

# Cisco Meeting Server

Cisco Meeting Server リリース 3.11

スケーラビリティとレジリエンスサーバー導入ガイド

2025 年 6 月 25 日

# コンテンツ

新機能 .....	11
1 はじめに .....	12
1.1 Meeting Server がホストする会議に参加するためのサポート対象アプリ .....	14
1.2 Meeting Server の導入で Cisco Expressway-E を Edge デバイス として使用する .....	15
1.3 コアネットワークで Meeting Server と Cisco Expressway-C を使用する .....	16
1.3.1 Call Bridge グループの Expressway サポート .....	16
1.3.2 Cisco Expressway H.323 ゲートウェイコンポーネントを使用する .....	17
1.4 Meeting Server の導入で Meeting Server を Edge デバイスとして使用する .....	17
1.5 このガイドの使い方 .....	18
1.5.1 コマンド .....	20
1.6 Meeting Server を設定する .....	20
1.6.1 MMP および API インターフェイス .....	21
1.6.2 Meeting Server の設定を容易にする新しいツール .....	21
1.7 Meeting Server のライセンス .....	24
1.7.1 ライセンスが必要な機能 .....	24
1.7.2 Smart Licensing .....	25
1.7.3 スマートアカウントおよびバーチャルアカウント情報 .....	26
2 展開の一般的なコンセプト .....	27
2.1 Web 管理 .....	28
2.2 Call Bridge .....	29
2.3 データベース .....	29
2.4 Web Bridge 3 .....	29
2.5 TURN サーバ .....	30
2.6 Meeting Server Edge .....	31
2.7 ミーティングの録画 .....	31
2.7.1 録画のライセンスキー .....	32
2.8 ミーティングのストリーミング .....	32
2.8.1 ストリーミングのライセンスキー .....	32
2.9 ブランディング ファイルをローカルにホストする .....	33
2.10 オンスクリーンメッセージ .....	33
2.11 SIP トランクとルーティング .....	33
2.12 Lync および Skype for Business のサポート .....	34

2.12.1	Lync および Skype for Business クライアントのサポート .....	34
2.12.2	デュアルホーム会議のサポート .....	34
2.13	ウェブスケジューラ .....	35
2.13.1	ウェブ アプリ UI のスケジューラ .....	35
2.14	スケーラビリティとレジリエンスに関する一般的なポイント .....	36
2.14.1	複数の「統合」サーバーの使用例 .....	36
2.14.2	データベースのクラスタリング .....	39
3	前提条件 .....	42
3.1	Meeting Serverのインストールと設定の前提条件 .....	42
3.1.1	DNS 設定 .....	42
3.1.2	セキュリティ証明書 .....	42
3.1.3	ファイアウォールの構成 .....	42
3.1.4	Syslog サーバ .....	42
3.1.5	Network Time Protocol サーバ .....	44
3.1.6	通話詳細記録のサポート .....	44
3.1.7	ホスト名 .....	45
3.1.8	その他の要件 .....	45
3.1.9	仮想化導入の特定の前提条件 .....	46
3.2	Meeting Serverの Edge ハードウェア構成 .....	46
3.2.1	Edge サーバの設定 .....	46
3.2.2	導入の考慮事項 .....	48
3.3	Meeting Server Edge のネットワーク計画 .....	49
3.3.1	技術的な説明 .....	49
3.3.2	ネットワークの計画 .....	50
3.3.3	Meeting Server ウェブエッジを導入する .....	54
4	MMP の設定 .....	56
4.1	MMP およびウェブ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 .....	56
4.2	ソフトウェアをアップグレードする .....	56
4.3	Call Bridge リッスン インターフェイスの設定 .....	58
4.4	HTTPS アクセスのためのWeb 管理インタフェースの設定 .....	59
4.5	ステージ Edge サーバインスタンス .....	60
4.6	Web Bridge 3 を設定する .....	61
4.6.1	Web Bridge 3 の設定に役立つ情報 .....	61
4.6.2	Web Bridge 3 サービスを有効にする .....	63

4.6.3	CallブリッジのC2W接続を設定する.....	64
4.6.4	Web Bridge アドレスを使用して Call Bridge を設定する.....	65
4.7	TURN Server の設定.....	66
4.7.1	TURN サービスを有効にする.....	67
4.7.2	TURN アドレスを使用して Call Bridge を設定する.....	68
4.8	MMP ユーザーのLDAP 認証.....	70
5	データベースの設定.....	71
5.1	別のサーバー上にあるデータベース.....	72
5.1.1	別のサーバ上のデータベースの要件.....	72
5.1.2	別のサーバーにデータベースを展開する.....	72
5.2	データベースと Call Bridge サーバーへの証明書の展開と検証.....	72
5.3	クラスタのプライマリデータベースを選択する.....	74
5.4	他のデータベースインスタンスをデータベースクラスタに添付する.....	76
5.5	データベースクラスタにリモート Call Bridge を接続する.....	79
5.6	データベーススキーマをアップグレードする.....	80
5.7	データベースクラスタに関する詳細情報.....	81
6	Call Bridge の展開.....	82
6.1	Call Bridge の証明書の設定.....	82
6.2	Call Bridge のセットアップ.....	82
6.3	Call Bridge のクラスタリング.....	83
6.3.1	Call Bridge クラスタの検証.....	85
6.3.2	クラスタ化された Call Bridge 展開での DTMF シーケンスの使用.....	86
6.4	ダイヤルプラン情報.....	86
6.4.1	相互ピア通話のダイヤル プラン ルールを設定する.....	87
6.4.2	例.....	88
6.5	Meeting Server 間のコールのロードバランシング.....	89
6.5.1	Call Bridge グループ.....	90
6.5.2	着信通話を負荷分散するための Call Bridge の設定.....	91
6.5.3	発信 SIP 通話の負荷分散.....	94
6.5.4	ウェブアプリの呼び出しを負荷分散する.....	96
6.6	Lync アカウント情報.....	97
6.7	参加者を Lync 電話会議に接続するための Call Bridge モードを選択する.....	97
7	Web Bridge 3 を導入する.....	102
7.1	複数の Web Bridge 3 を展開する.....	102

7.2	Web Bridge 3 証明書をセットアップする .....	102
7.3	Web Bridge 3 をセットアップする .....	102
7.3.1	Web Bridge プロファイルを作成して適用する方法の例 .....	103
7.4	Web Bridge 3 の通話フロー .....	106
7.5	ウェブアプリ情報 .....	107
7.6	HTTP リダイレクトとWeb Bridge 3 を有効にする .....	108
8	TURN サーバーを導入する .....	109
8.1	TURN サーバーの設定 .....	109
9	分散導入のウェブアプリ .....	111
10	ダイヤル プランの構成 – 概要 .....	115
10.1	はじめに .....	115
10.2	着信通話と発信通話のダイヤル プラン ルール。 .....	117
10.2.1	/outboundDialPlanRules .....	117
10.2.2	/inboundDialPlanRules .....	120
10.2.3	/forwardingDialPlanRules .....	121
10.3	ダイヤル変換 .....	123
11	ダイヤル プランの構成 - SIP エンドポイント .....	125
11.1	はじめに .....	125
11.2	クラスタ化されたMeeting Serverで主催されているミーティングに ダイヤルする SIP ビデオエンドポイント .....	125
11.2.1	SIP コール制御の構成 .....	125
11.2.2	Meeting Serverの設定 .....	126
11.3	SIP 通話のメディア暗号化 .....	128
11.4	TIP サポートを有効にする .....	129
11.5	IVR 設定 .....	129
11.6	次のステップ .....	130
12	ダイヤル プランの構成 – Lync/Skype for Business の統合 .....	131
12.1	Lync クライアントがクラスタ化されたMeeting Server上の通話に ダイヤルインする .....	131
12.1.1	Lync フロントエンドサーバーの構成 .....	132
12.1.2	クラスタ化されたMeeting Serverにダイヤルプランルール を追加する .....	134
12.2	SIP エンドポイントと Lync クライアントの統合 .....	135
12.3	Lync クライアントと SIP ビデオエンドポイント間の通話を追加する .....	136

12.3.1	Lync フロントエンドサーバーの構成 .....	137
12.3.2	VCS 構成 .....	137
12.3.3	Meeting Serverの設定 .....	137
12.4	Lync Edge サービスを使用した Lync の統合 .....	140
12.4.1	Lync Edge 通話フロー .....	140
12.4.2	Lync Edge を使用するためのMeeting Serverの構成 .....	141
12.5	Microsoft Lync および Skype for Business 通話で共有コンテンツの 帯域幅を制御する .....	143
12.6	Lync 直接フェデレーション .....	144
12.7	スケジュール済みの Lync ミーティングに直接または IVR 経由で発信する .....	145
13	OBTP スケジュールでの Office 365 デュアル ホーム エクスペリエンス .....	148
13.1	概要 .....	148
13.2	構成 .....	148
13.3	会議中の体験 .....	149
14	Web Bridge 3 の設定 .....	150
14.1	Web Bridge 3 接続 .....	150
14.1.1	Web Bridge 3 の通話フロー .....	150
14.2	Web Bridge 3 の設定 .....	152
14.2.1	Web Bridge プロファイルを作成して適用する方法の例 .....	152
15	ミーティングの録画とストリーミング .....	155
15.1	新しい内部 SIP レコーダーとストリーマの機能の利点 .....	155
15.2	新しい内部 SIP レコーダーとストリーマを実装する際の注意事項 .....	155
15.3	録画の概要 .....	156
15.3.1	サードパーティの外部 SIP レコーダーのサポート .....	157
15.3.2	Meeting Server内部 SIP レコーダーコンポーネントのサポート .....	157
15.3.3	スケーラビリティとレジリエンスのためのレコーダー/ ストリーマを導入する .....	159
15.4	新しい内部 SIP レコーダー コンポーネントを VM サーバーに導入する例 .....	160
15.5	外部のサードパーティ SIP レコーダーの設定 .....	163
15.6	レコーディングの状況を確認する .....	164
15.7	デュアル ホーム会議の録画インジケータ .....	164
15.8	Vbrick で録画する .....	165
15.8.1	Meeting Serverの前提条件 .....	165
15.8.2	Vbrick で動作するようにMeeting Serverを設定する .....	166

15.9	ミーティングのストリーミング .....	168
15.10	VM サーバーに新しい SIP ストリーマ コンポーネントを展開する .....	169
15.10.1	既知の制限事項 .....	172
16	LDAP 設定 .....	173
16.1	LDAP を使用する理由は何ですか? .....	173
16.2	Meeting Server の設定 .....	173
16.3	例 .....	177
16.4	LDAP フィールド マッピングの詳細 .....	178
16.5	すべてのユーザスペースへの非メンバーアクセスにパスコード 保護を適用する .....	179
17	Cisco Meeting Server web app のシングルサインオン (SSO) .....	180
17.1	Meeting Server web app で使用する SSO を設定する .....	180
17.1.1	例 1 config.json ファイル .....	184
17.1.2	例 2 単純なサービスプロバイダメタデータファイル .....	185
17.1.3	例 3 詳細なサービスプロバイダメタデータファイル .....	185
18	ActiveControl のサポート .....	187
18.1	Meeting Server の ActiveControl .....	187
18.2	制約事項 .....	187
18.3	ActiveControl と iX プロトコルの概要 .....	187
18.4	SIP 通話内の UDT を無効にする .....	188
18.5	Cisco Unified Communications Manager で iX サポートを有効にする .....	188
18.6	Cisco VCS で iX をフィルタリングする .....	189
18.7	iX のトラブルシューティング .....	190
19	スケジューラ - 導入 .....	191
19.1	スケジューラを導入する .....	192
20	セキュリティに関するその他の考慮事項と QoS .....	195
20.1	Common Access Card (CAC) 統合 .....	195
20.2	Online Certificate Status Protocol (OCSP) .....	195
20.3	FIPS .....	195
20.4	TLS 証明書の検証 .....	196
20.5	ユーザ コントロール .....	196
20.6	ファイアウォールルール .....	196
20.7	DSCP .....	197
20.8	SSH 指紋を確認する .....	197

21 問題をトラブルシューティングするのに役立つ Cisco サポートの診断ツール.....	198
21.1 SIP トレース .....	198
21.2 ログバンドル.....	198
21.3 特定のコールレグのキーフレームを生成する機能.....	199
21.4 syslog に登録されたメディアモジュールを報告する .....	200
22 追加のライセンス情報.....	201
22.1 ライセンス .....	201
22.1.1 Meeting Server でのスマートライセンスの仕組み - 概要 .....	201
22.1.2 期限切れライセンス機能の強制アクション .....	203
22.1.3 ライセンス情報を取得する方法 (Smart Licensing) .....	204
22.1.4 Smart Licensing 登録プロセス .....	205
22.1.5 マルチパーティライセンス .....	206
22.1.6 ユーザーに Personal Multiparty ライセンスを指定する .....	207
22.1.7 Cisco Multiparty ライセンスの割り当て方法 .....	207
22.1.8 Cisco Multiparty ライセンスの使用状況を確認する.....	208
22.1.9 SMP Plus ライセンスの使用数を計算する .....	208
22.1.10 ミーティングサーバーからライセンス使用状況のスナップショット を取得する .....	209
22.1.11 ライセンスレポート .....	209
22.1.12 レガシーライセンスファイルによる方法.....	209
23 ホストされた会議の情報を取得する .....	211
23.1 コール詳細レコード (CDR) .....	211
23.2 イベント .....	211
付録 A 導入に必要な DNS レコード .....	213
付録 B 導入に必要なポート .....	216
B.1 Meeting Server を設定する .....	217
B.2 サービスへの接続.....	217
B.3 Meeting Serverのコンポーネントを使用する .....	218
B.4 スケーラビリティとレジリエンスに必要な追加ポート .....	221
B.5 ループバック上の開放ポート .....	222
付録 C クラスタ内で Call Bridge ライセンスを共有する .....	224
C.1 Cisco Meeting Serverのアクティベーション PAK コードの登録.....	224
C.1.1 クラスタ全体で機能ライセンスを共有する .....	225

C.2 既存の Call Bridge クラスタへのライセンスの追加.....	229
付録 D クラスタリング解除.....	230
D.1 Call Bridge のアンクラスタリング .....	230
付録 E Cisco Meeting Server プラットフォーム別の通話容量.....	231
E.1 Cisco Meeting Server web app のコールキャパシティ .....	233
E.1.1 Cisco Meeting Server web app のコールキャパシティ - 外線通話.....	233
E.1.2 Cisco Meeting Server web app の容量 - 混合（内部 + 外部）通話.....	233
E.2 Cisco Meeting Server でサポートされるユーザー数.....	234
付録 F 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 .....	235
F.1 非暗号化 SIP メディア モード.....	235
F.2 Call Bridge メディア モードの決定 .....	236
付録 G デュアルホーム電話会議.....	237
G.1 概要 .....	237
G.2 デュアルホーム会議での一貫したミーティング エクスペリエンス.....	237
G.2.1 ユーザエクスペリエンスの要約.....	238
G.3 デュアルホーム会議のミーティングコントロールをミュート/ ミュート解除する .....	239
G.4 デュアルホームの Lync 機能の設定.....	240
G.4.1 トラブルシューティング.....	241
付録 H NAT の背後で TURN サーバーを使用する .....	242
H.1 候補を特定する .....	242
H.1.1 ホスト候補.....	242
H.1.2 サーバリフレキシブ候補.....	242
H.1.3 リレー候補.....	243
H.2 接続を確認しています .....	245
H.3 TURN サーバーの前の NAT.....	246
付録 I ウェブ管理インタフェース - 設定メニューオプション.....	249
I.1 全般 .....	249
I.2 Active Directory.....	249
I.3 通話設定.....	250
I.4 発信通話と着信通話.....	251
I.5 CDR 設定 .....	251
I.6 スペース.....	252

I.7 クラスタ.....	252
I.8 API.....	252
付録 J API の例.....	254
J.1 クラスタ内の特定の Call Bridge のための発信ダイヤルプランルー ルを作成する.....	254
J.2 Meeting ServerにWeb Bridgeを設定する.....	255
J.3 Call Bridge 上に Web Bridge のカスタマイズを作成する.....	256
J.4 TURN サーバーをセットアップして Call Bridge に接続する.....	257
J.5 スペースを作成してメンバーを追加する.....	257
J.5.1 スペースにメンバーを追加する.....	258
J.6 コールレグ プロファイルの作成.....	259
J.7 アクセス方法をスペースに適用する.....	260
Cisco の法的情報.....	262
Cisco の商標または登録商標.....	263

# 新機能

バージョン	変更内容 (Change)
	バージョン 3.11 で更新

# 1 はじめに

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

---

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

---

このガイドでは、スケーラブルでレジリエントなソリューションとして導入される Meeting Server について説明します。このタイプのアーキテクチャを導入するための概念、要件、および方法について説明します。複数のホストサーバーを導入することで、以下を設定できます。

- 同じタイプの複数のコンポーネントが 1 つのレジリエントな「ユニット」として機能します。例えば、Call Bridge がクラスタリングされている場合、1 つの Call Bridge がダウンした場合であっても、他の Call Bridge でミーティングを開催できます。
- スケーラビリティ（容量の増加）。例えば、すべての参加者をホストするのに十分な容量がない場合、1 つのミーティングを複数の Call Bridge に分散してホストできます。（原則として、可能な場合、各ミーティングは単一の Call Bridge で主催されます）。
- 効率性。Meeting Server は、効果的かつ効率的なミーティングを提供するためにどのコンポーネントを使用するかを決定します。例えば、異なる場所からミーティングにコールする参加者は、よりシンプルなデプロイメントのユーザーエクスペリエンスを維持しながら、異なるコンポーネントを使用できます。
- 各 Meeting Server はすべてのコンポーネントをホストすることも（「組み合わせ導入」）、Edge または Core サーバー（「分割導入」の一部）をホストすることもできます。

---

**注：** 展開内のすべての Meeting Server は、同じバージョンのソフトウェアを実行している必要があります。

---

**メモ：** Meeting Server 3.0 では Cisco Meeting Management 3.0（またはそれ以降）が必須となりました。Meeting Management は、Smart Licensing サポートのための製品の登録とスマートアカウント（セットアップされている場合）との対話を処理します。Smart Licensing の詳細については、「Cisco ライセンス」を参照してください。

---

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

Meeting Server Web エッジ ソリューションの展開の詳細については、「開発の 基本概念」を参照してください。

図 1 は統合型サーバ展開で利用できるコンポーネントを示しています。レコーダー、アップローダー、ストリーマの各コンポーネントは、ミーティングを主催するサーバとは別のサーバで有効にする必要があります Cisco Meeting Server 2000 の概略図は、Cisco Expressway が TURN サービスを提供することを想定しています。

図 1 : 統合サーバの導入

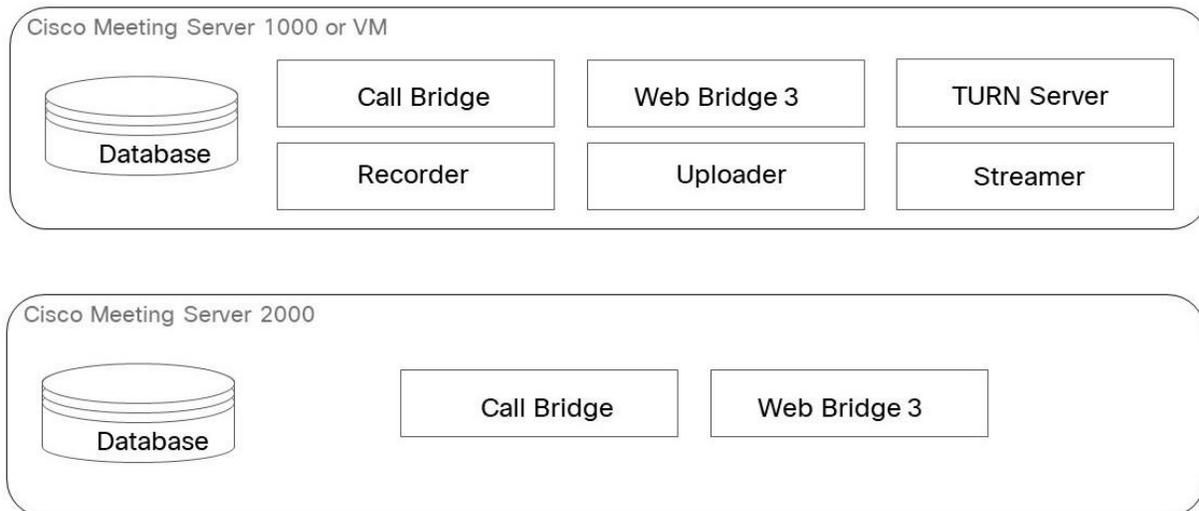


図 2 および図 3 は分割サーバ導入で利用できるコンポーネントを示しています。図 2 は、Cisco Expressway により提供される TURN サービスを示します。図 3 は、Meeting Server の TURN サーバコンポーネントを使用して Meeting Server により提供される TURN サービスを示します。Meeting Server で TURN サーバコンポーネントが有効な場合、Web Bridge 3 は Edge サーバに移動することに注意してください。レコーダー、アップローダ、ストリーマの各コンポーネントは、ミーティングを主催するとは別コアサーバのサーバで有効にする必要があります。

図 2 : TURN サービスを提供する Cisco Expressway での分割サーバ展開

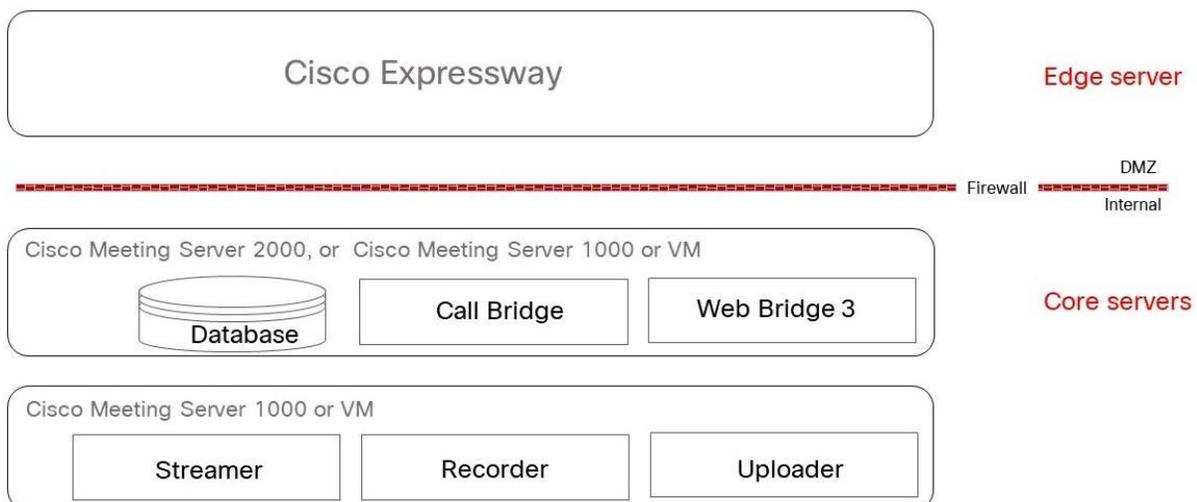
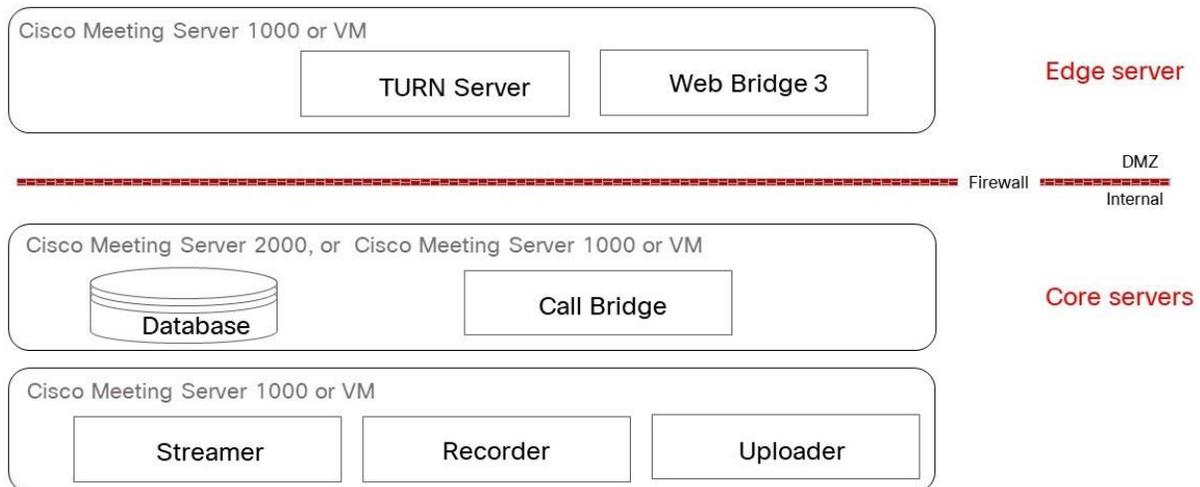


図 3 に示すように、エッジサーバーとして使用する場合、Meeting Server は既存の TURN サーバーとウェブアプリコンポーネント（Call Bridge コンポーネントではなく）を使用します。

図 3 : TURN サービスを提供する Cisco Meeting Server による分割サーバー導入



これらのコンポーネントのすべてを設定する必要はありません。導入に適したコンポーネントを設定するだけで十分です。これについては、「デプロイメントの一般的な概念」で説明します。

**重要情報：**バージョン 3.0 から、XMPP サーバ、ロードバランサー、SIP Edge および H.323 ゲートウェイのコンポーネントが Cisco Meeting Server ソフトウェアから削除されました。さらに、新しい SIP レコーダーおよびストリーマーコンポーネントは、サーバーソフトウェアから削除された以前の XMPP クライアントバージョンのレコーダーおよびストリーマーに置き換わるものです。TURN サーバーはバージョン 3.0 ソフトウェアのままで、ブラウザベースの Cisco Meeting Server web app を Meeting Server 電話会議に接続するために使用される場合があります。ネイティブおよびブラウザベースの Cisco ミーティングアプリクライアントはバージョン 3.0 ではサポートされていません。

## 1.1 Meeting Server がホストする会議に参加するためのサポート

### 対象アプリ

Meeting Server が主催する会議に参加するためのサポートされているアプリは、Cisco Meeting Server web app と Cisco Jabber です。これは、SIP エンドポイントとデュアル ホーム会議の Lync/Skype for Business クライアントに加えたものです。

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

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

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

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

---

### 警告 : Expressway ユーザーのための重要な注意点

Web Bridge 3 およびウェブ アプリを展開する場合、Expressway バージョン X14.3 以降を使用する必要があります。以前のバージョンの Expressway は Web Bridge 3 ではサポートされていません。

---

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

---

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

---

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

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

Edge 機能	このガイドで説明されている構成
リモートブラウザベースの Meeting Server web app を接続する	<a href="#">Cisco Meeting Server 用 Cisco Expressway ウェブプロキシ 導入ガイド</a>

---

Edge 機能	このガイドで説明されている構成
リモートの Lync および Skype for Business クライアントを接続する	<a href="#">Cisco Expressway 対応 Cisco Meeting Server 導入ガイド</a>
SIP レジストラまたは内部コール制御プラットフォームへの登録をプロキシする	<a href="#">Cisco Expressway-E および Expressway-C Basic 構成 (X14.3)</a>

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

Cisco Expressway-E バージョン	Edge 機能	Meeting Server のバージョン
X14.3	Cisco Meeting Server web app をサポートしています。 <a href="#">Cisco Meeting Server (X14.3) 用 Cisco Expressway ウェブプロキシ</a> を参照してください。	3.8 以降

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

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

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

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

機能	このガイドで説明されている設定
クラスター化された Meeting Server の負荷を分散する通話コントロールデバイス	<a href="#">Cisco Meeting Server による Cisco Meeting Servers 間の通話のロードバランシング</a>
SIP レジストラ	<a href="#">Cisco Expressway-E および Expressway-C Basic 構成 (X14.3)</a>
H.323 ゲートキーパー	<a href="#">Cisco Expressway-E および Expressway-C Basic 構成 (X14.3)</a>

### 1.3.1 Call Bridge グループの Expressway サポート

X8.11 以降のソフトウェアを実行している Cisco Expressway は、クラスタ化された Call Bridge 間で着信および発信通話の負荷分散をサポートする Call Bridge グループをサポートし

ています。ロードバランシングは、単一の電話会議をできるだけ少数の Call Bridge に配置することで実現します。これにより、電話会議で参加者を接続するために必要な配信リンクの数が減るため、Meeting Server 全体の負荷が軽減されます。詳細については、[セクション 6.5](#) を参照してください。

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

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

Expressway-E または Expressway-C に登録された H.323 エンドポイントは、Expressway バージョン X8.10 以降から Cisco Meeting Server にコールインする際に、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。

## 1.4 Meeting Server の導入で Meeting Server を Edge デバイスとして使用する

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

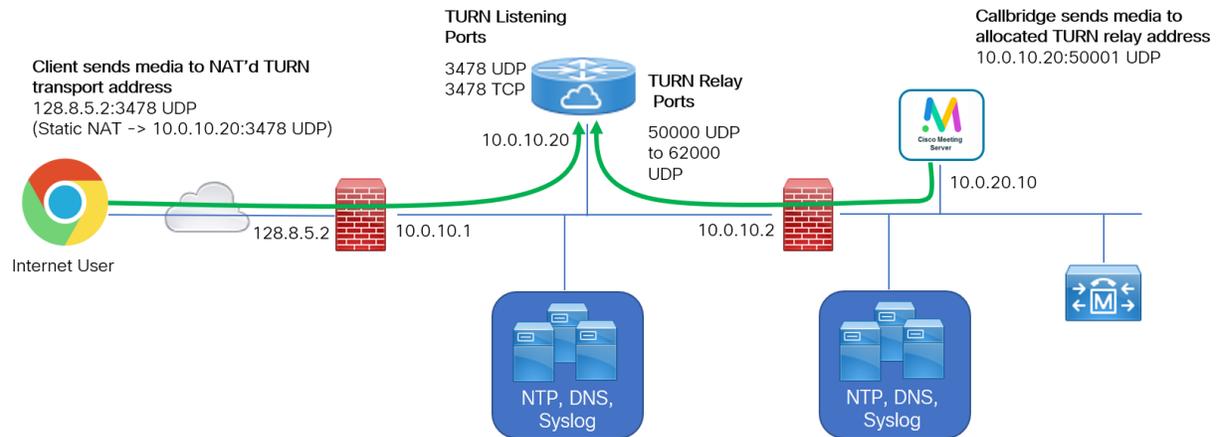
ウェブアプリケーションの接続は、Call Bridge を TLS を使用して Web Bridge の C2W インターフェイスに発信接続させ、Web Bridge 機能のためにコアと Edge の間で安全なコントロールチャンネルを確立することで実現します。外部ブラウザ クライアントは、HTTPS を使用して Edge の Web Bridge に接続します。

