミーティングに参加（Join meeting）]（手順 3 を参照）、または[サインイン（Sign in）]（手順 4 を参照）を求めるプロンプトが表示されます。
3. [ミーティングに参加（Join meeting）]を選択すると、コール ID/URI とパスコードを入力して名前を設定するように求めるプロンプトが表示されます。
    a. コールの詳細は、HTTPS を経由して Web Bridge 3 に送信されます。Web Bridge 3 は、C2W 接続を使用して Call Bridge に照会し、コールの詳細を検証します。
    b. 成功した場合、ユーザはメディアの設定を選択するよう求められます。
    c. メディア設定を選択すると、コールの詳細と必要な名前が HTTPS を経由して Web Bridge 3 に送信され、C2W を使用して Call Bridge に転送されます。Call Bridge はコールアクセストークンを使用して応答し、ブラウザに返されるコールアクセストークンと、ブラウザで使用する TURN サーバーの詳細を示します。
    d. Call Bridge は構成されている TURN サーバーから割り当てを要求します。
    e. Web アプリは、提供された TURN サーバから割り当てを要求します。
    f. ブラウザで Web Bridge 3 への WebSocket 接続を開き、C2W 接続を使って Call Bridge に転送されます。コールアクセストークンは、この Websocket を使用して送信されます。
    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 Websocket を通じて SDP を交換します。

h. ICE 交渉は、すべてのブラウザメディアの 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との間で、この UDP パケットを送信します。ICE 交渉は、TCP メディア リレーアドレス/ポートへの TCP 接続を試行します。

i. ブラウザと Call Bridge 間でメディアを送信するには、直接、TURN UDP リレーを介して、または TURN TCP リレーを介して（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）のうち、成功した最も短いメディアパスが使用されます。

4. [サインイン（Sign in）]を選択すると、ユーザー名とパスワードの入力を求められます。

a. HTTPS を経由して Web Bridge に送信されます。これは、成功した場合にポータルアクセストークンを取得するために Call Bridge に転送されます。

b. ユーザーポータルを入力すると、すべての要求が HTTPS 送信ポータルアクセストークンをヘッダーとして使用します。

c. 参加コール要求が行われた場合、フローはステップ 3c から上述の手順と同じですが、コールの詳細と必要な名前をコールアクセストークンの取得のために送信する代わりに、ブラウザがコール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：コール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、ユーザがユーザポータルにアクセスできるようにします。コールアクセストークンは、コールにユーザが参加している間のみ有効であり、コールに参加するためにのみ使用されます。ポータルアクセストークンを取得するには、ユーザ名とパスワードでサインインする必要があります。コールアクセストークンは、ゲスト参加を実行するか、ポータルアクセストークンとユーザが参加するミーティングの詳細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 ごとに設定するのではなく、共通の場所で Web Bridge の構成オプションを設定できます。すべての Web Bridge または指定された Web Bridge のグループに対して同じ設定を適用できます。

/web BridgeProfiles API オブジェクトには、さまざまな Web Bridge 構成オプションが含まれています。新しく定義した Web Bridge プロファイルは、個別の webBridge オブジェクト、トップレベル（グローバル）プロファイル、テナントのいずれかに割り当てることができます。

Web Bridge 3 の構成の詳細については、『API リファレンスガイド』の Web Bridge と Web Bridge プロファイルメソッドのセクションを参照してください。

10.2.1 Web Bridge プロファイルの作成と適用の方法の例

注：単一の分散型展開では、Web Bridge 3 の構成が Edge サーバーを指している必要があります。

開始する前に、セクション 4.6 に記載されている Web Bridge 3 証明書をインストールし、Web Bridge 3 を構成したことを確認します。次に、次の手順を実行します

1. Meeting Server Web 管理インターフェイスを使用して webBridgeProfile を作成するには、次の手順を実行します。
    a. Meeting Server Web 管理インターフェイスにログインし、[設定（Configuration）] > [API] を選択します。
    b. API オブジェクトのリストから、/api/v1/webBridgeProfile の後ろにある ▶ をタップします
    c. [新規作成（Create new）] をクリックします。
    d. [名前（name）] フィールドに、この Web Bridge プロファイルを呼び出すのに使用する名前を設定します。
    e. Meeting Server でこの Web Bridge プロファイルを使用して Web Bridge で使用するカスタマイズ アーカイブ ファイルがあれば、そのアドレスを [resourceArchive] フィールドに設定します。
    f. [allowPasscodes] フィールドを true または false のいずれかに設定します。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 で、ユーザーがパスコードと数値 ID/URI を組み合わせて coSpace（および coSpace アクセス方式）をルックアップでき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、デフォルトは true になります。
    g. [allowSecrets] フィールドを true または false のいずれかに設定します。このフィールドによって決定されるのは、この Web Bridge プロファイルを使用する Web Bridge で、ユーザが数値 ID とシークレットを使用してミーティング参加リンクから coSpace（および coSpace アクセス方式）にアクセスすることを許可するかどうかです。このパラメータが指定されていない場合、デフォルトは true になります。
    h. [userPortalEnabled] フィールドを true または false のいずれかに設定します。このフィールドによって決定されるのは、この Web Bridge プロファイルを使用する Web Bridge で、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です。このパラメータが指定されていない場合、デフォルトは true になります。

i. [allowUnauthenticatedGuests] フィールドを true または false のいずれかに設定します。true に設定した場合、この Web Bridge プロファイルを使用する Web Bridge で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 に設定した場合、ゲストアクセスは、ユーザーポータルへのログイン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、デフォルトは true になります。

j. [resolveCoSpaceCallIds] フィールドを true または false のいずれかに設定します。このフィールドによって決定されるのは、この Web Bridge プロファイルを使用する Web Bridge で、coSpace ミーティングへのゲストの参加を許可する目的で coSpace と coSpace アクセス方式のコール ID を受け付けるかどうかです。このパラメータが指定されていない場合、デフォルトは true になります。

k. [resolveCoSpaceUris] フィールドを、off、domainSuggestionDisabled、domainSuggestionEnabled のいずれかに設定します。このフィールドによって決定されるのは、この Web Bridge で、coSpace ミーティングへのゲストの参加を許可する目的で coSpace および coSpace アクセス方式の SIP URI を受け付けるかどうかです。off に設定した場合、URI を使用した参加は無効になります。domainSuggestionDisabled に設定した場合、この Web Bridge で URI を使用した参加は有効になりますが、URI のドメインの自動入力または検証は行われません。domainSuggestionEnabled に設定した場合、この Web Bridge で URI を使用した参加が有効になり、URI のドメインの自動入力と検証を使用できます。このパラメータが指定されていない場合、デフォルトは off になります。

l. [作成（Create）] をクリックします。

2. プロファイルを作成すると、アドレスを追加できます。これは、ミーティングの招待の生成に使用される Web Bridge URI と Web アプリケーションの相互起動 URL です。

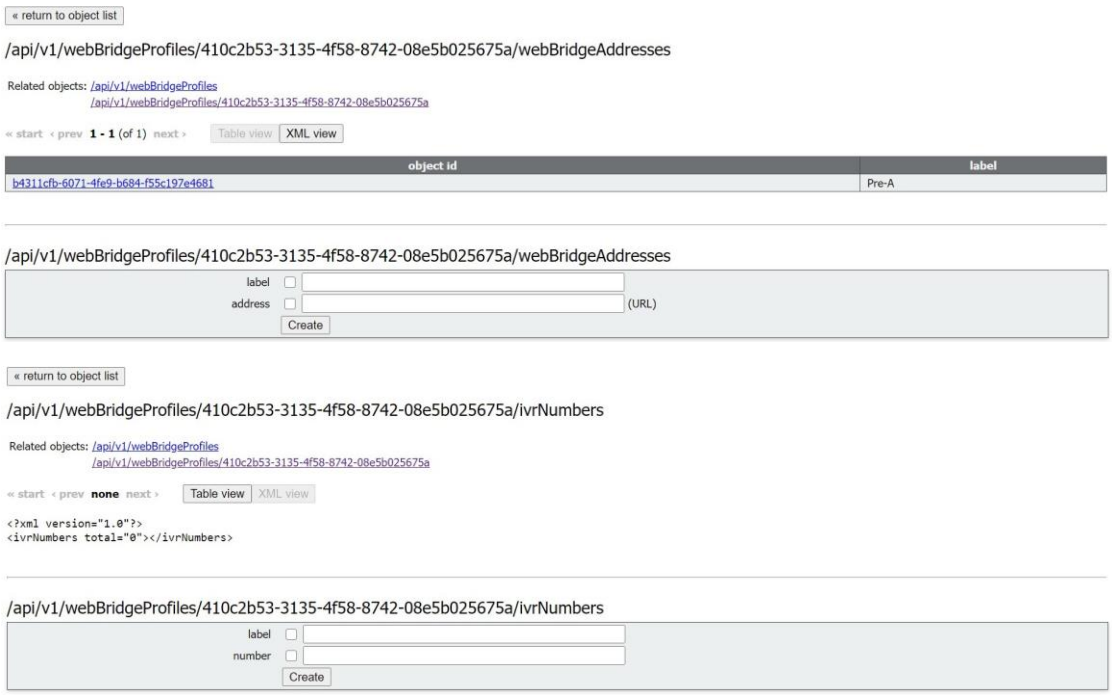
注：バージョン 3.1 以降、複数の IVR 番号と Web Bridge アドレスを指定できます。最大 32 個の IVR 番号と Web Bridge プロファイル 1 件あたり最大 32 個の Web Bridge アドレスを指定できます。これらは、参加情報の表示、および電子メール招待の生成に使用されます。

この例では、Web Bridge URI および IVR の電話番号が web BridgeProfile に対して次のように適用されます。

a. API オブジェクトのリストから、/api/v1/webBridgeProfiles の後ろにある ► をタップします

b. [表示（View）] または [Edit（編集）] をクリックします

c. 結果として表示される「webBridgeProfile オブジェクト セレクタ ウィンドウ」で、手順 1 で作成した webBridgeProfile のオブジェクト ID の [選択（Select）] をクリックして、Web Bridge URI および IVR 番号を割り当てます。Web Bridge のラベルと URL アドレスを入力し、必要に応じて IVR のラベルと番号を入力します。



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 を以下のいずれかまたはすべてに割り当てます。

   - 最上位レベル（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、以下の手順で、更新された webBridgeProfile を最上位レベル（グローバル）プロファイルに割り当てます。

   a. API オブジェクトのリストから、/api/v1/system/profiles の後ろにある ▶ をタップします
   b. [表示（View）] または [Edit（編集）] をクリックします
   c. パラメータを webBridgeProfile まで下にスクロールし、[選択（Choose）] をクリックします。
   d. 結果として表示される「webBridgeProfile オブジェクト セレクタ ウィンドウ」で、最上位レベルのグローバルプロファイルに割り当てる、手順 1 で作成した webBridgeProfile のオブジェクト ID に対して [選択（Select）] をクリックします。
   e. [変更（Modify）] をクリックします。
   f. 新たに割り当てた webBridgeProfile のオブジェクト ID が、[オブジェクト コンフィギュレーション（Object configuration）] の下にリストされます。

注：Web アプリの詳細については、『Cisco Meeting Server Web アプリケーションの重要事項』を参照してください。

11 ミーティングの録画およびストリーミング

3.0 以前は、Meeting Server の内部レコーダコンポーネント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 サーバーが削除されています。バージョン 3.0 では、SIP ベースの新しい内部レコーダーおよびストリーマが導入されています。

新しい内部レコーダとストリーマコンポーネントとサードパーティ製にダイヤルアウトする SIP レコーダはすべて SIP URI を使用して構成されています。録音またはストリーミングが開始される場合は、管理者が構成した SIP URI が呼び出されます。

11.1 新しい内部 SIP レコーダーおよびストリーマ機能の利点

- 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。レコーダーおよびストリーマは他の SIP コールと同様の方法で、つまり callLegProfile 階層または coSpace オブジェクトの defaultLayout パラメータからレイアウトを取得します。また、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、カスタマイズ ライセンスが必要です）。
- callLegProfiles および callLegs の qualityMain パラメータを使用して、最大解像度を callLeg 単位で制御できます。
- 従来の XMPP ストリーマは 720p の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ます。また、3.0 では、MMP コマンド **`streamer sip resolution`** を使用してストリーマの解像度を選択できます。
- callLegProfile の presentationViewingAllowed パラメータ設定を変更することで、ストリーマまたはレコーダーで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 **`recorder limit`** と **`streamer limit`** の導入により、拡張性が向上しました。

11.2 新しい内部 SIP レコーダーおよびストリーマ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、Meeting Server の Call Bridge によって渡される特定の SIP ヘッダーパラメータに依存するため、外部の録音サービスまたはストリーミングサービスとして使用することはできません。Meeting Server の Call Bridge ではない他のソースからのコールが接続されると、想定されている特定の SIP ヘッダーが見つからないため、レコーダーおよびストリーマーはそのコールを拒否します。

レコーダーの実稼働での使用に推奨される展開環境は、少なくとも vCPU コア 4 つと RAM 4GB を搭載した専用 VM で実行することです。次の表に、録音タイプごとのパフォーマンスとリソース使用率を示します。

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 あたりの録音数	録画に必要な RAM	1 時間あたりのディスク予算	最大同時録画数
720p	2	0.5 GB	1GB	40
1080p	1	1GB	2GB	20
音声	16	100 MB	150MB	100

注意すべき重要事項（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）：

- ホストの物理コア数まで vCPU を追加するとパフォーマンスが比例して拡張されます。

ストリーマの実稼働での使用に推奨される展開環境は、少なくとも vCPU コア 4 つと RAM 4GB を搭載した専用 VM で実行することです。次の表に、推奨される 3 つの最小仕様と、その仕様で処理可能なストリーム数を示します。

表 9：内部 SIP ストリーマの推奨仕様

vCPU の数	RAM	720p ストリームの数	1080p ストリームの数	オーディオのみのストリームの数
4	4 GB	50	37	100
4	8GB	100	75	200
8	8GB	200	150	200

注意すべき重要事項（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 数が物理コア数をオーバーサブスクライブすることは避けるべきです。
- サポートされる 720p ストリームの最大数は、vCPU の増設に関係なく 200 です。
- サポートされる 1080p ストリームの最大数は、vCPU の増設に関係なく 150 です。
- サポートされるオーディオ専用ストリームの最大数は、vCPU の増設に関係なく 200 です。

11.3 録画の概要

Meeting Server を使用する場合、ミーティングを録音するには、次の 2 つの方法があります。

- サードパーティ製外部 SIP レコーダー
- Meeting Server 内部の SIP レコーダーコンポーネント

11.3.1 サードパーティ製外部 SIP レコーダーのサポート

Meeting Server で外部のサードパーティ SIP レコーダーの構成が可能になり、録画開始時に、Meeting Server の内部レコーダーコンポーネントを使用するのと同じ方法で、管理者が構成した SIP URI が呼び出されます。

注：外部のサードパーティ SIP レコーダーのサポートについても、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 レコーダー機能には、次の内容が含まれます。

- ビデオとコンテンツの別々のストリームを受信するように BFCP をネゴシエートすることをレコーダーに許可します。これにより、録画のフォーマット方法について、より柔軟なオプションが提供されます。
- 標準 SIP コールの場合と同じ解像度をサポートします。
- 標準 SIP コールと同じ音声コーデックおよびビデオ コーデックをサポートします。
- 既存の Meeting Server 内部レコーダーの場合と同様に、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 レコーダー機能では、TIP またはアクティブコントロールはサポートされません。

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 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、ミーティングの録音と、録音をネットワーク 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、別の Meeting Server から会議をホストしているサーバーに対して有効にする必要があります（図 18 を参照）。展開のテストを目的として、会議をホストしている Call Bridge と同じ Meeting Server 上（ローカル）にレコーダーのみを配置します。

低遅延と高ネットワーク帯域幅を実現するために、可能な場合は、レコーダーをターゲット ファイル システムと同じ物理的な場所に展開することをお勧めします。NFS は安全なネットワーク内にあることが期待されます。

注：録音の保存方法によっては、レコーダー、アップローダ、保管システムが通信できるよう、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。たとえば、ポートマッピング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 と 111 を使用します。

注：レコーダーまたはアップローダのいずれかを使用している場合は、Meeting Server のファイアウォール コンポーネントを使用しないでください。

注：ミーティングの録音の最後に、録音は自動的に MP4 に変換されます。変換されたファイルは、ドキュメントの保管/配布システム内に配置するのに適しています。たとえば、ネットワーク ファイル システム（NFS）内には、これらは、NFS フォルダ spaces/<space ID; tenant spaces are stored in 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録音の展開を示しています。

図 18：録画に許可されている展開：リモートモード

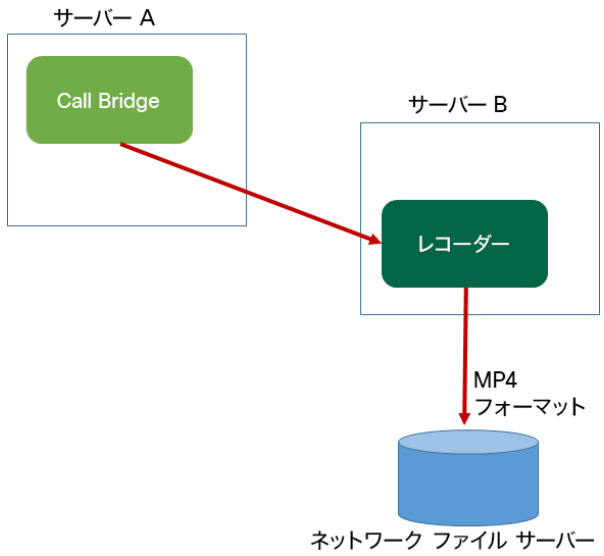
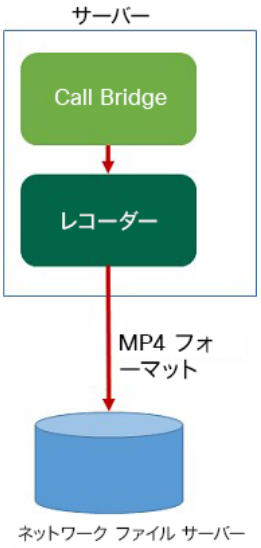


図 19：テストのみを目的として許可されている展開：ローカルモード



11.4 VM サーバー-上に新しい内部 SIP レコーダーコンポーネントを展開する例

注：Windows 2008 R2 SP1 を実行している NFS サーバー上に録画を保存する場合、許可の問題を修正するために必要な windows のホットフィックスプログラム https://support.microsoft.com/en- us/kb/2485529 があります。この修正を適用する前に、Microsoft Windows 管理者にお問い合わせください。

これは 2 段階からなるプロセスです。

- MMP を使用した Meeting Server レコーダーの設定
- API を使用したレコーダー URI の設定

タスク 1：MMP を使用した Meeting Server レコーダーの設定

1. バージョン 3.0 にアップグレードします。
2. SSH を MMP に入力し、ログインしてレコーダーを構成します（MMP コマンド **recorder** と入力して、すべての利用可能なコマンドのリストを表示します）。
3. **recorder nfs <hostname/IP>と入力して、<directory>** NFS の場所を設定します。
4. **recorder resolution <audio|720p|1080p>** と入力し、希望の解像度を設定します（またはコールの音声のみの録音を設定します）。

5. 次を使用して、レコーダーのリスニングインターフェイスと、リッスンする SIP TCP ポートおよび TLS ポートを設定します。MMP コマンド **recorder sip listen <interface> <tcp-port|none> <tls-port|none>**。サービスを無効にするには、該当するポートを **none** 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は、次の値を入力します。**recorder sip listen a none 6000**
   b. デフォルトの TCP/TLS ポート（5060/5061）以外を指定する場合は、後で必要になるため、ポートを書き留めておきます。

   注：デフォルトの SIP TCP/TLS ポート（5060/5061）をリッスンする場合は、Call Bridge が同じインターフェイスをリッスンしないように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。MMP コマンド **callbridge listen none** を入力して該当するインターフェイスを削除することで、Call Bridge を無効にする必要があります。

   ---

6. TLS を設定した場合は、必要に応じて、使用する SIP TLS 証明書を設定します。
   a. MMP コマンド **recorder sip certs <key-file> <crt-file> [<crt- bundle>]** を入力します。

   注：このオプションを使用して SIP TLS 証明書を設定しない場合、SIP TLS サービスは開始されません。

   ---

7. TLS を設定した場合は、必要に応じて、レコーダーでの SIP の TLS 検証を次のように実行できます。
   a. MMP 子マント **tls sip trust [<crt-bundle>]**を入力します。
   b. MMP コマンド **tls sip verify enable** を入力します。

   注：TLS 接続をセキュアにするためには、TLS 検証を有効にすることを推奨します。

   ---

8. 構成が正しいことを確認します。MMP コマンド **recorder** を入力して、構成を表示します。
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 を使用したレコーダー URI の設定

新しい SIP レコーダーが有効になると、API コール プロファイル オブジェクトで指定する **sipRecorderUri** API パラメータを使用して、サードパーティの SIP レコーダーと同様に Call Bridge で構成して使用することができます。

必要に応じて、outboundDialPlan ルールにマップされるカスタム URI を設定することもできます（ドメインは、「recording.com」のように任意に指定できます）。**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 に指示するために、outboundDialPlan ルールを構成する必要があります。これにより、優先度の値、暗号化などを制御できます。outboundDialPlan ルールの構成の詳細については、「ダイヤルプランの構成：概要」の章を参照してください。

注：設定される URI のユーザー部分（@ 記号より前の部分）は特に意味を持ちませんが、新しい内部 SIP レコーダーコンポーネントの場合は必須であるため、「recording@recorder.com」のように任意の値を設定できます。ただし、サードパーティの SIP レコーダーでは、たとえば URI のユーザ部分をユーザのログイン上方として使用する可能性があるため、このことが該当しない場合があります。URI で重要なのはドメインの部分です。

Meeting Server Web 管理インターフェイスを使用して **sipRecorderUri** パラメータを設定するには、次の手順を実行します。

1. Meeting Server Web 管理インターフェイスにログインし、[設定（Configuration）] > [API] を選択します。
2. API オブジェクトのリストから、/api/v1/callProfiles の後ろにある ► をタップします
3. 既存のコール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、[sipRecorderUri] フィールドに希望の URI を入力します。

   注：新しい SIP レコーダーを使用する際は、recording@recorder.com のように 1 つの SIP URI を使用するだけで済みます。異なるプロファイルに異なる SIP URI を使用する必要はありません（使用しても違いはありません）。

   ---

4. 以前に設定していない場合は、[recordingMode]フィールドを（会議の録画方法に応じて）manual または automatic のいずれかに設定します。
5. [変更（Modify）] をクリックします。

必要に応じて、更新された callProfile を、coSpace、テナント、または最上位レベル（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、以下の手順で、更新された callProfile をグローバル レベルに割り当てます。

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

d. 結果として表示される「callProfile オブジェクト セレクタ ウィンドウ」で、最上位レベルのグローバルプロファイルに割り当てる callProfile のオブジェクト ID に対して[選択（Select）]をクリックします。

e. [変更（Modify）] をクリックします。

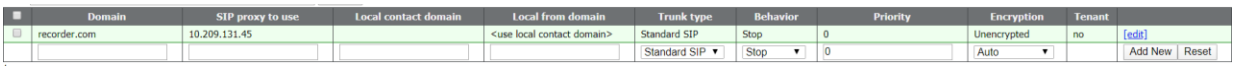
f. 新たに割り当てた callProfile オブジェクトの ID が、[オブジェクトコンフィギュレーション（Object configuration）]の下にリスト表示されます。

11.4.0.1 callProfile の設定例（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）

この例では、前述の手順を使用して recordingMode は automatic に設定され、sipRecorderUri は recording@recorder.com に設定されています。

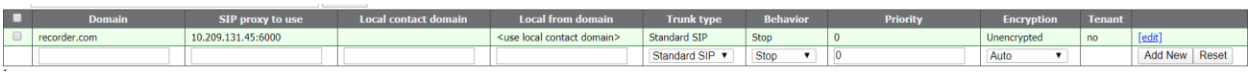
Object configuration	
recordingMode	automatic
sipRecorderUri	recording@recorder.com

Meeting Server Web 管理インターフェイスから [設定（Configuration）] > [発信コール（Outbound calls）] を選択して、一致する発信ダイヤルプランルールを表示します。



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）と異なる SIP TCP/TLS ポートを使用するようにレコーダーを MMP で構成した場合は、次のように、リスニングポートを[sipRecorderUri]フィールドで指定するか、発信ダイヤルプランルールを使用している場合はマッチングする発信ダイヤルプランルールで指定する必要があります。



Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption	Tenant	
recorder.com	10.209.131.45:6000		<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必要があります。たとえば、SIP TLS ポートを使用する場合は、[暗号化（Encryption）]モードを[暗号化（Encrypted）]に設定します。

11.5 外部サードパーティ製 SIP レコーダーの構成

- SIP レコーダーの指定：/callProfile オブジェクトの sipRecorderUri API パラメータを使用します。これを設定した場合、録音が有効化されたときにダイヤルアウト先としてこの URI が使用されます。設定しない場合は、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 管理インターフェイスを使用し、[設定（Configuration）] > [API] を選択します

  b. API オブジェクトのリストから、/callProfiles の後ろにある ▸ をタップします

c. 既存のコールプロファイルのオブジェクト ID をクリックするか、新しいコールプロファイルを作成します。

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> で recordingMode パラメータを使用して、会議を録画できるかどうかを選択します。このオプションは次のとおりです。
  - 自動（automatic）：録画はユーザーの介入なしに行われます。会議の録画が実行できない場合でも会議は発生します。
  - 手動（manual）：ユーザは 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（disabled）：ユーザーは録画できません。
- callLegProfiles の recordingControlAllowed パラメータを設定して、録画の開始および停止の権限を持つユーザを制御します。
- /dtmfProfiles と /dtmfProfiles/ の startRecording パラメータと stopRecording パラメータを使用して、録音を開始および停止する DTMF トーンをマッピングします。<dtmf profile id>

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 録画ステータスの確認

録音のステータスを確認するには、次の情報を参照してください。

- Meeting Server の Web 管理インターフェイスを使用し、[設定（Configuration）] > [API] を選択します
- API オブジェクトのリストから、/callLegs の後にある▶をタップします
- 既存のコールレッグのオブジェクト ID をクリックします。

callLegs/<call leg id> で GET を実行します。ここで示す **status** 出力の **recording** 値は、この callLeg が録画中（**true**）なのか、録画中ではないのか（**false**）かを示します。

11.7 デュアルホーム会議用の録画インジケータ

デュアルホーム会議の場合は、Lync/Skype エンドポイントで Microsoft の録音方法を使用して録音を行う必要があります。デュアルホーム会議の録音に Cisco Meeting Server を使用することは推奨していません。

録画アイコンは、Meeting Server に接続されている SIP 参加者に対して、Lync/Skype エンドポイントが Lync/Skype 側で会議を録画中かどうかを示します。

Meeting Server は、ActiveControl 以外のエンドポイント用に構成されたビデオペインに録画アイコンを追加します。次の 表 10 に、Meeting Server に表示されるアイコンを示します。このアイコンは、デュアルホーム会議が録画されているということを示します。

表 10：録画インジケータ

表示アイコン	説明
	ミーティングは Meeting Server 経由で録画されています。
	ミーティングは、Lync/Skype エンドポイントによって録画されています
	ミーティングは、Meeting Server および Lync/Skype エンドポイントによって録画されています。
	ミーティングは録画されていません（表示アイコンなし）。

注：Web 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、ローカル録画とリモート録画の区別はしません。Meeting Server のアイコンは、Web アプリのビデオペインにはオーバーレイされません。

11.8 Vbrick を使用した録画

注：この セクションは Meeting Server 内部の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を使用すると、Meeting Server に接続されている構成済みの NFS から、ビデオコンテンツマネージャの Vbrick へ Meeting Server の録画をアップロードするワークフローが簡単になります。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構成され有効になると、録音が NFS から Vbrick にプッシュされ、所有者が録音に割り当てられます。Rev ポータルは、管理者によって設定されるセキュリティをビデオ コンテンツに適用し、ユーザがアクセスを許可されているコンテンツにのみアクセスできるようにします。所有者の Rev ポータルで録画が利用可能になると、その所有者に電子メールが送信されます。録音の所有者は、Rev ポータルを通じて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布できます。

注：スペースディレクトリ内でファイルを NFS 共有に追加すると、有効な録音であるのと同じ方法で、そのファイルが Vbrick にアップロードされます。お使いの NFS 共有に許可を適用する場合は、レコーダーだけが書き込みができるよう、注意してください。

注：録音の保存方法によっては、レコーダー、アップローダ、保管システムが通信できるよう、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。たとえば、ポートマッピング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 と 111 を使用します。

注：レコーダーまたはアップローダのいずれかを使用している場合は、Meeting Server のファイアウォール コンポーネントを使用しないでください。

11.8.1 Meeting Server 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、または別のサーバにインストールできます。レコーダーと同じサーバにインストールされている場合は、使用する vCPU を 2 つ追加します。別のサーバで実行する場合は、少なくとも 4 つの物理コアと 4GB の RAM を含む、レコーダー専用 VM の場合と同じサーバ仕様を使用します。

注意：アップローダは、会議をホストする Call Bridge に対して別の Meeting Server 上で実行する必要があります。

NFS 共有に対する読み取りおよび書き込みアクセス。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時に、アップローダが mp4 ファイルの名前を再書き込みするには、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 に継続的にアップロードします。これは、アップローダーがアップロード完了としてファイルをマークできないためです。これを回避するには、NFS が読み取り/書き込みアクセス権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 上のユーザの API アクセスを構成します。

Trust Store は、Vbrick Rev サーバーから取得した証明書チェーン、そして Call Bridge に対して Meeting Server が実行する Web 管理インターフェイスから取得した証明書チェーンを保存します。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人を決定します。アップロードされたビデオ録画へのアクセスは、すべてのユーザー、プライベートユーザー、およびスペースの所有者とメンバーに対してのみ設定できます。

ビデオ録画のデフォルトの状態。アップロード後すぐにビデオ録画を利用できるかどうか（アクティブ）、またはビデオ録画の所有者が録画を公開して録画を利用可能にする必要があるか（非アクティブ）どうかを決定します。

表 11：ポートの要件

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	Call Bridge の Web 管理者	アップローダ設定で指定されている 443 またはポート
アップローダ	Vbrick Rev サーバー	ビデオのアップロードと、Vbrick Rev サーバーへの API アクセスの場合は 443

11.8.2 Vbrick と動作する Meeting Server の構成

これらの手順は、録音を保存するためにすでに NFS をセットアップ済みであることを前提にしています。

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. Vbrick のインストールの場合は、この手順を無視します。Vbrick のインストールを再設定する場合は、最初に Meeting Server へのアクセスを無効にします。
   `uploader disable`
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. 録画に関連付けられているスペースをホストしている Meeting Server の名前など、録画情報についてアップローダがクエリする 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 Web 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、デフォルトはポート 443 です。
   `uploader cms port <port>`
6. Call Bridge を実行している Meeting Server で API アクセスを持つユーザを指定します。パスワードは個別に入力します。
   `uploader cms user <username>`
7. 手順 6 で指定したユーザのパスワードを設定します。タイプ
   `uploader cms password`
   パスワードを入力するよう求められます。
8. Call Bridge を実行している Meeting Server の Web 管理用に、ルート CA の証明書のコピーと、そのチェーン内のすべての中間証明書を保持する証明書バンドル（crt-bundle）を作成します。
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デバイスの Vbrick ホストとポートを構成します。
    `uploader rev host <hostname>`
    `uploader rev port <port>`

注：特に指定されていない場合、ポートのデフォルトは 443 です。

11. ビデオ録音をアップロードする API 権限を持つ Vbrick Rev ユーザを追加します。
    uploader rev user <username>
12. 手順 11 で指定したユーザのパスワードを設定します。タイプ
    uploader rev password
    パスワードを入力するよう求められます。
13. Vbrick Rev サーバー用に、ルート CA の証明書のコピーと、そのチェーン内のすべての中間証明書を保持する証明書バンドル（crt-bundle）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. ビデオ録音へのアクセスを設定します。
    uploader access<Private|Public|AllUsers>
16. スペースのメンバーに録音を表示または編集する機能を与えます。
    uploader cospace_member_access <view|edit|none>

    注：この手順では、リストに登録されているメンバーに、有効な電子メールアドレスが必要です。このアドレスは、Vbrick の口座に関連付けられている必要があります。たとえば、**user1@example.com**

17. スペースの所有者がビデオ録音の単一の所有者かどうかを決定します。
    uploader recording_owned_by_cospace_owner <true|false>

    注：この手順では、ビデオ録画の所有者も有効な電子メールアドレスが必要です。このアドレスは、Vbrick のアカウントに関連付けられている必要があります。

18. スペースの所有者が、Vbrick Rev のリストにない場合は、フォールバック所有者のユーザ名を設定します。フォールバック所有者が指定されていない場合、所有者は MMP で構成されたユーザにデフォルト設定されます。
    uploader fallback_owner <vbrick-user>
19. ビデオ録音に対するコメントを有効にします。
    uploader comments enable
20. ビデオ録音の評価を有効にします。
    uploader ratings enable
21. ビデオ録音のダウンロード許可を設定します。
    uploader downloads enable
22. ビデオ録音のデフォルトの状態を設定します。最初に Vbrick Rev にアップロードした時です。
    uploader initial_state <active|inactive>
23. アップロードの完了後に、ビデオ録音を削除するかどうかの決定します
    uploader delete_after_upload <true|false>
24. アップローダを有効にして Meeting Server にアクセスします
    uploader enable

注：**messageBoardEnabled** を **true** に設定すると、スペースに投稿されたメッセージが表示されます。このメッセージには、録画が可能であることを示します。

11.9 会議のストリーミング

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、スペースに保持されているミーティングをストリーミングする機能を、スペース上に構成された RTMP URL に追加します。

この RTMP URL をリッスンするように外部ストリーミングサーバを構成する必要があります。外部ストリーミング サーバは、ユーザにライブ ストリーミングを提供することも、後で再生するためにライブ ストリームを録画することもできます。

注：ストリーマコンポーネントは RTMP 標準規格をサポートしており、同様に RTMP 標準規格をサポートしているサードパーティ製ストリーミングサーバーで使用できます。Vbrick は、公式にサポートされている外部ストリーミングサーバです。ただし、他のサーバもテスト済みです。

注：ストリーマコンポーネントは RTMP 標準規格をサポートしており、同様に RTMP 標準規格をサポートしているサードパーティ製ストリーミングサーバーで使用できます。Vbrick は、公式にサポートされている外部ストリーミングサーバです。ただし、他のサーバもテスト済みです。

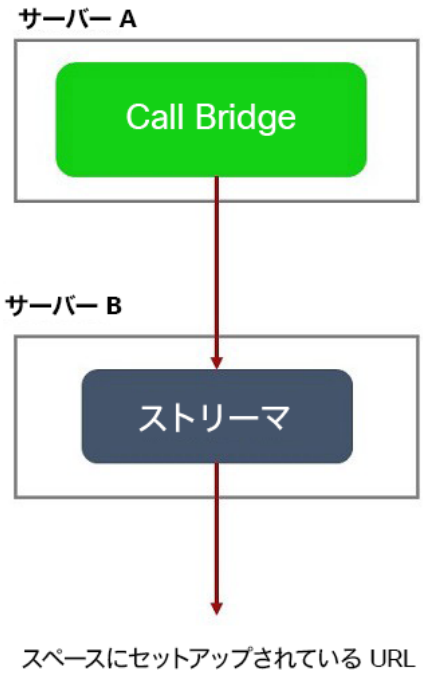
注：ストリーミング先の RTMP URL がファイアウォールの外部側にある場合は、ファイアウォールポートを開く必要があります。

バージョン 3.1 は、内部 SIP ストリームアプリケーションの RTMP サポートを RTMPS に拡張します –TLS 接続を使用した基本的な RTMP です。これまでは、ストリームと RTMP サーバ間のすべてのトラフィックが暗号化されていませんでしたが、3.1 RTMPS がサポートされることで、このトラフィックを暗号化できます。

既存の **tls** MMP コマンドが拡張され、オプションで RTMPS 用 の TLS 信頼 の構成が許可されます。この手順はオプションですが、推奨しています。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の展開を示します。

図 20：ストリーミングに許可されている展開：リモートモード



テストの目的でのみ、ストリーマを Call Bridge と同じサーバー上に同じ場所に接続することができます。これは、1 ~ 2 つの同時ストリーミングをサポートする場合があります。

11.10 VM サーバーでの新しい SIP ストリーマコンポーネントの展開

これは 2 段階からなるプロセスです。

- MMP を使用した Meeting Server ストリーマの設定
- API を使用したストリーマ URI の設定

タスク 1：MMP を使用した Meeting Server ストリーマの設定

1. バージョン 3.0 にアップグレードします。
2. MMP に SSH 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`** を入力すると、使用可能なすべてのコマンドのリストが表示されます）。
3. MMP コマンド **`streamer sip listen<interface> <tcp-port|none>`** を使用して、ストリーマのリスニングインターフェイスと、リッスンする SIP TCP ポートおよび TLS ポートを設定します。**`<tls-port|none>`**を使用して無効にすることができます。サービスを無効にするには、該当するポートを **`none`** に設定します。
   a. たとえば、TLS ポートのみをリッスンし、TCP ポートはリッスンしない場合は、**`streamer sip listen a none 6000`** と入力します。
   b. デフォルトの TCP/TLS ポート（5060/5061）以外を指定する場合は、後で必要になるため、ポートを書き留めておきます。

4. 必要に応じて、MMP コマンド **streamer sip resolution<audio|720p|1080p>** を使用して、ストリーマで使用する最大解像度を設定できます（またはコールの音声のみをストリームするように設定できます）。設定しない場合、デフォルトで 720p になります。
   a. たとえば、1080p に設定する場合は **streamer sip resolution 1080p** と入力します。

   注：1080p を使用する場合は、ビデオの品質を最適化するために、送信 SIP コールの帯域幅を 3,500,000 ビット/秒に増やすことを推奨します。それには、Web 管理 UI で [設定（Configuration）] > [コール設定（Call settings）] > [帯域幅設定（SIP）（Bandwidth settings (SIP)）]を選択し、必要な値に設定します。

5. TLS を設定した場合は、必要に応じて、使用する SIP TLS 証明書を設定します。
   a. MMP コマンド **streamer sip certs <key-file> <crt-file> [<crt-bundle>]** を入力します。

   注：このオプションを使用して SIP TLS 証明書を設定しない場合、SIP TLS サービスは開始されません。

6. オプションで、TLS が構成されている場合は、たとえば次のようにストリーマで SIP（または LDAP または RTMPS）の TLS 検証を実行できます。
   a. MMP 子マント **tls sip trust [<crt-bundle>]** を入力します。
   b. MMP コマンド **tls sip verify enable** を入力します。

   注：TLS 接続をセキュアにするためには、TLS 検証を有効にすることを推奨します。

7. 構成が正しいことを確認します。MMP コマンド **streamer** を入力して、構成を表示します。
8. MMP コマンド **streamer enable** 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 を使用したストリーマ URI の構成

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する API パラメータ **sipStreamerUri** を使用して、Call Bridge で設定して使用することができます。

必要に応じて、outboundDialPlan ルールにマップされるカスタム URI を設定することもできます（ドメインは、「streaming.com」のように任意に指定できます）。**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 に指示するために、outboundDialPlan ルールを設定する 必要があります。これにより、優先度の値、暗号化などを制御できます。**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：構成される URI のユーザ部分（「@」記号より前の部分）は特に意味を持ちませんが、新しい内部 SIP ストリーマコンポーネントの場合は必須であるため、「streaming@streamer.com」のように任意の値を設定できます。URI で重要なのはドメインの部分です。