外部ウェブアプリケーションのメディアトラフィックは、Meeting Server の TURN サーバーを通じた TURN リレーセットアップを使用して処理されます。Web Bridge に接続して確認されると、ウェブクライアントは TURN サーバーのリスニングポートに接続し、TURN サーバーのインターフェイスで自分に割り当てられるリレー トランスポート アドレスをリクエストします。ICE を使用して、クライアントと Call Bridge はこのリレーを介してお互いにトラフィックを送信できることを確認します。結果として得られたリレーにより、両当事者はネットワーク境界を越えてメディアを送受信できます。

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

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

図 4 : Meeting Server Edge TURN サーバーの例



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

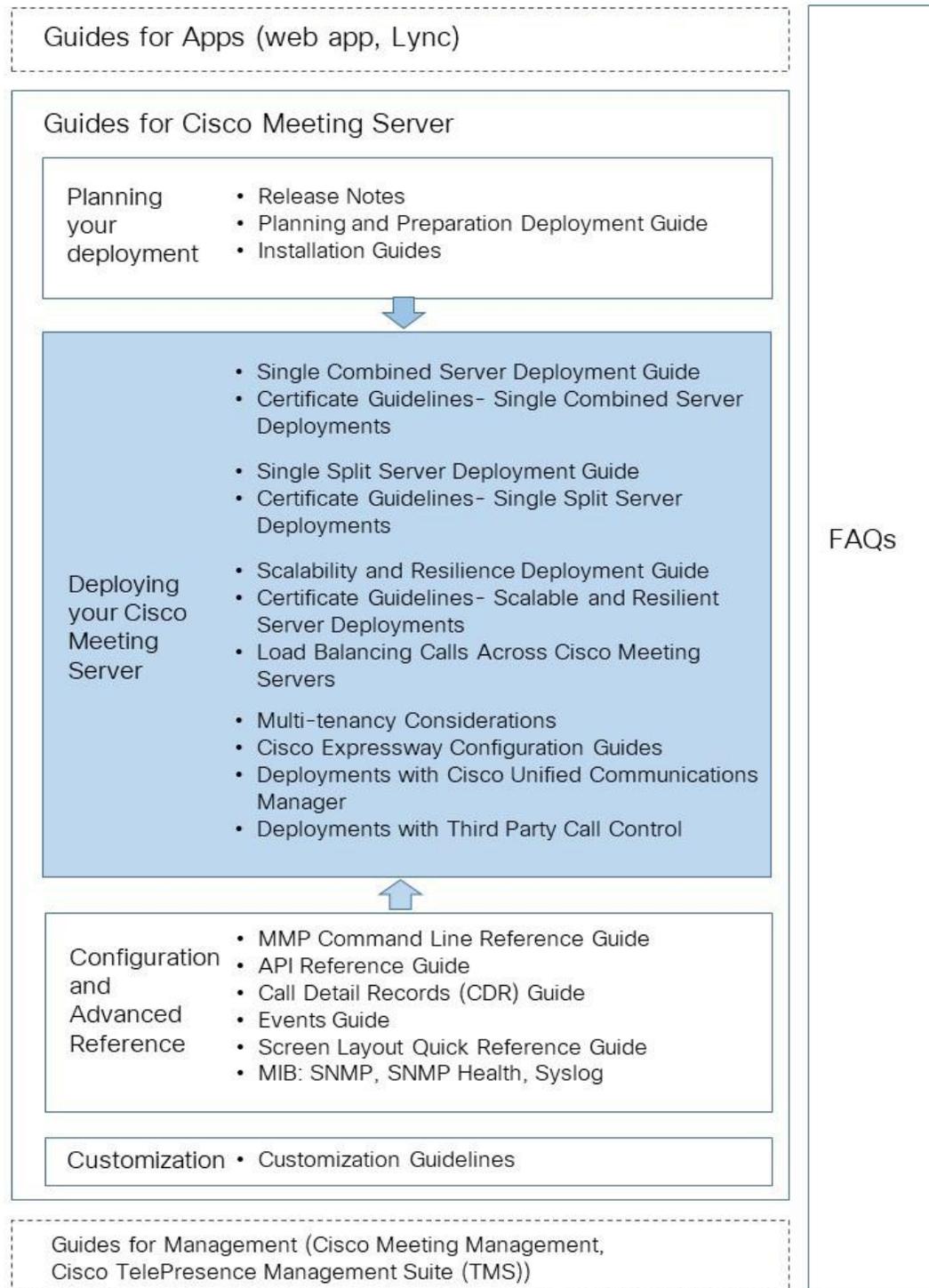
## 1.5 このガイドの使い方

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

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

**注 :** このガイドでは、coSpace をスペースと記載しています。

図 5 : Meeting Serverに関するガイドの概要



---

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

---

### 1.5.1 コマンド

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

## 1.6 Meeting Server を設定する

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

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

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

## 1.6.1 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の MMP および API 用に設定されたネットワークインターフェイス

Platform	MMP へのアクセス	ウェブ管理インターフェイスおよび API へのアクセス
Cisco Meeting Server 2000	ブレード 1 で Serial over LAN SoL 接続。 注 : MMP にアクセスする前に、Fabric Interconnect モジュールのネットワーク設定を構成する必要があります。	MMP の構成中に作成されたインターフェイス A。これは、Fabric Interconnect モジュールのポート 1 で構成されたアップリンクを介して外部ネットワークに接続される仮想接続です。 注 : Cisco Meeting Server 2000 プラットフォームは、複数のインターフェイスをサポートしていません (つまり、「ipv4 b c」の設定)。(「 d」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デプロイメント	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 ウェブ管理インターフェイスと API は、A-D イーサネットインターフェイスのいずれか 1 つで実行するように設定できます。

## 1.6.2 Meeting Server の設定を容易にする新しいツール

管理者が Meeting Server を設定および展開するために役立つ以下のツールが利用できます :

- [インストールアシスタント](#) デモンストレーション、ラボ環境用の、または基本インストールの開始点として、簡単な Cisco Meeting Server インストールの作成を簡素化します。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。ミーティング管理と統合されており、ミーティング管理 UI から使用できます。
- [「Cisco Meeting Management 経由で Cisco Meeting Server web app ユーザーをプロビジョニングする」](#) は、バージョン 2.9 以降で利用できます。
- [Meeting Server のウェブインタフェースを通じた API アクセス](#)。バージョン 2.9 から、Meeting Server ウェブ管理インタフェースの **設定** タブから Meeting Server API にアクセスできます。このガイドに記載されているいくつかの例が、API メソッドの POST および PUT から、ウェブインタフェースを通じた API アクセスの使用に変更されています。

### インストール アシスタント ツール

インストールアシスタントを使用すると、デモンストレーション、ラボ環境向けに、または基本インストールの開始点として、単一の Cisco Meeting Server インストールの作成を簡素化できます。このツールは、『[Cisco Meeting Server Single Server Simplified Deployment ガイド](#)』に記載されている **ベスト プラクティスの展開に基づいて Meeting Server を構成します**。バージョン 3.3 以降、ミーティング管理と統合され、セットアップに関する情報を収集し、その構成をサーバーにプッシュします。API、SFTP、または Meeting Server のコマンドライン インターフェイスにアクセスするためのユーティリティを使用する必要はありません。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用の

ソフトウェア要件、ソフトウェアのインストールと実行の詳細、および Meeting Server の設定手順については、『[ミーティング管理インストールガイド](#)』を参照してください。

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

インストールアシスタントは、空の、未設定の Meeting Server での使用を想定しています。Meeting Server の管理ツールではありません。また、既存の Meeting Server の再設定を行うためのツールでもありません。このツールは、Meeting Server 仮想マシンの設定専用構築されています。Cisco Meeting Server 2000 プラットフォームでは使用できません。

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

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

LDAP サーバを Meeting Server クラスタに接続する方法、1 つ以上のユーザ 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する方法、最後に LDAP 同期を実行する方法については、『[Cisco Meeting Management ユーザ ガイド \(管理者用\)](#)』を参照してください。

## ウェブ インターフェイスでの API アクセス

図 6 で示されている通り、サードパーティアプリを必要とせずに Call Bridge API の使用を簡素化するために、バージョン 2.9 では、Meeting Server の Web インターフェイスの [設定 (Configuration)] タブ経由でアクセスできる Call Bridge API のユーザーインターフェイスが導入されました。

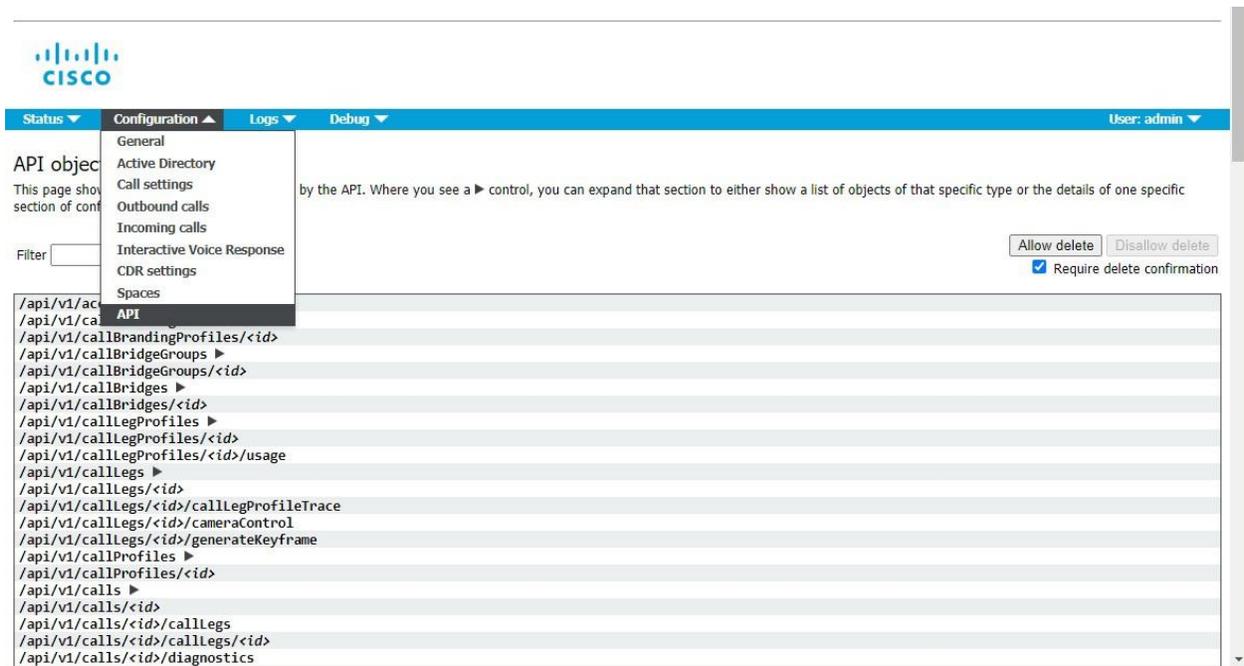
バージョン 3.3 で導入されたスケジューラ API はこのインターフェイス経由ではサポートされていません。「[スケジューラ API](#)」を参照してください。

---

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

---

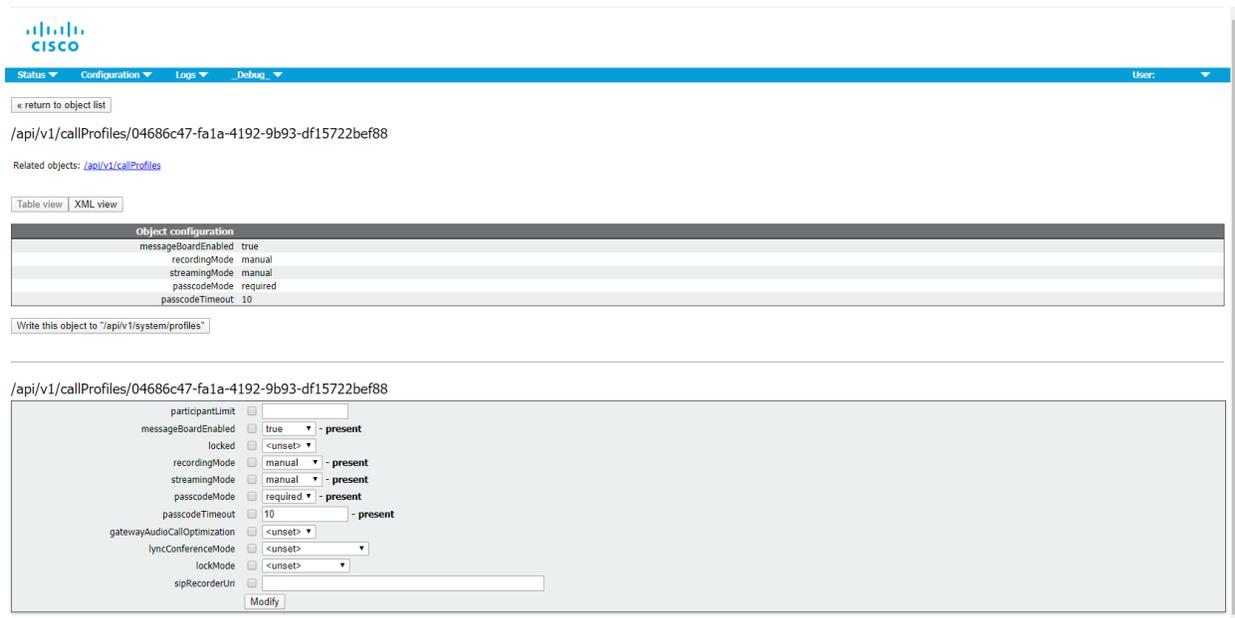
図 6 : ミーティング Server Web インターフェイス経由で Call Bridge API にアクセスする



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

Web インタフェース経由で API を使用すると、より視覚的なアプローチで Meeting Server を設定するためのユーザーフレンドリーな方法が提供されます。たとえば、図 7 に示すチェックボックスとフィールドを使用して、callProfiles の設定を行うことができます。

図 7 : Web インターフェイスで API アクセスを使用して callProfiles を設定する



## 1.7 Meeting Serverのライセンス

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

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

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

### 1.7.1 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)
- 録画またはストリーミング
- ミーティング参加者のスナップショット

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

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

詳細は [マルチパーティライセンス](#) を参照してください。

---

**注：** Cisco ミーティング管理では、ライセンスなしでトライアルモードを 90 日間のフル機能で使用できます。

---

### 1.7.2 Smart Licensing

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

---

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

---

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

詳細およびスマートアカウントの作成については、<https://software.cisco.com> に移動して Smart Licensing を選択してください。

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

- Cisco Meeting Management バージョン 3.0（またはそれ以降）はバージョン 3.0 で必須です。ミーティング管理は Meeting Server ライセンスファイルを読み取り、製品の登録とスマートアカウント（セットアップされている場合）との対話を処理します。
- スマートアカウントの 1 セットの Meeting Server ライセンスで複数のクラスタのライセンスを取得できるようになり、3.0 以前の場合のように、個々の Meeting Server インスタンスにライセンスファイルをロードする必要がなくなりました。
- Smart Licensing を含むミーティング管理は、クラスタごとに Call Bridge の数を追跡するため、R-CMS-K9 アクティベーション ライセンスの必要性を排除します。

- 既存のライセンスを持たない新規展開の場合：
  - 新しく購入したライセンスは、デフォルトで Smart が有効になっており、スマートアカウントを必要とする場合があります。ライセンスの詳細をミーティング管理に入力すると、スマートアカウントに保持されているものに対してライセンスの詳細が検証されます。
- 各 Call Bridge にローカルライセンスファイルがある既存の展開の場合：
  - Cisco Smart Software Manager (CSSM) ポータル を使用してスマートアカウントに移行し、既存のライセンスをスマートに変換するオプションを選択できます。
- SMP Plus および PMP Plus ライセンスの使用数が組み合わせられて、日を超過使用数としてカウントされるかどうか決定されます（いずれかのライセンスが期限切れの場合、1日は使用資格の超過使用数とみなされます）。他の機能ライセンス（例えば、録画またはカスタムレイアウト）については、個別に評価され、Meeting Management 経由で権限付与で有効化されます（ライセンスがスマートアカウントに存在すると想定）。

---

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

---



---

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

---

### 1.7.3 スマートアカウントおよびバーチャルアカウント情報

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

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

- 単一のミーティング管理に対する各 Meeting Server クラスタは、ユーザー定義のスマートバーチャルアカウントにリンクされている必要があります。
- 各バーチャルアカウントは、Smart Licensing を処理するように設定された単一のミーティング管理サーバーのみに接続できます。
- 1つのミーティング管理のみをスマートに設定します。Smart Licensing の 2 つ目の冗長ミーティング管理を Smart に設定しないでください。ライセンス使用数の二重カウントが発生するため、お勧めしません。
- PMP Plus、SMP Plus、および録画/ストリーミングライセンスは、単一のバーチャルアカウント内の単一のミーティング管理インスタンスおよび Smart Licensing を使用して、複数のクラスターにわたって共有できます。
- ACU ライセンスはミーティング管理ライセンスダッシュボードでは利用できません。ACU は 3.0 以降ではサポートされていません。

ライセンスの詳細は、[追加のライセンス情報をご覧ください](#)。

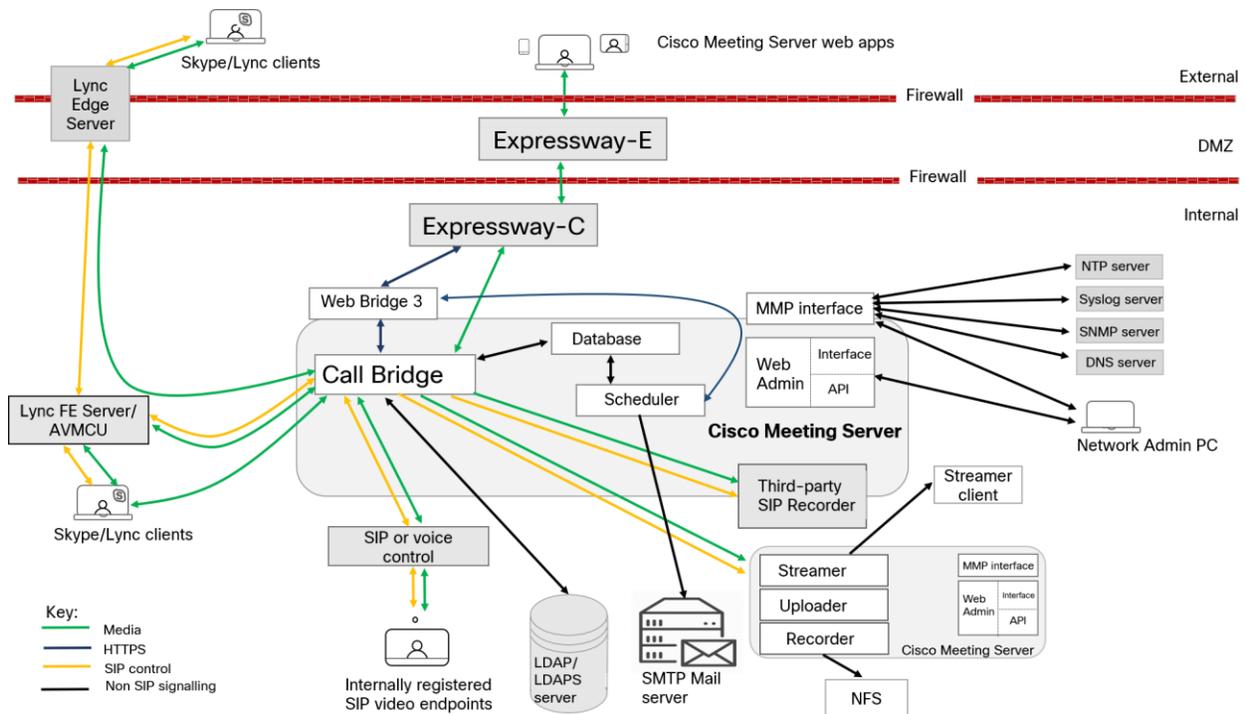
## 2 展開の一般的なコンセプト

この章では、スケーラブルでレジリエントなサーバー導入における Meeting Server の一般的な概念について説明します。図 8 と 図 9 は一般的な展開を示しています。

**注：**導入内のすべての Meeting Server は、同じバージョンのソフトウェアを実行している必要があります。

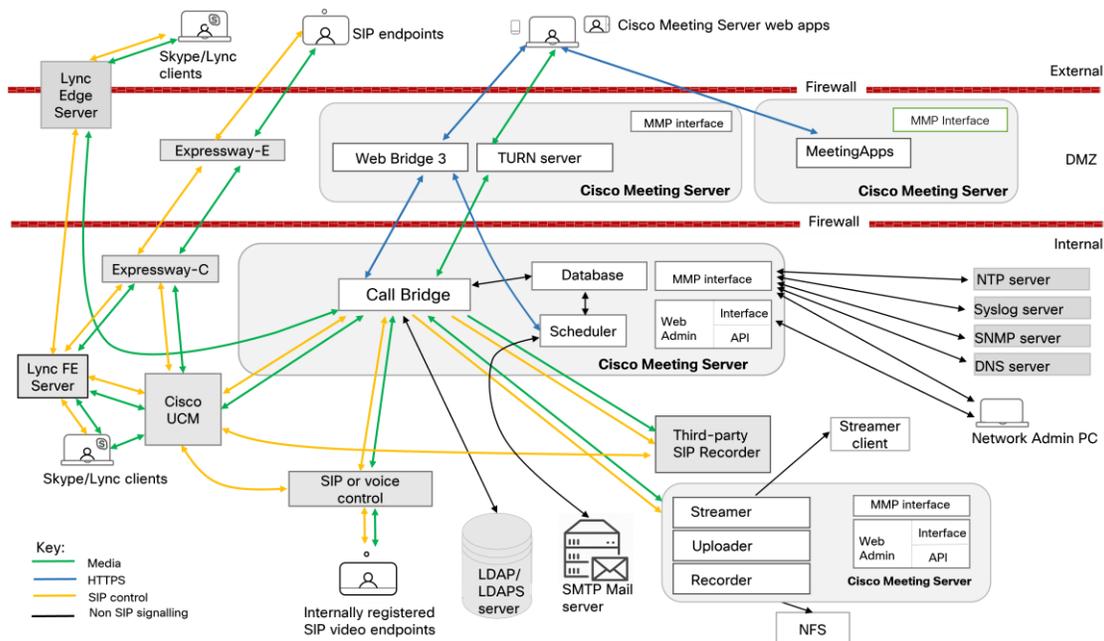
Expressway (大規模 OVA または CE1200) は、中規模のウェブアプリのスケール要件を持つ導入 (つまり、800 コール以下) に推奨されるソリューションです。Expressway (中規模 OVA) は、小規模なウェブアプリスケール要件を持つ導入 (つまり、200 コール以下) に推奨されるソリューションです。しかし、より大きなウェブアプリスケールを必要とする導入では、バージョン 3.1 以降、必須のソリューションとして Cisco Meeting Server ウェブエッジを推奨します。

図 8 : エッジでの Cisco Expressway による Meeting Server の導入の例



在宅勤務の需要が高まり、ウェブアプリのスケールが増大するにつれて、Cisco Meeting Server バージョン 3.1 がこの増大するウェブアプリのスケールにエッジサポートを提供するために開発およびテストされました。図 9 は、Meeting Server のウェブエッジソリューションを導入し、より大規模なウェブアプリの導入に最適化する方法の例を示しています。

図 9 : 分割サーバ展開での TURN サーバコンポーネントを使用した Meeting Server 展開の例



## 注：

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

## 2.1 Web 管理

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

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

ウェブ管理は、Meeting Serverの管理者ウェブページを提供することに加えて、Meeting Serverの REST API のインタフェースも提供します。REST API は、Postman または ChromePoster などの従来の REST ツールでアクセスできます。バージョン 2.9 以降、Web 管理インタフェースには、管理者が API エクスプローラーインタフェースを使用して作業できる機能が含まれています。

追加のツールやソフトウェアなしで Meeting Server API を使用できます。API リファレンスガイドは [ここ](#) から参照できます。

## 2.2 Call Bridge

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

スケーラブルでレジリエントな導入では、Call Bridge をクラスタ化して、複数の Call Bridge を単一のエンティティとして動作させ、単一の Call Bridge のキャパシティを超えてスケールすることができます。クラスタ内の Call Bridge は、ピアツーピアにリンクするか、クラスタ化された Call Bridge 間のコール制御デバイス経由で通話をルーティングするように設定できます。詳細については、[クラスタリング コールブリッジのセクションを参照してください](#)。

---

**注：**Lync（または Skype for Business）と SIP 間のゲートウェイ通話が主な導入では、単一のスタンドアロン Call Bridge を使用して通話をプロキシすることをお勧めします。これは、Lync FE が 1 つの Call Bridge のみを使用し、複数の Call Bridge のラウンドロビンを実装しないことが原因です。

---

## 2.3 データベース

Call Bridge は、スペースのメンバーやスペース内での最近のアクティビティなど、スペース情報を保存するデータベースの読み取りと書き込みを行います。

スケーラブルでレジリエントな導入では、データベースを Call Bridge からデタッチし、別のコンポーネントとして実行できます。それは Call Bridge と同じサーバーに保持することも、別のサーバーに保持することもできます。データベースの複数のインスタンスは、展開で復元性を提供するために一緒にクラスタ化することができます。データベースのクラスタリングについては、[第 5 章](#) を参照してください。

## 2.4 Web Bridge 3

Web Bridge 3 は、参加者がブラウザベースの Cisco ウェブアプリクライアントを使ってミーティングに参加できるようにする Meeting Server のコンポーネントです。Web Bridge 3 は Cisco Meeting Server web app の参加者にウェブサーバーを提供し、Call Bridge および TURN サーバーコンポーネントと連携してクライアントをサポートします。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はバージョン 3.0 で削除されました。デスクトップおよび iOS 用の Cisco Meeting App もサポートが終了し、Cisco Meeting Server web app に置き換えられています。

---

**注：**ウェブアプリを使用していない場合、Web Bridge 3 を展開する必要はありません。

---

ウェブアプリを使用している場合（つまり、Web Bridge 3 を導入している場合）、[Cisco Meeting Server ウェブアプリの重要な情報](#) を参照してください。そこには、機能がリリースされるタイミングやウェブアプリの問題が解決されるタイミングの詳細が記載されています。

ブアプリに関連するすべての情報はこの別のドキュメントに含まれており、Meeting Serverのリリースノートには含まれていません。

「重要な情報」ガイドには次の内容が記載されています。

- ウェブアプリの新機能または変更された機能、ウェブアプリに関連する解決済みの問題と未解決の問題の詳細と、この機能/修正が利用可能なMeeting Serverのバージョン。
- ウェブ アプリに影響を与えるブラウザの今後の変更、および影響を受けるウェブ アプリのバージョンと推奨される回避策。

---

**注意：** Web Bridge 2 から Web Bridge 3 への自動アップグレード移行はありません。Web Bridge 3 バージョン 2.9 をすでに導入している場合は、アップグレード後に設定を確認する必要があります。それらはWeb Adminや古い設定から移行されません。  
/webBridges/<webbridge id>.