Meeting Server Web 管理インターフェイスを使用して **sipStreamerUri** パラメータを設定するには、次の手順を実行します。

1. Meeting Server Web 管理インターフェイスにログインし、[設定（Configuration）] > [API] を選択します。
2. API オブジェクトのリストから、/api/v1/callProfiles の後ろにある ► をタップします
3. 既存のコールプロファイルを構成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、[sipStreamerUri]フィールドに希望の URI を入力します。

   注：新しい SIP ストリーマを使用する際は、streaming@streamer.com のように 1 つの SIP URI を使用するだけで済みます。異なるプロファイルに異なる SIP URI を使用する必要はありません。

4. 以前に設定していない場合は、**streamingMode** パラメータドを（ストリーミング方法に応じて）**manual** または **automatic** のいずれかに設定します。
5. [変更（Modify）] をクリックします。

必要に応じて、更新された callProfile を、coSpace、テナント、または最上位レベル（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、以下の手順で、更新された callProfile をグローバル レベルに割り当てます。

1. Web 管理インターフェイスを使用して、[設定（Configuration）] > [API] を選択します。
   a. API オブジェクトのリストから、/api/v1/system/profiles の後ろにある ► をタップします
   b. [表示（View）] または [Edit（編集）] をクリックします
   c. パラメータ callProfile まで下にスクロールし、[選択（Choose）]をクリックします。
   d. 結果として表示される「callProfile オブジェクト セレクタ ウィンドウ」で、最上位レベルのグローバルプロファイルに割り当てる callProfile のオブジェクト ID に対して[選択（Select）]をクリックします。
   e. [変更（Modify）] をクリックします。
   f. 新たに割り当てた callProfile オブジェクトの ID が、[オブジェクトコンフィギュレーション（Object configuration）]の下にリスト表示されます。

ストリーミングを有効にする API 内の coSpace ごとに、coSpace API の [**streamUrl**] フィールドでストリーミング先の RTMPS ストリーム URL を構成する必要があります（例：rtmps://mystream.com/live/app）。これを設定するには、次の手順を実行します。

1. Meeting Server Web 管理インターフェイスにログインし、[設定（Configuration）] > [API] を選択します。
2. API オブジェクトのリストから、/api/v1/coSpaces の後ろにある ► をタップします
3. 既存の coSpace を構成または変更するには、必要な coSpace のオブジェクト ID を選択して、[streamUrl] フィールドにストリーム先の 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

注意：ストリーム URL は SIP ヘッダーを使用して送信されるため、ログイン情報を含む RTMP ストリーム URL はコール制御プロバイダーに公開され記録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 アプリのシングルサインオン（SSO）

この機能により、Web アプリユーザは 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、Web アプリケーションユーザーがサインインごとにパスワードを入力する必要が生じ、アイデンティティ プロバイダーとのセッションを 1 つで行える状態になります（一元的な場所でユーザーを認証し、それぞれのセッションを維持するエンティティ。OAuth、gmail など）。

これにより、Web アプリユーザは同じ Web Bridge 上の異なる SSO プロバイダーでログインできるようになります。

この SSO メカニズムでは、オープン標準であり、広く使用されている業界標準プロトコルである SAML（セキュリティ アサーション マークアップ言語）2.0 を使用します。

注: 現在 Meeting Server は、SAML 2.0 プロトコルで HTTP-POST バインドのみをサポートしています。つまり、メッセージは HTTP-POST の、3 つ以上のメッセージのみを受け入れ、HTTP-POST バインドが利用できないアイデンティティプロバイダーを拒否します。

注：SSO ログインを有効にした場合、LDAP ログインは使用できなくなります。

12.1 Meeting Server Web アプリケーションで使用するための SSO の設定

SSO を使用するには、以下に詳細を示す、アイデンティティ プロバイダーと Meeting Server（SAML 2.0 Exchange のサービスプロバイダと見なされる）のいくつかの構成が必要です。

タスク 1：アイデンティティプロバイダーと Meeting Server ユーザのマッピング

Meeting Server がアイデンティティプロバイダーのユーザを自身のユーザに正しくマップされるようにするには、SSO で認証されるユーザごとに authenticationId を設定する必要があります。これは、標準の ldap 同期プロセスの一部として行なわれます。このフィールドの内容は、アイデンティティプロバイダーから渡されたカスタムパラメータに対して検証され、応答が成功します（タスク 2 を参照）。

ユーザごとに一意の識別子を選択することを推奨しています（たとえば、$sAMAccountName$）。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 ldapSync を変更します。

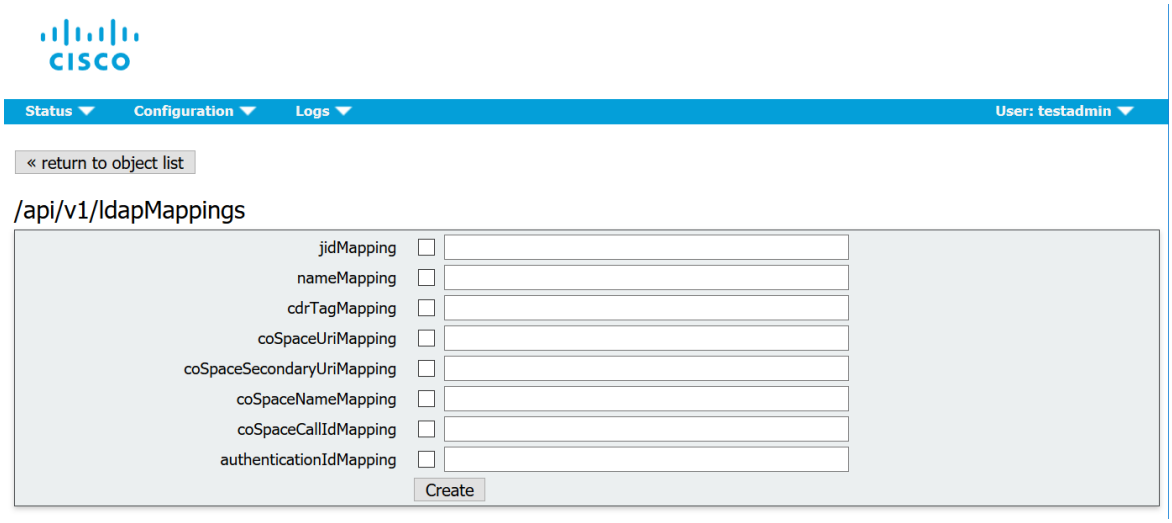
次に、ldapMapping を作成/変更し、authenticationIdMapping パラメータに適切な値（たとえば、$sAMAccountName$）を入力する必要があります。

Meeting Server Web 管理インターフェイスを使用する場合:

a. Meeting Server Web 管理インターフェイスにログインし、[設定（Configuration）] > [API] を選択します。

b. API オブジェクトのリストから、/api/v1/ldapMappings の後ろにある ► をタップします

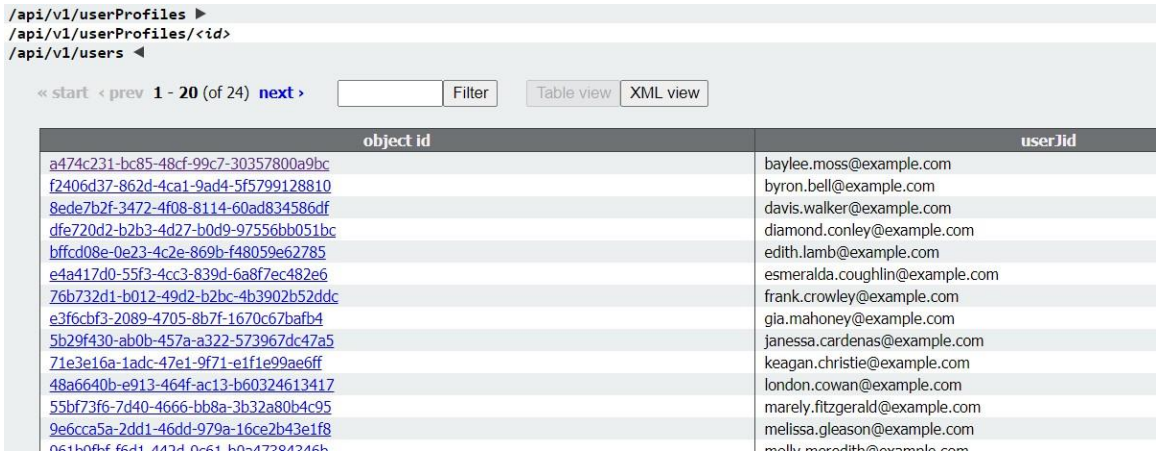
c. [新規作成（Create new）] をクリックするか、変更する既存の LDAP マッピングの ID を選択します。



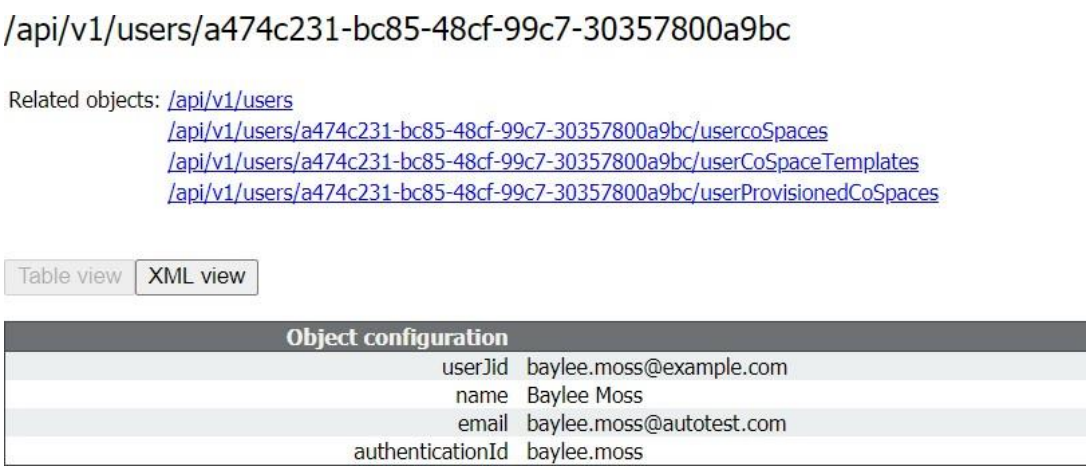
d. authenticationIdMapping パラメータに適切な値（$sAMAccountName$ など）を入力し、必要に応じて[作成（Create）]または[変更（Modify）]をクリックします。

e. ミーティングサーバ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 の後にある ► をタップし、必要に応じてオブジェクト ID または[新規作成（Create new）]を選択します。ldapSync が終了したら、Meeting Server ユーザーの 1 人を調べて、このプロセスが成功したと確認します。

f. まず、API オブジェクトのリストから、 /api/v1/users の後にある ► をタップして、この例に示すユーザーのリストを表示します。



g. authenticationId を設定する必要があるユーザーを 1 人選択します（[フィルタ] フィールドを使用する必要がある場合があります）。この例に示すように、ユーザエントリには ldapSync から正しい値の authenticationId フィールドが含まれる必要があります。



タスク 2：アイデンティティプロバイダーの設定

1. すべてのアイデンティティ プロバイダーは、サービスプロバイダーが登録されている（つまり、この場合の Meeting Server）を表す、メタデータの xml ファイルをアップロードできます。一部のアイデンティティプロバイダーは、最も重要な情報を構成できるようにすることで、プロセスを簡素化します。メタデータ xml ファイルの例はここにあります。

   アイデンティティプロバイダーにアップロードされるメタデータの xml ファイルに含める値は次のとおりです。

   a. entityID：これは Web Bridge の 3 アドレス（つまり、https://<domain>）です。このアドレスは、Web アプリケーション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：展開環境に複数の Web Bridge 3 が導入されている場合は、負荷分散されたアドレスを使用する必要があります。

      ---

   b. 形式「https://<domain>:<port>/api/auth/sso/idpResponse」に従って entityId として定義された Web Bridge アドレスの HTTP-POST AssertionConsumerService。

   c. オンプレミスの場合、HTTPのデフォルトは8090、HTTPSのデフォルトは8181です。アイデンティティ プロバイダーが AuthnRequest 署名を検証する署名用の公開キー。

   d. オンプレミスの場合、HTTPのデフォルトは8090、HTTPSのデフォルトは8181です。アイデンティティプロバイダーが上記のアドレスを介して転送可能な Web Bridge 3 に送り返される情報を暗号化する暗号化用の公開キー。

注：Meeting Server では、メッセージに送信されたメッセージは、応答および/または電子メールレベルのアイデンティティ プロバイダーによって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. アイデンティティプロバイダーから渡されたカスタムパラメータを正常な応答で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（たとえば、$sAMAccountName$）と一致する必要があります。通常、アイデンティティ プロバイダーには、サービスプロバイダー エントリの作成の一部として特別なフォームまたはダイアログが表示されます。このパラメータは、任意の名前を選択できます。ただし、「uid」など、覚えやすいものを選択することをお勧めします（タスク 3 で名前が必要です）。

タスク 3：SSO アーカイブ zip ファイルの作成

1. Meeting Server を構成するには、その Meeting Server 上の Web Bridge 3 用に構成する SSO ごとに、sso_ <name>.zip 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。ファイル名は「sso_」で始まり、その後に意味のある名前を付ける必要があります。

   次のファイルを含む zip アーカイブファイルを作成します。

   a. idp_config.xml：これは、管理者がアイデンティティ プロバイダーから受け取るファイルです。

   b. config.json：次が含まれます。

      - supportedDomains（文字列の配列）：Meeting Server ユーザーがこのアイデンティティ プロバイダーに対して認証を受け取るすべてのドメインの一覧です。つまり、タスク 1 の例を使用すると、supportedDomains には「example.com」の単一のエントリが含まれます。
      - authenticationIdMapping（文字列）– Meeting Server の authenticationIds と一致するタスク 2（つまり、「uid」など）の一部として構成されたアイデンティティ プロバイダー応答からのパラメータ名。SSO 用の Web アプリユーザには、authenticationIds がセットアップされている必要があります（タスク 1 を参照）。
      - ssoServicePro providererAddress（文字列）：アイデンティティ プロバイダーが応答を送信するアドレス。これはタスク 2 の entityID で指定されている Web Bridge 3 と一致します。

   c. 省略可。sso_sign.key：アイデンティティプロバイダ側で設定された公開署名キーの秘密キー。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 プロバイダー側の公開キーを使用して検証できます。

   d. オプション。 sso_encrypt.key：アイデンティティ プロバイダー側で設定された公開暗号キーの秘密キー。これは、アイデンティティプロバイダー側の公開キーで暗号化された Meeting Server メッセージの復号化に使用されます。

注：アイデンティティプロバイダー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は、SSO ファイルを含むフォルダを圧縮して使用することはできません。これを行うと、フォルダの追加レイヤーが作成されます（zipファイル > フォルダー >SSOファイル）。代わりに、SSO ファイルを強調表示して右クリックして圧縮します（または、zip アプリケーションを開いてまとめて圧縮します）。これにより、フォルダの追加レイヤーを作成せずに、SSO ファイルを含む zip ファイルが作成されます（たとえば、zipファイル> SSOファイル）。

タスク 4：SSO アーカイブ zip のアップロード

SSO アーカイブ zip をアップロードし、ローカルの Web Bridge 3 でホストする必要があります。

注: 次の手順のコマンドは、コンソール/端末環境 (コマンドプロンプトまたは端末) 用であり、WinSCP などの SFTP クライアントには対応していません。

1. この zip アーカイブをローカルにホストする予定の Web Bridge 3 を有効化した Meeting Server ごとに、次の手順を実行します。
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 の admin ユーザのログイン情報を使用してログインします。
   c. zip ファイル **sso_<name>.zip** をアップロードします。例：
      PUT sso_.zip<name>
   d. SSH クライアントを MMP の IP アドレスに接続します。
   e. MMP の admin ユーザのログイン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、再起動後にピックアップされます。

注：Web アプリユーザがログインすると、Web アプリ アプリケーション上で、アイデンティティプロバイダーを持つユーザとは別のセッションが行われます。これは、同じユーザ名を入力した後に 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、アイデンティティプロバイダーからサインアウトした場合、Web アプリアプリケーションからサインアウトされません。Web アプリアプリケーションから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に再度ログインできないようにするには、Web アプリケーションと 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

次は 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ーのメタデータファイル

これはシンプルなサービスプロバイダーのサンプルです。管理者は関連値を設定し、<domain> と <port> を変更する必要がある点に注意してください。

```
<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 包括的なサービスプロバイダーのメタデータファイル

これは、署名キーと暗号キー用の xml を含む、包括的なデータファイルの例です。

注：キーは、使用パラメータ（「encryption」または「signing」）に従って、対応する KeyDescriptor 要素の X509 証明書のサブ要素に配置する必要があります。キーのテキストコンテンツを「...」に置き換える必要があります（例：ds:X509CertificateMIID**<omitted_key_text>**+gb</ds:X509Certificate>）。

注：署名証明書を含める場合、値 AuthnRequestsSigned は「true」に設定されます（例 2 のより単純なメタデータファイルでは「false」に設定されます）。