---

## 2.5 TURN サーバ

TURN サーバはファイアウォール トラバース技術を提供するため、Meeting Server をファイアウォールまたは NAT の背後に導入することができます。外部ウェブアプリユーザーまたは SIP エンドポイントから導入に接続するには、TURN サーバを有効にする必要があります。

「[TURN サーバの導入](#)」の項を参照してください。ウェブ アプリを使用している場合は、ウェブ管理インターフェイスを設定して、Call Bridge と外部クライアントが TURN サーバにアクセスできるようにする必要があります。TURN サーバの使用にライセンスは必要ありません。

TURN サーバは、Call Bridge からの UDP 接続をポート 3478 でリッスンし、リモート接続にも使用できます。

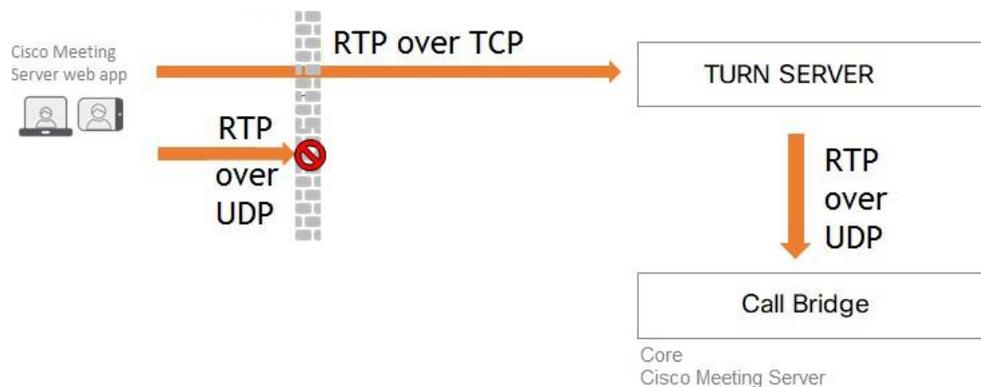
TURN サーバは、クライアント接続からの TCP の 2 番目のポートでリッスンすることもできます。通常は 443 です ('turn tls <port>' 設定が必要です)。

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

ファイアウォール ルールが Call Bridge から TURN サーバへの UDP ポート 3478 を許可していることを確認します。

TCP で送信されるメディアは SRTP を使用して暗号化されます。TURN サーバは TCP から UDP へのインターワーキングをサポートしています (図 10 参照)。ブラウザは TCP メディアを TURN サーバに送信し、TURN サーバがそれを標準の UDP メディアに変換します。これは、ブラウザからの UDP トラフィックがブロックされている場合に役立ちます。

図 10 : TCP および UDP をサポートする TURN サーバ



TURN サーバーのデフォルト構成が変更されました。変更が展開にどのように影響するかは、統合サーバまたは分割サーバを展開しているかによって異なります。

- 統合サーバ展開の TURN サーバーは、ループバックインターフェースでリスンするように設定する必要があります。詳細は [セクション 4](#) を参照してください。
- 分割サーバ導入の TURN サーバーは、Call Bridge からの TCP 通信を、以前のリリースのポート 443 ではなく、ポート 3478 でリスンするようになりました。[UDP 3478 および TCP 3478 ポートをファイアウォールで開く](#) 必要があります。

## 2.6 Meeting Server Edge

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

## 2.7 ミーティングの録画

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

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

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

ミーティングの録画の詳細については、次を参照してください。[セクション 15](#)。

### 2.7.1 録画のライセンスキー

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

## 2.8 ミーティングのストリーミング

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

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

---

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

---

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

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

### 2.8.1 ストリーミングのライセンスキー

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

## 2.9 ブランディング ファイルをローカルにホストする

ブランディングファイルの 1 セットは、Meeting Server上でローカルに保持できます。ローカルでホストされているこれらのブランディング ファイルは、Meeting Serverが稼働状態になると、Call Bridge およびWeb Bridgeで使用できるようになり、ウェブ サーバーの問題が原因でカスタマイズを適用する際に遅延が生じるリスクを排除します。画像と音声のプロンプトが、Meeting Serverソフトウェアに組み込まれた同等のファイルに置き換わります。起動時に、これらのブランディングファイルが検出され、デフォルトファイルの代わりに使用されます。ローカルでホストされているブランディングファイルは、ウェブサーバからのリモートブランディングによって上書きされます。

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

---

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

---

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

## 2.10 オンスクリーンメッセージ

Meeting Serverは、Meeting Serverで主催されるミーティングの参加者に画面上にテキストメッセージを表示する機能を提供します。一度に 1 つのメッセージしか表示できません。API を使用して、メッセージが表示される継続時間を設定するか、新しいメッセージが設定されるまで永久的にすることができます。API オブジェクト/calls 用に、`messageText`、`messagePosition`、`messageDuration` パラメータを使用します。

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

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

## 2.11 SIP トランクとルーティング

Meeting Serverは、SIP 通話コントロール、音声通話コントロール、および Lync フロントエンド (FE) サーバーの 1 つ以上から SIP トランクをセットアップする必要があります。相互運用のためにWeb Bridgeサービスを必要とする Meeting Serverに通話をルーティングするには、これらのデバイスでの通話ルーティング設定の変更が必要です。

## 2.12 Lync および Skype for Business のサポート

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

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

Meeting Serverは以下を使用します。

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

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

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

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

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

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

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

デュアルホーム会議機能は、Meeting Server と Lync AVMCU の通信方法を改善し、Lync/Skype for Business と Cisco Meeting Server web app のユーザーの両方にとってより豊かなミーティングエクスペリエンスをもたらします。付録 G では、デュアルホーム会議について説明しています。

### 2.12.2 デュアルホーム会議のサポート

デュアルホーム会議では、電話会議のルックアップのために、Lync Edge サーバの設定を Meeting Serverで設定する必要があります。すでにオンプレミスの Lync 展開または Lync フェデレーションの展開が Meeting Serverの展開と連携している場合、

Meeting Serverでの追加設定は必要ありません。これが新規の導入である場合、Lync Edge サーバーを使用するためにMeeting Serverをセットアップする必要があります。[章](#)を参照してください。

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

- [Lync 参加者のミーティング体験の改善に関する FAQ。](#)
- [RDP サポートに関する FAQ。](#)
- [マルチプル ビデオ エンコードのサポートに関する FAQ。](#)

## 2.13 ウェブスケジューラ

スケジューラは、エンドユーザーがウェブ アプリ経由でミーティングをスケジュールできるようにするMeeting Server コンポーネントです。Meeting Server 1000、Meeting Server 2000、および VM 展開上のMeeting Serverでサポートされています。スペックベースの VM プラットフォーム上のMeeting Serverでは、スケジューラコンポーネントを実行するために、追加で 4 GB の RAM が必要です。Meeting Server 1000 および Meeting Server 2000 には、追加 RAM 要件はありません。スケジューラは、SMTP メールサーバーの設定により、メール通知の送信をサポートします。メールサーバーの設定の詳細については、[Cisco Meeting Server インストールガイドを参照してください。](#)

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

詳細については、[「スケジューラ - 展開」を参照してください。](#)

### 2.13.1 ウェブ アプリ UI のスケジューラ

- ミーティングをスケジュールするためのユーザ インターフェイスがウェブ アプリ ユーザーに表示されます。ただし、少なくとも 1 人のスケジューラがWeb Bridgeへの接続を確立している必要があります。スケジューラが有効になっていない場合、ウェブ アプリ ユーザーにはミーティングをスケジュールするためのユーザ インターフェイスは表示されません。
- 管理者が Call Bridge /Web Bridge API 経由でWeb Bridgeを追加、削除、または変更しても、スケジューラが自動的にこれらの変更を認識することはありません。そのため、スケジューラを再起動する必要があります。同様に、スケジューラが無効になっている場合、Web Bridgeはスケジューラが予期せぬ理由でダウンしているのではなく、意図的に無効になっているとは気づきません。スケジューラが管理者によって故意に無効にされた場合、Web Bridgeを再起動して、スケジューリングのユーザインターフェイスが表示されないようにすることをお勧めします。

- スケジューラが無効になっているか、または他の問題のためにダウンしている場合、Web Bridgeは別のスケジューラを使用します可能な場合。そうでない場合は、ウェブアプリ ユーザーにエラーが表示されます。

## 2.14 スケーラビリティとレジリエンスに関する一般的なポイント

---

**注：**この項の Web Bridge に関する言及は、Web Bridge 3 に適用されます。

---

スケーラビリティとレジリエンスのために、Meeting Server は以下で導入できます。

- 複数の結合サーバ (各サーバーで適切なコンポーネントが有効になっている)。これらのサーバーの場所は要件によって異なりますが、各ポイントオブプレゼンスに 1 台ずつ設置することもできます (必須ではありません)。

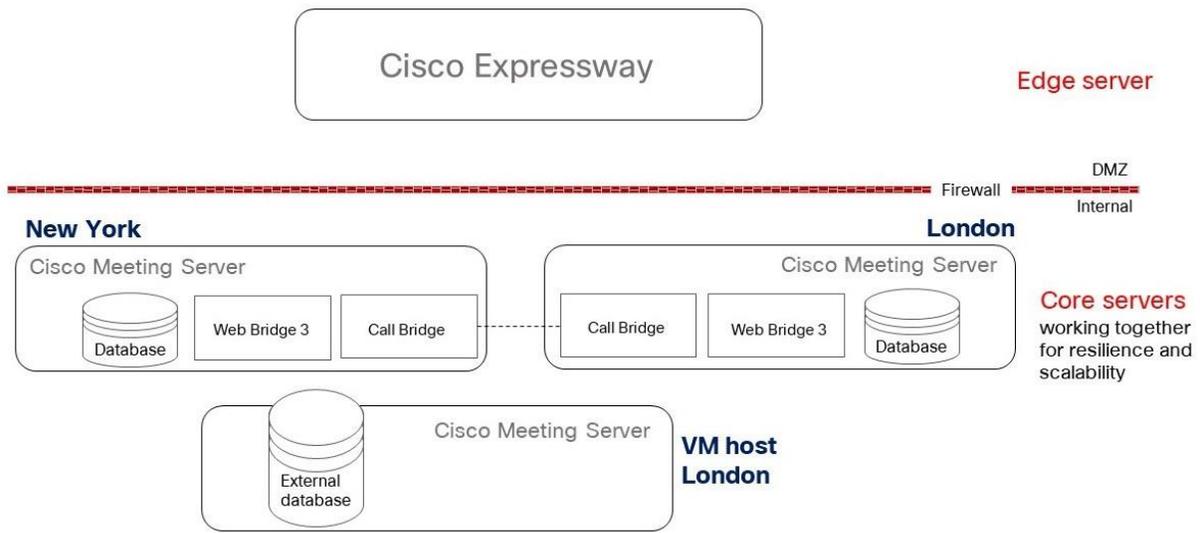
大規模な展開にスケールアップする場合、すべてのインスタンスですべてのコンポーネントを有効にする必要はありません (常に推奨されるわけではありません)。これについては後で詳しく説明します。

- 複数の Edge や Core サーバー (Edge サーバーではエッジコンポーネントが有効になり、Core サーバーではコアコンポーネントが有効になります。Call Bridge とデータベースは常にコアコンポーネントです)。これらの Edge および Core サーバーの場所は要件によって異なり、Core および Edge サーバーを同じデータセンター内に共存させることもできます (必須ではありません)。
- 大規模な分割導入では、Edge と Core のサーバーの数を同じにする必要はなく、むしろ望ましくない場合もあります。たとえば、1 つの Call Bridge で複数の Web Bridge を管理できます。これらの Web Bridge は、場合によっては複数の個別のユニットに解決する単一の DNS 名で外部から到達可能です。

### 2.14.1 複数の「統合」サーバーの使用例

Meeting Server を導入するトポロジは多数ありますが、簡単な例を以下に示します。これにより、単一のホスト サーバー ソリューションのレジリエンスと 2 倍のキャパシティが得られます。

図 11 : 最も単純なスケーラビリティとレジリエンスのある設定



この導入では、それぞれすべてのコンポーネントが有効になっている 2 つのホストサーバーと、仮想化 (VM) ホストの可能性が高いデータベースのみを持つ第 3 のホストサーバーが示されています。理想的には、この 3 番目のホストは、他のいずれかのサーバーとは別のサイトに配置されます。これにより、どちらかのサイトが完全に停止しても対応できます。データベース VM ホストの場合、以下を推奨します。

- ハイパースレッディングを有効にする
- デフォルトの ESXi システムパラメータを変更しない

**注：**レジリエンシーを高めるのではなく低下させるため、2 ノードのデータベースクラスタを作成しないでください。奇数のノードを使用すると、ネットワークがパーティション分割された場合のレジリエンシーが向上します。Cisco では、少なくとも 3 つのデータベースノードを実行することを推奨しています。

このような実装は以下を提供できます。

- 地理的な場所の考慮
  - レジリエンス (通話開始時にいずれか 1 つのコンポーネントが利用できない場合、その「パートナー」が使用されるため)
- 同様に、通話中にコンポーネントが利用できなくなった場合、コンポーネントを使用している PC/WebRTC クライアントからは通話が切断されます。参加者が再度発信すると、新しいルートで新しい通話が確立され、参加者は新しいルートに気づかずに再参加できます。
- 両方の Call Bridge をシームレスに使用して拡張する機能

### 図 11 の注意点：

- [セクション 5.3](#) で説明されているように、3 つのデータベースサーバーは MMP を使用してクラスタ化されます。クラスタ化されたデータベースのコンテンツが同期されます。
- 各データベースは、Call Bridge のあるサーバー（ほとんどの導入で推奨）と同じサーバー上、別個の仮想サーバー上、あるいは前の図に示したように、これらの組み合わせ上に置くことができます。

---

#### 注：

複数のコア サーバーを含む大規模な展開では、Call Bridge ごとにデータベース インスタンスを持つ必要はありません。プレゼンスのあるすべてのポイント (POP) に 1 つをお勧めします。（例えば、データベースはローカルのデータセンターに置き、物理的なアクセスは制御できるものの、世界中の Call Bridge が必要な場合があります。

---

- [「Call Bridge を展開する」](#) で説明されているように、2 つの Call Bridge はウェブ管理インターフェイスを使用してクラスタ化されます。さらに、他のホストサーバー上の Web Bridge 3 を認識しています。また、データベース クラスタに接続して読み書きを行います。

各 Call Bridge は、ホストしているコールレグの CDR を提供します。各 CDR はスペース ID を識別するため、同じスペース ID を持つ通話を収集することで、異なる Call Bridge 上の同じミーティングを識別することができます。

---

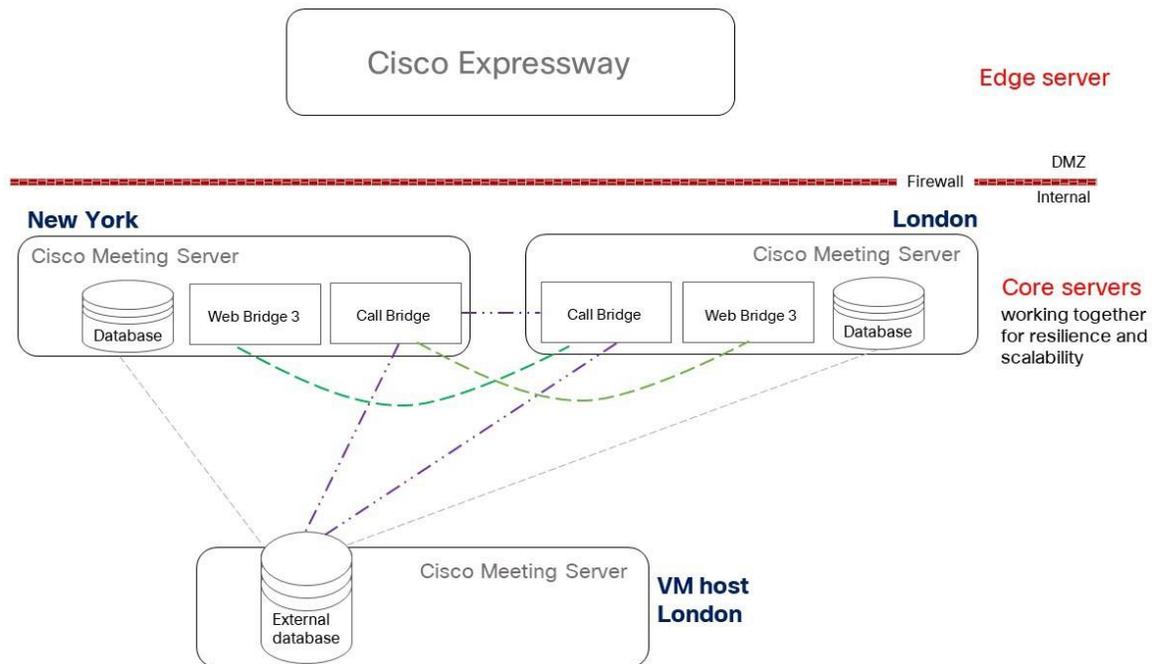
**注：**クラスタ化された Call Bridge は、クラスタ化されていない Call Bridge と同じデータベース（またはデータベースクラスタ）を使用できません。

---

- [付録 1.2](#) で説明されているように、2 つの Web Bridge は Web 管理インターフェイスから API 設定を使用して設定されます。
  - Web Bridge サービスは、単一の DNS A レコードを外部で持つように設定できます。ただし、Call Bridge に Web Bridge を設定する場合、Call Bridge に設定された各 Web Bridge に固有のホスト名または IP アドレスがなければなりません。これにより、各 Web Bridge が各 Call Bridge によって一意に識別できるようになります。

接続が表示される場合、図 11 は図 12 に変わります。

図 12 : 接続を示す単純な導入



### 2.14.2 データベースのクラスタリング

データベースクラスターに関する注意事項：

- データベースサーバー間、および Call Bridge とプライマリデータベース間のネットワーク遅延制限（またはラウンドトリップ時間）は 200 ms 以下です。
- データベース クラスター ピア間のすべてのデータベース間通信は、セキュリティのために SSL を介して処理されます。
- データベース クラスター内では、すべての Call Bridge は常に 1 つのデータベースのみを使用します。これは「プライマリ」データベースです。すべての読み取りと書き込みはこのデータベースインスタンスで実行されます。
- このプライマリデータベースのコンテンツは、レジリエンスのために「レプリケーション/ホットスタンバイ」に複製されます。これは、[第 5 章](#)の図に示されています。
- プライマリデータベースに障害が発生した場合、複製データベースが新しいプライマリに「昇格」し、他の複製は新しいプライマリデータベースに再登録されます。障害が修復されると、古いプライマリデータベースはそれ自体を複製物として指定し、新しいプライマリデータベースにも登録します。
  - プライマリデータベースの電源が落ちると、データベースは起動時にレプリカに戻ります。

- ・ プライマリデータベースとの間のすべてのネットワーク接続が失われると、接続が復元されたときにそのデータベースはレプリカになります。
- ネットワークパーティションが発生した場合、クラスター内の半数以上を認識できるデータベースのみが、プライマリデータベースへのプロモーション対象と見なされます。同様に、半数以上のデータベースクラスタを認識できない既存のプライマリは、レプリカに降格されます。これにより、複数のプライマリが作成されず、データベースのコンテンツがクラスター全体で一貫した状態に保たれます。
- ネットワークが分割され、半数を超えるサーバーが含まれる部分がない場合、その後、安全のため、データベースクラスタはプライマリデータベースが含まれない状態に戻ります。この状況は、クラスターに含まれるノードの数が偶数の場合、またはネットワークが3つ以上の切断された部分に分割されている場合にも発生します。

---

**警告：**プライマリデータベースを選択できない場合、システム管理者はクラスタを再初期化する必要があります。これは、「[データベースを設定する](#)」で説明されている初期化とアタッチの手順に従うことで実行できます。このため、データベース クラスタリングを使用する場合は、少なくとも3つのデータベースを用意することをお勧めします。

---

- Call Bridge が複製データベースしか見ることができない場合、機能は継続しますが、データベースの読み書きはできなくなります。これには、API 経由の変更操作、Cisco Meeting Server web app 経由のスペースの変更、および LDAP 同期が含まれます。新しい通話はサポートされず、Call Bridge に接続されているアクティブコールのみが機能します。
  - Call Bridge とデータベースが通信するには、2つが互換性のあるデータベーススキーマを実行する必要があります。シングルノード (非クラスター化) システムでは、Call Bridge は、最初の起動時に、データベーススキーマを最新バージョンに自動的にアップグレードします。ただし、クラスターシナリオでは、このプロセスを手動にすることで、いつアップグレードを行うかをより細かくコントロールできるようになっています。[データベーススキーマのアップグレードを参照してください](#)。
  - 2つの重要な時間要素があります。
    - ・ 隔離状態になった後、プライマリデータベースが複製に戻るまでの時間：5-6 秒
    - ・ プライマリデータベースがダウンしてから複製がプライマリになるまでの時間：10-15 秒
  - バージョン 2.7 以降、データベースクラスタはクラスター中のデータベースを保持または接続する各 Meeting Server で設定された同じ CA によって署名されたクライアントとサーバ証明書を必要とします。証明書の使用を強制することで、クラスター全体の機密性と認証の両方が保証されます。
  - **注意：**証明書を必要としない以前のバージョンの Meeting Server ソフトウェアを使用してデータベースクラスタが証明書なしで構成されていた場合、バージョン 2.7 にアップグレー
-

---

ドすると証明書が設定され、データベース クラスターが再作成されるまで、データベースは停止し、アクセスできない状態になります。

---

- **警告** : データベースクラスタを形成するノードは、信頼できるルート CA 証明書で設定する必要があります。これにより、正当なノードだけがクラスタに接続できます。ノードは、信頼できるルート証明書で終わる証明書チェーンを提示する接続を信頼します。そのため、各データベースクラスタは専用のルート証明書を使用する必要があり、ルート証明書または中間証明書は他の目的には使用されてはいけません。
  - **警告** : バージョン 3.5 以降では、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ノードのクラスタを解除します。ユーザーはノードをクラスタ解除し、Meeting Server をアップグレードし、MMP コマンドを使用してノードをクラスタリングする必要があります。データベースのクラスタリングに関する手順は、[第 5 章](#) 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しなければならないネットワーク設定の変更について説明します。一部の項目は事前に構成することができます。

#### 3.1.1 DNS 設定

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

DNS 名は、それぞれに優先順位と重みを付けて複数の IP アドレスを解決するように構成できます。高度な構成では、DNS 解決の結果が要求者のロケーションに依存するようにセットアップできます。

#### 3.1.2 セキュリティ証明書

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

スケーラブルで復元力のある展開のための [証明書ガイドライン](#) には、証明書の背景情報と説明が記載されています。これには Meeting Server の MMP コマンドを使って自己署名証明書を生成する方法も含まれます。これらの証明書はラボでの構成のテストに役立ちます。しかし、本番環境では認証局 (CA) によって署名された証明書を使用することを強く推奨します。

これまでこのガイドに記載されていた証明書に関する指示が削除され、[証明書のガイドライン](#) を参照する単一の手順に置き換えられました。

---

**注：**証明書に自己署名したものを使用する場合、サービスは信頼されていませんという警告メッセージが表示される場合があります。これらのメッセージを回避するには、証明書を再発行し、信頼できる CA によって署名させます。このコンポーネントへのパブリックアクセスが必要な限り、これは内部 CA でかまいません。

---

#### 3.1.3 ファイアウォールの構成

ファイアウォール上で開く必要があるポートのリストは [付録 B](#) を参照してください。また、ファイアウォールルールの作成については [セクション 20.6](#) を参照してください。

#### 3.1.4 Syslog サーバ

Meeting Server は Syslog 記録を作成します。この Syslog 記録はローカルに保存され、リモートロケーションに送信することもできます。これらの記録は、Meeting Server の内部ログペー

ジよりも詳細なログが含まれているため、トラブルシューティングの際に役立ちます。内部 syslog メッセージは SFTP 経由でダウンロードできますが、Cisco はリモート 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（混合、Edge、Core）を設定することを推奨しています。これは、単一の Syslog サーバまたは複数のサーバーにできます。ただし、何らかの形式のクラスタリングを使用している場合、すべてのサーバーに同じ Syslog サーバーを使用すると、トラブルシューティングを簡素化できます。問題に関係するすべての Meeting Server のログを必ず確認してください。

---

**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 を使用するように設定されていることを確認してください。

---

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

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

例：

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

3. 次を入力して、Syslog サーバーを有効にします。

```
syslog enable
```

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

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

- a. 監査ロールを持つユーザーを作成します。

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

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

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

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

---

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

---

### 3.1.5 Network Time Protocol サーバー

1 つまたは複数の Network Time Protocol (NTP) サーバーを設定して、Meeting Server コンポーネント間で時刻を同期します。

---

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

---

各 Meeting Server 上：

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

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

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

[MMP コマンドリファレンス](#)で ntp コマンドの一覧を参照してください。

### 3.1.6 通話詳細記録のサポート

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

スケーラブルなサーバー導入のコアサーバーは最大 4 つの CDR レシーバーをサポートするため、Meeting Management などの異なる管理ツールを導入したり、レジリエンスのために Meeting Management の複数のインスタンスを導入したりできます。復元力のある展開では、各コアサーバーが個別の CDR を生成します。導入全体の一貫した全体像を得るために、Core サーバーは同じ CDR レシーバーを使用する必要があります。

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

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

---

**注意：**CDR 受信者のリストは、個々の Call Bridge に対してローカルに保持されます。クラスタ化された Call Bridge 間で共有されるデータベースには保存されません。

---

### 3.1.7 ホスト名

Cisco は、各 Meeting Server に独自のホスト名を与えることを推奨しています。これにより、クラスター展開での問題の診断が容易になります。

1. 必要に応じて、MMP に SSH で接続し、ログインします。
2. タイプ :
 

```
hostname <name>
hostname london1
ホスト名 mybox.example.com
```
3. タイプ :
 

```
リブート (reboot)
```

---

注：このコマンドを発行した後は再起動が必要です。

---

### 3.1.8 その他の要件

- LDAP サーバーにアクセスしてユーザーをインポートします。これは Microsoft Active Directory (AD) サーバまたは OpenLDAP サーバーです。
 

ユーザーがウェブアプリを利用して Meeting Server に接続する場合、LDAP サーバーが必要です。ユーザアカウントは LDAP サーバからインポートされます。[LDAP 設定](#)で説明されているように、LDAP からフィールドをインポートすることでユーザ名を作成できます。パスワードは Meeting Server 上にキャッシュされません。LDAP サーバ上で集中的かつ安全に管理されます。ウェブアプリが認証されると、LDAP サーバーへの呼び出しが行われます。
- Call Bridge でホストされている通話に到達するために使用するダイヤルプランを決定します。ダイヤルプランは環境によって異なります。これは、発信する通話タイプが Lync、SIP (音声を含む)、ウェブアプリ通話のどれかによって決まります。このダイヤルプランを展開する手順については、「[ダイヤルプランの構成 - 概要](#)」「[ダイヤルプランの構成 - 概要](#)」を参照してください。スケーラブルで復元力のある展開のダイヤルプランは、API 経由でセットアップする必要があります。
- ソリューションをテストするために次の 1 つ以上にアクセスします：Lync クライアント、SIP エンドポイント、SIP 電話、および/またはウェブアプリ (必要に応じて)。
- SIP 通話を発信する場合は、SIP 通話制御プラットフォームにアクセスします。[11 章](#) および [章](#) では Cisco VCS への SIP トランクのセットアップ方法を説明し、必要なダイヤルプラン設定の変更についてまとめています。Cisco Unified Communications Manager (CUCM)、Avaya CM および Polycom DMA への SIP トランクのセットアップに関する情報は、「[通話制御を使用した Cisco Meeting Server の展開](#)」ガイドを参照してください。このガイドに記載されていない他のコール制御デバイスを使用することもできます。

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

Meeting Serverは複数の Lync フロント エンド (FE) サーバーと統合されます。着信 (Lync から Meeting Server) 方向の場合、各 Lync FE プールは、複数の Call Bridge を解決する DNS レコードをポイントするように構成できます。フェイルオーバーは DNS 経由で行われます。Lync は各結果を順番に試します。地理的分散については、Lync FE プールが地理的に分散していることを想定しており、最も論理的なアプローチは、各 Lync FE プールを同じ地域内で共存する異なる Call Bridge セットをポイントすることです。

発信方向については、DNS 経由で Meeting Server のダイヤルプランを構成して、複数の Lync FE サーバまたは Lync ディレクターを解決することができます。各地域は、異なる FE プールを指すように構成できます。

Lync が展開されている本番環境では、Lync FE サーバーによって信頼されている証明書が必要です。

### 3.1.9 仮想化導入の特定の前提条件

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

## 3.2 Meeting Serverの Edge ハードウェア構成

Meeting Serverの Edge の役割は、単一のサーバまたは複数のサーバとして展開できます。この選択は、外部のウェブ アプリ参加者に必要な同時呼び出し容量によって決まります。参加者の高い割合が外部ウェブアプリ参加者であると予想される場合、Cisco は Edge サーバーを導入して、その容量がコアの Call Bridge 容量と同等か超えるようにすることを推奨します。Edge の容量が超過していても、Call Bridge のコア展開がサポートする数を超える参加者による接続はできないことに注意してください。Edge は参加者に Web Bridge と TURN の容量を提供します。ただし、コアはウェブ アプリの参加者に Call Bridge 容量を提供する必要があります。

### 3.2.1 Edge サーバーの設定

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

#### 「小規模」Edge サーバー

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

- 4 GB RAM

- 4 vCPU
- 1 Gbps ネットワークインタフェース

### 「大規模」 Edge サーバー

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

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

### 推奨プロセッサ仕様：

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

### NIC 要件：

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

### 共存サポート：

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

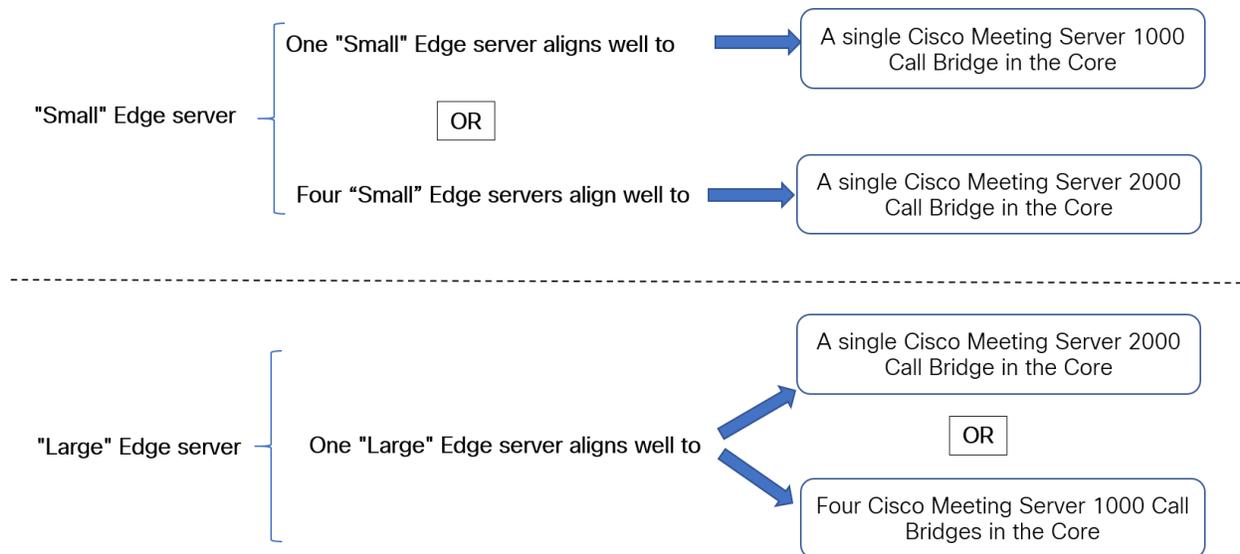
### 注：

- Meeting Server 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 10 Gbps NIC をサポートします。
- CMS 2000 は Meeting Server の Edge インスタンスとしては適していません。

表 5：Edge Server ウェブアプリのコールキャパシティ

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

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



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

### 3.2.2 導入の考慮事項

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

## 3.3 Meeting Server Edge のネットワーク計画

### 3.3.1 技術的な説明

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

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

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

---

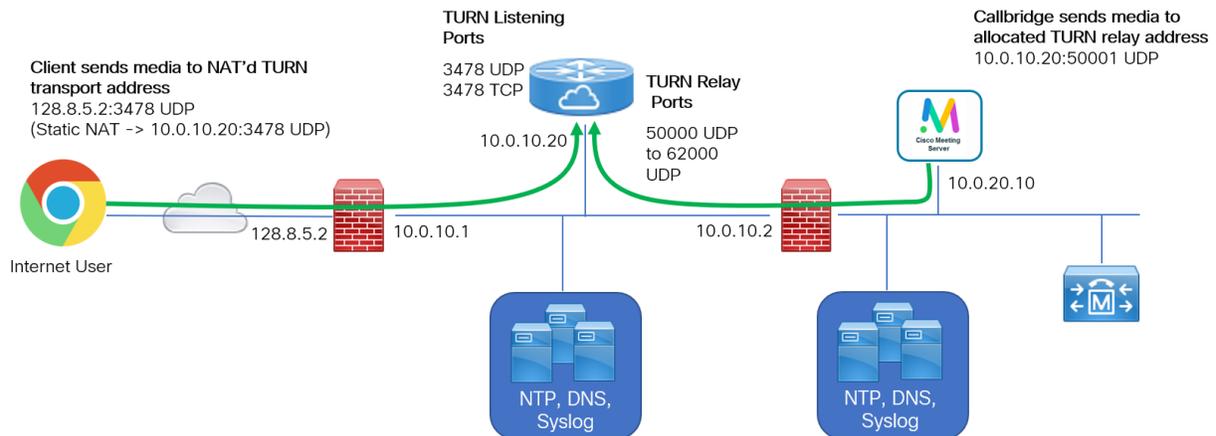
**注：**バージョン 3.0 から、単一インターフェイスの TURN Server のリスニングポートを設定することを推奨します。