```
<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>
```

13 ActiveControl のサポート

Meeting Server は、ホストされたコールに対して 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している参加者に対して、ActiveControl では、ミーティングの参加者がミーティングの詳細を受信し、エンドポイント インターフェイスを使用してミーティング中にいくつかの管理タスクを実行できます。

13.1 Meeting Server 上の ActiveControl

Meeting Server は、ActiveControl が有効なエンドポイントに次のミーティング情報を送信サポートしています。

- 参加者リスト（名簿リストとも呼ばれます）。コールに参加している他の参加者の名前と参加者の総数を確認できるようになります。
- 現在話している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している参加者を示すインジケータ。
- ミーティングが録画またはストリーミングされているかどうかを示すインジケータ、および通話中にセキュアでないエンドポイントがあ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画面メッセージ

また、ActiveControl が有効なエンドポイントで以下の管理タスクをサポートします。

- エンドポイントに使用するレイアウトを選択します。
- ミーティングの他の参加者の接続を解除します。

13.2 制限事項

- ActiveControl が有効になったコールが、Unified CM バージョンが 9.1（2）未満の Unified CM トランクを通過した場合、コールが失敗する可能性があります。古い Unified CM トランク（Unified CM 8.x 以前）で ActiveControl を有効にすべきではありません。
- 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 iX プロトコルを使用します。このプロトコルは、SIP Session Description Protocol（SDP）でアプリケーション回線としてアドバタイズされます。Meeting Server は ActiveControl を自動的にサポートしますが、この機能は無効にすることができます。セクション 13.4 を参照してください。遠端ネットワークが不明な場合、または iX プロトコルをサポートしていないことが明らかになっているデバイスの場合は、Meeting Server と他の通話制御デバイスまたはビデオ会議デバイスの間の SIP トランクで iX を無効にすることが最も安全な場合があります。例えば、次のような場合です。

- Unified CM 8.x 以前のシステムへの接続の場合、古い Unified CM システムは ActiveControl 対応デバイスからのコールを拒否します。これらのコールの失敗を回避するために、ネットワーク内の Unified CM 8.x デバイス宛てのトランクでは iX を無効にしてください。SIP プロキシ経由で 8.x デバイスに到達する場合は、そのプロキシのトランク上で iX が無効にされていることを確認します。
- サードパーティ製ネットワークへの接続の場合。このような場合、ActiveControl 対応のデバイスからのコールをサードパーティ製ネットワークが処理する方法を知る方法はありません。処理メカニズムが拒否する場合があります。このようなコールの失敗を回避するために、サードパーティ製ネットワークへのすべてのトランクで iX を無効にしたままにしてください。
- Cisco VCS を中心とした展開で、外部ネットワークに接続するか、古い Unified CM バージョンに内部で接続する場合。Cisco VCS X8.1 以降、ゾーンフィルタをオンにして、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 を無効にできます。（デフォルトでは、フィルタはオフになっています。）

13.4 SIP コール内での UDT の無効化

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

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

1. API オブジェクトのリストから、/compatibilityProfiles の後ろにある ► をタップします
2. 既存の互換性プロファイルのオブジェクト ID をクリックするか、新しい互換性プロファイルを作成します

3. パラメータ sip-UDT = false に設定します。[変更（Modify）] をクリックします。
4. API オブジェクトのリストから、/system/profiles の後ろにある ▶ 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. パラメータ compatiilityProfile の右側にある [選択（Choose）] をクリックします。上記の手順 3 で作成した compatibilityProfile 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 での iX サポートの有効化

一部の SIP プロファイルでは、Cisco Unified Communications Manager で iX プロトコルのサポートが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 プロファイルでサポートを構成してから、その SIP プロファイルを SIP トランクに適用する必要があります。

SIP プロファイルでの iX サポートの構成

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（Find and List SIP Profiles）] 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（Add New）] 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 プロファイルの設定（SIP Profile Configuration）] 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）] チェックボックスをオンにします
4. 追加の設定変更を加えます。
5. [保存（Save）] 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（Device）] > [トランク（Trunk）] を選択します。

   [トランクを検索して一覧表示（Find and List Trunks）] 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（Add New）] 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（Find）] 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。

   [トランクの設定（Trunk Configuration）] ウィンドウが表示されます。

3. [SIP プロファイル（SIP Profile）] 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（Save）] 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 での iX のフィルタリング

プロトコルをサポートしないネイバーゾーンの iX アプリケーション回線をフィルタ処理するように Cisco VCS を構成するには、SIP UDP/IX フィルタモードの詳細設定オプションが [オン（On）] に設定されているカスタムゾーンプロファイルでゾーンを構成する必要があります。

詳細ゾーンプロファイルのオプション設定を更新するには、次の手順を実行します。

1. 新しいネイバーゾーンを作成するか、既存のゾーンを選択します（[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）]）を選択します。
2. まだ選択されていない場合、[詳細パラメータ（Advanced parameters）] セクションの [ゾーンプロファイル（Zone profile）] で、*[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）] ドロップダウンリストから、[オン（On）] を 選択します。
4. [保存（Save）] 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 ヘッダーを含むコールのコール処理概要

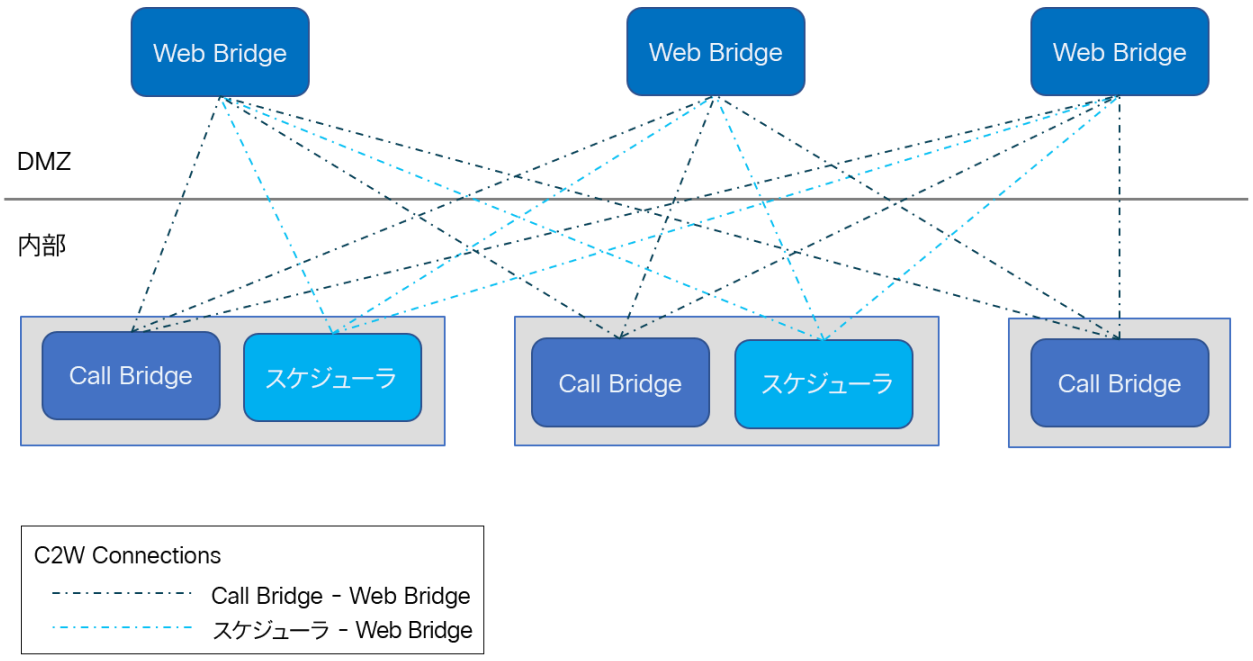
シナリオ	結果
Unified CM 8.x 以前	コールが失敗します
9.1(2) 以前の Unified CM 9.x	コールは通常処理されますが、ActiveControl は処理されません
Unified CM 9.1(2)	コールと ActiveControl は通常処理されます
エンドポイント：iX および SDP 実装はサポートされていません	エンドポイントが再起動、またはコールが失敗する可能性があります

14 スケジューラ：展開

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展開されます。スケジューラが有効になっている場合は、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。したがって、スケジューラは、Call Bridge もホストしている Meeting Server に展開する必要があります。リモート Call Bridge を使用するようにスケジューラを設定することはできません。

設定された 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。永続的な 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 に確立されます。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。これは、ループバック インターフェイスを介して自動的に行われるためです。同様に、C2W 接続はすべて自動ですが、スケジューラと Web Bridge の間に信頼バンドルを構成する必要があります。

注：スケジューラは、クラスタ内のすべての Web Bridge への C2W 接続を確立できる必要があります。



すべての Call Bridge と一緒にスケジューラを展開する必要はありません。Meeting Server 1000 および VM 展開上の Meeting Server のスケジューラは 150,000 の会議をサポートし、Meeting Server 2000 のスケジューラは 200,000 の会議をサポートします。2 つまたは 3 つのスケジューラを追加して、復元力を提供できます。スケジュールされた会議データは Meeting Server データベースに保存され、クラスタ化されたデータベースとシングル ボックス データベースの両方の展開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「スケジューラ」としてログに記録する場合があります。これはログ記録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、API コマンドを発行する信頼できるソースとして自動的に使用されます。

14.1 スケジューラの導入

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。これは、ループバック インターフェイスを介して自動的に行われます。同様に、C2W 接続はすべて自動ですが、スケジューラと Web Bridge 間でトラスト バンドルを構成する必要があります。

1. C2W 信頼を構成する

   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。スケジューラには、この接続に使用するクライアント証明書とキーの構成が必要です。これを行うには、証明書を作成し、それを 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。

   証明書を使用するようにスケジューラを構成する

   scheduler c2w certs <key-file> <crt-fullchain-file>
   例：

   scheduler c2w certs scheduler_c2w.key scheduler.cer
   スケジューラは、接続先の各 Web Bridge を信頼できる必要があります。SFTP 経由で、各 Web Bridge 証明書を含むトラスト バンドルをアップロードします。

   コマンドを使用してスケジューラを設定する

   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。したがって、次のコマンドを使用して構成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> に含まれています。

2. （オプション）スケジューラの HTTPS インターフェースを構成する。

   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会議を構成するために使用できます。ただし、Web Bridge は、管理 API を使用してスケジューラと通信しません。HTTPS サーバーを有効にすること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機能を提供するため、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 サーバーがリッスンするインターフェイスを構成します。

scheduler https listen <interface> <port>

例：

scheduler https listen a 8443

次のコマンドを使用して、サーバーの証明書キーペアを構成します。
scheduler https certs <key-file> <crt-fullchain-file>
例：
scheduler https certs scheduler_https.key scheduler_https.cer

3. （オプション）電子メール サーバ を設定する。

   電子メール サーバーの構成と電子メール構成のタイプの詳細については、『設置ガイド』を参照してください。

   サーバー アドレスとポートの構成、電子メール プロトコルの有効化、および認証用のユーザー名の構成は、次のスケジューラ MMP コマンドを介して指定されます。

   ```
   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、電子メールはスケジューラで設定されません。スケジューラが電子メール招待を送信するには、少なくとも 1 つの電子メール サーバーを設定する必要があります。電子メールは、会議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。電子メール サーバーがダウンすると、別のスケジューラが電子メールを送信します。

4. 電子メール サーバーを構成した後、次のコマンドを使用し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、サービスの構成とステータスをチェックします。

   scheduler status

   正常に動作した構成のサンプル出力：

```
cms> scheduler status
Status: enabled
Running
Database responsive at start
HTTPS configured
C2W configured
Email server configured

```

```
Scheduler application status:
{
    "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 追加のセキュリティに関する検討事項および QoS

この章では、X.509 証明書および公開キーを介して提供される認証に加えて、Meeting Server で使用可能な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

共通アクセスカード（CAC）は、コンピュータ機能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 には秘密キーが含まれており、この秘密キーは抽出できませんが、カード所有者のアイデンティティを証明するためにオンカードの暗号化ハードウェアで使用できます。

Meeting Server は、CAC を使用した SSH および Web 管理インターフェイスへの管理者ログインをサポートしています。次の表 13 の MMP コマンドを使用して、展開用に CAC を構成します。

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]	CAC モードを有効または無効にします。オプションで、すべてのパスワード ベースのログインを排除するストリクト モードを指定します。
cac issuer <ca cert-bundle>	信頼できる証明書バンドルを指定して、CAC 証明書を確認します。
cac ocsp certs <keyfile> <certificatefile>	OCSP サーバーを使用している場合に、OCSP サーバーとの TLS 通信用の証明書と秘密キーを指定します。
cac ocsp responder <URL>	OCSP サーバーの URL を指定します。
cac ocsp enable|disable	CAC OCSP の検証を有効または無効にします。

15.2 オンライン証明書ステータスプロトコル（OCSP）

OCSP は、証明書の有効性と失効ステータスを確認するためのメカニズムです。MMP は OCSP を使用して、ログインに使用する CAC が有効であるかどうか、特に失効していないかどうかを調べます。

15.3 FIPS

FIPS 140-2 レベル 1 認定ソフトウェア暗号化モジュールを有効にできます。有効にすると、暗号操作はこのモジュールを使用して行われ、暗号操作は FIPS 承認取得済み暗号化アルゴリズムに制限されます。

表 14：FIPS を構成する 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操作に対して FIPS-140-2 モード暗号化を有効または無効にします。FIPS モードを有効または無効にした後は、リブートが必要です。
fips	FIPS モードが有効になっているかどうかを表示します。
fips test	組み込み FIPS テストを実行します。

15.4 TLS 証明書の検証

リモートの証明書が信頼されていることを検証するために、SIP および LDAP の相互認証を有効にできます。有効にすると、Call Bridge は（どちら側が接続を開始したかに関係なく）常にリモートの証明書を要求し、サーバでアップロードおよび定義された信頼ストアに対して提示された証明書を比較します。

表 15：TLS を構成する MMP コマンド

MMP コマンド	説明
tls <sip|ldap> trust <crt bundle>	信用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または無効にするか、または OCSP が検証に使用されるかどうかを指定します。
tls <sip|ldap>	現在の設定を表示します。

15.5 ユーザ制御

MMP 管理者ユーザは次の操作を実行できます。

- その他の管理者ユーザのパスワードをリセットします。
- ユーザーパスワードで繰り返すことができる文字の最大数を設定する。ユーザーパスワードルールの追加機能はほかにも多数あります。
- IP アドレスで MMP アクセスを制限します。
- 設定可能なアイドル期間後に MMP アカウントを無効にします。

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者インターフェイスの両方に対してシンプル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 ソリューションに代わるものではありません。その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、インターフェイスごとにそれぞれ指定する必要があります。インターフェイスでファイアウォールルールを設定した後は、そのインターフェイスでファイアウォールを有効にしてください。詳細および例については、『MMP コマンド リファレンス』を参照してください。

注意：ファイアウォールを設定するときはシリアルコンソールを使用することを推奨します。SSH を使用すると、ルール内のエラーによって SSH ポートにアクセスできなくなることがあります。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、ADMIN インターフェイスに対して **`ssh rule`** が作成されていることを確認します。

15.7 DSCP

Meeting Server 上のさまざまなトラフィックタイプの DSCP タグを有効にできます（『MMP コマンドリファレンス』を参照）。

1. MMP にサインインします。
2. **`dscp (4|6) <traffic type> (<DSCP value>|none)`** を使用して、必要に応じて DSCP 値を設定します。たとえば、**`dscp 4 oa&m 0x22`** は IPv4 の操作、管理、取り扱いを設定します。
3. また、**`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保証されていない DSCP 値の使用を強制します。例：**`dscp assured true`**

注：DSCP タグは、Meeting Server から送信される全パケットに対するタグ付けのみです。PC Client の DSCP タギングでは、希望する DSCP 値を定義するためにグループポリシーを使用する必要があります。これを制御するのは Windows であり、通常のユーザーアカウントには DSCP を設定するアクセス許可がありません。

15.8 SSH フィンガープリントの検証

SSH または SFTP 経由で Meeting Server に初めて接続する管理者は、ログインする前に Meeting Server にインストールされているキーのフィンガープリントを取得することにより、Meeting Server によって表示されるキーを確認できます。

表 16：キーを取得する MMP コマンド

MMP **コマンド**	**説明**
ssh server_key list	出力には、次のキーの中で、Meeting Server ホストのすべての既存のキーのサイズ、タイプ、およびフィンガープリントとともにキーのリストが表示されます。 - 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 Cisco サポートが問題をトラブルシューティングするのに役立つ診断ツール

Syslog レコード（セクション 3.1.4 を参照）を使用して展開の問題を診断するほかに、Meeting Server で次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フレームの生成
- 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 管理インターフェイスの [ログ（Logs）] > [詳細トレース（Detailed tracing）] ページを使用して、追加の SIP トレースを有効にできます。これらのログは、SIP エンドポイントのコールセットアップ障害問題の調査に役立てることができます。ただしそれ以外の場合は無効にしておいてください。必要以上に長い冗長ロギングを避けるために、自動シャットオフ時間として 1 分後、10 分後、30 分後、24 時間後を選択できます。トラブルシューティングの詳細については、Cisco の Web サイトの Meeting Server サポートの FAQ を参照してください。

ログイン試行に失敗した場合の診断には、次の情報が含まれます。

- ログインに関連したイベントログメッセージに含まれる遠端の IP アドレス
- ログインに失敗した場合に生成される監査メッセージ（ユーザ名を除く）とログイン セッション タイムアウト。これらは、正常なログインにも生成されます。

16.2 ログバンドル

Meeting Server では、Meeting Server 内のさまざまなコンポーネントの設定と状態を含むログバンドルを生成できます。このログバンドルには、syslog ファイルと live.json ファイルが含まれます。問題についてCisco サポートに連絡する必要がある場合、これらのファイルは、分析を迅速化するのに役立ちます。

Meeting Server ログバンドルは、次の方法で生成されます。

- Meeting Server 管理者は、MMP 管理者ユーザのログイン情報を使用して SFTP クライアントを MMP IP アドレスに接続することにより、ログバンドルの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 というファイル名のログバンドルを生成してダウンロードします。

- または、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 というファイル名のログバンドルが生成されます。

コマンド/例	説明/注意事項
generate_logbundle	それぞれの会議サーバーで 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、以前に生成されたログバンドルが最新のログバンドルに置き換えられます。

以下の手順を使用して、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 の admin ユーザのログイン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必要がある場所で、次のいずれか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. ファイルの名前を変更します。ファイル名の logbundle の部分を、ファイルを作成したサーバーを特定する名前に変更します。これは、複数サーバーの展開で重要です。
6. 分析のため、変更された名前のファイルをCisco サポートの連絡先に送信します。

log bundle.tar.gz の最初のファイルサイズは 1 Kb です。SFTP 経由で転送した後は、ファイル数とそのサイズに応じてサイズが増加します。

注：コンピュータと Meeting Server 間のネットワーク接続が遅いことが原因でログバンドルをダウンロードできない場合は、ログと live.json ファイルをダウンロードして、シスコサポートに送信できます。

16.3 特定のコールレッグ用のキーフレームを生成する機能

generateKeyframe オブジェクトが /callLegs/<call leg id> に追加されました。これはデバッグ機能付きであり、問題の診断時にCisco サポートからこの機能の使用を求める場合があります。

Web 管理インターフェイスを使用して、[設定（Configuration）] > [API] を選択し、次の手順を実行します。

1. API オブジェクトのリストから、/callLegs の後にある▶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. ページの上部にある関連オブジェクトのリストで、/callLegs/<call leg 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に対する発信ビデオストリーム内の新しいフレームの生成がトリガーされます。

16.4 syslog に登録済みのメディアモジュールのレポート

syslog は 15 分ごとにメッセージを出力し、すべてのメディアモジュールが健在かどうかをモニタリングできます。

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 ライセンスに関する追加情報

ライセンスの目的での Meeting Server 3.0 以降では、Meeting Management が必須です。スマート ライセンス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）のサポートを廃止し、ライセンス予約を導入しました。

注：セキュリティ上の理由により 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、代替のライセンスオプションについてCisco アカウントチームにお問い合わせください。

17.1 ライセンス

この章では、次の情報を見つけることができます。

- Meeting Server のスマートライセンスの仕組み
- ライセンス機能の有効期限切れによる強制アクション
- ライセンス情報の取得方法（スマートライセンス）
- スマートライセンス登録プロセス
- ユーザーに対する Personal Multiparty ライセンスの割り当て
- Cisco Multiparty ライセンスの割り当て方法
- Cisco Multiparty ライセンスの使用状況の判断
- SMP Plus ライセンスの使用率の計算
- Meeting Server からのライセンス使用状況スナップショットの取得
- ライセンスレポート

17.1.1 Meeting Server のスマートライセンスの仕組み：概要

Meeting Server 3.0 以降でライセンスが機能するためには Meeting Management が必須です。スマートを使用した新規ライセンス、または既存ユーザーの場合はインストール済みライセンスファイルをサポートするために、Meeting Server と Meeting Management の間の新しい信頼とやり取りが導入されています。Meeting Management が Meeting Server にライセンスを付与できるようにする仕組みが、この信頼リンクです。

注：スマートライセンスの管理に Cisco Meeting Management 使用する方法の詳細については、『Meeting Management 3.0 管理者ガイド』を参照してください。

スマート ライセンスを実装するための概要レベルのワークフローを以下に示します。

1. Meeting Management をスマート ライセンス バーチャル アカウントに登録します。
2. Meeting Server の初回起動時には、ライセンス ステータス値は定義されていない状態です。

   注：ライセンスがなくても 90 日間はフル機能をトライアルモードで使用できます。

3. スマートライセンス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 Meeting Server が初めて接続すると、その Meeting Server に以前にライセンスが適用されていたかどうかがチェックされます。適用されていなかった場合は、ライセンス有効期限が 90 日後に設定されます。

   付録 B.5 に示されているように、ライセンスの有効期限は Meeting Management に表示され、clusterLicensing API でも返されます。

   注：機能ライセンスはいずれも有効期限が最大で 90 日後までとなります。

4. Meeting Management は、Meeting Server の遵守状態を確保するのに必要なライセンスがあることをチェックするために、毎日、クラスタの Meeting Server ライセンス使用状況を照合し、スマートアカウントに対してレポートします。スマート アカウントは Meeting Management に応答し、Meeting Server が遵守状態であるかどうかを提示します。その後、Meeting Management は、次のようにして有効期限を適切に設定します。

   a. Meeting Management が、ライセンスが存在しており特定の機能の使用権があることを特定すると、有効期限が 90 日後に延長されます。

      注：Meeting Server が Meeting Management に接続して 90 日間の使用状況データを送信しなかった場合、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アクションの詳細については、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使用権を超えている場合、またはライセンスが見つからない場合は、次の強制措置が発生します。

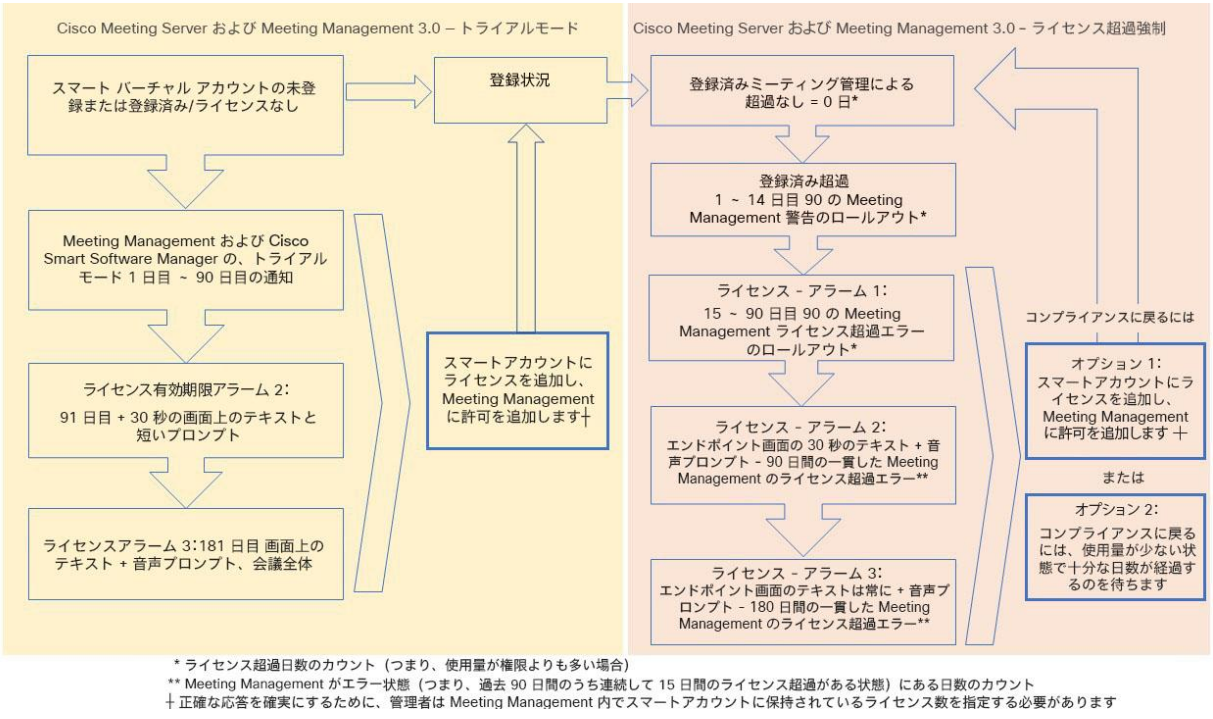
   b. 遵守状態でなかったのが過去 90 日間のうち 15 日未満であることを Meeting Management が特定した場合、これを許容して Meeting Server の有効期限をその時点から 90 日後に再設定します。管理者に、ライセンス不足を通知するビジュアル警告が表示されます。

   c. 遵守状態でなかったのが過去 90 日間のうち 15 日を超えていることを Meeting Management が特定した場合、第 1 レベルの強制（アラーム 1）、つまり、Meeting Management インターフェイスに非遵守の通知が表示されます。

d. 超過使用が続く場合、Meeting Management は 90 日間の計算をリセットせず、新規ライセンスの追加期限までの日数がカウントダウンされます。ライセンスが追加されない場合、図 21 に示すように、会議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 に、左側に示したトライアルモードでの初回起動から、右側に示した超過使用による強制までの、強制フローを示します。

図 21：Cisco Meeting Server と Cisco Meeting Management スマート ライセンスの強制フロー



17.1.2 ライセンス機能の有効期限切れによる強制アクション

従来は、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 以降では、機能にライセンスが付与されているかどうかの現在のステータスは動的に変化する可能性があります。たとえば、機能ライセンスの有効期限が切れた（従来はこれは再起動されるまで明らかになりませんでした）、API の変更があったなどの理由によるものです。Meeting Management は、スマートライセンスを使用して強制アクションを計算します。

注：スマートライセンスポータルを使用して、「ライセンス不足」の電子メール通知を有効にすることができます。

機能ライセンスが期限切れになると、表 17 に示したアクションが発生します。

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	期限切れの場合：すべての参加者およびすべてのミーティングに対し、ミーティング参加時にビジュアルなテキスト 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） 90 日以上前に期限切れとなりライセンスが存在しない場合：それ以前と同様ですが、メッセージは永続的に表示されます。「Your deployment is out of licensing compliance, please contact your administrator（ライセンスが遵守されていません。管理者に連絡してください）」という音声プロンプトが再生されます。（アラームレベル 3）。ただし、暗号化された呼び出しは、ライセンスのない状態では処理されません。 注：前述のアクションを回避するために必要なのは callBridge または callBridgeNoEncryption のみです。
callBridgeNoEncryption	
PMP/SMP	
customizations	期限切れであるか、ライセンスが存在しない場合、カスタマイズ機能は会議中にアクティブになりません。
recording	期限切れまたはライセンスが存在しない場合、（サードパーティのレコーダーであるかどうかにかかわらず）新規の録画を開始できなくなります。 このライセンスは録画とストリーミングに該当するため、ストリーミングにも同じ制限が適用されます。

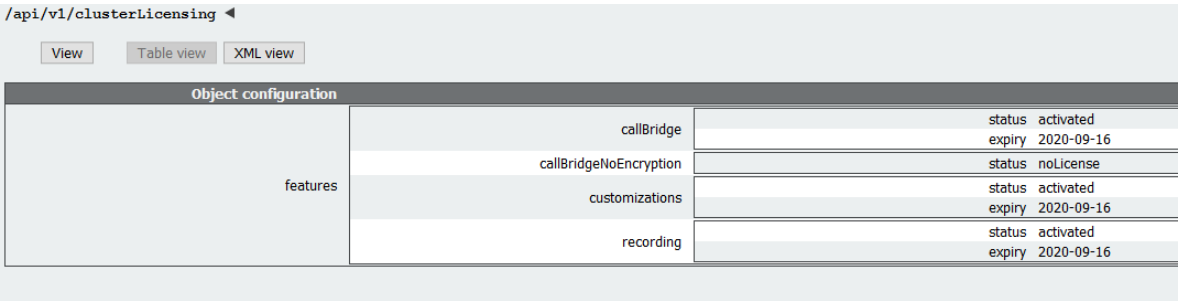
アラーム 2 と 3 をオフにするには、単純にライセンスをスマート アカウントに追加します。

17.1.3 ライセンス情報の取得方法（スマートライセンス）

Meeting Server Web 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、次の手順を実行します。

1. Meeting Server Web 管理インターフェイスにログインし、[設定（Configuration）] > [API] を選択します。
2. API オブジェクトのリストから、/api/v1/clusterLicensing の後ろにある ▶ をタップします
3. クラスタの現在のライセンス ステータスが、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



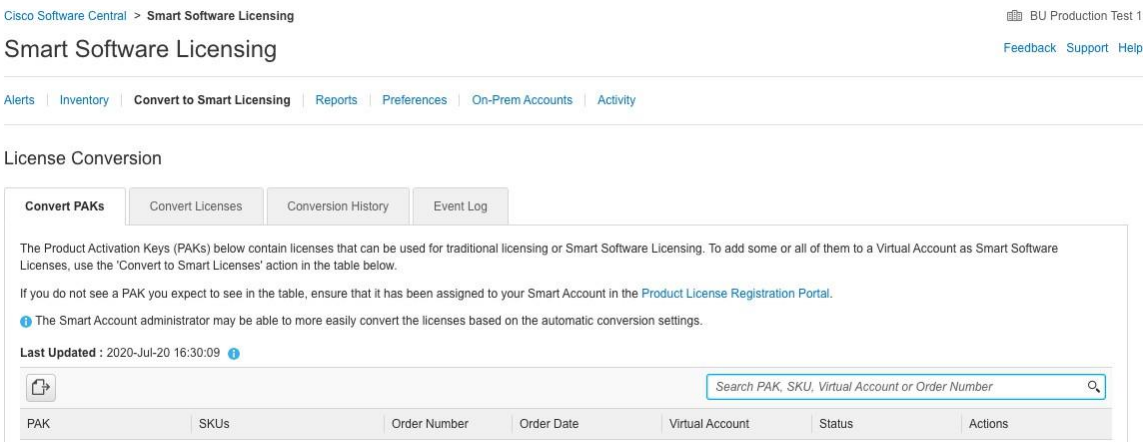
17.1.4 スマートライセンス登録プロセス

スマートライセンスを有効にするには、以下の手順を実行します。

1. Cisco Smart Software Manager（CSSM）ポータルにサインインし、Meeting Server ライセンスを持つバーチャルアカウントを選択します。
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（Settings）] ページ の [ライセンス（Licensing）] タブに移動します。
6. [変更（Change）] をクリックします。
7. [スマートライセンス（Smart Licensing）] を選択して、[保存（Save）] 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 はスマートライセンスポータルに接続できます）。
10. [登録（Register）] をクリックします。
11. 登録された場合は、バーチャルアカウントにあるライセンスの数を確認します。
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にあ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内でライセンスが表示されない場合、[ライセンスの変換（Convert Licenses）] タブを使用して PAK を検索します。その後、 図 23 のとおりに [ライセンスの変換（Convert Licenses）] を選択します。（ライセンスが見当たらない場合は、licensing@cisco.com にE メールを送信してケースをオープンしてください）。

図 23：スマートライセンスのライセンス転換



17.1.5 Multiparty ライセンス

17.1.5.1 Personal Multiparty Plus ライセンス

Personal Multiparty Plus（PMP Plus）は、特にビデオ会議を頻繁に主催するユーザに対して、ネームド ホスト ライセンスを個別に割り当てます。これは、Cisco UWL ミーティングまたは Flex ミーティング（PMP Plus を含む）経由で購入できます。Personal Multiparty Plus は、ビデオ会議向けのオールインワン ライセンスです。（導入されている Cisco Meeting Server ハードウェアの制限内である限り）主催できる会議の参加者数に制限はありません。会議には、任意のエンドポイントから誰でも参加できます。ライセンスでは、フル HD 1080p60 品質までのビデオ、オーディオ、およびコンテンツ共有がサポートされています。

注：Unified Communications Manager を使用すると、アドホック会議の開催者を特定することができます。また、開催者に PMP Plus ライセンスが割り当てられている場合は、そのライセンスが会議で使用されます。

注：個人の PMP Plus を使用したアクティブなコール数を決定するには、次の API オブジェクトでパラメータ **`callsActive`** を使用します：**`/system/multipartyLicensing/activePersonalLicenses`**。通常、2 件のコールをアクティブにし、1 つの開始と他方の終了を可能にします。Call Bridge のクラスタ上にコールがある場合、次の API オブジェクトでパラメータ **`weightedCallsActive`** **を使用します。** **`/system/multipartyLicensing/activePersonalLicenses`**（クラスタ内の各 Call Bridge について）。クラスタ全体の **`weightedCallsActive`** の合計数は、個人の PMP Plus ライセンスを使用したクラスタ上で区別されるコール数に一致します。PMP Plus ライセンスが超過した場合は、SMP Plus ライセンスが割り当てられます（セクション 17.1.1 を参照）。

17.1.5.2 Shared Multiparty Plus ライセンス

Shared Multiparty Plus（SMP Plus）では同時ライセンスが提供されており、ビデオ会議を主催する頻度が低い複数のユーザが共有できます。Shared Multiparty Plus は、PMP Plus ホスト ライセンスを持たないすべての従業員が、ビデオ会議へのアクセスに使用できます。これは、導入しているルーム システムが多数の従業員によって共有される場合に最適です。PMP Plus または SMP Plus ライセンスを使用しているすべてのユーザは、同じエクスペリエンスを享受でき、スペースでのミーティングのホスト、アドホックミーティングの開始、または今後のミーティングのスケジュール設定を行うことができます。共有ホスト ライセンスごとに 1 つの同時ビデオ会議がサポートされます。（導入されているハードウェアの制限内である限り）参加者数の制限はありません。

注：必要な SMP Plus ライセンスの数を決定するには、API オブジェクト **/system/multipartyLicensing** でパラメータ **callsWithoutPersonalLicense** を使用します。Call Bridge のクラスタ上にコールがある場合、クラスタ内の Call Bridge ごとに API オブジェクト **/system/multipartyLicensing** でパラメータ **weightedCallsWithoutPersonalLicense** を使用します。クラスタ全体の **weightedCallsWithoutPersonalLicense** の合計数は、SMP Plus ライセンスを必要とする、クラスタ上で区別されるコール数に一致します。

17.1.6 ユーザに対する Personal Multiparty ライセンスの割り当て

このプロセスでは、ユーザを単一の LDAP ソースからインポートする必要があります。『Meeting Management 3.0 管理者ガイド』の「プロビジョニング：ユーザーをインポート」の章を参照してください。

17.1.6.1 特定のユーザにライセンスがあるかを判断する方法

1. API オブジェクトのリストから、/users の後ろにある ▶ をタップします。
   a. 特定のユーザーの object id を選択します。
   b. このユーザに関連付けられている userProfile の object id を特定します
2. API オブジェクトのリストから、/userProfiles の後ろにある ▶ をタップします
   a. 特定の userProfile の object id を選択します。
   b. パラメータ hasLicence の設定を検索します。true に設定されている場合、手順 1 で特定されたユーザーは Cisco Multiparty ユーザーライセンスに関連付けられています。false に設定されている場合、ユーザは Cisco Multiparty ユーザライセンスに関連付けられていません。

      注：userProfile が削除されている場合、userProfile は ldapSource とインポートされたユーザに対して設定されていません。

17.1.7 Cisco Multiparty ライセンスの割り当て方法

スペースで会議を開始すると、Cisco のライセンスがそのスペースに割り当てられます。Cisco Meeting Server がどのライセンスを割り当てるかは、次のルールによって決まります。

- 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た Meeting Server がインポートした LDAP ユーザに対応している場合、そのユーザが会議でアクティブであるかどうかに関係なく、そのオーナーのライセンスが割り当てられます。割り当てられていない場合は、その後
- Cisco Unified Communications Manager のアドホックエスカレーション経由で会議が作成された場合、Cisco Unified Communications Manager は会議をエスカレーションしたユーザの GUID を提供します。その GUID が、Meeting Server によってインポートされ、Cisco PMP Plus ライセンスを割り当てられているユーザに対応している場合 、そのユーザのライセンスが割り当てられます。それ以外の場合で、

- 会議が Cisco TMS バージョン 15.6 以降を使用してスケジュールされている場合、TMS は会議の所有者を提供します。そのユーザが、ユーザ ID/電子メールアドレスを使用して割り当てられた Cisco PMP Plus ライセンスを持つ Meeting Server のインポートされた 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割り当てられます。割り当てられていない場合は、
- Cisco SMP プラスライセンスが割り当てられています。

17.1.8 Cisco Multiparty ライセンスの使用状況の判断

Meeting Management を使用して、Multiparty ライセンスの使用状況を確認することを推奨します。ただし、API は使用できます。

以下の表 18 には、Multiparty ライセンスの使用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をリストしています。

表 18：Multiparty ライセンスの使用状況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	使用先
/system/licensing	personal, shared	Cisco Meeting Server のコンポーネントが Multiparty ライセンスを持ち、アクティブ化されているかどうかを確認します。値は次のとおりです：ライセンスなし、アクティブ化、猶予、有効期限切れ。 有効期限と番号の上限も提供します。
/system/multipartyLicensing	PersonalLicenseLimit、 sharedLicenseLimit、 personalLicenses、 callsWithoutPersonalLicense、 weightedCallsWithoutPersonalLicense	ライセンス数について、使用可能なものと使用中のものを示します
/system/multipartyLicensing/ activePersonalLicenses	callsActive、 weightedCallsActive	Personal Multiparty Plus ユーザライセンスを使用しているアクティブコールの数を示します。
/userProfiles	hasLicense	ユーザが Cisco Multiparty ユーザライセンスに関連付けられているかどうかを示します

これらの追加オブジェクトと、Cisco Multiparty ライセンスをサポートするフィールドについての詳細は、『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 ライセンスの使用率の計算

次の特定のシナリオでは、会議に使用される SMP Plus ライセンスは、フル SMP Plus ライセンスの 1/6 に減少します。

- 参加者がビデオを使用していない場合の音声のみの会議は、
- Meeting Server が録音またはストリーミングを行っている場合を除き、Lync ゲートウェイコールは、その時点では完全な会議と見なされ、完全な SMP Plus ライセンスが消費されます。
- Web アプリと SIP エンドポイント、または 2 つの Web アプリが関係するポイントツーポイントコール（Meeting Server が録音またはストリーミングの場合を除く）は、この時点ではフル会議と見なされ、SMP Plus のフルライセンスが使用されます。

SMP Plus のフルライセンスでは、オーナープロパティが定義されていないスペースから、または PMP Plus ライセンスのないインポート済み LDAP ユーザが所有している、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済み LDAP ユーザが所有している、すべての音声ビデオ会議に使用されます。これは参加者の数に関係ありません。

注：ポイント ツー ポイント コールは次のように定義されます。

- Meeting Server に永続的なスペースがない
- レコーダーまたはストリーマーを含む、2 人以下の参加者
- LYNC AVMCU でホストされている参加者がいない

これには、Lync ゲートウェイコール、および他のタイプのコール（ポイントツーポイント Web アプリから Web アプリ、Web アプリから SIP、SIP から SIP まで）が含まれます。

17.1.10 Meeting Server からのライセンス使用状況スナップショットの取得

管理者は Meeting Server からライセンス使用状況を取得できます。Web 管理インターフェイスを使用している間は、POSTMAN などの API ツールを使用しますが、これらのツールにはアクセスできません。

展開内の Meeting Server のホスト 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ホスト 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。

指定されたホスト ID を持つ Meeting Server の Call Bridge からライセンスの使用状況を取得するには、 **`/system/MPLicenseUsage`** で GET を使用します。スナップショットの開始時刻と終了時刻を指定します。
使用中の個人ライセンスの数、使用中の共有ライセンスの数（音声のみ、ポイントツーポイント、または録音でもポイントツーポイントでもない）、録音されているコールの数、およびストリーミングされたコールの数に関する情報を提供します。

注：個人ライセンスと共有ライセンスは、コールがまたがる Call Bridges の数によって正規化されます。

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/使用状況の情報があり、Cisco Smart Software Manager にもライセンスレポート情報があります。録音ライセンスの使用状況は、同時に録音する会議の数を示します。同様に、ストリーミングライセンスの使用状況は、同時にストリーミングされている会議の数を示します。

17.1.12 レガシー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式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非推奨になりました。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たCisco のユーザーライセンスの取得

このセクションでは、Cisco パートナーから Meeting Server に必要なライセンスをすでに購入し、PAK コードを受け取っていることを前提としています。

この手順に従い、シスコ製品ライセンス登録ポータル を使用して、PAK コードと Meeting Server の MAC アドレスを登録してください。

1. Meeting Server の MAC アドレスを取得するには、サーバの MMP にログインして **`iface a`** の MMP コマンドを入力します。

   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. シスコライセンス登録ポータルを開いて、PAK コードと Meeting Server の 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 ライセンスが割り当てられていない場合は、機能ライセンスの他にこの PAK が必要です。
4. ライセンスポータルでは、ライセンスファイルの圧縮コピーが電子メールで送信されます。zip ファイルを解凍し、解凍後の xxxxx.lic ファイルの名前を **`cms.lic`** に変更します。
5. SFTP クライアントを使用して Meeting Server にログインし、Meeting Server ファイルシステムに **`cms.lic`** ファイルをコピーします。
6. MMP コマンド **`callbridge restart`** を使用して Call Bridge を再起動します。
7. Call Bridge を再起動した後、MMP コマンド
   `license`
   有効化された機能と有効期限が表示されます。

18 ホストされた会議における情報の取得

Meeting Server でホストされる会議に関する情報を取得する方法には、API を常に調査する必要がない 2 つのメカニズムがあります。これらは、コール詳細レコードとイベントです。

注：各 Call Bridge において、Cisco Meeting Management を CDR （コール詳細レコード）の受信側、さらにイベントクライアントとして構成することで、API 要求、CDR、Meeting Server イベントを介したアクティブな会議に関する情報を取得できます。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 では、サーバ側で接続される新しい SIP 接続や、アクティブ化または非アクティブ化されたコールなど、キーコール関連イベントに関するコール詳細レコード（CDR）が内部で生成されます。

これらのレコード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サーバーを構成できます。Meeting Server でレコードを長期間保存する規定や、Meeting Server 上の CDR を参照する方法はありません。

CDR システムは、イベントと診断を相互に参照できるよう、2 つのシステム間でコール ID とコールレッグ ID の値が一致する場合は、この 2 つのシステムを Meeting Server API と組み合わせて使用できます。

Meeting Server は CDR 受信者を最大 4 人までサポートし、さまざまな管理ツールや、Cisco Meeting Management などの同じ管理ツールの複数のインスタンスを展開できます。詳細については、『Cisco Meeting Server コール詳細レコードガイド』を参照してください。