---

外部クライアントによる TURN リレーセットアップの使用は、公開された通話キャパシティを達成するために、Edge サーバーに必要な導入モデルです。他の組み合わせやシナリオでは、メディア接続が確立される可能性があります。容量が減少し、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、お勧めできません。

Meeting Server Edge の推奨導入は、外部ウェブアプリの参加者が TURN over UDP を使用して Edge インスタンスに接続し、Call Bridge が UDP 経由で TURN Relay に接続することが可能です。この構成は、セキュリティとパフォーマンスのバランスをとるのに最適です。制限的なクライアントネットワークとの互換性を向上させるために、2 番目の DMZ インターフェイスを追加して TURN を独自のインターフェイスに移動し、TURN over TCP 443 をサポートするオプションのシナリオもカバーしています。ネットワークパスとサービス設定の他の組み合わせが技術的に実現可能である間、それらは他のセキュリティリスク、容量への影響を招く可能性があるため、Cisco によって文書化されていないか、バリエーションを減らすためにこのガイドから除外されています。

図 13 : UDP を使用した TURN のサンプルダイアグラム



### 3.3.2 ネットワークの計画

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

#### 3.3.2.1 DMZからインターネットへの境界

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

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

ウェブアプリをサポートするには、ファイアウォールは、インターネットから、Web Bridge 3 サービスをホストする Meeting Server の Edge サーバーのポート 443 への着信 TCP 接続を受け入れる必要があります。HTTP リダイレクトを有効にする場合は、オプションで TCP ポート 80 を有効にすることで、HTTP 接続を試みるユーザーが自動的に HTTPS にリダイレクトするようになります。参加者は通話に HTTP を使用できません。このポートは HTTPS へのリダイレクトのみをサポートします。

メディアは UDP 経由で送信するのが最適ですが、インターネット上の通話参加者は UDP トラフィックをブロックするファイアウォールの背後にいる場合があるため、オプションの TCP フォールバックが提供されます。メディアトラフィックの場合、ファイアウォールは TURN リスニングポート UDP 3478 で Edge サーバーへの着信接続を受け入れる必要があります。TCP を使用して TURN を有効にする場合、TURN サーバーはまた TCP 3478 および指定され

たポートでリッスンします。TCP 443 を使用して TURN を有効にする場合、TURN と Web Bridge 3 がそれぞれ異なるインターフェイスでリッスンする 2 番目の DMZ IP インターフェイスがサーバーに必要です。

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

### 3.3.2.2 DMZ からインターネットへのトラフィックルール

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

**注：**

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

### 3.3.2.3 イン트라ネットと DMZ の境界

デフォルトでは、イントラネットを保護するために、ファイアウォールは Meeting Server Edge サーバインスタンスからイントラネットへの TCP 接続を許可しない必要があります。

また、同じアドレス/ポートのペアで、すでに（そして最近）イントラネットからエッジボックスに UDP パケットが送信されていない限り、Meeting Server Edge サーバーからイントラネットに UDP パケットが送信されることを許可してはなりませんつまり、以前に <Intranet IP> : 50131 から <DMZ IP> : 50342 へのパケットが存在しない限り、<DMZ IP> : 50342 から <Intranet IP> : 50131 への UDP パケットはブロックされる必要があります。

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

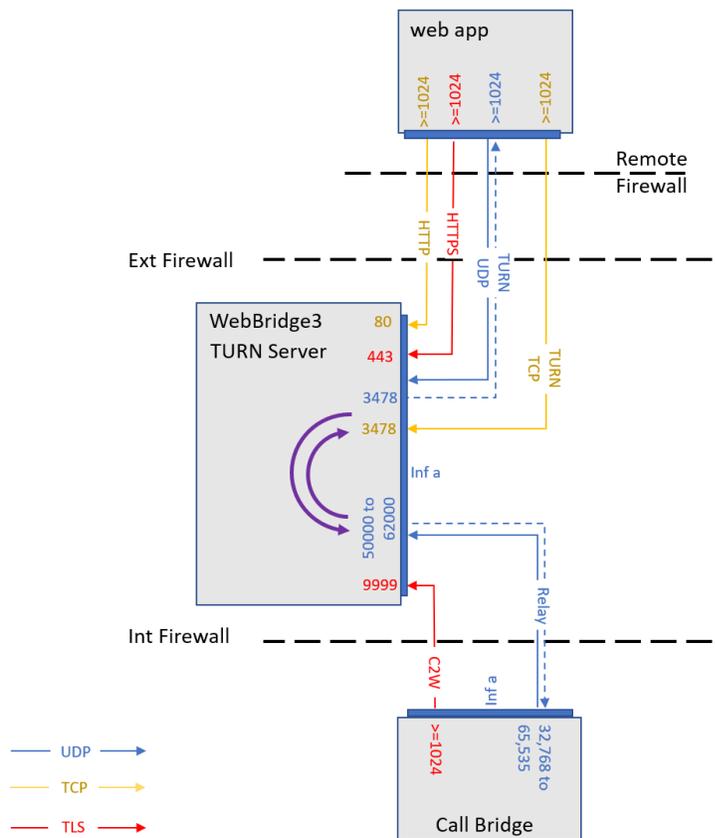
コア Call Bridge が Meeting Server の Edge ノードで直接ルーティング可能であることが望ましいですが、コア Meeting Server は DMZ サービスに対して NAT の背後にあり、外部クライアントによって割り当てられた TURN リレーを使用することができます。コア Meeting Server は、TURN リスニングポートに接続する必要がありません。これは、外部クライアントによるリレーセットアップが両当事者にとって十分であるためです。NAT を使用している場合、Callブリッジへのトラフィックは、ICE 接続テストでピア反射の候補と見なされます。

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

#### 注 :

- {WB3} = Web Bridge 3 サーバーの IP リスト
- {TURN} = TURN サーバーの IP リスト
- Call Bridge = コア システムの Call Bridge サーバーの IP リスト
- ファイアウォールは、TURN 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
- 単一インターフェイス上の TURN Server のリスニングポートを設定する必要があります。

図 14 : TURN 3478 UDP または 3478 TCP を使用するウェブアプリ



### 3.3.2.4 管理およびプラットフォーム トラフィック

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

Meeting Serverが TLS および証明書を適切に処理するには、Edge サーバーが NTP および DNS サービスにアクセスする必要があります。管理者はまた、SFTP および SSH を使用して、Meeting Serverソフトウェアを設定および更新する必要があります。集中ログの Syslog はオプションですが、強く推奨されます。これらのサービスは、既知のソースへのトラフィックの制限などの一般的なセキュリティ対策を遵守しながら、Edge の DMZ ネットワーク インターフェイスからアクセスできるように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	Direction	[ソースIP (Source IP) ]	ソース Pro-to : Port	ターゲット IP	ターゲットプロトコル : ポート
NTP	発信	{WB3} または {TURN}	UDP 123	{NTP サーバ}	UDP 123
DNS	発信	{WB3} または {TURN}	UDP {unreserved}	{DNS サーバ}	UDP 53
Syslog	着信	{WB3} または {TURN}	TCP {unreserved}	{Syslog サーバ}	TCP 514*
アプリ管理 (SSH、SFTP)	着信	{イントラネット/管理 IP}	TCP {unreserved}	{WB3} または {TURN}	TCP 22

#### 注：

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

### 3.3.3 Meeting Server ウェブエッジを導入する

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

1. MMP 経由で Meeting Server エッジ上の TURN サーバーを設定します。
2. MMP 経由で Meeting Server エッジ上の Web Bridge 3 を設定します。
3. Web Bridge 3 を Call Bridge にリンクします (つまり、callBridge パラメータを **設定 > API** の下で /api/v1/turnServers および /api/v1/webBridges にアクセスし、Web Bridge 3 証明書の要件を確認してください)。
4. 接続が正常に機能していることを確認します – これを行うには、ウェブアプリアドレス経由でログインして手動でテストするか、**状況 > 全般** を見て **障害の状態**、および **最近のエラーと警告**を確認します。(Web Bridge 3/TURN 接続失敗のメッセージは表示されないことに注意してください。)
5. 次のようにファイアウォール設定を追加します。
  - a. Call Bridge は、API の「c2w : //address : port」で指定されたとおり、TCP 接続 Web Bridge3 の c2w 接続ポートに接続できる必要があります。つまり、url フィールドにある/api/v1/webBridgesです。)

- b. Meeting Server のエッジの TURN リレー ポートは 50000 から 62000 までであるため、Call Bridge は UDP のポートに接続して、メディアを送信する必要があります。
- c. 外部ウェブアプリ クライアントは、UDP 3478 で TURN Server に到達する必要があります。TCP へのフォールバックが可能で、その場合のポートは「turn tls <port>」の設定に依存します。そのポートも開く必要があります。

## 4 MMP の設定

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

### 4.1 MMP およびウェブ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](#)』の手順に従って、各 Meeting Server に MMP 管理者ユーザアカウントを作成しておく必要があります。それが済んでいれば、追加のアカウントを設定する必要がない限り、次の項に進みます。同じアカウントがウェブ管理インターフェイスへのアクセスに使用されている。

(これらの MMP 管理者ユーザアカウントがない場合は、展開に適した [インストールガイド](#) に記載されている緊急管理者復元手順を使用する必要があります。)

MMP add user コマンド `user add <account name> <role>` を使用して、管理者レベルの権限を持つ MMP 用の追加ユーザアカウントを作成することができます。

1. MMP に SSH で接続します。
2. 管理者レベルのユーザアカウントを追加します。例：  
`user add adminuser2 admin`
3. このアカウントで使用するパスワードを 2 回入力して、アカウントの作成を完了してください。  
ログイン時に、ユーザーは新しいパスワードを設定するように強制されます。

---

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

---

### 4.2 ソフトウェアをアップグレードする

Cisco Meeting Server 2000 および Cisco Meeting Server 1000 は、その時点で最新のソフトウェアが使用された状態出荷されていますが、必ずしも最新のものではない場合があります。同様に、数日前にソフトウェアをダウンロードした場合は、Cisco のウェブサイトでの最新のバージョンが入手可能かどうかを確認し、入手可能な場合は最新バージョンにアップグレードすることをお勧めします。

---

**警告：**データベースクラスタが、証明書を必要としない以前のバージョンの Meeting Server ソフトウェアを使用して、証明書なしで構成された場合、バージョン 2.7 へのアップグレード時に、データベースは停止し、証明書が構成されてデータベースクラスタが再作成されるまで到達不能になります。

---

以下の手順は、すべてのタイプの導入に適用されます。

1. Meeting Server 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、サーバーの MMP に SSH で接続し、ログインして次のように入力します。

```
version
```

2. Meeting Server をアップグレードする前に：
  - a. 各サーバー上の現在の設定のバックアップを取ります。MMP コマンド `backup snapshot <name>` を使用します。バックアップをローカルサーバーに安全に保存します。詳細については、[MMP コマンドリファレンスガイド](#) を参照してください。アップグレードプロセス中に作成される自動バックアップファイルは使用しないでください。
  - b. `cms.lic` および証明書ファイルをローカル サーバーに保存します。
  - c. ウェブ管理インターフェイスを使用して、データベースクラスタの状況を確認し、すべての呼び出し (SIP およびクライアント) が機能しており、障害状態がリストされていないことを確認します。
  - d. 展開にクラスター化されたデータベースがある場合、**データベースクラスタ削除** コマンドを使用してノードのクラスターを解除します。
3. アップグレードするには、まず Cisco のウェブサイトから適切なソフトウェアファイルをダウンロードします。この [リンク](#) をクリックし、ウェブページの右側の欄から適切な Meeting Server のタイプをクリックして、ダウンロードリンクと共に表示される手順に従ってください。
4. SFTP クライアントを使用して、Meeting Server の MMP に新しいソフトウェアイメージをアップロードします。次に例を示します。

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

10.1.x.y は IP アドレスまたはドメイン名です。

5. すべてのコアサーバーを 1 つずつアップグレードし、SSH 経由で MMP に接続し、次を入力します。

#### アップグレード

最初に非データベースサーバーから開始し、複製データベースサーバー、プライマリ データベース サーバーの順で最後に行います。各サーバーが完全に起動し、データベースサーバーがデータベースクラスタに接続するのを待ってから、次のサーバーに移動します。

各サーバー：サーバーのアップグレード後、Web 管理が利用可能になるまで約 10~12 分待つ必要があります。ウェブ管理インターフェイスにログインします。この時点で、サーバーは、例えば「エラー：リモートデータベースのスキームバージョンが 7026 (現在のバージョンは 7045)」のようなエラーを報告する場合があります。ウェブ管理へのログインが成功するまでは、このポイントより先に進めないでください。MMP コマンド `version` を使用して、新しいバージョンを確認します。バージョンが正しくない場合は、新しい画像をこのサーバーにアップロードし、MMP コマンド `upgrade` を使用して、このポイントに戻るのを待ちます。

6. すべてのサーバーのアップグレードが完了したら、[第 5 章](#)で説明されている手順に従って、ノードを再度クラスタ化します。
7. MMP コマンド `データベース クラスタ ステータス`を使用して、データベース サーバーが接続され、同期されていることを確認してください。データベース サーバーが同期されるまで、次の手順に進まないでください。
8. 各 Call Bridge の Web 管理インターフェイスがスペースのリストを表示できることを確認します。
9. すべての Edge サーバーをアップグレードし、アップグレードが成功したことを確認します。

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

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

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

---

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

---

### 4.3 Call Bridge リッスン インターフェイスの設定

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

---

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

---

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

次のように、各 Call Bridge でリスニング インターフェイスを設定します。

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

```
callbridge listen a
```

---

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

---

3. 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
```

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

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

```
callbridge restart
```

## 4.4 HTTPS アクセスのためのWeb 管理インターフェイスの設定

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

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

1. インストール時に、Web 管理インターフェイスがインターフェイス A のポート 443 を使用するように自動的に設定されます。ただし、Web ブリッジも TCP ポート 443 を使用します。Web 管理インターフェイスと Web ブリッジの両方が同じインターフェイスを使用する場合は、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。MMP コマンド `webadmin listen <インターフェイス><ポート>`。次に例を示します。

```
webadmin listen a 445
```

2. ウェブ管理インターフェイスにアクセスできるかどうかをテストするには、同等の情報をウェブブラウザに入力します：<https://meetingserver.example.com:445>

機能する場合は、次のセクションに進みます。

3. ウェブ管理インターフェイスに到達できない場合：

- a. MMP にログインし、次を入力して出力を確認します。

```
webadmin
```

出力の最終行には、"webadmin running" と表示されます。

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

```
webadmin enable
```

- c. `webadmin` コマンドの出力では、インストールした証明書の名前も確認できます。

例：webadmin.key および webadmin.crt。

---

**注：**以前にアップロードした証明書と同じ名前を指定する必要があります。

---

これらが名前であると想定して、次を入力します。

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

これにより、キーと証明書が一致することが確認されます。

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

## 4.5 ステージ Edge サーバーインスタンス

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

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

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

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

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

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

## 4.6 Web Bridge 3 を設定する

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

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

---

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

---

### **警告：** Expressway ユーザーのための重要な注意点

Web Bridge 3 とウェブ アプリを展開する場合、Expressway バージョン X14.3 以降を使用する必要があります。以前の Expressway バージョンは Web Bridge 3 ではサポートされません。

---

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

---

### 4.6.1 Web Bridge 3 の設定に役立つ情報

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

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

- C2W 接続は内部サービス間のみであるため、公的機関によって署名された証明書を明示的に使用する必要はありません。MMP 内で作成された自己署名証明書を使用できます。
- Web Bridge C2W 証明書の SAN/CN は、Call Bridge API で Web Bridge 3 を登録するために使用される c2w:// URL で使用される FQDN または IP アドレスと一致する必要があります。これが一致しない場合、Call Bridge は TLS ネゴシエーションに失敗し、Web Bridge が提示する証明書を拒否し、Web Bridge との接続に失敗します。

---

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

---

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

#### 4.6.2 Web Bridge 3 サービスを有効にする

Cisco Expressway プロキシを使用している場合、または Call Bridge に直接到達できるウェブアプリケーションをサポートしている場合、Web Bridge サービスはコア Meeting Server インスタンスで有効になっている必要があります。Meeting Server の Edge 導入を使用する場合、Web Bridge 3 はすべての Edge インスタンスで実行する必要があります。オプションで、Call Bridge が実行されているコア Meeting Server インスタンスでも実行できます。

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

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

```
webbridge3 https listen <interface>:<port>.
```

最初のインターフェイスとポート 443 の使用を推奨します。例：

```
webbridge3 https listen a:443
```

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

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

```
webbridge3 https certs wb3-https.key wb3-https-fullchain.crt
```

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

```
webbridge3 c2w listen <interface> : <port> .
```

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

```
webbridge3 c2w listen a:9999
```

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

例：

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

---

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

---

6. Web Bridge 3 の C2W トラストストアは、どの Call Bridge がこの Web Bridge に接続できるかを制御するように設定する必要があります。信頼バンドルには、この Web Bridge に接続するすべての Call Bridge の Call Bridge 証明書、または Call Bridge 証明書に署名した CA の証明書が含まれている必要があります。最大限のコントロールを行うために、署名機関の証明書ではなく、バンドル中の個々の Call Bridge 証明書 (証明書ピンング) を使用することを推奨します。Web Bridge の `c2w trust` バンドルを次のコマンドで設定します：`webbridge3 c2w trust <certificate bundle>`

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

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

```
webbridge3 http-redirect を有効にする
```

8. Web Bridge サービスを有効にする

```
webbridge3 enable
```

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

#### 4.6.3 Call ブリッジの C2W 接続を設定する

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

1. Call Bridge を実行している内部 Meeting Server の MMP インターフェイスに接続します。

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

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

**注：** 範囲で制限されている場合を除き、Call Bridge は、Meeting Server API で定義されているすべての Web Bridge への接続を試みます。

4. Call Bridge を再起動します

```
callbridge restart
```

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

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

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

Status Configuration Logs

### API objects

This page shows a list of the objects supported by the API. Where you see a ► control, you can expand that section

Filter  (13 of 126 nodes)

- /api/v1/system/profiles/effectiveWebBridgeProfile ►
- /api/v1/tenants/<id>/effectiveWebBridgeProfile
- /api/v1/webBridgeProfiles ►
- /api/v1/webBridgeProfiles/<id>
- /api/v1/webBridgeProfiles/<id>/ivrNumbers
- /api/v1/webBridgeProfiles/<id>/ivrNumbers/<id>
- /api/v1/webBridgeProfiles/<id>/webBridgeAddresses
- /api/v1/webBridgeProfiles/<id>/webBridgeAddresses/<id>
- /api/v1/webBridges ►
- /api/v1/webBridges/<id>
- /api/v1/webBridges/<id>/effectiveWebBridgeProfile
- /api/v1/webBridges/<id>/status
- /api/v1/webBridges/<id>/updateCustomization

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

- uri フィールドには、`c2w://<Web Bridge FQDN>:<c2w port>` の形式で、追加する Web Bridge の C2W インターフェースの FQDN アドレスを入力します。例：  
`c2w://cmsedge1.company.com:9999`

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

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

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

## 4.7 TURN Server の設定

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

- 展開でウェブ アプリ クライアントを使用していない場合は、この項をスキップできます。
- ウェブプロキシおよび TURN プロバイダとして Cisco Expressway を使用している場合、[Cisco Meeting Server \(X14.3\) 用 Cisco Expressway ウェブプロキシ](#) の TURN サーバーと Call Bridge の設定方法についての指示を参照してください。
- Meeting Server の Edge 展開を使用している場合、TURN Server は各 Edge インスタンスで設定されている必要があります。この項の手順を完了して、TURN サービスを設定します。

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

### 4.7.1 TURN サービスを有効にする

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

```
turn short_term_credentials_mode enable
```

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

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

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

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

---

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

---

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

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

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

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

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

```
turn listen a
```

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

例：

```
turn tls 3478
```

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

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

```
turn certs turnCert.key turnCert.crt CABundle.crt
```

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

8. TURN Server を有効にする

```
turn enable
```

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

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

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

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

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



3. 表示されたリストから `[/api/v1/turnServers]` 行を見つけ、[▶] アイコンをクリックして導入します。

4. [新規作成] をクリックして新しい turnServer オブジェクトを作成します。次のパラメータフィールドが表示されます：

The screenshot shows the Cisco Meeting Server configuration interface. At the top, there is a navigation bar with 'Status', 'Configuration', and 'Logs' tabs. Below the navigation bar, there is a link to '« return to object list'. The main heading is '/api/v1/turnServers'. The form contains the following fields:

- serverAddress:  [text input]
- clientAddress:  [text input]
- username:  [text input]
- password:  [text input]
- useShortTermCredentials:  [dropdown menu, value: <unset>]
- sharedSecret:  [text input]
- type:  [dropdown menu, value: <unset>]
- numRegistrations:  [text input]
- tcpPortNumberOverride:  [text input]
- callBridge:  [text input] [Choose]
- callBridgeGroup:  [text input] [Choose]

At the bottom of the form, there is a 'Create' button.

5. 追加する TURN Server の以下のフィールドに入力します。

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

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

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

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

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

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

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

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

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

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

## 4.8 MMP ユーザーの LDAP 認証

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

---

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

---

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

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

---

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

---

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

---

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

---

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

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

## 5 データベースの設定

他のコンポーネントのようにデータベースを作成したり有効にする必要はありません。

Meeting Server ソフトウェアイメージを各ホストサーバーにインストールすると、各ホストサーバー上に空のデータベースが作成されます。

データベースクラスタリングは、Call Bridge クラスタとは異なる働きをします。データベースクラスタは本質的には実行中のデータベースの「オンライン」バックアップであるものを作成し、システムの実行中に維持されます。また、障害が検出された場合に、自動的にバックアップの使用に移行する機能も提供します。

クラスタリングプロセス中に、プライマリデータベースを持つノードを選択し、クラスタに「レプリカ」データベースノードを追加します。クラスタ内に 1 つのデータベースノード、またはクラスタ内に 3 つのデータベースノードがあることを確認してください。2 個のデータベースノードからなるクラスタは使用しないでください。もし使用していてプライマリノードに障害が発生した場合、残りの複製ノードは、それ自体をプライマリに昇格させて、データベースリクエストにサービスを提供しても安全かどうかを確認できなくなります。3 番目のデータベースノードを追加することで、データベースクラスタは障害の場所を特定し、別のデータベースをプライマリとして選択しても安全かどうかを判断し、Meeting Server の操作を中断することなく続行できるようにします。

データベースクラスタに参加できる Cisco Meeting Server は 3 つまでです。それ以上のサーバーは、**データベースクラスタ接続** コマンドを使用してクラスタに追加する必要があります。

データベース クラスタリングは、いかなる種類のロード バランシングやキャッシュも行いません。また、地理的に分散した配置の中でデータのシャーディングを実行し、より効率的なローカルアクセスを可能にすることはありません。すべてのクエリは、現在のプライマリデータベースがどこにあっても、ダイレクトされます。複製を読み取り専用インスタンスとして使用することはできません。

---

**注：**データベースサーバ間、および Call Bridge とプライマリデータベース間では、200 ms 以下のネットワーク遅延制限（または往復時間）があります。

---

この項の指示に従ってクラスタを作成します。特に断りのない限り、これらの手順は統合展開と分割展開に同じように適用されます。

---

**注：**クラスタ化されたデータベースノード間に WAN オプティマイザが導入されている場合、生存確認チェックが完了せず、ログにエラーが記録される場合があります。クラスタノード間で WAN オプティマイザが使用されている場合、すべての生存確認トラフィックがタイムリーに送信されるようにすることが重要です。

特定の IP アドレス間でこの機能を無効にする方法、または適用する最適化を制御するオプションについては、WAN オプティマイザのドキュメントを参照してください。

---

## 5.1 別のサーバー上にあるデータベース

### 5.1.1 別のサーバ上のデータベースの要件

---

**注：**この項は、1 つまたは複数の外部データベースを使用する場合にのみ適用されます。

---

データベースのホストサーバーの CPU 要件は中程度ですが、大きなストレージとメモリを必要とします。認定済み VM ホストの使用を必須にするものではありませんが、この [リンク](#) で指定することを推奨しています。さらに、

- データストアは、高 IO/秒 SAN またはローカル SSD ストレージのいずれかに存在する必要があります
- データは、OS と同じ仮想ディスク上にある必要があります。

Cisco Meeting Server 1000 のホストとして現在使用されている Cisco UCS C220 M4 を使用できますが、VM データベースはサーバーリソースのわずかな割合しか使用しません。必要に応じて、このサーバーを使用して、他の VM を VM データベースと同じサーバーでホストすることもできます。

必要に応じて、同じホストサーバー上で他の VM を実行できる必要があります。

### 5.1.2 別のサーバーにデータベースを展開する

1. Meeting Server の画像を各外部データベースホストサーバーにインストールします。空のデータベースは自動的にセットアップされます。
2. ホストサーバーは証明書を要求します。次の項を参照してください。

## 5.2 データベースと Call Bridge サーバーへの証明書の展開と検証

データベースクラスタリングは、機密性と認証の両方のために公開/秘密鍵暗号化を使用し、単一の共有認証局 (CA) を使用します。証明書が使用されない場合、機密性も認証もありません。データベースクラスタはユーザーがアクセスできないため、証明書はローカル CA によって署名できます。証明書および証明書バンドルの作成、アップロード、および割り当てについての詳細は、[『証明書ガイドライン』](#) を参照してください。

---

**注：**本番環境では、データベーストラフィックの暗号化を使用する必要があります。これは証明書を使用することで実現します。ただし、テストの場合は (テストのみの場合)、証明書の使用をスキップできます。証明書を使用しない場合、データベースに対するセキュリティおよびアクセス制御はありません。

---

---

**警告：**証明書は無効なデータベースクラスタにのみ割り当てることができます。すでにデータベースクラスタをセットアップしている場合は、クラスタ内のすべてのサーバーで `database cluster remove` コマンドを実行し、ホストサーバーに証明書をアップロードし割り当てるコマンドを実行してから ([『証明書ガイドライン』](#)を参照)、次のセクションの手順に従ってクラスタを再作成する必要があります。

---

Meeting Serverはルート証明書までの証明書チェーンをチェックすることでノードを検証します。バージョン 3.5 から、クラスタに追加されたMeeting Serverのアイデンティティ (ホスト名/IP アドレス) も検証できます。Meeting Server は他の検証と共に、サーバー ID がサーバー証明書に保管された名前と一致するかどうかを検証します。

データベースのクラスタ検証モードの `<full/ca>` コマンドを使えば、必要に応じて検証の基本設定を指定することができます。コマンドが `full` に設定されている場合、Meeting Server は他の検証と共に、サーバーのアイデンティティがサーバー証明書に保存されている名前と一致するかどうかを確認します。コマンドが `ca` に設定されている場合、Meeting Server は Certificate Authority のみを検証します。

検証モードをフルに設定してサーバー ID を検証する場合、次のことを確認します。

1. サーバーの名前は、対応するサーバ証明書の FQDN と正確に一致する必要があります。
2. 展開に DNS レコードがない場合、DNS RR レコードを作成してローカルでサーバ ID を解決する必要があります。
3. クラスタに複製データベースノードを追加する際：
  - a. 複製データベースノードがホスト名を使って追加される場合、ホスト名はMeeting Serverデータベースサーバ証明書の CN または SAN リストに追加されなければなりません。
  - b. 複製データベースノードが IP アドレスを使用して追加される場合、IP アドレスは Meeting Serverデータベースサーバ証明書の SAN リストに追加される必要があります。
  - c. クラスタ内のすべての複製データベースは、同じ参加方法 (ホスト名または IP アドレス) を使用して追加する必要があります。
4. サーバー証明書で IP アドレスが使用されている場合、証明書用の SAN を生成する際に、IP アドレスは、IP アドレスフィールドとともに、SAN の DNS 名として追加する必要があります。

次に例を示します。

```
pki csr dbserver CN: server.db.example.com subjectAltName: 10.1.1.1
```

上記のコマンドは、証明書署名リクエストで次の SAN エントリを生成します：

**IP アドレス：**10.1.1.1、**DNS：**10.1.1.1、**DNS：**server.db.example.com

証明書の作成と生成の詳細については、[『証明書ガイドライン』](#)を参照してください。

5. クラスタ内のすべてのノードのサーバ ID は、サーバ証明書の IP アドレスと一致する必要があります。

---

**注：**

- 検証モードは、クラスタ内のすべてのノードで同じ値 (full/ca) に設定する必要があります。
  - 検証モードは非クラスタ化データベースでのみ変更できます。すでにデータベースクラスタをセットアップしている場合は、クラスタ内のすべてのサーバーで `database cluster remove` コマンドを実行してから、検証モードの設定を指定する必要があります。
- 

### 5.3 クラスタのプライマリデータベースを選択する

データベース クラスタを展開するには、どれをプライマリ データベースにするか、つまり最初にすべての Call Bridge で使用されるデータベース インスタンスを決定します。スケーラビリティなしで導入している場合、データが失われないように、最初はプライマリデータベースを現在のデータベースにする必要があります。そのため、このデータベースは Call Bridge と同じ場所に配置されます。

---

**注：** 単一のデータベースを 1 つまたは複数の Call Bridge で使用（「接続されている」）できるという点で、「クラスタ」にすることができます。ただし、レジリエンスはありません。

---

1. プライマリとして起動するデータベースを持つサーバーで、MMP にログインします。
2. データベースクラスタ証明書をまだ設定していない場合は、次のコマンドを使用して証明書を設定します。

```
database cluster certs <server.key> <server.crt> <client.key>
<client.crt> <ca.crt>
```

```
データベースクラスタ証明書 db01server.key db01server.crt
db01client.key
```

```
db01client.crt db01cert-bundle.crt
```

3. 次のコマンドを入力して、このデータベースクラスタのインタフェースを選択します：

```
database cluster localnode <interface>
```

```
database cluster localnode a
```

<interface> は、次の形式であることができます。

- [a|b|c|d|e] - インターフェイスの名前（最初の IPv6 アドレスが優先されます。そうでない場合は、最初の IPv4 アドレスが選択されます）