18.2 イベント

Meeting Server は、Meeting Server 上で発生した変更をリアルタイムで「イベントクライアント」に通知できます。Meeting Server はイベントのサーバとして機能し、イベント クライアントは Web ベースの管理アプリケーションなどになります。Cisco Meeting Management は、イベント クライアントとして機能します。

注：ユーザーは、API クライアントの構築に似た方法で、独自のイベントクライアントを構築できます。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ます。これらは、Python のような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、Web 管理用に設定したのと同じポートです。これは通常、インターフェイス A の TCP ポート 443 になります。

Meeting Server の API リソースを継続的にポーリングするのではなく、イベント クライアントは、イベント リソースにサブスクライブして更新を受信します。たとえば、イベントクライアントと Meeting Server の間の WebSocket 接続を確立した後に、イベントクライアントはイベントリソース **`callRoster`** に登録し、アクティブな会議の参加者リストの最新情報を受け取り、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するのを確認できます。

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 サーバで構成されていないか、上書きする必要がある値を返す DNS リゾルバを構成できます。外部 DNS サーバを照会する代わりに、返されるカスタムリソースレコード（RRs）を構成できます。（クライアントは RR を利用できません）。詳細については、『MMP コマンドリファレンス』を参照してください。

注：以下のレコードを定義する前に、Meeting Servers の A レコードまたは SRV レコードが既に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** 解決対象 Web Bridge の IP アドレス。 説明： このレコードは、Meeting Server では直接使用されません。ただし、エンドユーザに、ブラウザに入力する FQDN を提供して、Web Bridge を解決する方法は一般的です。このレコードの形式に制約や要件はありません。
A / AAAA	**ukcore1.example.com** 解決対象 Call Bridge の IP アドレス。 説明： Lync FE サーバーが Call Bridge に接続するために使用します。
A / AAAA	**ukcoreadmin.example.com** **ukedgeadmin.example.com** 解決対象 MMP インターフェイスの IP アドレス。 説明： このレコードは管理目的でのみ使用します（システム管理者が MMP インターフェイスごとに FQDN を設定する場合）。

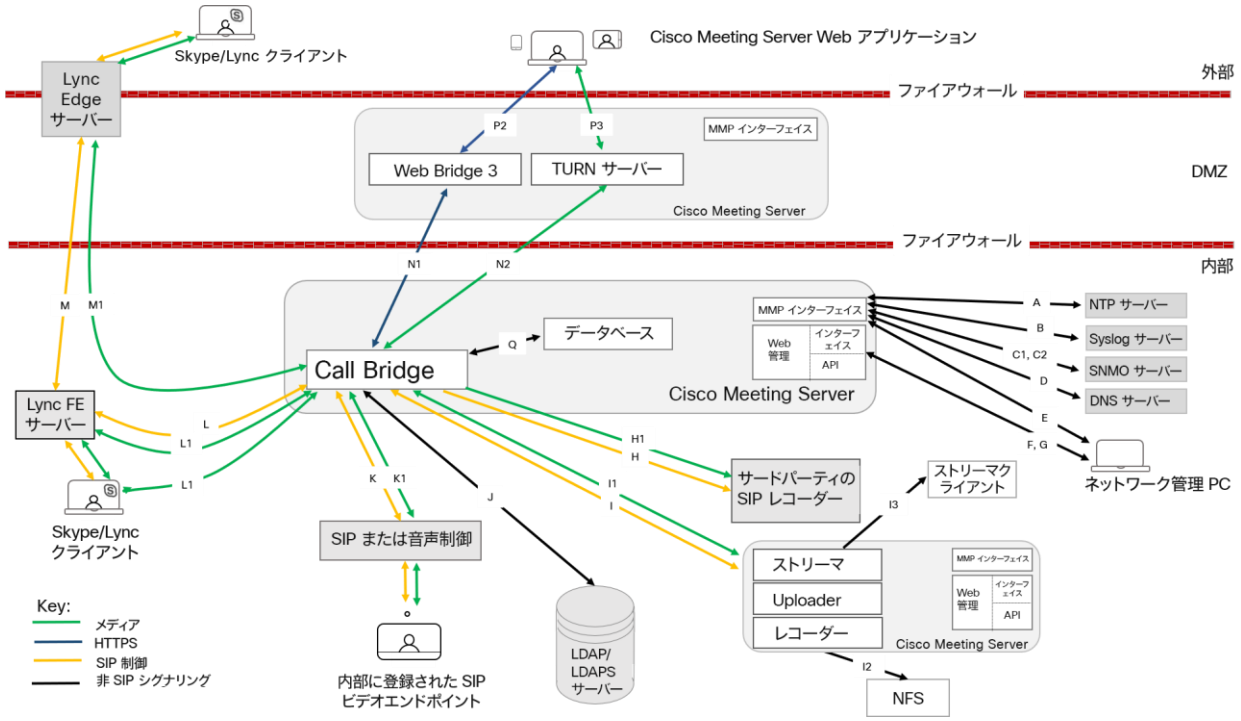
タイプ	例と説明
SRV（*）	**_sipinternaltls._tcp.<yourLyncdomain>** 解決対象 Lync FE サーバーまたは FE プールの A レコード。 説明： FE プールがある場合は、プール内の個々の FE サーバーを指す複数の FE レコードを使用できます。 Meeting Server で Lync ミーティングを Lync ミーティング ID によって解決する場合は、このレコードも必要です。
A / AAAA	**fe.<yourLyncdomain>** 解決対象 Lync FE サーバーの IP アドレス。 説明： 個々の FE サーバーに対して 1 つのレコードが必要です。
SRV（*）	**_sipfederationtls._tcp.<yourSIPdomain>** 解決対象 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** 解決対象 Call Bridge の IP アドレス。 説明： Call Bridge にはパブリック IP アドレスが必要であるため、Lync フェデレーションに必要です。 このシナリオでは NAT がサポートされていません。

（*）SRV レコードは、IP アドレスへ直接解決されません。SRV の要件を満たすには、関連する A または AAAA 名前レコードを作成する必要があります。

付録 B 展開に必要なポート

次の図は、Meeting Server への接続と、分散型サーバー展開内のファイアウォールの場所を示しています。どのポートを開くかを特定するには、図の下の表を使用します。

図 24：DMZ 内の TURN サーバーと Web Bridge 3 コンポーネントを使用して分散型サーバー展開で開く必要があるポート



B.1 Meeting Server の構成

表 20 は、Meeting Server の構成に使用するポートを示します。

表 20：Meeting Server の管理用のポート

コード	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 に関するトラフィックの方向	関連情報
E	MMP	22	SSH	TCP	着信	MMP へのセキュア ログイン
F	API または Web Admin	80	HTTP	TCP	着信	MMP を介したポートの有効化/無効化
G	API または Web Admin	443	HTTPS	TCP	着信	MMP 経由でポートを構成可能

B.2 接続サービス

表 21 を使用して、Web アプリに異なるサービスを接続するために使用するポートを特定します。

表 21：サービスを接続するために開くポート

コード	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	コンポーネントを基準にしたトラフィックの方向	その他の情報
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 ポート（MMP 経由で別のポートを構成可能）
C1	MMP	SNMP サーバー	161	UDP	着信	
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 Admin インターフェイスで、または API オブジェクト /system/cdrReceivers/ を使用して API で、CDR 受信デバイスの URI を設定します。

B.3 Meeting Server コンポーネントの使用

表 22 を使用して、Meeting Server のコンポーネントおよびファイアウォールを介して開く必要があるポートへの接続に使用す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

コード	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	コンポーネントを基準にしたトラフィックの方向	その他の情報
H	Call Bridge	サードパーティの SIP レコーダー	5060	TCP（SIP）	発信	
			5060	UDP（SIP）		
			5061	TLS(SIP)		

コード	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	コンポーネントを基準にしたトラフィックの方向	その他の情報
H1	Call Bridge	サードパーティの SIP レコーダー		メディア	発信	サードパーティの SIP レコーダーによって決定されるポート
			32768-65535	UDP（STUN、RTP、BFCP）	着信	
I	Call Bridge	レコーダー/ストリーマ	5060	TCP（SIP）	発信	MMP 経由でポートを構成可能。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（lo:8443 など）を使用します
			5061	TLS(SIP)		
			5060	TCP（SIP）	受信	
			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	
I2	レコーダー	ネットワーク ファイル サーバー（NFS）				NFS 上の録画保存場所を指定するには、MMP コマンド recorder nfs <host-name/IP><directory> を使用します。
I3	ストリーマ	ストリーマクライアント	1935	RTMP	発信	
J	Call Bridge	LDAP/LDAPS（アクティブディレクトリ）	389/636（注 1）	TCP/TCP（SIP TLS）	発信	Web Admin インターフェイス経由でポートを構成可能
K	Call Bridge	内部に登録された 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）		

コード	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	コンポーネントを基準にしたトラフィックの方向	その他の情報
K1	Call Bridge	内部に登録された 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	
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（注 2）	UDP（STUN、RTP）	発信	
			32768-65535	UDP（STUN、RTP）	受信	
			1024-65535（注 2）	TCP（RDP）	発信	
			32768-65535	TCP（RDP）	着信	
M	Call Bridge	Lync エッジサーバー	3478	UDP	発信	
			443	TCP	発信	
M1	Call Bridge	Lync エッジサーバー	32768-65535	UDP（STUN、RTP）	受信	
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定義です
N2	Call Bridge	TURN サーバー	50000-62000（注 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 アプリケーション	443	TCP（HTTPS）	着信および発信	HTTP のポート 80 オプション >HTTPS リダイレクト
P3	TURN サーバー	Cisco Meeting Server Web アプリケーション	3478（注 3） （注 4）	UDP（RTP、STUN）	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、ファイアウォールにオープンポートは不要

注：

注 1：ポート 636（セキュア）と 389（非セキュア）は通常この機能で使用されますが、ポートは Web Admin インターフェイスで構成できます。3268 および 3269（非セキュアおよびセキュア）なグローバルカタログ LDAP 要求も同様です。
注 2：正確な範囲は、Lync サーバーの構成によって異なります。
注 3：管理者は、オプションで TURN 用に 3478 TCP または別の顧客の TCP ポートを有効にすることができます。
注 4：TURN およびメディアの範囲は、このガイドに記載されているように、Web アプリが TURN リレーを割り当て、Call Bridge が TURN リレーを作成しないことを前提としています。

B.4 ループバックで開くポート

表 23 にリスト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きます。

表 23：ループバック上のポート

ポート	使用方法	方法
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内部への接続	
3521	configd	
5432	postgres	
5060	SIP	常に開いています
5061	暗号化された SIP	Call Bridge に適用された証明書の場合のみ
5070	BFCP	IPv6 上のみ
8080	HTTP	常に開いています
8081	HTTP	Webadmin が有効な場合
3478	STUN	

付録 C Cisco Meeting Server プラットフォームによるコールのキャパシティ

下記の表 24 は、新しいソフトウェアバージョンにアップグレードした場合の Meeting Server の最大キャパシティの詳細を示しています。単一またはクラスタの Meeting Server のキャパシティは、Call Bridge グループ内のコールのロードバランシングとは異なります。

表 24：Meeting Server のコールキャパシティの進化

ソフトウェアのバージョン		2.9			3.0、3.1 および 3.2			3.2	
Cisco Meeting Server プラットフォーム		1000 M4	1000 M5	2000	1000 M4	1000 M5	2000	1000 M5v2	2000 M5v2
Meeting Servers：個々のクラスタまたはクラスタ内（注 1、2、3、4） そして Call Bridge グループ内の Meeting Server	1080p30 720p 30 SD 音声	48 96 192 1700	48 96 192 2200	350 700 1000 3000	48 96 192 1700	48 96 192 2200	350 700 1000 3000	60 120 240 2200	437 875 1250 3000
	サーバーごとの会議あたりの HD 参加者数	96	96	450	96	96	450	120	450
	Web アプリのコールキャパシティ（3.0 からの内部コールと 3.1 からの CMS Web Edge 上の外部コール）：								
	フル HD HD SD 音声通話				48 96 192 500	48 96 192 500	350 700 1000 1000	60 120 240 500	437 875 1250 1250
Call Bridge グループ内の Meeting Server	サポートされるコールタイプ	インバウンド SIP アウトバウンド SIP Cisco ミーティング アプリケーション							
	負荷制限	96,000	96,000	700,000（注 5）	96,000	96,000	700,000	120,000	875,000

注 1：クラスタあたりの最大 24 個の Call Bridge ノード。ノード 8 個以上のクラスタ設計は、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。

注 2：Call Bridge グループが設定されていないクラスタ Cisco Meeting Server 2000 では、最大コール数の整数倍（700 HD コールの整数倍など）をサポートします。

注 3：SIP コールまたは Web アプリケーション コールにクラスタあたり最大 16,800 の HD 同時コール（24 ノード X 700 HD コール）が適用されます。

注 4：クラスタ内の Meeting Server プラットフォームに応じて、1 つのクラスタの会議あたり最大 2600 の参加者。

注 5：バージョン 3.2 以降、Meeting Server は Meeting Server 1000 M5v2 と Meeting Server 2000 M5v2 のハードウェアバリアントでコールキャパシティの増加をサポートします。

- Meeting Server 1000 M5v2 の負荷制限は 96,000 から 120,000 に増加しました。720p ビデオコールの Meeting Server 1000 のコールキャパシティが、新しいプラットフォームで最大 96 から 120 に増加しました。
- Meeting Server 2000 M5v2 の負荷制限は 700,000 から 875,000 に増加しました。720p ビデオコールの Meeting Server 2000 のコールキャパシティが、新しいプラットフォームで 700 から 875 に増加しました。

注 6： 表 24 は、ビデオ通話で最大 2.5 Mbps-720p5 コンテンツ、音声通話で最大 G.711 のコールレートを想定しています。その他のコーデックや高いコンテンツ解像度/フレームレートは、容量の減少につながります。会議が複数の Call Bridge にまたがる場合は、分散リンクが自動的に作成され、サーバーのコール数とキャパシティに対してもカウントされます。負荷制限の数値は H.264 にのみ使用されます。

注 7：クラスタでサポートされるコールの設定レートは、SIP コールでは 1 秒あたり最大 40 コール、Cisco Meeting Server Web アプリケーションのコールでは 20 コールです。

C.1 Cisco Meeting Server Web アプリケーションのコール キャパシティ

このセクションでは、外部コールおよび混在コールに Web Bridge 3 と Web アプリケーションを使用する展開でのコールキャパシティの詳細について説明します。（内部コールの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 アプリケーションのコール キャパシティ：外部コール

Expressway（Large OVA または CE1200）は、中規模の Web アプリの要件（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、小規模の Web アプリの要件（つまり 200 コール以下）の導入に推奨されるソリューションです。ただし、Web アプリの規模を大きくする必要がある導入の場合は、バージョン 3.1 から、SIP 容量まで拡張する必要なソリューションとして Cisco Meeting Server Web Edge をお勧めします（表 24 を参照 ）。

外部コールとは、クライアントがリバース プロキシおよび TURN サーバとして Cisco Expressway を使用して、Web Bridge と Call Bridge に到達する場合を言います。

Web アプリケーションのコールのプロキシとして Expressway を使用する場合、表 25 に示すように、Expressway により最大コール数の制限が適用されます。

注：Web Bridge 3 と Web アプリケーションを導入する場合は、Expressway バージョン X12.6 以降を使用する必要があります。それより前のバージョンの Expressway は、Web Bridge 3 でサポートされていません。

表 25：Cisco Meeting Server Web アプリのコール キャパシティ：外部コール

セットアップ	コール タイプ	CE1200 プラットフォーム（Platform）	大規模 OVA Expressway	中 OVA Expressway
Cisco Expressway（X12.6 以降）ペア	フル HD	150	150	50
	その他	200	200	50

Expressway ペアをクラスタリングすることで、Expressway のキャパシティを増大させることができます。Expressway ペアのクラスタリングは、最大 6 ノードまで可能です（4 ノードは拡張のために使用され、2 ノードは冗長性のために使用されます）。その結果、1 ペアのキャパシティの 4 倍の合計コールキャパシティが得られます。

注：Cisco Meeting Server Web アプリケーションのコールについては、Expressway クラスタのコールセットアップレートが 1 秒あたり 6 コールを超えることはできません。

C.1.2 Cisco Meeting Server Web アプリケーションのキャパシティ：混在（内部 + 外部）コール

スタンドアロンとクラスタのどちらの導入環境でも、内部と外部を組み合わせたコールの使用をサポートできます。内部参加者と外部参加者の混在をサポートする場合、Web アプリケーションの合計キャパシティは、内部コールについては付録 C のとおりですが、外部から接続できる合計の範囲内での参加者数は、表 25 の制限を受けます。

たとえば、1 つのスタンドアロン Meeting Server 2000 と 1 つの 大規模 OVA の Expressway のペアでは、音声のみの Web アプリケーションコールであれば混在で 1,000 までサポートしますが、外部参加者の数は、合計 1,000 のうち最大 200 に制限されます。

C.2 Cisco Meeting Server でサポートされるユーザー数

バージョン 3.3 以降、Cisco Meeting Server クラスタは、データベースが配置されているサーバーに応じて、最大 300,000 のユーザをサポートできます。クラスタ内のすべてのデータベースは、同じ仕様のサーバー上にある必要があります。

表 26: Cisco Meeting Server でサポートされるユーザー数

Cisco Meeting Server	最大ユーザ数
Meeting Server 2000 M5v2	300,000
Meeting Server 2000 M5v1	200,000
Meeting Server 2000 M4、Meeting Server 1000 M4、M5v1、M5v2、および仕様ベースのサーバー	75,000

注：多数のユーザの LDAP 同期により、通話の参加時間が長くなる可能性があります。メンテナンス時間帯またはオフピーク時に、新しいユーザ/coSpace を Meeting Server に追加することをお勧めします。

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 1000、Cisco Meeting Server 2000、VM ソフトウェア画像について、SIP メディア暗号化が有効になった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たアクティベーションキー（暗号化されていない SIP メディア）の購入を選択することができます。ソフトウェア pids R-CMS-K9 および R-CMS-2K-K9 の下で、暗号化または暗号化されていないオプションのいずれかを選択します。メディアには、オーディオ、ビデオ、コンテンツビデオ、ActiveControl データが含まれます。

注：SIP メディア暗号化を無効にしたアクティベーションキーがアップロードされていない限り、現在の Call Bridge のアクティベーションは影響を受けません。

D.1 暗号化されていない 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た場合、次のようなメッセージが表示されます。

- 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ません。
- クラスタ化された Call Bridge 間の配布リンクを使用して送信されるメディアは暗号化されません。
- コールのシグナリングは暗号化された状態が維持されます。
- Meeting Server と Web アプリケーション間の通話中のメディアは、どのプラットフォーム上でも暗号化された状態が維持されます。
- 次の API オブジェクトで sipMediaEncryption パラメータが禁止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/ /callLegProfileTrace<call leg id>
- Web 管理インターフェイスの[設定（Configuration）] > [コール設定（Call settings）] Web ページ上の[SIP メディア暗号化（SIP media encryption）]フィールドが disabled 以外の場合、エラーメッセージが表示されます。

注：SIP メディア暗号化を無効にした場合でも、必要に応じて /outboundDialPlanRules に sipControlEncryption パラメータを設定することで、発信コールでコールシグナリングを暗号化できます。

D.2 Call Bridge メディアモードの決定

Call Bridge が暗号化された SIP メディアまたは暗号化されていない SIP メディアを使用するかどうかを判断するには、Web Admin インターフェイスを使用して、[設定（Configuration）] > [API]を選択してから、

1. API オブジェクトのリストから、/api/v1/system/licensing の後ろにある ► をタップします。

features オブジェクト callBridgeNoEncryption の status が activated に設定されている場合、暗号化されていないメディアのアクティベーションキーが Call Bridge にロードされます。callBridgeNoEncryption のステータスで有効なその他設定は、noLicense、grace または expired です。

callBridgeNoEncryption には、文字列の形式で有効期限フィールドも含まれます。

付録 E デュアルホーム会議

E.1 概要

デュアルホーム会議により、Lync のスケジュール済みミーティングでも、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ます）でも、Lync のクライアントユーザと Web アプリユーザの両方に対するユーザエクスペリエンスが向上します。Lync の参加者は、ドラッグアンドドロップを使用して Web アプリユーザを Lync ミーティングに追加できます。また、会議コントロールを使用して Web アプリユーザをミュートしたり、接続解除したりすることができます。Lync のスケジュール済み会議に参加している Web アプリケーションユーザーには、最大 5 名の Lync 参加者からのビデオと Web アプリケーションユーザーのビデオが表示されます。Lync ユーザには、すべての Web アプリユーザおよびミーティング内の Lync ユーザからビデオがギャラリー形式で表示されます。Lync ユーザと Web アプリユーザの両方に、ミーティングの参加者の完全な統合リストが表示されます。

注：Lync/Skype for Business クライアントの [参加者の追加（Add Participant）] ボタンは、アドホックのデュアルホーム会議では機能しません。この場合、Meeting Server と AVMCU の間でアクティブなコールが残りますので、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。

Lync の参加者は、Meeting Server スペースに直接ダイヤルするか、ドラッグアンドドロップして Meeting Server スペースを Lync ミーティングに追加することもできます。これは、Lync ユーザが参加する Cisco Meeting Server スペースで大規模なミーティングを開く場合に便利です。最初のケースでは、複数の参加者からなる組み合わせレイアウトを受信します。完全なスペースを Lync ミーティングに追加すると、Lync ユーザはスペースから 1 つのビデオストリーム（メインスピーカー）のみを受信し、参加者の完全な統合リストを受信しません。引き続き、Lync の参加者を通常通り追加できます。

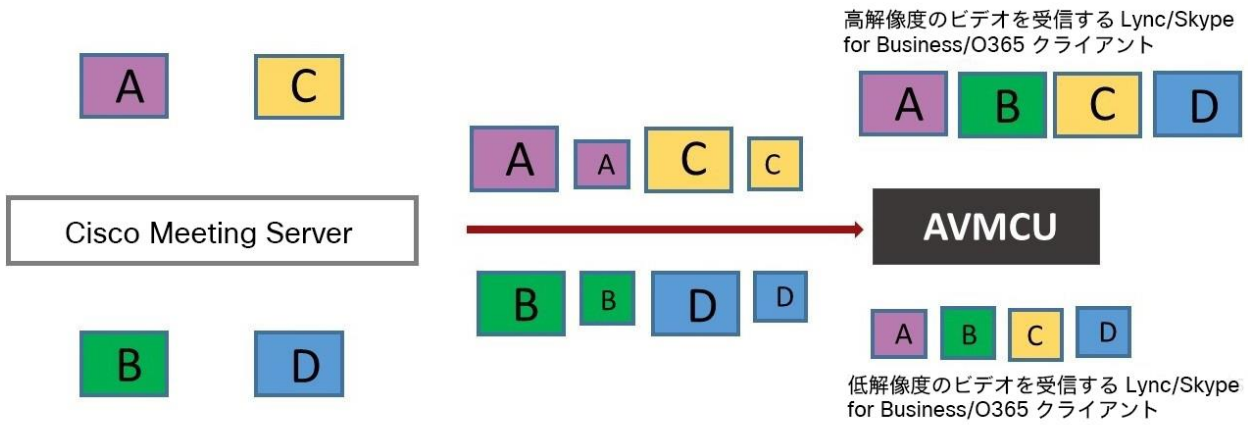
注：Meeting Server クラスタを備えたデュアルホームの会議は、クラスタ内の Meeting Server の 1 つと（Expressway を経由するのではなく）Microsoft のインフラストラクチャとの間を直接フローする Microsoft トラフィックがない限り、Meeting Server のエッジとして Expressway X8.11 では現在サポートされていません。デュアルホームは、スタンドアロンの Meeting Server のエッジとして Expressway X8.11 でサポートされています。

E.2 デュアルホーム会議での一貫性のあるミーティングエクスペリエンス

Meeting Server は、ビデオ参加者 1 人あたり 2 つ（高解像度のビデオストリームと低解像度のビデオストリーム）の H.264 ビデオストリームを AVMCU に送信します。 図 25 を参照してください。Lync、Skype for Business、および O365 クライアントで高解像度をサポートし、高品質のビデオストリームに登録および受信します。帯域幅の制限、ウィンドウサイズ、レイアウト、CPU 電力、モバイルデバイスでの使用を理由として低品質を選択したクライアントは、低品質のストリームに登録して受信し、他の参加者に対してビデオ品質を低下したりビデオエクスペリエンスを劣化させたりしません。

注：SIP トランクの帯域幅が 2 本のビデオストリームに対応するために十分に高く設定されるようにしてください。LAN には 8MB、WAN には 2.5MB を使用することを推奨します。

図 25：AVMCU へのデュアルメディアストリーム



注：Microsoft RT ビデオを使用しているデバイスではこの機能を利用できません。

E.2.1 ユーザエクスペリエンスの概要

RDP のサポートと複数のビデオエンコーダのサポートが組み合わされたデュアルホーム会議では、Lync と Web アプリの両方のユーザーに対する会議エクスペリエンスが向上します。

- Lync クライアントユーザと Web アプリユーザの両方に、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と Web アプリユーザの両方が、接続場所に関係なく、ミーティングに参加しているすべての参加者の完全な統合リストを受信します。
- Lync クライアントユーザには、SIP エンドポイントや Web アプリからのビデオについて、正方形以外の縦横比が表示されます。

- Lync クライアントユーザーは、メインのビデオエリアではなく、画面の別の領域にコンテンツを表示します。
- Meeting Server は、Lync ミーティングの各参加者がサポートする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 Lync クライアントのバージョンが複数使用されているミーティング中のすべての Lync クライアントユーザのエクスペリエンスが最適化されます。
- Meeting Server は、ビデオ参加者 1 人あたり 2 本（高解像度のビデオストリームと低解像度のビデオストリーム）の H.264 ビデオ ストリームを AVMCU に送信し、低解像度のみをサポートするクライアントがミーティングに参加した場合に、高解像度のビデオストリームをサポートするクライアントに高解像度エクスペリエンスを維持できるようにします。
- チャットは、スペース内の Web アプリユーザと Lync AVMCU 会議で動作します。Web アプリユーザと Lync クライアント間の直接コールで実行されます。

注：ミーティング中に最適なユーザ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、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 Web アプリユーザが、複数の Lync 参加者を表示できます。Lync 2010 では、最も大きなスピーカーがすでに会議の Meeting Server 側にある場合、最も大きなスピーカーストリームを 1 つしか提供しません。すると、Web アプリユーザと SIP エンドポイントユーザには、Lync の参加者が表示されません。

RDP と複数のビデオエンコーダのサポートの詳細については、次の 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サポート。

E.3 デュアルホーム会議でのミーティングのミュート/ミュート解除制御

Meeting Server ソフトウェアのバージョン 2.4 では、次の点について、デュアルホーム会議でのミュート/ミュート解除のミーティング制御が改善されました。

- オンプレミスと Office 365 の Lync/Skype for Business クライアント
- エンドポイントユーザー
- Web アプリケーションユーザー。

注：このセクションでは、Meeting Server の API を使用してミュートとミュート解除が有効になっていることを前提としています。

ミュート/ミュート解除：

- Lync クライアントは、デュアルホーム会議で誰でもミュートおよびミュート解除できます。つまり、自身と他のクライアントは、聴衆者のミュートとミュート解除を行えます。
- すべてのエンドポイントユーザが、Lync クライアントをミュートできるようになります。
- AVMCU の Lync 側のエンドポイントユーザーは、自身（セルフ）および他のエンドポイント（AVMCU に接続されている Lync クライアント/エンドポイント、または Meeting Server 側）のミュートとミュート解除を行えるようになります。バージョン 2.4 より前の場合、AVMCU の Meeting Server 側のエンドポイントユーザだけが、自分や他のユーザのミュートとミュートを解除することができます。
  - 非 ActiveControl エンドポイントの場合、Meeting Server は、ミュートとミュート解除ごとに DTMF キーシーケンスを送信し、メディアストリーム上のアイコンをエンドポイントにオーバーレイして、エンドポイントがミュートまたは非ミュートのいずれかを示します。
  - CE 9.2.1or 以降のソフトウェアを実行している ActiveControl エンドポイントでは、エンドポイントがアイコンとメッセージを処理します（Meeting Server ではアイコンがオーバーレイされません）。
- ActiveControl エンドポイントをミュートにした後は、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を解除する必要があります。たとえば、リモート参加者が ActiveControl エンドポイントをミュートしてからミュートを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が解除されるまで、もう一度自身をミュートします。
- リモートの参加者が非 ActiveControl エンドポイントのミュートを解除しようとすると、非 ActiveControl エンドポイントはミュート解除されます。
- Web 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を解除できます。また、ミーティングに参加しているすべての参加者の正しいミュート状態が表示されます。

Web アプリ**ユーザーのミュート/ミュート解除：**

- Web 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、デュアルホーム会議で Lync クライアントに渡されません。ただし、Lync クライアントが Web アプリユーザーをリモートでミュートし、Web アプリ自体がミュートを解除した場合、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。
- リモート参加者が Web アプリユーザーのミュートを解除しようとすると、Web アプリユーザーはローカルでミュートされた状態のままです。注：他の参加者にはミュートされていないと表示されますが、実際にはミュートされています。
- Web アプリには、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が表示されます。Meeting Server のアイコンは、Web アプリのビデオペインにはオーバーレイされません。

E.4 デュアルホーム Lync 機能の構成

Meeting Server 展開を使用するオンプレミス Lync 展開または Lync フェデレーション展開がすでにある場合は、Meeting Server 上で追加の構成は必要ありません。

これが新しい展開の場合は、Meeting Server の Lync Edge 設定を必ず構成してください。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 を介して Lync 会議に参加できない場合や、「Lync」に解決するダイヤルプランルールを使用する場合は、まずは「Lync Edge」の設定が設定済みであることを検証します。これは、Edge サーバーの検索に使用されるのと同じ方法で Lync 会議を解決するのと同じ仕組みです。Meeting Server は、Lync FE サーバを照会して、両方を検索する必要があります。

失敗すると、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 conference resolution: conference "1234" not found`
これは、会議が存在しないが、他に考えられる原因も存在する可能性があります。

SIP トラフィックトレースが有効になっている場合は、上記のメッセージがログに記録される直前に Lync FE サーバに「SERVICE」メッセージが送信される必要があります。これは 200 OK で返信する必要があります。このメッセージが正しい IP に送信されるかを確認します。これは、Lync FE サーバの IP である必要があります。

このメッセージが送信されない（ログに表示されない）場合は、Call Bridge が **`_sipinternaltls._ tcp.lyncdomain`** レコードの DNS SRV ルックアップを使用して Lync サーバーを検索できない可能性があります。そのため、このメッセージの送信先が不明になります。DNS トレースと再試行を有効にすると、これを確認できます。ただし、これは、Lync Edge の設定が Meeting Server 上で構成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が、Lync サーバーが「403 未認証」と返信する場合、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内のローカル連絡先ドメインが正しく設定されていない場合です。これは 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 に設定した LDAP フィールドマッピングの追加情報を提供します。

次のように、LDAP フィールド値の一部には、SED に似た構造を代わりに使用できます。

$<LDAP field name>|'/<regex>/<replacement format>/<option>'$

定義：

> **<option>** は g でもよく、 **<regex>** のそれぞれの一致を **<replacement format>** に置き換えるか、最初のみ一致するよう空白にします。
>
> **<regex>** の一部は **<replacement format>** で使用できるよう、丸括弧で囲むことによってタグ付けできます。
>
> タグ付き一致は **<replacement format>** で参照できます。\x の x は 0 ～ 9 の数字が入ります。照合 0 は全体一致に対応し、照合 1 ～ 9 は 1 ～ 9 番目のタグ付きサブ表現に対応します
>
> 代替表現内の一重引用符は、バックスラッシュでエスケープされる必要があります。バックスラッシュ文字そのものの場合も同様です。
>
> 代替表現の要素を区切るフォワードスラッシュの代わりに、一重引用符、バックスラッシュ、数字 0 ～ 9 以外の任意の文字を使用できます。
>
> 区切り文字を表現内で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。

以下の例は、次の形式のアドレス

firstname.lastname@test.example.com

を次の形式に変換します。

firstname.lastname@example.com JIDs
$mail|'/@test/@xmpp/'$

さらに、以下の例は、ユーザのフルネームから小文字の「a」をすべて削除します。

$cn|'/a//g'$

使用する適切な表現は次のようになります。

```
Full name:                $cn$
JID:                     $mail|'/@test/'$ space
URI:                     $mail|'/@.*//'$.space
space dial-in number:    $ipPhone$
```

注：LDAP サーバーのログイン情報は、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により、これらのログイン情報を使用して利用可能なフィールドと権限を制限できます）。

- mail
- objectGUID
- entryUUID
- nsuniqueid
- telephoneNumber
- mobile
- sn
- givenName

付録 G NAT の内側での TURN サーバーの使用

TURN サーバーを NAT の内側に展開し、MMP コマンド **`turn public-ip`** を使用して NAT アドレスを指定します。ただし、Interactive Connectivity Establishment（ICE）の機能により、接続が常に機能するために NAT の慎重な構成が必要になります。

この付録では、ICE の機能の概要を示します。次について説明します。

- 候補の特定方法
- 接続性のチェック方法
- TURN サーバの正面にある NAT の影響
- NAT が外部 Web アプリユーザにどのように影響するか

注：唯一の利用可能なパスに両方のリレー候補が含まれる場合に問題が発生する可能性があります。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、ファイアウォールを正しく構成する必要があります。

G.1 候補の特定

また、候補アドレスとポートのリストを収集し、これらの候補のペアを特定してメディアの交換を可能にしています。複数の候補ペアが使用可能な場合は、優先順位スキームを使用して、どのペアが使用されるのか決定します。

通常、次の 3 つの候補が存在する可能性があります。

1. ホスト候補
2. サーバー再帰候補
3. リレー候補

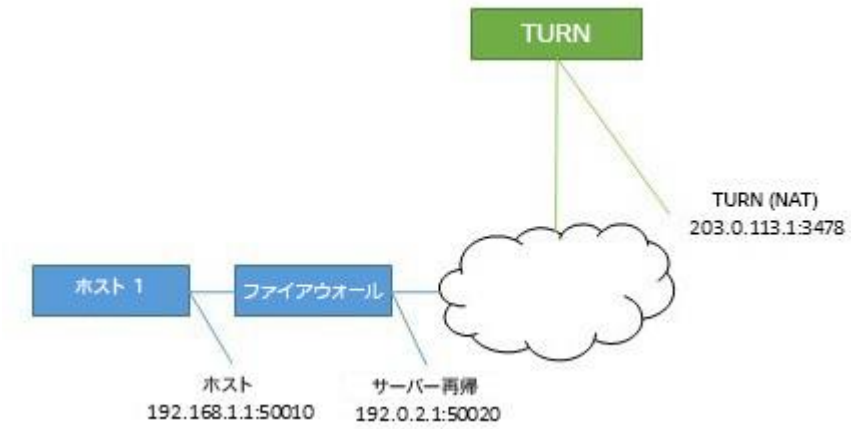
G.1.1 ホスト候補

最も簡単な候補がホスト候補です。これはホストインターフェイスで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で実行され、振り分けできません。

G.1.2 サーバー再帰候補

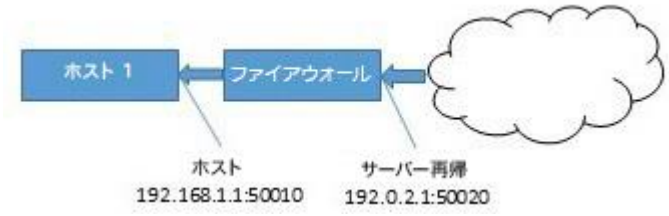
サーバ再帰候補は、TURN サーバが着信パケットを受信するアドレスです。これを確認するために、ホストは TURN サーバの定義されたポート（通常はポート 3478）にパケットを送信し、TURN サーバはパケットの受信場所に関する情報を返します。

図 26：サーバー再帰候補



ホストが NAT を実行するファイアウォールの背後にある場合、これはホスト候補とは異なります。多くの場合、このポートおよびアドレスに送信されたパケットはホストに送り返されます。

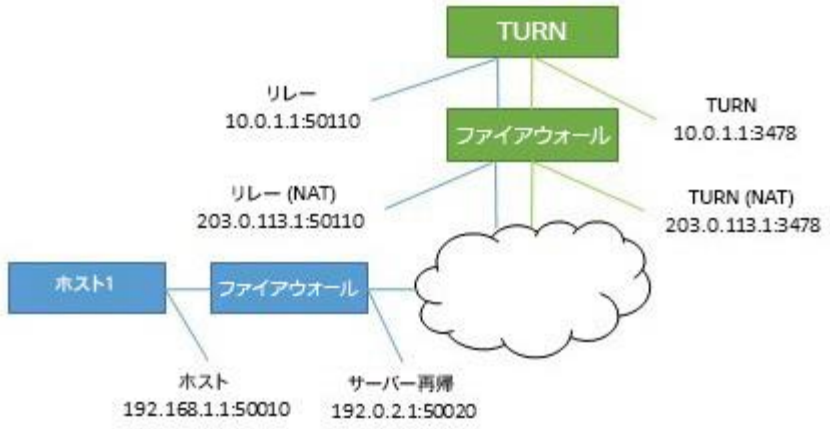
図 27：NAT を実行するファイアウォールの背後にあるホストの影響



G.1.3 リレー候補

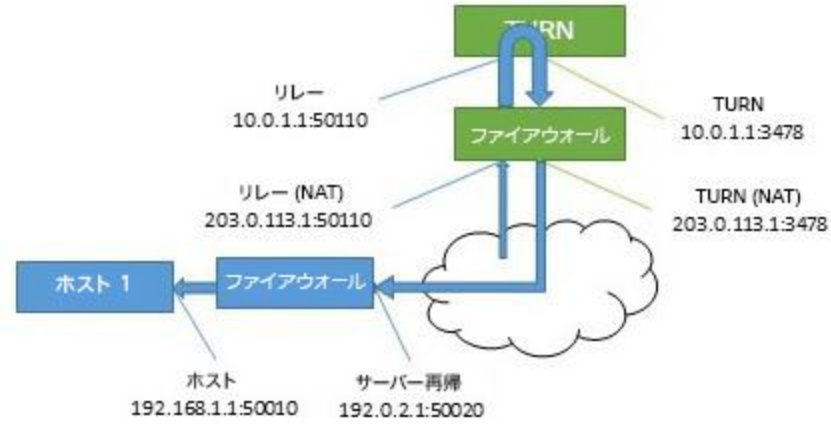
最終的な候補はリレー候補です。この候補は、ホストからの要求に応答して TURN サーバによって作成されます。この候補のリレーアドレスは、NAT が使用されている場合、リレーアドレスが NAT からアドレスに変更される TURN サーバ インターフェイス アドレスです。

図 28：リレー候補



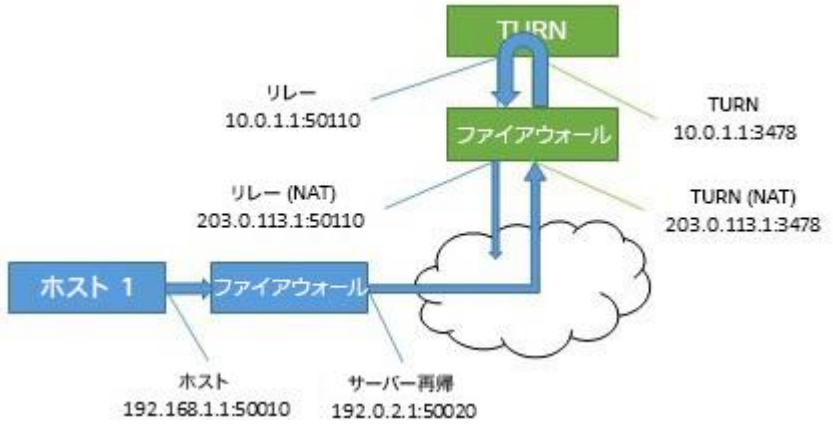
このリレーアドレスに送信されたデータは、TURN サーバを介してホストに送り返されます。

図 29：TURN サーバーがホストにリレーアドレスを返す



このリレー候補は 2 回使用されています。ホストはパケットを遠端に送信するためにも使用できます。これは、他にパスがない場合に発生します。これらのパケットは TURN サーバそのものから送信される形式なので、ファイアウォールで書き換えた場合にのみ NAT アドレスが取得されますので、注意してください。

図 30：遠端へパケットを送信するホスト



G.2 接続の確認

候補が既知の場合は、接続性チェックが実行されます。各ホストは、遠端のホスト、サーバー再帰、およびリレーアドレスに直接接続します。また、リレーを使用して、同じ遠端候補への接続を試行します。

表 27：2 つのホストの候補（同じ TURN サーバーを使用）

ホスト	タイプ	アドレス：ポート
1	ホスト	192.168.1.1:50010
1	サーバー再帰	192.0.2.1:50020
1	リレー	203.0.113.1:50110
2	ホスト	172.16.1.1:50100
2	サーバー再帰	198.51.100.1:50040
2	リレー	203.0.113.1:50510

表 28：ホスト 1 によって形成された候補ペア

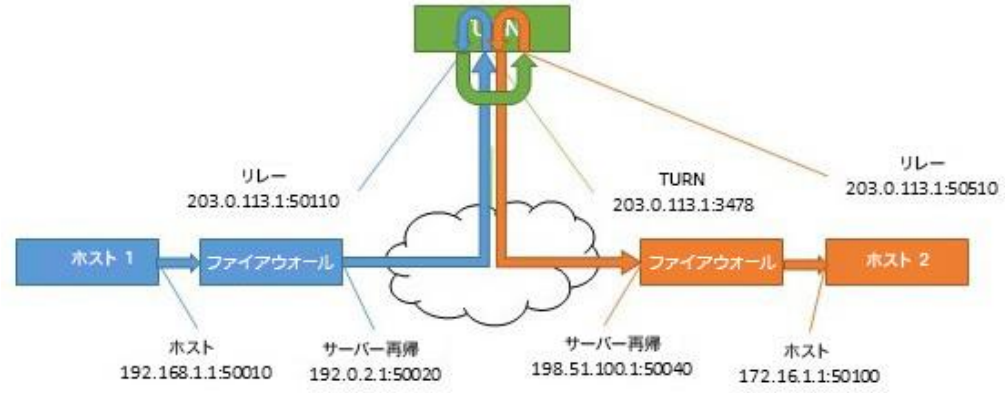
送信元	接続先タイプ	接続先アドレス
ホスト（192.168.1.1:50010）	ホスト	172.16.1.1:50100
ホスト（192.168.1.1:50010）	サーバー再帰	198.51.100.1:50040
ホスト（192.168.1.1:50010）	リレー	203.0.113.1:50510
リレー（10.0.1.1:50110）	ホスト	172.16.1.1:50100

送信元	接続先タイプ	接続先アドレス
リレー（10.0.1.1:50110）	サーバー再帰	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。たとえば、コーヒーショップやホテルにいるユーザは、値の大きいポートに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している場合は、両方のリレー候補を含むパスを作成できます。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フローアウトしてから、遠端に転送されます。

図 31：リレー間のパスを使用したホスト間のメディアパス（NAT なし）



G.3 TURN サーバーの正面にある NAT

TURN サーバの正面に NAT が存在する場合、フローが複雑になります。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必要があります。パケットが TURN サーバ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書き換えられていない場合、不明なアドレスから送信されているように表示されます。これにより、接続性チェックが必ず回避され、他のパスが利用できない場合には、メディアが使用できるルートはありません。

図 32：リレー間のパスを使用したホスト間のメディアパス（NAT あり）

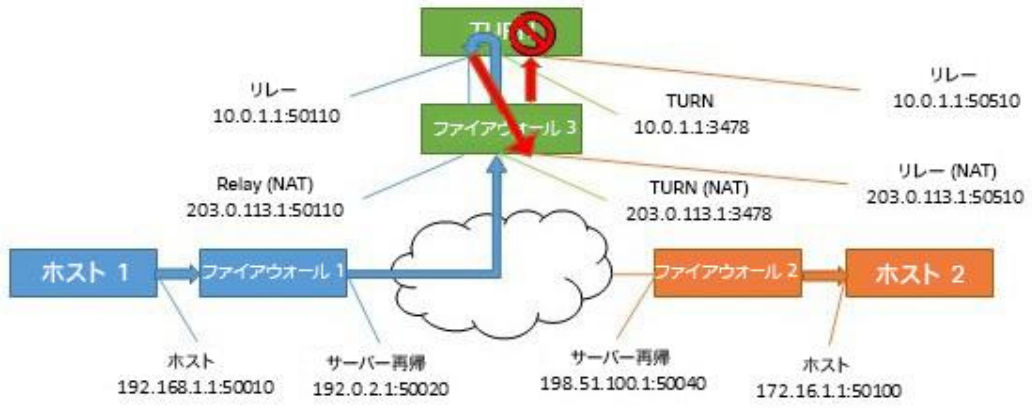


表 29：リレー間のパスを使用したホスト間のメディアパス（NAT あり）

送信元アドレス（パケット内）	宛先	接続先でのアクション
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換えます
192.0.2.1:50020	203.0.113.1:3478	ファイアウォール 3 は接続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 サーバーは内部でこれをこの送信元のリレーアドレスにマップし、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	ファイアウォール 3 が接続先アドレスを書き換えます
10.0.1.1:50110	10.0.1.1:50510	TURN サーバーに予期せぬ送信元アドレスが表示され、トラフィックがドロップされます。

この解決策は、ヘアピン NAT、ループバック NAT、NAT 反射と呼ばれる方法です。この場合、トラフィックの送信元アドレスと接続先が書き換えられます。次に、送信元アドレスはファイアウォールのアドレスです。これは、候補の 1 つと一致します。

表 30：リレー間のパスを使用したホスト間のメディアパス（ヘアピン NAT あり）

送信元アドレス（パケット内）	宛先	接続先でのアクション
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換えます
192.0.2.1:50020	203.0.113.1:3478	ファイアウォール 3 は接続先アドレスを書き換え、TURN サーバーに転送します。

送信元アドレス（パケット内）	宛先	接続先でのアクション
192.0.2.1:50020	10.0.1.1:3478	TURN サーバーは内部でこれをこの送信元のリレーアドレスにマップし、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	ファイアウォール 3 は、送信元アドレスと宛先アドレスの両方を書き換えます。
203.0.113.1:50110	10.0.1.1:50510	TURN サーバーは、リレーからのトラフィックを割り当てられたホストに内部でマップします。
10.0.1.1:3478	198.51.100.1:50040 ファイアウォール経由	ファイアウォール 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	ファイアウォール 2 が接続先アドレスを書き換えます。
203.0.113.1:3478	172.16.1.1:50100	最終的な宛先に到着します。

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マニュアルを参照してください。

付録 H スタンバイの Meeting Server の使用

この付録の手順は、Cisco Meeting Server 1000 など仮想化された展開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 や PuTTY などの SSH ユーティリティを使用して、現在使用されている 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。

   backup snapshot <name>

   このバックアップには、<name>.bak という名前のファイルに IP アドレス、パスワード、および証明書が含まれます。servername_date の形式で名前を使用することを推奨します（test_server_2014_09_04 など）。

   バックアップの作成に成功すると、次のように返されます。

   cms> backup snapshot test_server_2014_09_04.bak ready for download
3. SFTP クライアント（WinSCP など）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 のバックアップのコピーは 1 日に 1 回など、定期的にバックアップを作成し、バックアップを外部の Meeting Server とスタンバイサーバーに保存することを推奨します。

H.2 スタンバイサーバーへのバックアップの転送

スタンバイ サーバは常に稼働し続け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は、すべての証明書とスタンバイサーバーから cms.lic ファイルをコピーします。安全な場所に保存してください。
2. スタンバイ サーバとの SFTP 接続を確立します。
3. 以前に保存したバックアップ ファイルをスタンバイ サーバにアップロードします。
4. MMP backup list 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。次のように返されます。

   cms> backup list test_server_2014_09_
5. 次のコマンドを入力して、バックアップ ファイルからの復元を確認します。

   backup rollback <name>

   既存の構成が上書きされ、Meeting Server が再起動します。そのため、警告メッセージが表示されます。確認は大文字と小文字が区別され、大文字の **Y** を押す必要があります。押さない場合は操作が中断されます。

注：あるタイプの展開環境からバックアップを作成し、その他のタイプにロールバックすることはできません（たとえば、仮想化された Meeting Server 1000 から Meeting Server 2000 にロールバックはできません。その逆もできません）。

操作に成功すると、次のように返されます。