```
database cluster localnode a
```

- ipv4 : [a|b|c|d|e] - IPv4 に制限されたインターフェイス名（初めの IPv4 アドレスが選択されます）。例：`database cluster localnode ipv4 : a`

- ipv6 : [a|b|c|d|e] - IPv6 に制限されたインターフェイス名（初めの IPv6 アドレスが選択されます）例 : `database cluster localnode ipv6 : a`
  - <IP アドレス>- 特定の IP アドレス、IPv4 または IPv6 です。  
データベースクラスターローカルノード 10.1.3.9
  - データベースのクラスタリングに管理インタフェースを使用しないでください。
4. オプションで、サーバー証明書に保存されている名前を使用して、サーバーのアイデンティティ（ホスト名/IP アドレス）を確認することができます。次のコマンドを使用して、検証の設定を設定します。

**データベースクラスター検証モード<full/ca>**

**ca** - Meeting Serverは、サーバーのアイデンティティを検証することなく、ルート証明書までの証明書チェーンからノードを検証します。

**full** - Meeting Server は他の検証と共に、サーバー ID がサーバー証明書に保管された名前と一致するかどうかを検証します。

---

**注：**このコマンドを使用しない場合、Meeting Serverは認証局のみを検証します。

---

5. このデータベースクラスタのプライマリデータベースとして初期化するプロンプトに対して、MMP コマンド `database cluster initialize` および `Y` を入力します。

**データベースクラスタ初期化**

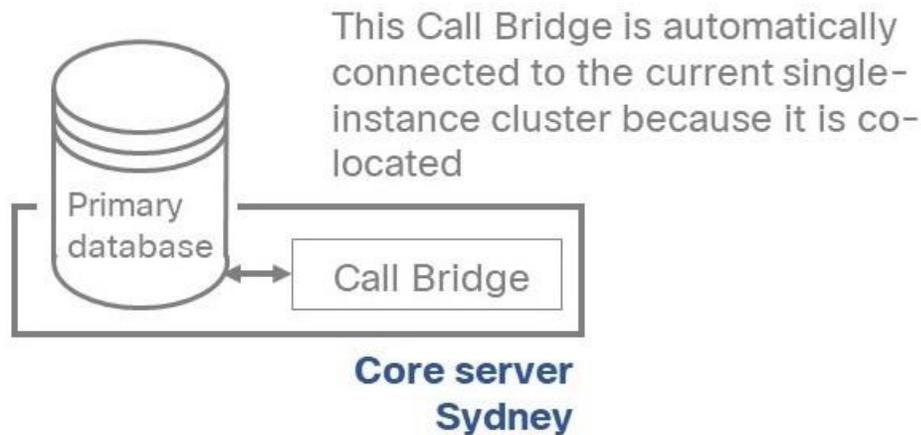
**警告！**

このノードを新しいデータベースクラスタとして初期化してもよろしいですか？（はい/いいえ）  
このノードのデータベースのコンテンツは、新しいクラスタのデータベースのプライマリバージョンになります。

初期化が開始されました...

これは、ローカル Call Bridge の再起動をトリガーし、約 30 秒かかります。

図 15 : 同じ場所に配置された Call Bridge は自動的に接続されます



8. 次のコマンドを入力して、[ステータス (Status)] が [有効 (Enabled)] と表示されるまで初期化が正常に完了したことを確認します。

```
database cluster status
```

次のようなメッセージが表示されます。

```
Status : Initializing
```

```
Nodes : 10.1.2.3 (me)      : プライマリ インターフェイス  
に接続されています      : a
```

後でステータスコマンドを再実行した場合 :

```
Status : Enabled
```

```
Nodes : 10.1.2.3 (me)      : プライマリ インターフェイス  
に接続されています      : a
```

## 5.4 他のデータベースインスタンスをデータベースクラスタに添付する

**注 :** これらのサーバーは、空のデータベースを持つことができます。また、Call Bridge を同じサーバーに配置する必要はありません。例えば、仮想サーバーをセットアップして外部データベースのみにすることができます。これらのホストサーバーは、データベースクラスタ証明書とキーを必要とします。

**警告 :** 現在このサーバー上にあるデータベースのコンテンツ (存在する場合) は破壊されます。

データベースクラスタ証明書をまだ設定していない場合は、次のコマンドを使用して証明書を設定します。

```
database cluster certs <server.key> <server.crt> <client.key>  
<client.crt> <ca.crt>
```

```
database cluster certs db01server.key db01server.crt db01client.key  
db01client.crt db01cert-bundle.crt
```

1. このデータベースクラスタの一部とするデータベースをホストしている他のサーバーを添付します。
  - a. そのような各サーバーで、次のコマンドを使用して、待機インタフェースを設定します。

```
database cluster localnode <interface>
```

---

**注：** <interface> は、この項で以前にリストされた形式のいずれかにすることができます

---

次に例を示します。

```
cms> データベースクラスタローカルノード  
インタフェースが更新されました
```

- b. オプションで、サーバ証明書に保存された名前ですerverアイデンティティ (ホスト名/IP アドレス) を検証できます。次のコマンドを使用して、検証の設定を設定します。

データベースクラスタ検証モード <full/ca>

**ca** - Meeting Serverは、サーバーのアイデンティティを検証することなく、ルート証明書までの証明書チェーンからノードを検証します。

**full** - Meeting Server は他の検証と共に、サーバー ID がサーバー証明書に保管された名前と一致するかどうかを検証します。

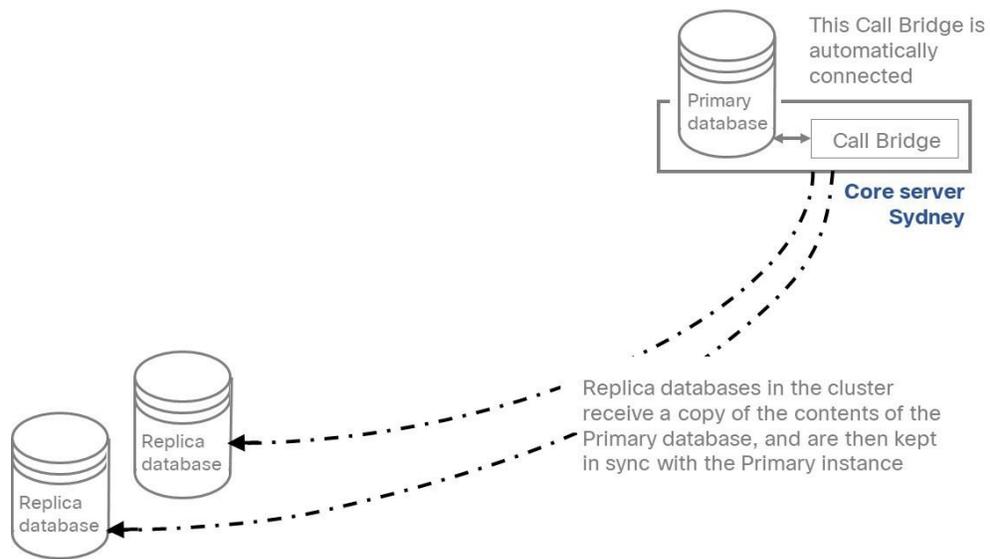
---

**注：** このコマンドを使用しない場合、Meeting Server は認証局のみを検証します。

---

- c. コマンド `database cluster join <primary hostname/IP>` を使用して、このデータベースをプライマリデータベースに「添付」し、次に `database cluster status` コマンドを使用して、以下に示すように進行状況を監視します。

図 16 : データベースを添付する



注：ホスト名は、下記の `database cluster join <primary hostname/IP>` コマンドで使用できますが、プライマリデータベースに指定されているインターフェースの IP アドレスに置き換えられます。

アタッチコマンドはプライマリデータベースのフルコピーをこのサーバーに取得するため、接続速度によっては時間がかかる場合があります。空のデータベースの場合、この処理には約 30 秒かかります。

```
cms> データベースクラスタ参加 10.1.2.3
```

警告!

このノードを既存のデータベースクラスタに添付してよろしいですか? (はい/いいえ)

このノードのデータベースのコンテンツは削除されます。

添付を開始しました...

```
cms> database cluster status>
```

```
Status      ;           : Attaching
```

```
Nodes :
```

```
  10.1.2.3           : Connected Primary
```

```
  10.1.2.8 (自分)   : Connected Replica
```

```
Interface      : a
```

```
cms> database cluster status
```

```
Status          : 有効
```

```
ノード :
```

```
  10.1.2.3           : Connected Primary
```

```
  10.1.2.8 (自分)   : Connected Replica
```

```
Interface      : a
```

これにより、ローカル Call Bridge がある場合、その再起動がトリガーされます。

- d. プライマリ データベース ホスト サーバーの MMP に `database cluster status` コマンドを入力して、プライマリデータベースが接続されたデータベースを認識していることを確認します。（この情報は、`join` コマンドが完了してから 10 秒以内に自動的に伝達されます。）

```

cms> database cluster status
Status                : Enabled
Nodes :
  10.1.2.3 (me)       : Connected Primary
  10.1.2.8            : Connected Replica
Interface             : a

```

## 5.5 データベースクラスタにリモート Call Bridge を接続する

データベース（プライマリまたは複製）と同じ場所にある Call Bridge は、その同じ場所にあるデータベースが属するデータベースクラスタに自動的に接続されます。

---

**注：**このホストサーバー上で `database cluster initialize` または `database cluster join` がすでに実行されている場合は、以下の `database cluster connect` コマンドを実行する必要はありません。サーバーはノード一覧に表示されます。`database cluster status` を実行して確認することができます。

---

「接続」とは、Call Bridge がクラスタ内のすべてのデータベースへのアクセス方法を認識していることを意味します。そのため、どのデータベースのアドレスを使って接続してもかまいません。（読み書きの対象となる実際のデータベースが、現在のプライマリデータベースです）。

1. 未接続の Call Bridge と Core サーバーの MMP にログインし、コマンド `database cluster connect <hostname/IP>` を発行します。ホスト名または IP アドレスは、クラスタ内のどのデータベースのものでもかまいません。

```

cms> database cluster connect 10.1.2.3
警告!!!
このノードを既存のデータベース クラスタに接続してもよろしいですか？（はい/いいえ）
接続が開始されました...

```

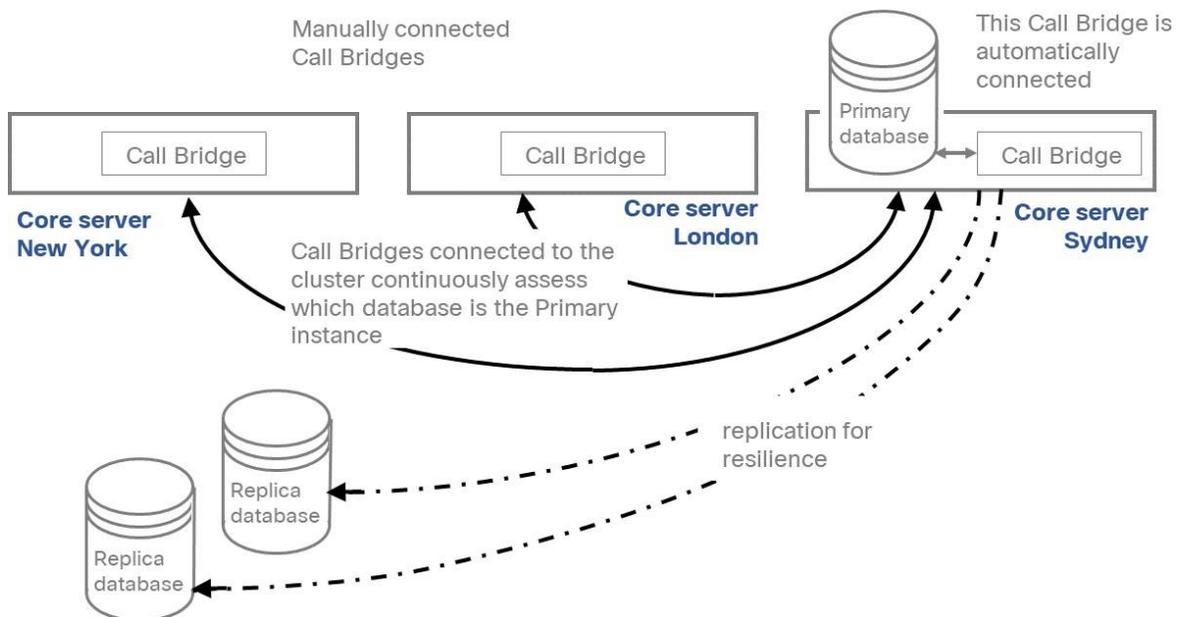
これにより、このコア サーバ上の Call Bridge が再起動されます。

---

**注：**前のセクションで使用したアタッチ コマンドとは異なり、接続コマンドはこの Call Bridge をホストするサーバ上の既存のデータベースを削除しません。そのため、既存のローカル データベースを持つコア サーバーでコマンドを使用する場合、データベースのコンテンツは破壊されませんが、ローカル データベースは、このサーバーの Call Bridge がクラスタから切断されるまで非表示になります。

---

図 17 : データベース クラスタリングと Call Bridge 接続の例



## 5.6 データベーススキーマをアップグレードする

**注：**最初にデータベースクラスタをセットアップするときは、この項は適用されません。しかし、以降のすべての Core サーバソフトウェアの更新後にこれらのステップを実行する必要があります。実行しない場合、Call Bridge とデータベースがデータベーススキーマに関して整合性が取れなくなることがあります。

クラスタ化システムのアップグレード手順は以下の通りです。

1. Meeting Server をアップグレードする前に、各サーバーの現在の設定のバックアップを取ります。 `backup snapshot <filename>` コマンドを使用します。バックアップをローカルサーバーに安全に保存します。

詳細については、[MMP コマンドリファレンス](#) ガイドを参照してください。アップグレードプロセス中に作成される自動バックアップファイルは使用しないでください。

2. `cms.lic` と証明書ファイルもローカルドライブに保存します。
3. データベースのクラスタステータスを確認してください。すべてのコール (SIP およびクライアント) が機能しており、障害状態が Web 管理ページにリストされていないことを確認します。プライマリデータベースを持つサーバーを特定します。
4. 複製データベースから開始し、プライマリデータベースで終了するまで、各データベースを 1 つずつアップグレードします。各サーバーが完全に起動し、データベースがデータベースクラスタに接続されるまで待ってから、次のサーバーをアップグレードします。クラスタへの完全な接続を確認するには、`database cluster status` コマンドを使用します。

この段階で、`database cluster status` は、すべてのノードが正常で同期中であるとレポートします。しかし、Call Bridge は正しく動作せず、データベースエラーが表示されます。

データベースサーバーが同期されるまで、次の手順に進まないでください。

5. プライマリデータベースをホストしているサーバーの MMP にログインし、次のコマンドを発行します。

```
database cluster upgrade_schema
```

6. データベースクラスタステータス を使って処理が正常に完了したことを確認する  
有効のステータスは成功を意味し、エラーは問題を示します。
7. 各 Call Bridge のウェブ管理インターフェイスがスペースのリストを表示できることを確認します。

## 5.7 データベースクラスタに関する詳細情報

データベースクラスタの詳細については、Cisco Meeting Server の [FAQ](#) を参照してください。

## 6 Call Bridge の展開

この章では、展開に複数の Call Bridge をセットアップして展開する方法について説明します。以下の内容が含まれます。

- [Call Bridge に必要な証明書](#)の概要
- [Call Bridge のリスニングインターフェイス](#)の設定
- [複数の Call Bridge](#) をクラスタ化する方法
- [ダイヤルプラン情報](#)
- Cisco Unified Communications Manager または Cisco Expressway で導入されている Meeting Server で、[着信および発信通話の負荷分散を行う Call Bridge グループの使用](#)
- [Call Bridge と Lync Edge のインテグレーション](#)に関する情報
- 適切な [Call Bridge モードを選択した、デュアルホーム電話会議の参加者の接続](#)
- 配信リンクでの[ビデオストリーム追加機能のプレビュー](#)

特に断りのない限り、この説明は結合されたマルチサーバまたは分割されたマルチサーバの展開に等しく適用されます。

### 6.1 Call Bridge の証明書の設定

Call Bridge には、SIP 通話制御デバイスおよび Lync フロントエンド サーバーとの TLS 接続を確立するために使用されるキーと証明書のペアが必要です。

Lync を使用している場合、この証明書は Lync FE Server により信頼されている必要があります。これを達成する最良の方法は、Lync FE サーバーの証明書を発行した CA サーバーの証明書に署名することです。

証明書の作成、アップロード、および Call Bridge への割り当てについての情報は、[『証明書ガイドライン』](#)に記載されているステップに従います。

### 6.2 Call Bridge のセットアップ

まだ行っていない場合は、各 Call Bridge で以下の手順を実行します。

#### 1. Call Bridge のリスン インターフェイスを設定する

コマンド `callbridge listen <インターフェイス>`を使用して、リスンするインターフェイスを設定できます (A、B、C または D から選択)。デフォルトでは、Call Bridge はどのインターフェイスもリスンしません。コマンドの完全な一覧については、[『MMP コマンドリファレンスガイド』](#)を参照してください。

リスニング インターフェイスを次のように設定します。

- a. インターフェイス A でリスンするように Call Bridge を設定します。

```
callbridge listen a
```

- b. 次のように入力して、セキュリティ証明書先に作成したものを使用するよう Call Bridge を設定します (これにより、Lync FE サーバーと Call Bridge 間の TLS 接続が確立されます)。

```
callbridge certs callbridge.key callbridge.crt
```

完全なコマンドと CA が提供する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 ドキュメントに記載されています。

- c. Call Bridge を再起動して変更を適用します。