```
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...
```

スマートライセンスユーザーにのみ関連：バックアップから復元すると、IP アドレスや証明書など、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サーバーと別のサーバーに復元する場合は、新しいサーバーで無効な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 サーバとの SFTP 接続を確立します。
2. 必要な場合：
   a. 証明書および秘密キーを元の場所に戻します（復元されたバージョンがスタンバイサーバーで無効な場合）。
   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します。

      callbridge restart
      webbridge3 restart
      webadmin restart

新しいサーバは、完全に起動すると完全な稼働状態になり、元のサーバのサービスを引き継ぎます。

付録 I Web 管理インターフェイス：構成メニューのオプション

Call Bridge の Web 管理インターフェイスの[設定（Configuration）]タブでは、次のオプションを設定できます。

- 全般
- Active Directory
- 通話設定
- 発信コールと着信コール
- CDR 設定
- スペース
- API

I.1 [全般（General）]

[設定（Configuration）] > [全般（General）] ページを使用して、設定と構成を行います。

- TURN サーバーの設定。Call Bridge と外部クライアントが TURN サーバーにアクセスを許可するには、次の設定を使用します。「*TURN サーバー用の Web 管理インターフェイス設定*」を参照してください。MMP コマンドを使用して、TURN サーバー自体を構成します。「MMP の構成」を参照してください。
- Lync Edge の設定。Call Bridge と Lync Edge を統合する場合は、これらの設定を使用します。「Lync Edge を使用する Meeting Server の構成」を参照してください。
- IVR。自動音声応答（IVR）を使用して事前設定されたコールに手動でルーティングする場合は、これらの設定を使用します。そのため、発信者は事前録画された音声メッセージによって、参加するコールまたはスペースの ID 番号を入力するように案内されます。「IVR 構成」を参照してください。

I.2 Active Directory

ユーザーが Web アプリケーションを使用して Meeting Server に接続する場合は、LDAP サーバーが必要です。Meeting Server は、LDAP サーバからユーザ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）を使用することもできますが、API を介して構成する必要があります。Web Admin インターフェイスを介して構成できません。

[設定（Configuration）] >[Active Directory] ページを使用して、Active Directory と動作する Meeting Server を設定します。「LDAP 設定」を参照してください。

I.3 コール設定

[設定（Configuration）] > [コール設定（Call settings）] ページで、次の設定を行います。

- SIP コール（Lync を含む）のメディア暗号化を許可します。
- SIP コールに参加者ラベルオーバーレイを表示するかどうかを指定します。
- 発信オーディオパケットの優先サイズ（ミリ秒単位）を 10ms、20ms、または 40ms で指定します。
- TIP サポートを有効にします（Cisco CTS 範囲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します。これが prohibited に設定されている場合、コンテンツチャネルビデオや BFCP 機能は遠端に一切提供されません。
- プレゼンテーション ビデオ チャネルの操作が SIP コールに対して許可されている場合、この設定によって Call Bridge の BFCP 動作が決定します。次のいずれかの操作を実行します。
    - サーバー の役割のみ：これは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）で使用することを目的としています。
      または
    - サーバーとクライアントの役割：このオプションにより、Call Bridge はリモートデバイスとのコールで BFCP クライアントまたは BFCP サーバーモードで動作できます。

  この設定により、リモート会議ホスティング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 コールのリソース優先順位ヘッダーフィールドの値を設定します。この設定では、プレゼンに帯域幅を割り当てる優先順位を Meeting Server に指示します。これは、ネットワーク環境の帯域幅の機能や、HD をプッシュするイマーシブシステムなど、その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。次のいずれかを設定します。
    - disabled|enabled：SIP over TCP を使用するか、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は無効にします。
    - 有効にな単一アドレスモードは 2.2 より前のバージョンの SIP over UDP 動作に対応し、デフォルトです。

  - enabled, multi address：Call Bridge が複数のインターフェイスでリッスンするように構成されている場合に使用します。
- Lync プレゼンスサポートを有効にします。この設定により、この Call Bridge が、Lync プレゼンスサブスクライバに役立つ接続先 URI に関する情報を提供す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 default に設定されたままにします。Cisco サポートから指示されていない限り、設定を delay 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、個々のフィールドごとに表示されるホバーオーバー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。

また、[コール設定（Call settings）]ページでは、SIP、Cisco Meeting Server（Web アプリ）、サーバー再帰、リレー、VPN、および Lync コンテンツの帯域幅の設定を変更できます。設定はビット/秒で測定されます（たとえば、2000000 は 2Mbps）。音声には少なくとも 64kbps を指定します。720p30 コールには 2Mbps、1080p30 コールには約 3.5Mbps を推奨します。60fps にはより多くの帯域幅が必要です。

SIP メディア暗号化を許可する場合や、TIP サポートを有効にする場合など、帯域幅の設定の一部を変更する必要がある場合があります。3 画面の TIP コールの場合、[コール設定（Call settings）]ページで表示される帯域幅の番号は自動的に 3 倍になります。そのため、手動で 6Mbps に設定する必要はありません。ただし、通常、ほとんどの CTS コールには（3 倍）4Mbps を推奨します。

I.4 発信コールと着信コール

[設定（Configuration）] > [発信コール/着信コール（Outbound calls / Incoming calls）]ページを使用して、Meeting Server が各コールを処理する方法を決定します。

[発信コール（Outbound calls）]ページは、発信コールの処理方法を制御します。[着信コール（Incoming calls）]ページでは、着信コールが拒否されたのか、一致したのか、転送されたのかを決定します。一致して転送される場合は、転送する方法に関する情報が必要です。[着信コール（Incoming calls）]ページには、一致/拒否を設定する表と、転送動作を構成する表の 2 つがあります。

これらのフィールドの入力方法の詳細については、 *コールを処理する Web 管理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（Configuration）] > [CDR 設定（CDR settings）]ページで、CDR 受信者の URI を入力します。

Meeting Server では、サーバー側で接続される新しい SIP 接続や、アクティブ化または非アクティブ化されたコールなど、重要なコール関連イベントに関するコール詳細レコード（CDR）が内部で生成されます。この 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構成できます。Meeting Server にはレコードを長期間保存したり、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の入力方法の詳細については、「コール詳細レコードのサポート」および『コール 詳細レコードガイド』を参照してください。

また、API を使用して、Meeting Server を、CDR 受信者の URI で構成することもできます。『API リファレンスガイド』を参照してください。

I.6 Spaces

[設定（Configuration）] > [スペース（Spaces）]ページを使用して、ダイヤルするスペースを Meeting Server 上に作成します。これにより、エンドポイントや Web アプリなどへのダイヤルインが可能になります。

スペースを、以下を指定して追加します。

- 名前（例： **Call 001**
- URI（例：）**88001**）

このページでは、セカンダリ URI のユーザー部分、コール ID、パスコード、デフォルトレイアウトをオプションで指定することもできます。

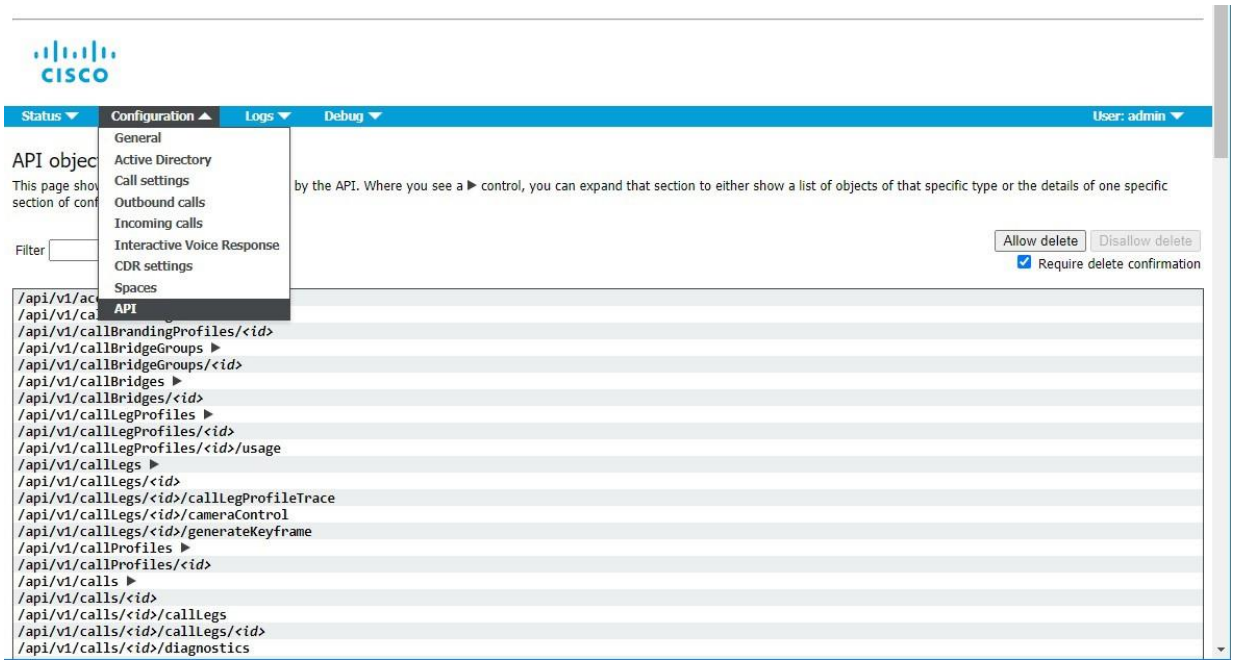
API を使用してスペースを作成することもできます。『API リファレンスガイド』を参照してください。

注：コール ID パラメータ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 以降、API メソッドやサードパーティ製アプリケーションではなく、Meeting Server Web 管理インターフェイスを使用して API にアクセスできます。Web 管理インターフェイスにログインした後、[設定（Configuration）]タブに移動し、プルダウンリストから[API]を選択します。 図 33 を参照してください。

図 33：Meeting Server Web 管理インターフェイスを介した API へのアクセス



注：Web インターフェイスから API にアクセスするには、サードパーティ製アプリケーションを使用する場合のように、MMP を使用して Meeting Server の構成設定および認証を実行する必要があります。

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表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されており、これらは、参考資料によって本書に含まれています。添付されていない場合には、代理店にご連絡ください。

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

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

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

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

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