```
callbridge restart
```

---

**注：** Web Bridge を設定した後、すべての Web Bridge のトラストストアに Call Bridge の証明書を追加する必要があります。詳細は、[『証明書ガイドライン』](#) を参照してください。

---

### 6.3 Call Bridge のクラスタリング

Meeting Server 展開内で、Call Bridge クラスタリングを有効にできます。これにより、複数の Call Bridge が単一のエンティティとして動作し、単一の Call Bridge のキャパシティを超えてスケールすることができます。

ピアツーピアでリンクするようにクラスター内の Call Bridge をセットアップするか、クラスター化された Call Bridge 間の通話制御デバイス経由で通話をルーティングするかを選択できます。

Call Bridge をピアツーピアにリンクする：

- 通話のルーティングを妨げる中間のものがいないため、Call Bridge A から Call Bridge B に直接移動するため、通話の複雑さが軽減されます。
- これにより、通話コントロールデバイスの負荷が軽減され、通話コントロールデバイスを経由してルーティングする必要がある通話を処理するためのリソースを解放します。これは、通話制御デバイスが通話ベースでライセンスされている場合に重要です。

通話コントロールデバイス経由のルーティング：

- Meeting Server とローカル SIP デバイスに一貫したコールフローを作成します。これにより、ネットワーク構成が少し簡単になります。特に、通話コントロール デバイスを介してルーティングされる通話のみを許可する固定の「許可ルール」を持つネットワーク間にファイアウォールがある場合に役立ちます。

クラスタ化された Call Bridge の導入で通話がルーティングされる方法は、ピアリンク SIP ドメインフィールド (下記を参照) とダイヤルプラン ([セクション 6](#) を参照) によって決定されます。

次の手順に従って、Call Bridge をクラスタ化します。

---

**注：** この項の手順は、以下を想定しています。

- すべてのデータベースがクラスタとして実行されている。
-

- 
- クラスタの一部を形成するすべての Call Bridge は、スタンドアロンの Call Bridge として設定されている。
  - すべての Call Bridge がデータベースクラスタに接続されている。
- 

Call Bridge クラスタに含まれるようになる、すべての Call Bridge について、

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

---

**注：**まだデータベースクラスタを作成していない場合、**[設定 (Configuration)]** ドロップダウンメニューに **[クラスタ (Cluster)]** は表示されません。

---

2. **[Call Bridge のアイデンティティ]** セクションで、Call Bridge の一意の名前を入力し (例、「London- Core1」)、**[送信]** をクリックします。

---

**注：**固有の名前にはスペースを含めることはできません。一意の名前にスペースが含まれる場合、Call Bridge クラスタリングは失敗します。

---

3. ピアリンクビットレートを入力します。これは、サーバーが分散通話で接続する 1 通話あたりのレートです (オプション)

クラスタの一部となる Call Bridge の一つで、

4. Web 管理インターフェイスにサインインし、**[設定 (Configuration)]** > **[クラスタ (Cluster)]** に移動します。**[クラスタ化された Call Bridge (Clustered Call Bridges)]** の見出しがついた表で、

- a. ステップ 2 で入力したこの Call Bridge の一意の名前を使用して、この Call Bridge のエントリーを追加します。
- b. クラスタ内の他のサーバーから HTTPS 経由で Call Bridge の Web 管理インターフェイスに到達できるアドレスを追加します。このアドレスは、例えば参加者リストなどの管理メッセージに使用されます。注：ウェブ管理は、インターフェース A から D だけでなく管理インターフェースでもリッスンするように設定できます。
- c. **[ピアリンク SIP ドメイン]** を指定する場合、ピア コールでリモート サーバーに発信するときに、そのドメインが使用されます。SIP プロキシとして使用するために定義されたコール制御を持つアウトバウンドルールをセットアップした場合、コール制御デバイスにルーティングすることができます。または、コールコントロールなしで直接のルーティングに使用する SIP プロキシとして、発信通話に Meeting Server の FQDN を入れることで、直接発信することもできます。既存のコール制御を通してルーティングする場合、ピアリンク SIP ドメインには固有のドメインまたは各サーバーの FQDN を使用することを推奨します。これにより、すべてで同じドメインを使用している場合に発生する偶発的な呼び出しループを防ぐことができます。
- d. **[追加]** をクリックします。

- e. クラスターの一部となる Call Bridge ごとに、ステップ [4a](#) から [4d](#) を繰り返し、各 Call Bridge に対してステップ [2](#) で設定した固有の名前を入力します。

[クラスター化された Call Bridge] という見出しのテーブルには、クラスターの一部となる Call Bridge ごとに 1 つのエントリがあり、[Call Bridge アイデンティティ] セクションの [一意の名前] により、これがどの Call Bridge であるかが識別されます。

Call Bridge identity

Unique name: London-Core1  
Peer link bit rate: 2000000  
Submit

Clustered Call Bridges

	Unique name	Address	Peer link SIP domain	Status	
<input type="checkbox"/>	London-Core1	https://192.186.5.33		[this Call Bridge]	<a href="#">[edit]</a>
<input type="checkbox"/>	London-Core2	https://192.186.75.10		connection active; time since last heartbeat: 0 seconds	<a href="#">[edit]</a>
<input type="checkbox"/>	Sydney-Core3	https://172.61.31.85		connection active; time since last heartbeat: 7 seconds	<a href="#">[edit]</a>
<input type="checkbox"/>	NY-Core4	https://172.62.33.46		connection active; time since last heartbeat: 1 second	<a href="#">[edit]</a>
<input type="checkbox"/>	HK-Core3	https://175.10.55.35		connection active; time since last heartbeat: 4 seconds	<a href="#">[edit]</a>

1  
Delete

クラスター化された Call Bridge テーブルの情報は、クラスター内のすべての Call Bridge に複製されます。そのため、任意の Call Bridge サーバーに移動して Web ウェブ管理インターフェイスにログインし、[設定 (Configuration)] > [クラスター (Cluster)] に進み、クラスター化されたすべての Call Bridge のステータスを確認します。

これで Call Bridge クラスターがセットアップされ、クラスター化された Call Bridge は同じダイヤルプラン (着信、発信、および着信転送のダイヤルプランルール) を共有します。次のステップでは、クラスター化された Call Bridge 間のピア間コールのダイヤルプランを設定する必要があります。「[ピア間通話のダイヤルプランルールを設定する](#)」を参照してください。

**注:** [設定 (Configuration)] > [クラスター (Cluster)] ページでは、Web 管理者の IP アドレスを使用する必要があります。ただし、Call Bridge 間でコールをルーティングする発信ダイヤルプランを設定する場合は ([ピアリンク SIP ドメイン (Peer link SIP domain)] フィールドが空の場合)、Call Bridge の [domain] フィールドと [sip proxy address] フィールドの両方で Call Bridge の IP アドレスを使用する必要があります。詳細は、「[相互ピア通話用のダイヤルプランルールを設定する](#)」を参照してください。

### 6.3.1 Call Bridge クラスターの検証

クラスター内の Call Bridge を検証するための Call Bridge 信頼ストアを使用することで、Call Bridge クラスターのセキュリティを向上させることができます。Call Bridge はウェブ管理の前面にある HTTPS を介してお互いに接続するため、クラスター化された Call Bridge のウェブ管理証明書を持する証明書バンドルを作成し、クラスター内のそれぞれの Call Bridge の信頼ストアに証明書バンドルをアップロードする必要があります。

---

**注：**バージョン 3.4 以降、「`callbridge trust cluster`」が有効な場合に証明書名の検証が実装されました。このため、クラスタリングで設定されたピアは、

---

対応する Web 管理証明書の正確な FQDNと一致する必要があります。この設定を行わないと Call Bridge クラスタが失敗します。

---

詳細については、[『スケーラブルでレジリエントなサーバー導入のための証明書ガイドライン』](#)を参照してください。

### 6.3.2 クラスタ化された Call Bridge 展開での DTMF シーケンスの使用

---

**注：**この機能は、デュアルホーム電話会議の Lync 参加者への DTMF シーケンスの送信には対応していません。

---

参加者の DTMF シーケンスを設定できます。これにより、電話会議の参加者がどの Call Bridge に接続しているかに関係なく、DTMF シーケンスをその参加者に送信できます。同様に、コールアウトの参加者 API を使用して、Call Bridge クラスタからコールアウトするときに、DTMF を送信できるようになりました。これは、発信コールの Call Bridge が、負荷分散、ダイヤルプランルール、または Call Bridge グループまたは Call Bridge の選択によって、暗黙的または明示的に選択される場合に適用されます。

- クラスタ化された負荷分散された導入で遠端に DTMF キー シーケンスを送信するには、次の手順を実行します。

`calls/<call id>/participants` への POST、`dtmfSequence` パラメータに 0 から 9 までの数字、#、および数字と数字の間にポーズを追加する「,」で構成される文字列を指定します。

これにより、参加者が最初に作成されたとき、または通話中に、DTMF シーケンスが遠端に送信されます。

- 通話中の特定の参加者に再生する DTMF シーケンスを設定する方法：  
`/participants/<participant id>` への PUT、パラメータは `dtmfSequence`。

## 6.4 ダイヤルプラン情報

[第 1 章](#)では、スケーラブルでレジリエントな導入のためのダイヤルプラン（着信ダイヤルプランルール、発信ダイヤルプランルール、着信転送ルール）の設定について説明します。必要な特定のダイヤルプランルールとその優先順位は、展開によって異なります。Meeting Server の展開のトポロジだけでなく、通話制御プラットフォームにも依存し、ローカル リソースを使用するか、通話をロード バランシングするかどうかも決定します。

この項では、ダイヤルプランを設定するときに行う必要があるいくつかの決定について説明します。ダイヤルプランはデータベース サーバーに保存されます。ダイヤルプランは、Call Bridge クラスタ内の任意の Call Bridge から修正できます。任意の Call Bridge のウェブ管理インターフェイスで完全なダイヤルプランを確認することもできますが、API を使用してダイヤ

ルプランをセットアップすることをお勧めします。これにより柔軟性が向上するためです。発信ダイヤルプランルールは、クラスター化された Call Bridge の API 経由で設定する必要があります。付録 1 に API の使用例を示します。

たとえば、クラスター内のすべての Call Bridge で同じ発信ダイヤルプランを使用することができますが、これにより地理的な違いが許容されなくなります。ロケーションとトポロジを考慮するために、すべての Call Bridge に適用されるルールと、API で指定する 1 つの Call Bridge に固有のルールを組み合わせることも可能です。たとえば、+01 番号への発信を常に米国の Call Bridge から行う場合などです。

[設定 (Configuration) ] > [発信通話 (Outbound calls) ] のウェブ管理者インターフェイスのページに、[Call Bridge の範囲 (Call Bridge Scope) ] という列があります。この列を編集することはできません。API で設定された内容を表示するだけです。特に、ルールが特定の Call Bridge に適用される場合、ルールが適用される Call Bridge は表示されません。

---

**注：**もし [Call Bridge の範囲 (Call Bridge Scope) ] が [All] に設定されている場合、これは API 範囲設定が「global」に相当し、[Call Bridge の範囲 (Call Bridge Scope) ] が [One] の場合は、API の「callbridge」の範囲に相当します。

---

ダイヤルプランルールを設定するときは、次のことを確認します。

- 通話の発信ダイヤルプランエントリは、クラスター内のすべての Call Bridge で有効です。つまり、[Call Bridge の範囲 (Call Bridge Scope) ] が [All] である Web 管理者インターフェイスで使用するか、[One] の設定を持つルールは、ルールが適用される Call Bridge を指定するために API を使用して完全に定義されています。
- SIP 通話用に構成された着信ダイヤルプランは、クラスターの外部からクラスター内の Call Bridge にルーティングされるドメインのセットをカバーします。

#### 6.4.1 相互ピア通話のダイヤルプランルールを設定する

Call Bridge 間のピア間通話は、発信側の Call Bridge の発信ダイヤルプランルールを使用して発信されます。

Call Bridge 間で直接通話を発信する場合は、[ピアリンク SIP ドメイン (Peer link SIP domain) ] フィールドを空白にしておく必要があります ([設定 (Configuration) ] > [クラスタ (Cluster) ] ページ)。コール制御デバイス経由で Call Bridge 間でピア間通話を行う場合、各 Call Bridge の FQDN で [ピアリンク SIP ドメイン (Peer link SIP domain) ] フィールドを設定する必要があります。発信ダイヤルプランルールは、導入で使用した方法に応じて設定する必要があります。

- [設定 (Configuration) ] > [クラスタ (Cluster) ] ページで [ピアリンク SIP ドメイン (Peer link SIP domain) ] フィールドを空にしている場合、ピア間通話は randomURI@callbridge\_ip\_address の形式で発信されます。例えば、Call Bridge A (IP アドレス 10.10.10.10) が Call Bridge B (IP アドレス 10.10.10.20) にピア間コールを発信する場合、Call Bridge A からの発信コールには、randomURI@10.10.10.20 の形式の SIP アドレスが割り当てられます。

この場合、各 Call Bridge は、ピアの IP アドレスに基づいて、各ピアへの発信ダイヤルプランルールを必要とします。そのため、発信ダイヤルプランルールは、[ドメイン (Domain) ] フィールドと [使用する SIP プロキシ (Sip proxy to use) ] フィールドの両方で、ピア Call Bridge の IP アドレスで設定する必要があります。

- [ピアリンク SIP ドメイン (Peer link SIP domain) ] をピア Call Bridge の FQDN で設定している場合、ピア間コールは randomURI@callbridge\_FQDN の形式で発信されます。例えば、Call Bridge A (FQDN : callbridgeA.example.com) が Call Bridge B (FQDN : callbridgeB.example.com) にピア間通話を発信する場合、Call Bridge A からの発信通話には、randomURI@callbridgeB.example.com の形式の SIP アドレスが割り当てられます。

この場合、各 Call Bridge は、ピアの FQDN に基づいて、各ピアへの発信ダイヤルプランルールを必要とします。そのため、発信ダイヤルプランルールは、[ドメイン (Domain) ] フィールドにピア Call Bridge の FQDN を使用し、[使用する SIP プロキシ (SIP proxy to use) ] フィールドにコール制御デバイスのアドレスを使用して設定する必要があります。

---

**注：** Call Bridge 間のピア間通話は、発信側の Call Bridge の発信ダイヤルプランルールを使用して発信されます。そのため、発信が IP アドレスに対するものである場合、発信ダイヤルプランルールを追加して、SIP プロキシ経由ではなく、もう一方の Call Bridge に直接発信する必要があります。ただし、ドメインダイヤルを使用している場合、既存の発信ダイヤルプランルールは、ピア間通話をすでにカバーしている可能性があります。

---



---

**注：** Call Bridge 間のピア間シグナリングは HTTPS を使用します。

---



---

**注：** 同じダイヤルプランルールの優先順位を持つ発信コールは、他の地理的な場所にあるコール制御デバイスよりもローカルのものを優先します。

---

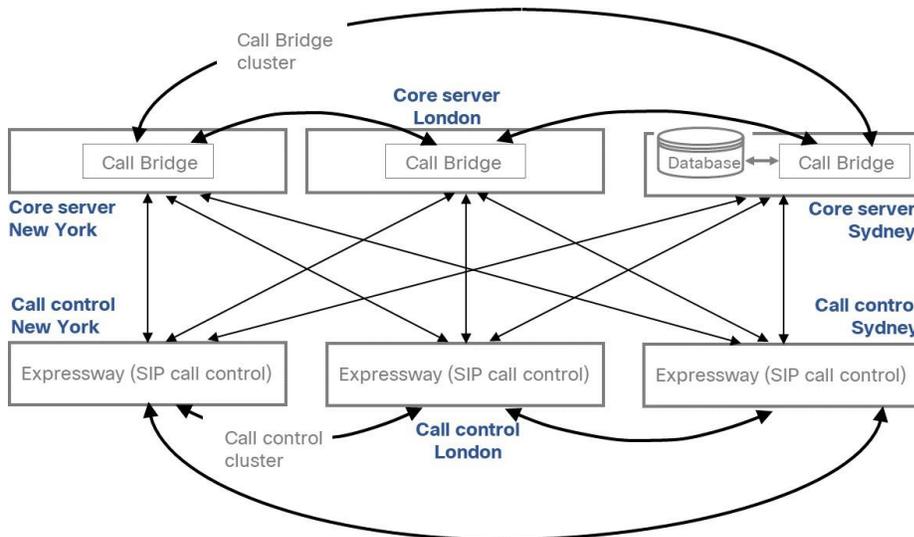
#### 6.4.2 例

これらの例では Cisco VCS を使用しますが、概念はコール制御装置から独立しています。

最も単純なケースでは、単一の VCS が Meeting Server に接続され (したがって単一の Call Bridge にも)、SIP エンドポイントとの統合が提供されます。複数のデータセンターにまたがる複数の Call Bridge の大規模な導入では、ダイヤルプランについてより詳細に考える必要があります。

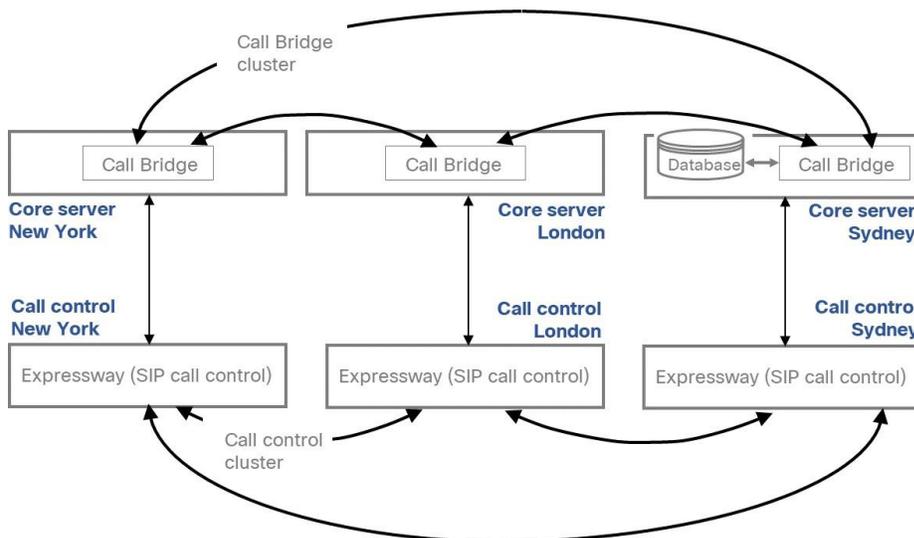
例 1 オプションの 1 つは、VCS のクラスターを設定して、Call Bridge のクラスターに通話を転送することです。これにより、任意の VCS が通話を任意の Call Bridge にルートでき、任意の Call Bridge からの通話は任意の VCS にルートできるため、レジリエンスが確保されます (下の図を参照)。

図 18 : SIP コール制御のメッシュ構成



例 2 : 地理的に分散したコール制御システムがある場合、これらの VCS を選択的にローカルな Call Bridge にトランキングするように選択できます。例えば、ロンドンの VCS をロンドンの Call Bridge にトランキングし、ニューヨークの VCS をニューヨークの Call Bridge にトランキングすることができます。これにより、メディアがデータセンター間で不必要に移動することがなくなり、複数のロケーションにまたがる電話会議がある場合でも、データセンター間の帯域幅の使用を最小限に抑えるために、Call Bridge 間に単一のピアリンクが存在します。

図 19 : SIP コール制御の地理的な設定例



## 6.5 Meeting Server 間のコールのロードバランシング

Call Bridge のグループ機能を使用して、クラスタ化された Meeting Server で着信および発信通話の負荷を分散し、クラスタ内の個々の Meeting Server の過負荷を回避します。

Call Bridge グループを設定すると、Meeting Server クラスタは、同じロケーション内の Call Bridge または異なるロケーションにあるノード間で、インテリジェントにコールの負荷分散を行うことができます。通話の発信先であるインテリジェントな判断は、Meeting Server が行います。コール制御システムは、コールを適切なロケーションに転送するために、Meeting Serverからの SIP メッセージを処理できる必要があります。この機能は、Cisco Unified Communications Manager および Cisco Expressway を通話制御システムとして使用してテストされています。これらは、この機能に対して Cisco がサポートする唯一の通話制御システムです。Cisco Expressway による負荷分散については、Cisco Expressway リリース X8.11 以降と Cisco Meeting Server リリース 2.4 以降を使用してください。

[Cisco Meeting Server のロードバランシング通話に関するホワイトペーパー](#)は、Cisco Unified Communications Manager と Cisco Expressway をコール制御デバイスとして使用した導入例を示しています。

---

**注：**単一またはクラスタの Meeting Server と比較して、Call Bridge グループの Meeting Server のコールキャパシティは異なります。この文書は、コールキャパシティの違いの概要を示します。

---

**注：**Call Bridge グループでロードバランシングを使用していない場合、通話は拒否されませんが、負荷制限に達したときにすべての通話の品質が低下します ([セクション 6.5.2](#) を参照)。これが頻繁に発生する場合は、追加のハードウェアを購入することをお勧めします。

Meeting Serverにロードされているメディアを確認するには、API オブジェクトに対して GET を実行します `/system/load` にアクセスしてください。パラメータ `mediaProcessingLoad` の数値が返されます。これは Meeting Server の負荷を表します。

---

### 6.5.1 Call Bridge グループ

コールのロード バランシングは、同じロケーションに存在する Call Bridge のグループ間で発生します。各ロケーションにある Call Bridge を設定するために、Call Bridge グループの概念が使用されます。Call Bridge グループは、より緊密にリンクされ、同等のものとして扱われる必要があるクラスタ ノードのサブセットを定義します。これは、単一のデータセンターにあるもの、または同じ大陸にあるものを指します。Call Bridge をグループ化する方法の決定は、ネットワーク構成の詳細と望ましい動作によって異なります。

ロード バランシング機能が正しく動作するためには、Call Bridge グループのサーバーで往復時間 (RTT) が 100 ms 未満である必要があります。同じクラスタ内の任意の 2 つのノード間の最大 RTT は 300 ms のままです。

Cisco Unified Communications Manager を使用している場合、コールルーティングは Cisco Unified Communications Manager 展開全体のルートパターン、ルートグループ、およびルートリストに依存します。これらの概念について理解していることを前提としています。これらの機能の設定に関する情報は、[Cisco Unified Communications Manager のドキュメント](#)を参照してください。

Cisco Expressway を使用する場合、コール ルーティングはダイヤル プランとゾーンの使用に依存し、これらの概念を理解していることが前提となります。通話が置き換えられた場合に、Cisco Expressway が呼び出し先のドメインにルーティングできることを確認してください。ダイヤルプランとダイヤルゾーンの設定については、[Cisco Expressway のドキュメントを参照してください](#)。

通話のロードバランシングの例については、Cisco ホワイトペーパー [「Cisco Meeting Server 全体で通話負荷分散する」](#) 参照してください。

### 6.5.2 着信通話を負荷分散するための Call Bridge の設定

Meeting Server クラスタ全体でのコールのロードバランシングの設定には、3 つの側面があります。

- Call Bridge グループを作成する
- ロードバランシングを有効にする
- オプションで、各 Call Bridge のロード バランシングを微調整します。ほとんどのデプロイメントでは、これは必要ありません。

さらに、着信通話の負荷分散には、Call Bridge から Cisco Unified Communications Manager または Cisco Expressway への発信通話が含まれます。これらの発信通話を機能させるには、発信ダイヤル プラン ルールを構成する必要があります。次を参照してください。[発信 SIP 通話の負荷分散](#)。

---

**注：** Call Bridge から Cisco VCS への着信通話の負荷分散が、Cisco Expressway ではなく、Cisco VCS で行われる場合、VCS にトラバーサルライセンスが必要です。Meeting Server の負荷分散を行う場合、Cisco Expressway でのリッチメディアセッションライセンスは必要ありません。

---



---

**注：** Call Bridge グループで負荷分散を使用していない場合、通話は拒否されませんが、負荷制限に達したときにすべての通話の品質が低下します。これが頻繁に発生する場合は、追加のハードウェアを購入することをお勧めします。

---

#### Call Bridge グループの作成

1. 各 Meeting Server クラスタについて、例えばデータセンター、国や地域など、Call Bridge をグループ化する方法を決定します。
2. クラスタ内のいずれかのサーバーのウェブ管理インタフェースを使用して、**[設定>API]** を選択します。
3. 新しい Call Bridge グループの作成
  - a. API オブジェクトのリストで、/api/v1/callBridgeGroups の後ろの ▶ をタップします。
  - b. **[新規作成]** ボタンを選択し、新しい callBridgeGroup の名前を入力し、Call Bridge グループのパラメータを設定します。**[作成 (Create) ]** を選択します。
  - c. 新しいグループが callBridgeGroups のリストに表示されます。

4. グループ化する Call Bridge を特定する
  - a. API オブジェクトのリストで、/api/v1/callBridges の後ろの ▶ をタップします。
  - b. [callBridge id] をクリックして、グループに追加する各 Call Bridge を選択します
    - i. [callBridgeGroup] フィールドの隣にある [Choose] ボタンをクリックし、ステップ 3b で作成した callBridgeGroup を選択します。
    - ii. [変更 (Modify) ] をクリックします。
  - c. Call Bridge グループに追加する必要がある各 Call Bridge に対して、ステップ 4b を繰り返します。
5. 他のすべての Call Bridge グループについても繰り返します。

#### クラスターの負荷制限を指定し、負荷分散を有効にする

1. クラスターの各 Call Bridge で、そのサーバーの負荷制限を指定します
  - a. API オブジェクトのリストで、/system/configuration/cluster の後の ▶ をタップします。
  - b. [View or edit (表示または編集)] ボタンを選択して loadLimit の値を入力します。[変更 (Modify) ] ボタンをクリックします。これにより、サーバーの最大負荷制限が設定されます。負荷制限については、表 6 を参照してください。

表 6 : サーバプラットフォームの負荷制限

システム	負荷制限
ミーティングサーバ 2000 M5v2	875,000
ミーティングサーバ 2000 M6	1,296,000
ミーティングサーバ 1000 M5v2	120,000
ミーティングサーバ 1000 M6	160,000
VM	vCPU ごとに 1250

**注 :** Meeting Server 1000 M5v2 および Meeting Server 2000 M5v2 の負荷制限の増加には、Meeting Server ソフトウェアバージョン 3.2 が必要です。

Call Bridge に負荷制限を設定すると、現在の負荷に基づいて通話を拒否するようになります。デフォルトでは、新しい参加者からの通話の拒否は、通話を分配するための負荷制限の 80% で発生します。この値は微調整することができます。以下を参照してください。

2. クラスター内の各サーバーで負荷分散を有効にします。
 

Cisco Unified Communications Manager 展開の場合 :

  - a. API オブジェクトのリストで、[/callBridgeGroups の後ろの ▶ をタップします。
  - b. Cisco Unified Communications Manager にランキングされた Call Bridge グループの **オブジェクト ID** をクリックします。

c. loadBalancingEnabled=true に設定します。[変更 (Modify) ] をクリックします。

Cisco Expressway 導入の場合 :

- a. API オブジェクトのリストで、/callBridgeGroups の後ろの ▶ をタップします。
- b. Cisco Expressway にランキングされた Call Bridge グループの オブジェクト ID をクリックします
- c. loadBalancingEnabled=true および loadBalanceIndirectCalls= trueを設定します。[変更 (Modify) ] をクリックします。

---

**ヒント :** Call Bridge が 1 つしかなく、通話の品質を落とさずに拒否する場合は、単一の Call Bridge で Call Bridge グループを作成し、負荷分散を有効にします。

---

### 負荷分散の微調整

負荷分散パラメータを微調整することは可能ですが、ソリューションの可用性に影響を与える可能性があるため注意してください。デフォルト値を変更すると、サーバーに負荷がかかり、ビデオ品質が低下する場合があります。これは、電話会議が複数の Call Bridge に断片化しているか、または電話会議が単一の Call Bridge で使用するリソースが多すぎることで発生する可能性があります。

Call Bridge の負荷分散通話は、3 つのパラメータによって制御されます。

- loadLimit - 上記で設定した Call Bridge の最大負荷の数値。
- newConferenceLoadLimitBasisPoints - 負荷制限の基準点 (10,000 分の 1) の数値で、この数値に達すると、アクティブでない会議への着信が不利になります。範囲は 0 から 10000 で、デフォルトは 5000 (50% の負荷) です。値は LoadLimitを基準に調整されます。
- **既存の** ConferenceLoadLimitBasisPoints - この Call Bridge への着信を拒否する負荷制限のベースポイントの数値です。範囲は 0 から 10000 までで、デフォルトは 8000 (80% の負荷) です。値は LoadLimitを基準に調整されます。

Call Bridge のデフォルトのしきい値を変更するには、次の手順を実行します。

1. API オブジェクトのリストで、/system/configuration/cluster の後の ▶ をタップします。
2. [表示または編集 (View or edit) ] ボタンを選択して、newConferenceLoadLimitBasisPointsと existingConferenceLoadLimitBasisPoints の値を設定します。[変更 (Modify) ] をクリックします。

---

**注 :** ディストリビューションの呼び出しは常に受け付けられ、追加のリソースを消費します。負荷分散パラメータを変更する場合、これらの呼び出しに必要なオーバーヘッドが計算に含まれていることを確認してください。

---

## 設定がロードバランシングにどのように使用されるか

各 Call Bridge グループ内では、各スペースに選択される Call Bridge の特定の優先順位があります。Call Bridge グループ内のスペースへの着信は、この順序に基づいて優先的に Call Bridge にリダイレクトされます。リダイレクションは、既存の会議のしきい値と新しい会議のしきい値の 2 つのしきい値に基づいて行われます。

しきい値は次のように定義されます。

既存の会議しきい値 =  $\text{existingConferenceLoadLimitBasisPoints}/10000 \times \text{loadLimit}$

の新しい会議しきい値 =  $\text{newConferenceLoadLimitBasisPoints}/10000 \times \text{負荷制限}$

通話が Call Bridge に到達すると、負荷制限が確認され、負荷制限が既存の会議のしきい値を上回る場合、通話は拒否されます。通話は他の理由でも拒否されることに注意してください。拒否された通話は、通話制御デバイスによってリダイレクトされる必要があります。

負荷制限が既存の会議のしきい値を下回っている場合、通話に応答があり、IVR は通過します。電話会議が認識されると、グループ内の Call Bridge の優先順位が決定されます。この順序は、選択できる Call Bridge が複数ある場合に、Call Bridge 間で決定するために使用されます。

グループ内のいずれかの Call Bridge がすでに電話会議を実行している場合、これらの Call Bridge の負荷制限が確認されます。これらのいずれかが既存の電話会議のしきい値を下回っている場合、これらのいずれかが使用されます。

Call Bridge がまだ選択されていない場合は、負荷制限が既存の電話会議のしきい値よりも小さい Call Bridge の 1 つが選択されます。

### 6.5.3 発信 SIP 通話の負荷分散

Call Bridge グループは、着信 SIP 通話に加えて、発信 SIP 通話の負荷分散をサポートします。アウトバウンド SIP コールの負荷を分散するには、次の操作を行います。

- [スペースからの発信 SIP コールのロードバランシングを有効にする。](#)
- [アウトバウンド SIP コールのロードバランシングのための発信ダイヤルプランルールをセットアップする。](#)
- [発信 SIP 通話に Call Bridge グループまたは特定の Call Bridge を提供します。](#)

ロードバランシングが有効になると、発信 SIP 通話は次のロジックに従います。

- ドメインに一致する最も高い優先順位の発信ダイヤル プラン ルールを見つけ、
  - これがローカル Call Bridge に適用される場合、ローカル Call Bridge グループ内で通話を分散します。
  - これがリモート Call Bridge にのみ適用される場合、Call Bridge がメンバーである Call Bridge グループ内で通話の負荷分散を行います。

---

**注：**Lync クライアントからの、または Lync クライアントへの通話の負荷分散は、現在 Call Bridge グループではサポートされていません。

---

### 発信 SIP 通話の負荷分散を有効にする方法

スペースからのアウトバウンド SIP コールをロードバランシングしようとする特定の Call Bridge グループでの Call Bridge の設定方法は次のとおりです。

1. API オブジェクトのリストで、[/callBridgeGroups の後ろの ▶ をタップします。
2. 選択した Call Bridge グループの **オブジェクト ID** をクリックするか、[new (新規作成)] をクリックして、新しい Call Bridge グループを作成します。
3. loadBalanceOutgoingCalls = true に設定します。[変更 (Modify) ] をクリックします。

発信コールの負荷分散を行うには、グループ内の各 Call Bridge に同じダイヤル プラン ルールが設定されている必要があります。

### 発信 SIP 通話をロードバランシングするための発信ダイヤルプランルールをセットアップする方法

発信 SIP コールを負荷分散するための発信ダイヤル プラン ルールをセットアップするには、3 つの方法があります。

1. すべての発信ダイヤルプランルールで **スコープ** パラメータを global に設定します。これにより、すべての Call Bridge がすべての発信ダイヤル プラン ルールを使用して、一致するドメインに到達できるようになります。
2. Call Bridge グループの各 Call Bridge に同一の発信ダイヤルプランルールを作成します。Scope パラメータを callBridge に設定してください。callBridge パラメータを使用して、Call Bridge の ID を設定します。
3. 特定の Call Bridge グループの発信ダイヤルプランルールを作成します。Scopeパラメータを callBridgeGroup に設定し、callBridgeGroup パラメータをIDの Call Bridge グループに変更します。

発信コールの負荷分散を使用する前に、Call Bridge グループの各 Call Bridge について、既存の発信ダイヤル プラン ルールを確認します。

1. API オブジェクトのリストで、/outboundDialPlanRules の後 の ▶ をタップします。
2. 新しい発信ダイヤルプランルールを作成するか、または発信 SIP 通話の負荷分散に使用する既存の発信ダイヤルプランの **オブジェクト ID** をクリックします。
3. によるダイヤルプランの使用計画に応じて、scope、callBridge、callBridgeGroup の設定を選択します。（上記の 3 つの代替方法を参照）

### 参加者への発信 SIP 通話に使用する Call Bridge グループまたは特定の Call Bridge の提供方法

特定の Call Bridge グループから発信するには、

1. API オブジェクトのリストで、/calls の後ろの ▶ をタップします。
2. 個々の通話の **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**から `api/v1/calls/<call id>/participants` を選択します。
4. パラメータを下にスクロールして `callBridgeGroup` に移動し、ボックスにチェックを入れ、**[Choose (選択)]** をクリックします。この通話に使用する Call Bridge グループの **オブジェクト ID** を選択します。**[作成 (Create)]** をクリックします。

#### アクティブで空の電話会議のロードバランシングを処理する

ロード バランシング アルゴリズムは、電話会議がすでにアクティブになっている Call Bridge に新しい通話を優先的に発信します。空の電話会議を Call Bridge で開始するには、次を選択します：`/calls` を API オブジェクトリストから選択して、**[新規作成]** をクリックします。既定では、これらの空の電話会議はアクティブとして扱われます。つまり、空の電話会議への最初の通話は、優先的にこの Call Bridge にロード バランシングされます。空の電話会議を使用して優先的にロードバランシングされないようにするには、会議を作成する際にパラメータ `active whenEmpty` を `false` に設定します。

#### 6.5.4 ウェブアプリの呼び出しを負荷分散する

Cisco Unified Communications Manager または Cisco Expressway を通じたインバウンドとアウトバウンドの SIP 通話に加えて、Call Bridge グループを使用した負荷分散は、ウェブアプリの参加者にも適用できます。

- スペースのメンバーとして参加するウェブ アプリ ユーザ
- ウェブ アプリ ユーザーがスペースの非メンバーとして、パスコードあり、なしで参加する
- ゲスト ユーザーがスペースに参加する

ロード バランシングが機能していることを確認するために、Call Bridge グループ内の各 Call Bridge は、同じ Web Bridge に接続する必要があります。

---

**注：**ウェブアプリのみを使用して発信する (SIP 通話は除く) 展開では、通話の負荷分散にコール制御デバイスは必要ありません。

---

#### ウェブアプリ参加者の負荷分散を有効にするウェブアプリ参加者の負荷分散を有効にするには：

1. API オブジェクトのリストで、`/api/v1/callBridgeGroups` の後ろの ▶ をタップします。
2. Call Bridge グループのオブジェクト ID を選択します。
3. `loadBalancingEnabled = true` に設定します。
4. `loadBalanceUserCalls = true` に設定します。
5. **[変更 (Modify)]** をクリックします。

#### ウェブ アプリ参加者の負荷分散を無効にする

SIP 通話の負荷分散を継続しながら、ウェブアプリ参加者の負荷分散を無効にするには：

1. API オブジェクトのリストで、`/api/v1/callBridgeGroups` の後ろの ▶ をタップします。
2. Call Bridge グループのオブジェクト ID を選択します。

3. `loadBalanceUserCalls = false` に設定します。[変更 (Modify) ] をクリックします。

## 6.6 Lync アカウント情報

Call Bridge と Lync Edge の統合については、競合が生じないように、独自のログイン アカウントで各 Call Bridge を設定することを推奨します。Call Bridge との間の Lync 通話ごとに、Meeting Serve はそのアカウントを使用して、Lync Edge に TURN リソースを要求します。その通話が切断されるまで、そのリソースは Lync の観点から「使用済み」と見なされます。Lync では、ユーザーアカウントごとに最大 12 の TURN 割り当てのみが許可されます。したがって、1 回の登録では、最大 12 通のコールが可能です。

---

**注：**その 1 つのアカウントを複数の Call Bridge で共有する場合、すべての Call Bridge で許可される Lync 通話は合計 12 件までになります。

---

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

参加者を Lync 電話会議に接続するときの Call Bridge の動作を選択できます。への POST 時のリクエストパラメータ `lyncConferenceMode` が追加されました。

`/callProfiles` または `/callProfile/<通話プロファイル ID >` に設定してください。

クラスター化された Call Bridge 間で通話を分配したい場合は、`lyncConferenceMode` を `dualHomeCluster` に設定し、その一つの Call Bridge が AVMCU ミーティングにコールアウトします。これはバージョン 2.2 以前と同じ動作です。

クラスタ化された Call Bridge 間で通話を分配したくない場合は、`dualHomeCallBridge` に設定しますが、同じ Call Bridge 上の通話は 1 つの電話会議に結合する必要があります。これにより、各 Call Bridge で 1 つの電話会議が開催され、各 Call Bridge が AVMCU ミーティングをコールアウトします。

通話を Call Bridge 間で分配することなく、または同じ Call Bridge 上の通話を 1 つの電話会議に結合することなく、`gateway` に設定します。各 SIP 参加者は、関連付けられた AVMCU ミーティングへの発信を持つ自分の会議に参加します。

---

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

---

たとえば、3 人の SIP 参加者が 2 つの Meeting Server 経由で AVMCU 電話会議に接続する展開で、2 人の SIP 参加者が同じ Meeting Server にいる場合、異なるモードを選択することで次のような動作が見られます。

- **dualHomeCluster** : メディアストリームはクラスター化された Meeting Server 間で送信されます。図 20 を参照してください。SIP 参加者からのすべての通話は、両方の Call Bridge にまたがる 1 つの電話会議に統合されます。1 つの Call Bridge が AVMCU を呼び出

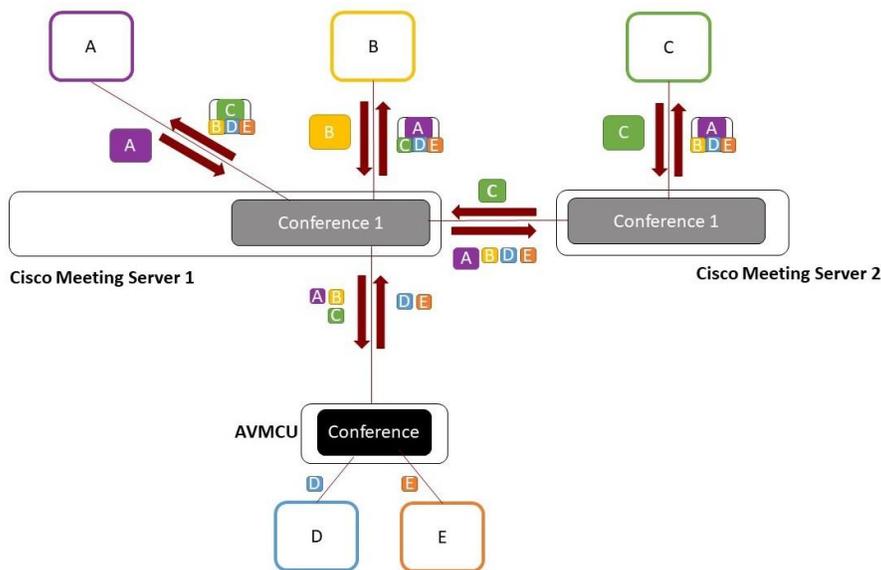
します。デュアルホームクラスタ は 1 つの電話会議に 1 つのマルチパーティプラスライセンスを使用します。

**注意：デュアルホームクラスタ モードでは、AVMCU に直接接続している参加者のビデオストリームは AVMCU から取得されます。Lync2013 または Skype for Business を使用して、4 人以上の参加者がミーティングに参加する場合、これらのストリームの解像度は最大 360p に制限されます。**

通常、このモードではより多くのビデオストリーム (多くの場合は高解像度) を利用できます。これは2つの要素によるものです。1 つ目は、Lync から要求されるメディア ストリームの数が少ない場合、これらのストリームの解像度が高くなるということです。もう 1 つは、SIP デバイスをソースとするストリームは通常、高解像度で利用できるということです。ただし、すべての音声ストリームを送信する必要があるため、ビデオがなくても、帯域幅要件の増加につながるかなりのオーバーヘッドになる可能性があります。ビデオ ストリームは複数のホップを通過するため、さらに帯域幅が必要になります。また、複数のホップにより、遅延が増加する可能性があります。

**注：このモードでは予測可能性が低下します。ユーザーが電話会議に参加する順番によって接続が変化し、利用できるストリームが変化するためです。さらに、Lync に接続する最初の Call Bridge は、最良の選択とは言えない可能性があります、場合によっては、表示される参加者がより少なくなる可能性があります。**

図 20 : dualHomeCluster モードを使用した Lync AVMCU/Meeting Server のデプロイメント



- **DualHomeCallBridge** : 同じ Call Bridge 上の 2 人の SIP 参加者が 1 つのコンファレンスに参加することになります。図 21 を参照してください。エンドポイント C から見えるストリームは AVMCU 経由ですが、エンドポイント B から見えるエンドポイント A のストリームは AVMCU 経由ではありません。dualHomeCallBridge モードでは Meeting Server 上の複

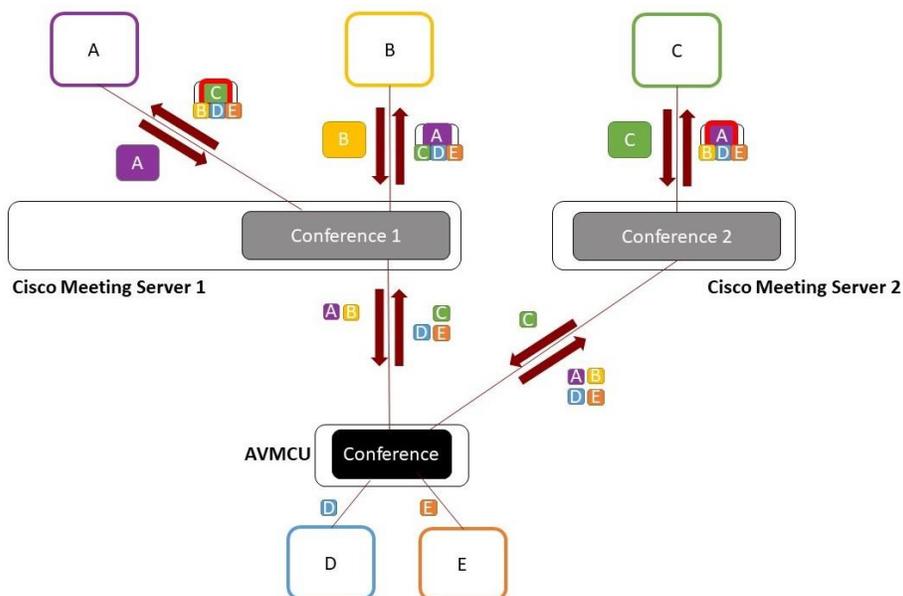
数の会議が複数の Multiparty Plus ライセンスを消費します。図 21 の例では、2 つの Multiparty Plus ライセンスが消費されます。

**注：** dualhomeCallBridge モードでは、AVMCU に直接接続されている別の Call Bridge 上の参加者のビデオ ストリームは AVMCU から送信されます。Lync2013 または Skype for Business を使用していて、4 人以上の参加者がミーティングに参加する場合、これらのストリームの解像度は最大 360p に制限されます。

このモードでは、AVMCU に向かうメディアストリームを単一の Meeting Server に送信する必要がないため、帯域幅の使用量を削減できます。ただし、AVMCU からのビデオは低解像度になる可能性があります (影響を受ける可能性のある図 21 のメインペインの周りに赤の枠線で示されています)。

**注：** このモードは、ミーティングに参加するユーザーの順番は関係ないため、予測しやすくなっています。

図 21 : dualHomeCallBridge モードを使用した Lync AVMCU/Meeting Server の展開



- **ゲートウェイ** これにより、3つのMeeting Server会議すべてがAVMCUミーティングに通話します。エンドポイント A、B、C に表示されるビデオ ストリームはすべて AVMCU 経由で送信されます (図 22 を参照)。解像度が低くなる可能性があり、影響を受ける可能性のあるメイン ペインの周囲に赤い枠線で示されます。

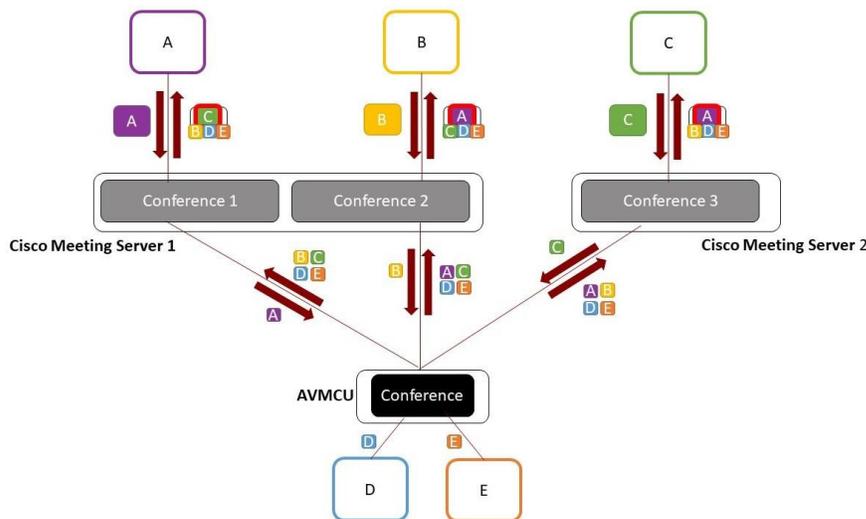
各コール レッグは個別に処理されるため、単一の Call Bridge が同じビデオ ストリームの複数のコピーを要求し、より多くの帯域幅を消費する場合があります。

Shared Multiparty Plus ライセンスでは、6 回のゲートウェイ通話が可能です。ゲートウェイモードを使用して、別のユーザーに CMS を通じて、または Microsoft Lync AVMCU ミーティングにダイヤルする各参加者は、SMP Plus ライセンスの 6 分の 1 を消費します。

図 22 の例では、Shared Multiparty Plus ライセンスの半分 (3/6) が消費されます。API を介したライセンス使用状況のレポートにはまだ反映されていないことに注意してください。現在、ゲートウェイの各呼び出しで、実際に消費された 6 分の 1 (1/6) のライセンスではなく、1つのフルライセンスが消費されたと報告されます。

**注意：**ゲートウェイ モードでは、すべてのビデオストリームは AVMCU から送信されます。Lync 2013 または Skype for Business を使用しており、4人以上がミーティングに参加する場合、各ストリームの解像度は最大で 360p に制限される場合があります。

図 22 : ゲートウェイモードを使用した Lync AVMCU/Meeting Serverの展開



**注：**ベータ版の機能です。

バージョン 2.3 以前では、最大 4 人のリモート参加者からのビデオを、クラスタ化された Call Bridge 間の各配信リンクで送信できました。バージョン 2.3 から、Meeting Server は配信リンク上で最大 9 個のビデオストリームをサポートします。シングル、デュアル、および 3 スクリーンのエンドポイント システムを使用する参加者は、電話会議がクラスタ化された Call Bridge でホストされているか、またはシングル Call Bridge でホストされているかに関係なく、より一貫した会議エクスペリエンスが得られるようになりました。

クラスタ Call Bridge 間で各配信リンクを介して送信されるビデオ ストリームの最大数を設定するには、API オブジェクトの `maxPeerVideoStreams` パラメータを設定します。

`/system/configuration/cluster` を 1、4、または 9 の値に設定します。このパラメータが設定されていない場合、デフォルトは 4 になります。

**注：**API パラメータ `maxPeerVideoStreams` パラメータには、1~9 間の任意の値を指定できます。しかし、送信される画面解像度は 1、4、9 に最適化されます。このため、変数を 2、3、5、6、7、8 に設定すると、画面全体が使用されるわけではありません。例えば、「5」に設定すると、5 人の参加者それぞれが画面の 1/9 の部分を占め、同様に「2」に設定すると 2 名の参加者が画面の 1/4 の部分を占めます。

配信リンクで 4 つ以上のビデオストリームをサポートするには、リンクの帯域幅を 2Mbps 以上に設定することをお勧めします。API またはウェブ管理インターフェイスを使用して帯域幅を設定します。API を使用する場合、`peerLinkBitRate` パラメータの値を API オブジェクト `/system/configuration/cluster` に PUT します。この値は、クラスター内の Call Bridge 間の配信リンクを使用する最大メディアビットレートになります。または、ウェブ管理インターフェイスを使用して、[設定 (Configuration)] > [クラスタ (Cluster)] > [Call Bridge ID (Call Bridge identity)] の順に選択し、[ピアリンクビットレート (Peer link bit rate)] を入力します。

## 7 Web Bridge 3 を導入する

---

**注：** ウェブアプリを使用していない場合は、この章をスキップしてください。

---

特に記載のない限り、これらの手順は、統合または分割スケーラブル展開に等しく適用されます。

### 7.1 複数の Web Bridge 3 を展開する

Meeting Server クラスタに複数の Web Bridge を展開することができます。特定の A レコードが指向するすべての Web Bridge が、同じ Call Bridge グループに関連付けられていることを確認する必要があります。

### 7.2 Web Bridge 3 証明書をセットアップする

各 Web Bridge には、ウェブ アプリ クライアントが TLS 接続を確立するときに使用されるキーと証明書のペアが必要です。まだ行っていない場合は、証明書を作成、アップロードし、Web Bridge に割り当ててください。詳細については、[セクション 4.6](#)、および [証明書のガイドラインを参照してください](#)。

---

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

---

### 7.3 Web Bridge 3 をセットアップする

API を使用して以下を設定します。

- Call Bridge が Web Bridge に到達するために使用する URL の FQDN。これは単一の Web Bridge 3 だけのためのもの必要があります。複数の Web Bridge の URL を指定しないでください。Call Bridge は、任意の時点で特定の Web Bridge 3 への C2W 接続を開くことができる必要があります。
- (オプション) Web Bridge に関連付けられる場合は、Call Bridge id または CallBridgeGroup id のいずれか、
- スペースへのアクセスをコントロールします。これには、ゲストがミーティングの招待に含まれるウェブリンクをたどることでスペースにアクセスすることを Web Bridge 3 で許可するかどうかが含まれます。デフォルトではセキュアモードが設定されており、ゲストはスペースに参加する前にコール ID とパスコードの両方を入力する必要があります

があります。ウェブリンクを介したアクセスは、追加の詳細を提供することなくデフォルトで許可されます。

- 訪問者のスペースへの参加を許可するために、Web Bridge 3 がスペースとスペース アクセス メソッドのコール ID を受け入れるかどうかを指定します。このパラメータが指定されていない場合、デフォルトで [true] になり、訪問者は参加できます。
- Web Bridge 3 が Lync のスケジュール済み電話会議 ID を解決するために登録済みユーザー ID を受け入れるかどうか。このパラメータが指定されていない場合、既定で [false] になり、ID を Lync のスケジュール済み電話会議の ID に解決しません。このパラメータが true に設定されている場合、web app のユーザーは、web app のサインイン ページで Lync ミーティング ID を入力することで、スケジュールされた Lync 電話会議に参加できます。
- Web Bridge 3 に関連付けられたテナントとテナント グループ、必要に応じて、
- ランディング ページの背景画像とロゴのカスタマイズ (必要な場合)

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

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

Web Bridge 3 の設定の詳細については、「[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。

### 7.3.1 Web Bridge プロファイルを作成して適用する方法の例

1. Meeting Serverウェブ管理インターフェイスを使用して webBridgeProfile を作成するには：
  - a. Meeting Serverのウェブ管理インタフェースにログインして **設定 (Configuration)** >API を選択します。
  - b. API オブジェクトのリストで、/api/v1/webBridgeProfiles 後の ▶ をタップします。
  - c. **[新規作成]** をクリックします。
  - d. [name] フィールドにこのWeb Bridgeプロファイルに付けたい名前を設定します。
  - e. [resourceArchive] フィールドに、このWeb Bridgeプロファイルを使用するWeb Bridgeのために Meeting Server が使用するべきカスタマイズ アーカイブ ファイルのアドレスを設定します。
  - f. [allowPasscodes] フィールドを [true] または [false] に設定します。このフィールドは、このWeb Bridgeプロファイルを使用するWeb Bridgeが、数値 ID/URI と組み合わせられたパスコードで coSpace (および coSpace アクセス方法) のロックアップ

をユーザーに許可するかどうかを決定します。このパラメータが指定されていない場合、デフォルトで [true] に設定されます。

- g. [allowSecrets] フィールドを [true] または [false] に設定します。このフィールドは、このWeb Bridgeプロファイルを使用するWeb Bridgeが、数字の ID とシークレットのミーティング参加リンクを通じてユーザーが coSpaces (および coSpace のアクセス方法) にアクセスすることを許可するかどうかを決定します。このパラメータが指定されていない場合、デフォルトで [true] に設定されます。
  - h. userPortalEnabled フィールドを true または false **に設定してください**。このフィールドでは、この Web Bridgeのプロファイルを使用する Web Bridgeのインデックス ページにサインイン タブを表示するかどうかを指定します。このパラメータが指定されていない場合、デフォルトで [true] に設定されます。
  - i. allowUnauthenticatedGuests フィールドを true または false **に設定してください**。true に設定した場合、このWeb Bridgeのプロファイルを使用するWeb Bridgeのランディング画面からのゲストアクセスが許可されます。False に設定すると、訪問者アクセスは、ユーザーがユーザポータルにログインした後にのみ許可されます。このパラメータが指定されていない場合、デフォルトで [true] に設定されます。
  - j. resolveCoSpaceCallIds フィールドを true または false **に設定してください**。このフィールドは、このWeb Bridge プロファイルを使用するWeb Bridgeが、coSpace および coSpace アクセス メソッド コール ID を受け入れ、訪問者が cospace ミーティングに参加できるようにするかどうかを決定します。このパラメータが指定されていない場合、デフォルトで [true] に設定されます。
  - k. resolveCoSpaceUris フィールドを **オフ**、domainSuggestionDisabled または domainSuggestionEnabledに設定してください。このフィールドは、このWeb Bridgeが、coSpace および coSpace アクセス方式 SIP URI を、訪問者が cospace ミーティングに参加できるようにする目的で受け入れるかどうかを決定します。[off] に設定すると、URI による参加は無効になります。[domainSuggestionDisabled] に設定すると、URI による参加は有効になり、しかし、このWeb Bridgeでは URI のドメインは自動補完または検証されません。[domainSuggestionEnabled] に設定すると、URI による参加は有効になり、そして、このWeb Bridgeで URI のドメインが自動補完され、検証されます。このパラメータが指定されていない場合、デフォルトで [off] に設定されます。
  - l. **[作成 (Create) ]** をクリックします。
2. プロファイルを作成したら、アドレスを追加できます。これはミーティング招待状を生成するために使用されるWeb Bridge URI であり、ウェブ アプリのクロス起動 URL です。

---

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

---

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

- API オブジェクトのリストで、/api/v1/webBridgeProfiles 後の ▶ をタップします。
- [表示または編集] をクリックします。
- 結果の"webBridgeProfile オブジェクト選択ウィンドウ"から、**ステップ 1 で作成し、Web Bridge URI および IVR 番号を割り当てたい webBridgeProfile のオブジェクト ID を選択します。** Web Bridgeの **ラベル** および **URL アドレス** を入力し、必要に応じて IVR の **ラベル** および **番号** を入力します。

« return to object list

/api/v1/webBridgeProfiles/410c2b53-3135-4f58-8742-08e5b025675a/webBridgeAddresses

Related objects: [/api/v1/webBridgeProfiles](#)  
[/api/v1/webBridgeProfiles/410c2b53-3135-4f58-8742-08e5b025675a](#)

« start < prev **1 - 1** (of 1) next »

object id	label
b431cfb-6071-4fe9-b684-f5c197e4681	Pre-A

---

/api/v1/webBridgeProfiles/410c2b53-3135-4f58-8742-08e5b025675a/webBridgeAddresses

label

address   (URL)

---

« return to object list

/api/v1/webBridgeProfiles/410c2b53-3135-4f58-8742-08e5b025675a/ivrNumbers

Related objects: [/api/v1/webBridgeProfiles](#)  
[/api/v1/webBridgeProfiles/410c2b53-3135-4f58-8742-08e5b025675a](#)

« start < prev **none** next »

<?xml version="1.0"?>  
 <ivrNumbers total="0"></ivrNumbers>

---

/api/v1/webBridgeProfiles/410c2b53-3135-4f58-8742-08e5b025675a/ivrNumbers

label

number

- [作成 (Create) ] をクリックします。
- 必要に応じて、新しく作成された webBridgeProfile の ID を次のいずれかまたはすべてに割り当てます。
    - 最上位 (グローバル) プロファイル (/api/v1/system/profiles)
    - テナント (/api/v1/tenants/<id>)
    - WebBridges (/api/v1/webBridges/<id>)

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

- API オブジェクトのリストで、/api/v1/system/profiles 後の ▶ をタップします。
- [表示または編集] をクリックします。
- パラメータを下にスクロールして webBridgeProfile を選択し、[選択 (Choose) ] をクリックします。

- d. 結果の"webBridgeProfile オブジェクト選択ウィンドウ"から、**ステップ1で作成した、最上位のグローバルプロファイルに割り当てたいwebBridgeProfileのオブジェクトIDを選択** をクリックします。
- e. **[変更 (Modify) ]** をクリックします。
- f. 新しく割り当てられた webBridgeProfile オブジェクト ID が、**オブジェクトの設定** の下に表示されます。

## 7.4 Web Bridge 3 の通話フロー

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

1. ウェブブラウザが HTTPS 接続を開きます。
2. ユーザーには **ミーティングに参加** (手順 3 を参照) または **ログイン** (手順 4 を参照) の選択が提示されます。
3. **[ミーティングに参加]** が選択されている場合、ユーザーは呼び出し ID/URI とパスコードを入力し、名前を設定するように求められます。
  - a. 通話の詳細は、HTTPS 経由で Web Bridge 3 に送信されます。Web Bridge 3 は、通話の詳細を検証するために、C2W 接続を介して Call Bridge にクエリを実行します。
  - b. 成功した場合、ユーザーはメディア設定を選択するように求められます。
  - c. メディア設定を選択した後、通話の詳細と希望の名前が HTTPS 経由で Web Bridge 3 に送信されます。C2W 経由で Call Bridge に転送されます。Call Bridge は、ブラウザに返される通話アクセストークンで応答します。このトークンは、ブラウザが使用する TURN サーバーの詳細を示します。
  - d. Call Bridge は、設定された TURN サーバからの割り当てを要求します。
  - e. ウェブアプリは、指定された TURN サーバーに割り当てを要求します。
  - f. ブラウザが Web Bridge 3 へのウェブソケット接続を開きます。この接続は、C2W 接続経由で Call Bridge に転送されます。呼び出しアクセス トークンはこのウェブソケット経由で送信されます。
  - g. ブラウザと Call Bridge は、ローカル メディア IP アドレス/ポートおよびメディアリレー アドレス/ポートを含むウェブソケット上の SDP を交換します。
  - h. ICE ネゴシエーションは、すべてのブラウザメディア IP アドレス/ポートの組み合わせと、すべての Call Bridge アドレス/ポートの組み合わせの間で UDP パケットを送信し、TCP メディアリレーアドレス/ポートに TCP 接続を試みます。
  - i. ブラウザと Call Bridge の間のメディア転送には成功した最短メディア パスを使用され、これは直接、TURN UDP リレーを経由、または TURN サーバーが TCP ストリームと UDP の間でメディアパケットを変換する TURN TCP リレーを経由します。
4. **ログイン** が選択されている場合、ユーザーはユーザ名とパスワードの入力を求められます。
  - a. HTTPS 経由で Web Bridge に送信され、成功した場合、ポータルアクセストークンを取得するために Call Bridge に転送されます。

- b. ユーザーのポータルサイトに入ると、すべてのリクエストが HTTPS 経由で送信され、ポータル アクセストークンがヘッダーとして送信されます。
- c. 通話参加リクエストが行われた場合、フローはステップ 3c 以降と同じですが、通話の詳細と希望する名前を送信して通話アクセストークンを取得する代わりに、ブラウザは代わりに通話の詳細とポータルアクセストークンを送信します。

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

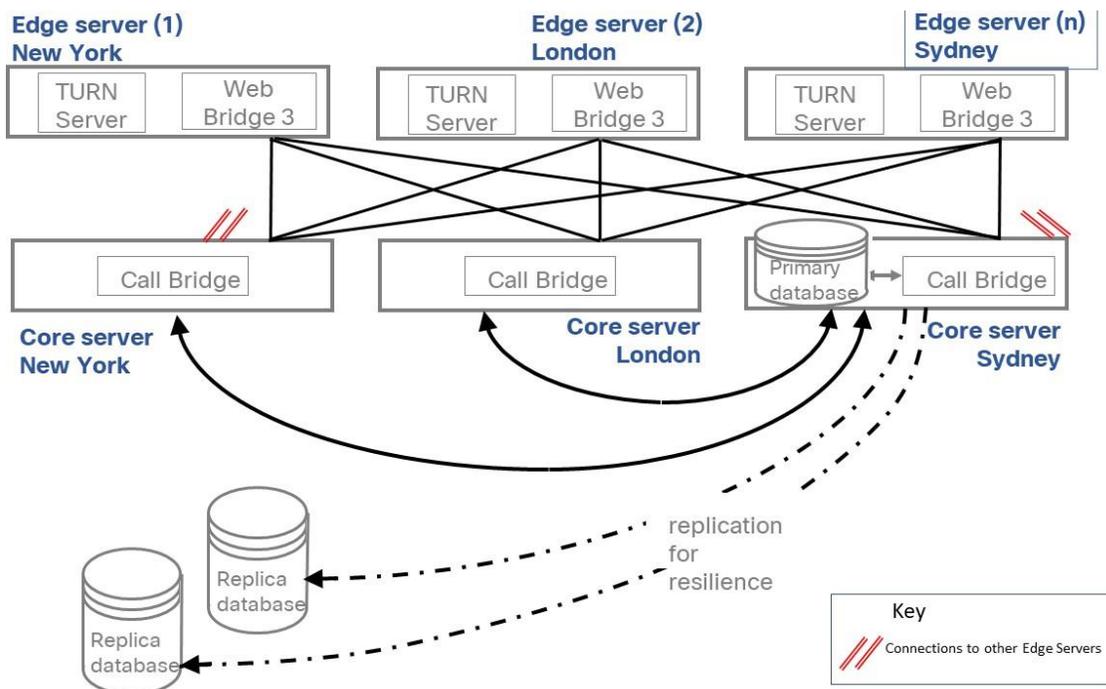
## 7.5 ウェブアプリ情報

ウェブアプリ ユーザーが発信した場合：

1. ユーザーのウェブブラウザは簡単な DNS A レコードルックアップを実行して、Web Bridge 3 を選択します。
2. Web Bridge 3 はウェブアプリが使用する TURN サーバーのアドレスを提供します。

通話に使用される Web Bridge 3 および TURN サーバーは、同じ場所に配置する必要はありません。

図 23：スプリットデプロイメントで構成された Web Bridge



## 7.6 HTTP リダイレクトとWeb Bridge 3 を有効にする

Web Bridge 3 は HTTPS をサポートします。「httpredirect」を使用するように構成されている場合、HTTP を HTTPS に転送します。これについては [セクション 4.6](#)で説明されています。

## 8 TURN サーバーを導入する

TURN サーバーは、Call Bridge からの UDP 接続をポート 3478 でリッスンし、リモート接続にも使用できます。

TURN サーバーは、クライアント接続からの TCP の 2 番目のポートでリッスンすることもできます。通常は 443 です ('turn tls <port>' 設定が必要です)。

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

ファイアウォール ルールが Call Bridge から TURN サーバーへの UDP ポート 3478 を許可していることを確認します。

### 8.1 TURN サーバーの設定

特に断りのない限り、これらの手順は統合展開と分割展開に同じように適用されます。

---

**注：** Web 管理インターフェイスから単一の TURN サーバーを設定することもできますが、複数の TURN サーバーがある場合は、で説明されているように、API のみを使用して設定することを強くお勧めします。 [Call Bridge 上の Turn サーバーの設定](#)。

---

1. MMP を使用して各 TURN サーバーを設定して有効にします。 [第 4 項](#)を参照してください。
2. /turnServer/<turn サーバ ID> ノードを Call Bridge 上の各 TURN サーバーに設定するか、または、複数のインスタンスを指す DNS レコードを持つ 1 つのノードを設定します。

例えば、Meeting Server のウェブ管理インタフェースを使用する：

- a. Meeting Server のウェブ管理インタフェースにログインして **設定 (Configuration)** > API を選択します。
- b. API オブジェクトのリストで、/api/v1/turnServers の後の ▶ をタップします。
- c. Call Bridge の TURN サーバーを設定または変更するには、**[新規作成]** または必要な既存の TURN サーバーのオブジェクト ID を選択し、次のパラメータ値を自分の値で置き換えます。

```
serverAddress = edge1.example.com
```

```
clientAddress = edge1.example.com
```

```
ユーザーネーム = fred
```

```
password = password
```

```
type = cms
```

3. MMP の構成時に、[TURN Server の TCP に非標準ポート](#)を設定した場合、API パラメータ `tcpPortNumberOverride` をオブジェクト `/turnServers/<turn Server id>`に適用して、Call Bridge でこの値を設定します。

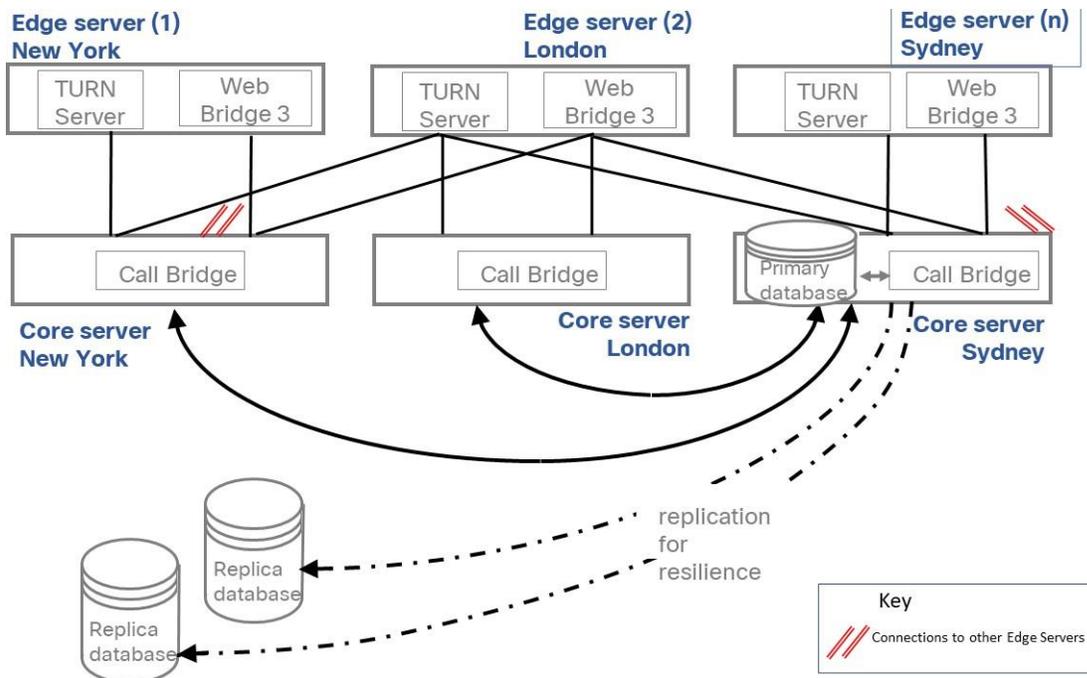
たとえば、メディアをインターワークする TURN サーバーの場合、Call Bridge の `/turnServers` ノードに以下のパラメータ値をあなたの値に置き換えます：

```
tcpPortNumberOverride = 447
```

**注：**このパラメータは、TCP ポート番号が常に自動的に決定される Lync Edge サーバーが構成されている場合には必要ありません。

完了した展開については、図 24 を参照してください。

図 24 : スプリットデプロイメントで設定された TURN サーバ



## 9 分散導入のウェブアプリ

スペースは、API 呼び出しを介してクラスター内の任意の Call Bridge に作成でき、これらのスペースは、このクラスターに接続されているすべての Call Bridge に表示されます。ウェブ管理インターフェイスから Meeting Server API を使用する例が J.5 に提供されています。

図 25 と 図 26 はそれぞれ、結合展開と分割展開における 2 つのウェブアプリ ユーザーの異なるスペースへの通話を示しています。この数字は次のことを示す：

- 場所に関係なく、すべての Call Bridge は同じデータベース インスタンスから読み取ります。データベースは、例えば各スペースのメンバー、スペースに関する情報を保持します。
- コントロール ルートとメディア ルート（したがって使用されるコンポーネント インスタンス）は、クライアントのロケーションによって異なります。これには複数のプレゼンス ポイントが含まれる場合があります。ロンドンにいるウェブ アプリ ユーザーが別の場所で Call Bridge と Web Bridge を使用して通話する場合などです。

図 25 : 2 人のウェブ アプリ ユーザーが統合された展開の異なるスペースに発信する

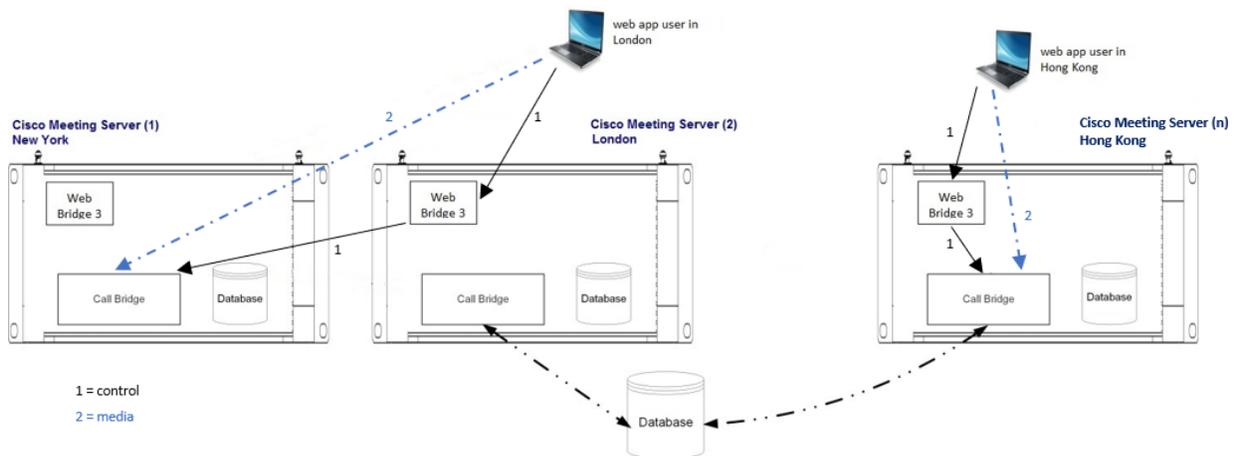
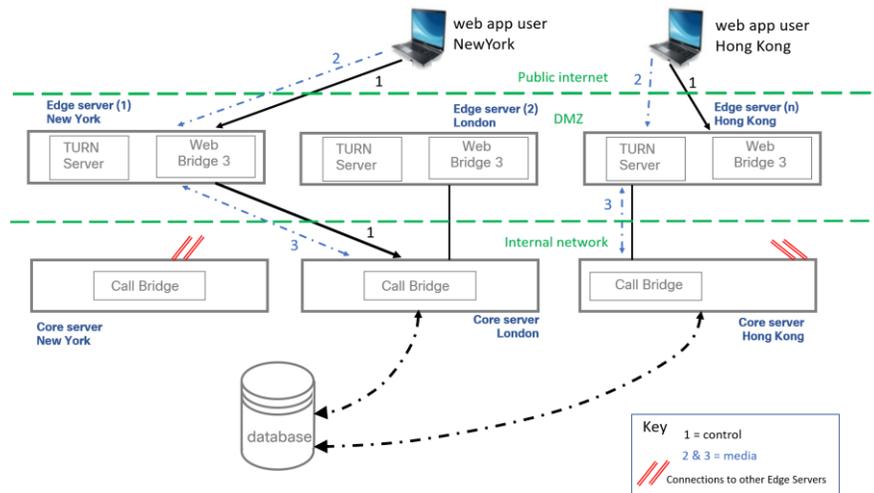


図 26 : 2 人のウェブ アプリ ユーザーが分割された展開の異なるスペースに発信する



ただし、ミーティングが複数の Call Bridge で主催されている分散型ミーティングの場合、これらの Call Bridge は必要な音声とビデオのストリームを交換するため、それぞれがすべての参加者を認識します。次を参照してください。図 27 および 図 28。スペースでミーティングに参加するすべての参加者は、場所や使用するコンポーネントに関係なく、スペースが単一の Call Bridge でホストされているかのように、同じ参加体験ができます。各参加者に表示されるレイアウトを含む、通話エクスペリエンスは、コール ログ (API 経由で設定) と、誰が話しているか、または前の発言者によって異なります。これは、1つの Call Bridge でホストされたミーティングと同じ通話体験です。

参加者には、自分と同じ Call Bridge に接続している同じミーティングのすべての参加者、および他の Call Bridge への分散リンク上の各最大 4 人の参加者が継続的に表示されます。

**例 1 :** 参加者 1 は、参加者 2、3、4 と共に Call Bridge A を使用します。参加者 5、6、7、8 は Call Bridge B に参加し、参加者 9、10、11、12 は、Call Bridge C。参加者 1 が「全員が等しく表示される」レイアウトを選択した場合、他の 11 人の参加者 (2 から 12 の番号) が表示されます。

**例 2 :** 参加者 1 は、参加者 2 と 3 と一緒に Call Bridge A です。参加者 4、5、6、7 は Call Bridge B にあり、参加者 8、9、10、11、12 は Call Bridge C です。参加者 1 が「全員が等しく表示される」のレイアウトを選択した場合、Call Bridge A および B の 2 から 7 の参加者と、Call Bridge C の参加者 8、9、10、11、12 の最新の 4 人の発言者が表示されます。

Call Bridge がエンドポイントから通話を受信するたびに、スペースのインスタンスがすでにあるかどうかを確認するために、他の Call Bridge にクエリを実行します。インスタンス化がある場合、通話を受信する Call Bridge とインスタンス化がある Call Bridge の間にリンクが確立されます。これを「通話分配リンク」と呼びます。(ただし、同じ Call Bridge グループ内にある場合、Call Bridge はエンドポイントを他の Call Bridge にリダイレクトすることもできます。) 配信リンクの場合、いずれかの Call Bridge でより多くのエンドポイントが通話に参加すると、リンクが 2 つの Call Bridge 間でアクティブな参加者のビデオ ストリームの送信を開始します。最後のエンドポイントがどちらかの側を離れるときにされる場合、その Call Bridge から別の 1 つへのリンクが切断され、通話は配信されなくなります。

図 27 : 統合展開における 2 つの Call Bridge によるスペース A への呼び出し

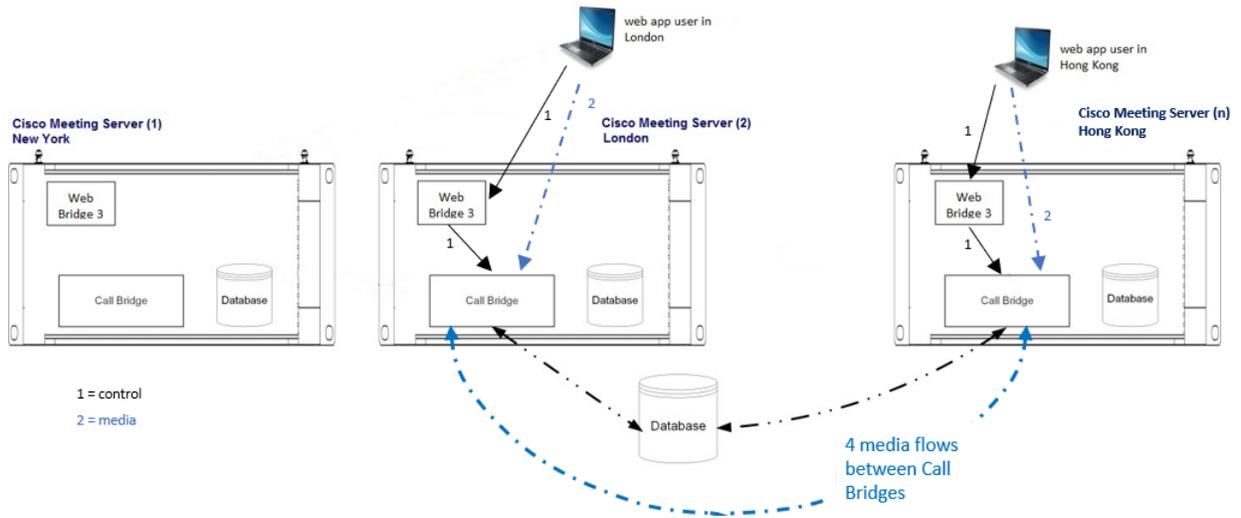
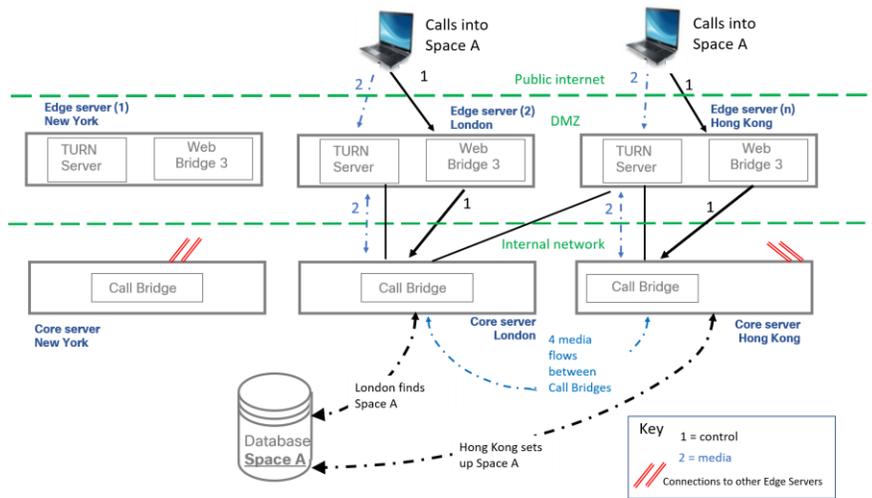


図 28 : 分割展開における 2 つの Call Bridge によるスペース A への呼び出し



スペースに 4 人の参加者がある場合のビューとメディア フローの例を次の 2 つの図に示します。

図 29 : 複合展開で PC クライアントがスペース A にダイヤルするときのメディア フローとビューの例

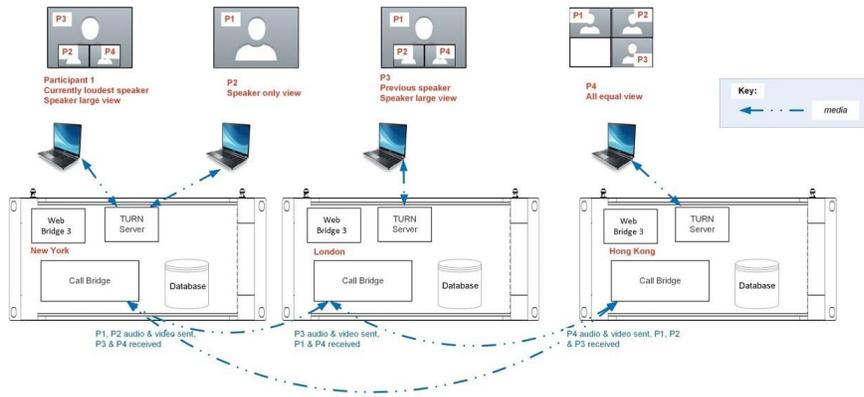
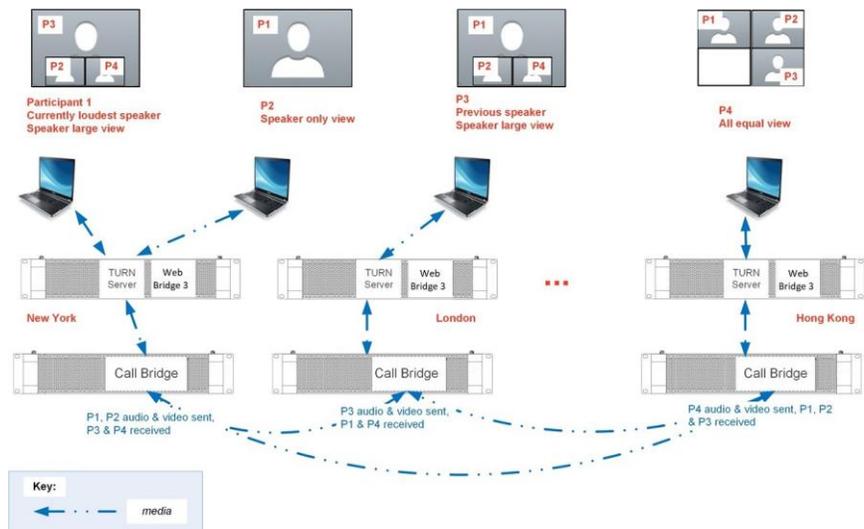


図 30 : 分割展開で PC クライアントがスペース A にダイヤルするときのメディア フローとビューの例



## 10 ダイアルプランの構成 – 概要

### 10.1 はじめに

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

図 31 は、SIP ビデオエンドポイント、Lync クライアント、および IP 電話が混在する会社の展開を想定しています。Meeting Server は、Lync クライアントと SIP ビデオエンドポイントの間、および Lync クライアントと IP 電話の間の接続を可能にします。

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

図 31 : ダイアルプラン設定の Meeting Server 導入の例 (エッジに Cisco Expressway あり)

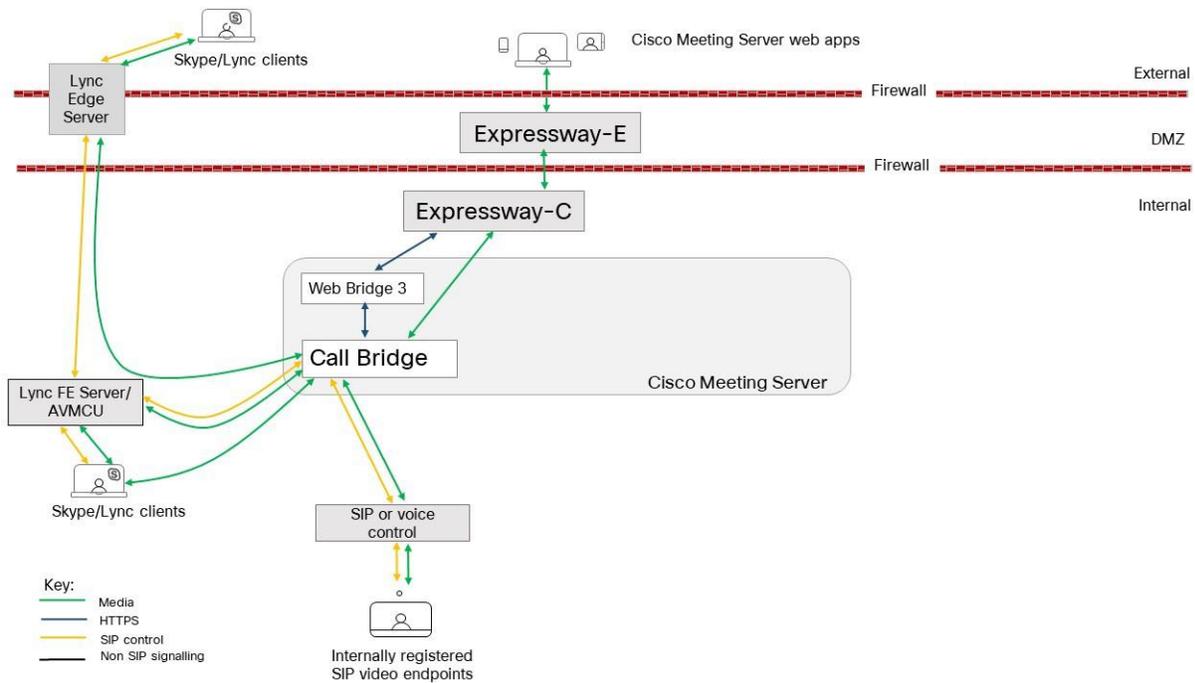
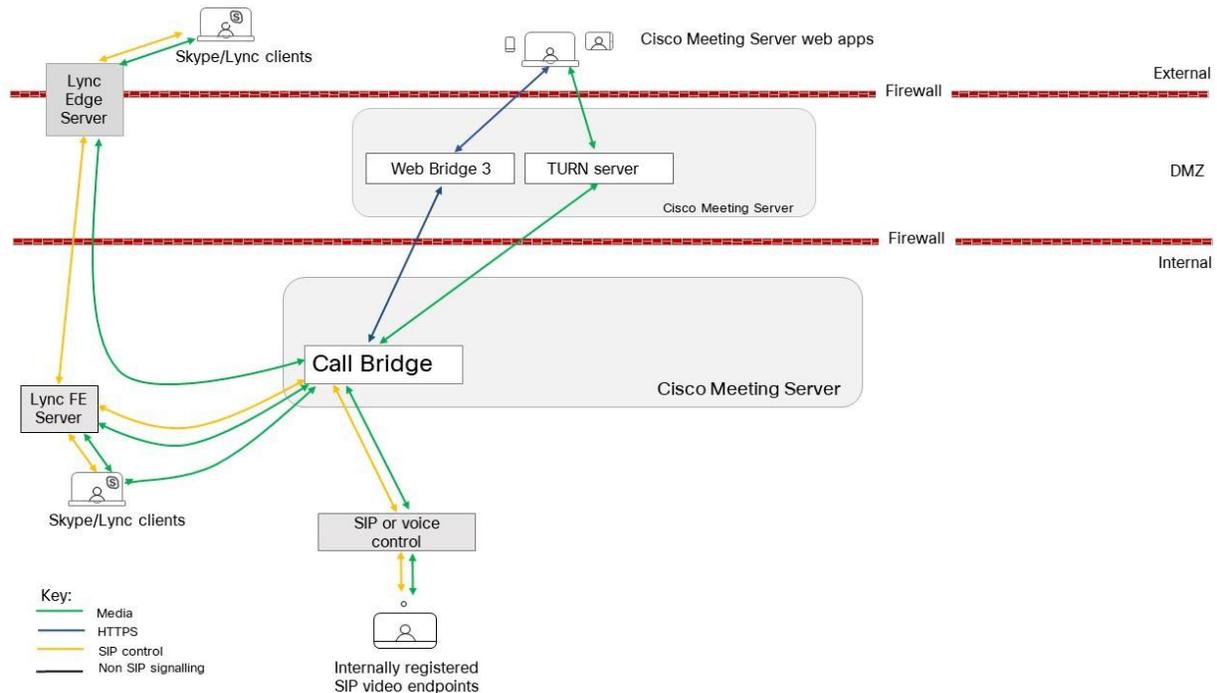


図 32 : ダイアルプラン構成のための Meeting Server 展開の例 (分割サーバ展開で TURN サーバーコンポーネントを使用)



上の図に示すように、Lync FE サーバーには Meeting Server への信頼できる SIP トランクが必要です。これは、Lync クライアントから発信されたコールを Meeting Server スペース、Cisco Meeting Server web app ユーザー、さらに SIP ビデオエンドポイントにルーティングするように構成されています。サブドメイン vc.example.com (SIP ビデオ エンドポイント用) および meetingserver.example.com (スペースおよび Cisco Meeting Server web app 用) は、Lync FE サーバーから Meeting Server にこのトランクを通じてルーティングされる必要があります。

**注：**別の組織で展開されている Office 365 またはオンプレミスの Lync への接続は、Cisco Expressway 経由で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 通話制御プラットフォームは、example.com ドメイン (Lync クライアントの場合) および meetingserver.example.com (スペースおよびウェブ アプリの場合) への通話を Meeting Server にルーティングするように SIP トランクをセットアップする必要があります。

Meeting Server は、ドメイン example.com の通話を Lync FE サーバーに、サブドメイン vc.example.com を SIP 通話制御プラットフォームにルートするためのダイアルプランを必要とします。

次のセクションでは、Meeting Server が着信通話と発信通話を処理する方法を決定する Meeting Server API オブジェクトについて説明します。

この章に続く第 11 章および第 12 章に、ソリューション全体の設定に関する手順を追った説明を示します。

## 10.2 着信通話と発信通話のダイアルプランルール。

この項では、Meeting Server API を使用して、着信および発信通話の処理方法を決定するルールを設定する方法について説明します。

---

**注：**「シングル統合およびシングル分割導入ガイド」では、ウェブ管理インターフェースを使用してダイアルプランルールを設定する方法について説明しています。しかし、スケーラブルで復元力のある展開には、通常、API を通じてのみ提供されるより多くの機能が必要です。

---

以下の API オブジェクトは、Meeting Serverのダイアルプランルールに影響を与えます：

- `/outboundDialPlanRules` は、発信通話の処理方法を制御します。
- `/dialTransforms` は、アウトバウンドコールに適用して、アウトバウンドコールのルーティングを制御することができます。「[ダイアル変換](#)」を参照してください。
- `/inboundDialPlanRules` は、着信通話の処理方法を指定します。着信 SIP 通話の接続先 URI の「ドメイン」部分が着信ダイアルプランルールと一致する場合、通話はそのルールによって処理されます。既存の着信ダイアルプランルールと一致しない場合、通話は着信転送ダイアルプランルールによって処理されます。任意のドメインの Meeting Server にルーティングされた通話は、そのサーバーの IVR、ウェブアプリユーザー、または事前設定されたスペースに対してテストできます。
- `/forwardingDialPlanRules` は、どの着信ダイアルプランルールにも一致しない呼び出しを転送する方法や、Lync電話会議に接続する方法に関する情報が含まれています。

---

**注：**着信コールが着信ダイアルプランルールのいずれにも一致しない場合、またはコール転送ダイアルプランルールのドメイン一致パターンのいずれにも一致しない場合、その着信コールは終了されます。

---

### 10.2.1 `/outboundDialPlanRules`

新しい発信ダイアルプランのルールを作成するには、次のパラメータセットを使用して、API オブジェクト `/outboundDialPlanRules` に POST します：

パラメータ	タイプ/値	説明/メモ
ドメイン *	String	ダイアルプランルールを適用するために照合するドメイン。完全な値 (例 "example.com") またはワイルドカード値 (例 "*.com") のいずれかです

パラメータ	タイプ/値	説明/メモ
優先順位	番号 (Number)	ダイアルプランのルール (ワイルドカードを含むドメインを含む) が適用される順序を決定する数値。優先順位の値が高いルールが最初に適用されます。ルールが一致したが、呼び出しを行うことができない場合、ルールの failureAction パラメーターに応じて、他の優先順位の低いルールが試される場合があります。
ローカル連絡先ドメイン	String	使用する明示的な連絡先ドメインを形成する際に使用します。このフィールドを空欄にしておくと、localContactDomain はローカル IP アドレスから取得されます。  Lync を使用している場合、localContactDomain を設定することをお勧めします。Lync を使用していない場合、SIP 通話フローでの予期せぬ問題を回避するために、localContactDomain を設定しないことをお勧めします。
localFromDomain	String	このダイアルプランルールを使って発信通話を行う際の発呼者を形成する際に使用されます。
sipProxy	String	発信に使用するプロキシ デバイスのアドレス (IP アドレスまたはホスト名) です。設定されていない場合は、直接通話になります。
トランクタイプ	sip  lync  avaya	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ためのルールをセットアップするために使用されます。Lync または avaya に設定すると、このルールを使用する発信は、特殊な動作で Lync または Avaya として発信されます。sip は、このルールを使用する通話が標準の SIP 通話になることを意味します。  Meeting Serverの一般的な用途は Avaya PBX です。これらの通話は音声のみになります。しかし、Meeting Serverは Avaya 製品 (ビデオをサポートする製品もあります) との相互運用性に関してこの制限を課しません。そのため、「avaya」の通話は、通話が音声のみであるという意味ではありません。
失敗アクション	停止  続ける	現在のダイアルプランが通話につながらなかった場合、次の発信ダイアルプランルールを試すかどうか。ルールに停止の失敗アクションがある場合、以降のルールは使用されません。

パラメータ	タイプ/値	説明/メモ
sipControlEncryption	auto  encrypted  unencrypted	<p>このルールで発信した通話で、暗号化されたコントロールトラフィックを使用するかどうか：</p> <ul style="list-style-type: none"> <li>• 暗号化：暗号化された SIP 制御トラフィック (TLS 接続) のみを許可する</li> <li>• 非暗号化：暗号化されていないトラフィックのみを使用します (TCP または UDP)</li> <li>• auto：最初に暗号化されたコントロール接続の使用を試みますが、障害が発生した場合に非暗号化コントロールトラフィックにフォールバックすることを許可します。</li> </ul> <p>注：すべての「Lync」発信ダイアルルールが明示的に [暗号化 (Encrypted)] モードに設定されていることを確認し、TLS 接続試行が失敗した場合に、Call Bridgeが非暗号化 TCP を使用しようとするのを防ぎます。</p>
scope	global  callBridge  callBridgeGroup	<p>この発信ダイアルプランルールが有効なエンティティ：</p> <ul style="list-style-type: none"> <li>• グローバル - すべての Call Bridge は、この発信ダイアルプランルールを使用して、一致するドメインに到達できます。</li> <li>• callBridge - この発信ダイアルプランルールは、callBridgeパラメータで ID が指定される、指名された単一の Call Bridge に対してのみ有効です。</li> <li>• callBridgeGroup - この発信ダイアルプランルールは、callBridgeGroupパラメータで指定される ID の指定された単一の Call Bridge グループに対してのみ有効です。(バージョン 2.2 以降)。</li> </ul> <p>このパラメータが作成 (POST) 操作で提供されない場合、既定で「global」になります。</p>
callBridge	ID	ルールの範囲が callBridge (上記参照) の場合、これはルールが有効な Call Bridge の ID です
callBridgeGroup	ID	ルールのスコープが callBridgeGroup の場合 (上記参照)、これはルールが有効な Call Bridge グループの ID です (バージョン 2.2 以降)。
tenant	ID	テナントが指定されている場合、このルールはそのテナントに関連付けられた通話からの発信通話部分を行うためのみ使用されます。そうでない場合、どの通話からもこのルールが使用される可能性があります。
コールルーティング (ベータ機能)	デフォルト  トラバーサル	<p>これは、このルールから発信される SIP 通話に使用されるメディアルーティングです：</p> <ul style="list-style-type: none"> <li>• デフォルト - このルールを使用する通話は、通常の、直接の、メディアルーティングを使用します</li> <li>• traversal - このルールを使用する通話のメディアは TURN サーバ経由で流れます</li> </ul> <p>このパラメータが作成 (POST) 操作で提供されない場合、既定で "default" になります。</p>

---

**注：** Call Bridge クラスタを含む展開では、一致する最も優先順位の高いルールに基づいて Call Bridge の選択が行われます。一致するルールが複数あり、それらの優先度が同じ場合は、ローカル Call Bridge をカバーする **スコープ** を持つルールが優先的に使用されます。Call Bridge が選択されると、その Call Bridge に適用されるルールのみが使用されます。選択した Call Bridge を含まない範囲を持つ他の一致がある場合、それらは使用されません。

---

既存の発信ダイアルプランルールを変更するには、API オブジェクトに PUT を指定します `/outboundDialPlanRules/<発信ダイアルプランルールID>` に変更したいパラメータを指定します。

設定済みの発信ダイアルプランルールの設定を取得するには、API オブジェクトで GET を使用します `/outboundDialPlanRules`。API の使用に関する詳細は、API リファレンスガイドを参照してください。

### 10.2.2 /inboundDialPlanRules

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

ドメインごとに、ユーザまたはスペースのどちらに通話をルーティングするかを選択できます。例えば、着信が `name.space@meetingserver.example.com` であり、`name.space` という設定済みのスペースがある場合、通話はその名前のスペースにルーティングされます。

`firstname.lastname@meetingserver.example.com` 宛ての着信であれば、その名と姓を持つユーザーにルーティングされます。

代わりに、ドメインごとにユーザまたはスペースに通話をルーティングするのではなく、スペースに 1 つの着信ドメインを使用し、ユーザーに別の着信ドメインを使用することもできます。

#### 注意事項：

- スペースおよび/またはユーザーの照合は、@ の前の URI の部分でのみ行われます。
- 高い優先順位の値を持つルールが最初に照合され、スペースに一致する最も優先順位の高いルールが、招待テキスト内の URI を形成するために使用されます。個々の IP アドレスやホスト名ではなく、展開全体に対して最も高い優先順位のルールが適用されることが期待されます。複数のルールが同じ優先順位を持つ場合、ドメインのアルファベット順に基づいて一致が発生します。
- **ドメイン** パラメータを空のままにしないでください。空にしておくと、Call Bridge が通話を拒否します。
- 着信ダイアルプランルールが構成されていない場合、すべてのドメインが照合されます。
- ルールが実行されると、リストの下の方のルールは呼び出して無視されます。

新しい着信ダイアルプランのルールを作成するには、次のパラメータセットを使用して、API オブジェクト `/inboundDialPlanRules` に POST します：

パラメータ	タイプ/値	説明/メモ
ドメイン *	String	ダイアルプランルールを適用するために照合するドメイン。完全な値でなければなりません (例 "example.com")。
優先順位	数字	着信ダイアルプランルールは、構成済みのドメイン値が常に着信通話と正確に一致します。着信を通知するための完全な URI を生成する目的で (特に複数のルールが適用される場合)、優先順位の数値を設定することもできます。値が大きいほど優先されます。
resolveTocoSpaces を解決する	true false	true に設定すると、このドメインへの通話は、coSpace URI に対して照合されます (一致が見つかった場合、着信コールレグは、coSpace の参加者になります)。
resolveTolvrs	true false	true に設定すると、このドメインへの通話は設定済みの IVR URI と照合されます (一致が見つかった場合、着信コールレグはその IVR に接続します)。
resolveToLyncConferences	true false	true に設定すると、このドメインへの通話は Lync 電話会議 URL に解決されます。解決が成功した場合、着信コールレグは Lync 電話会議の参加者になります。このパラメータが作成 (POST) 操作で提供されない場合、既定で false になります。
resolveToLyncSimplejoin	true false	true に設定すると、このドメインへの呼び出しは、指定された URL への HTTPS ルックアップによって解決されます。接続が成功した場合、着信コールレグは Lync 電話会議の参加者になります。このパラメータが作成 (POST) 操作で指定されない場合、デフォルトで「false」に設定されます。(バージョン 2.2 以降)。
テナント	ID	指定した場合、このインバウンドドメインへの呼び出しは、指定されたテナントの coSpace URI に対してのみ照合されます。

既存の発信ダイアルプランルールを変更するには、API オブジェクトに PUT を指定します `/inboundDialPlanRules/<inbound dial plan rule ID>` に変更したいパラメータを指定します。

設定済みの発信ダイアルプランルールの設定を取得するには、API オブジェクトで GET を使用します `/inboundDialPlanRules`。API の使用に関する詳細は、API リファレンスガイドを参照してください。

### 10.2.3 /forwardingDialPlanRules

着信通話が着信ダイアルプランルールのいずれかに一致しない場合、通話は転送ダイアルプランルールによって処理されます。転送ダイアルプランルールは重複することができ、ワイルドカードを含むことができます。優先順位パラメータ値を使用してルールを並べ替えます。番号の大きいルールから順に試されます。action パラメータを使用して、着信を転送するかどうかを決定します。特定の通話を「キャッチ」し、拒否することが適切な場合があります。

通話を完全に拒否するか、または「ブリッジ」モードで通話を転送する (ポイントツーポイント通話) かを決定するルールを持つことができます。

転送されるコールについては、次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 `destinationDomain` パラメータ。指定したドメインへの新しい通話を作成されます。

新しい転送ダイアル プラン ルールを作成するには、次のパラメータを設定して API オブジェクト `/forwardingDialPlanRules` に POST します。

パラメータ	タイプ/値	説明/メモ
マッチパターン	String	ダイアル プラン ルールを適用するために照合するドメイン。完全なドメイン名 (例、"example.com") またはワイルドカード名 (例、exa*.com) でなければなりません。ドメイン マッチング パターンのどの部分でもワイルドカードを使用できます。しかし、すべてに一致するように「matchPattern=*」を使用しないでください。呼び出しループが作成されてしまいます。
移動先ドメイン	String	このルールで転送された通話は、接続先ドメインがこの値に書き換えられます。
アクション	転送  reject	「Forward」に設定すると、一致するコール レッグが新しい接続先とのポイントツーポイント コールになります。「reject」を選択すると、着信コール レッグが拒否されます。
callerId モード	regenerate  preserve	着信を新しい接続先アドレスに転送する際に、元の発信者 ID を保持するか、新しい ID を生成するかを指定します。このパラメータが作成 (POST) 操作で提供されない場合、デフォルトで「再生成」になります。
優先順位	番号 (Number)	転送ダイアル プラン ルールを適用する順番を決定する際に使用される数値。値が大きいほど先に適用されます。
テナント	ID	テナントが指定されている場合、このルールを使用する通話は指定されたテナントに関連付けられます。
uriParameters	破棄 転送	着信を新しい接続先アドレスに転送する場合、このパラメータは、着信の接続先 URI に存在する追加パラメータを破棄するか、それらを発信コールの接続先 URI に転送するかどうかを決定します。このパラメータが作成 (POST) 操作で指定されない場合、デフォルトで「破棄」になります。このパラメータはバージョン 2.0 以降に存在します。

既存の転送ダイアル プラン ルールを変更するには、PUT を API オブジェクトに使用します `/forwardingDialPlanRules/<発信ダイアル プラン ルール ID>` 変更したいパラメータとともに使用します。

設定済みの転送ダイアル プラン ルールの設定を取得するには、GET を API オブジェクトに使用します `forwardingDialPlanRules`。API の使用に関する詳細は、API リファレンス ガイドを参照してください。

**注：**すべてに一致する転送ダイアル プラン ルールを追加することはお勧めしません。

**例えば、matchPattern=\*** 呼び出しループが発生するためです。

## 10.3 ダイアル変換

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

変換には 3 つのステージがあります。

- 変換に適用する前処理の種類を定義する「種類」が適用されます。
  - 未加工：1 つのコンポーネントを生成します - \$1
  - ストリップ：ドット、ダッシュ、スペースを削除して 1 つのコンポーネントを生成します - \$1
  - Phone：国際電話番号への変換に使用 - 2 つのコンポーネントを生成します \$1 国コードと \$2 番号

---

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

---

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

例：

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

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

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

ただし、Call Bridge クラスターリングを展開している場合、API オブジェクトを使用する必要があります。/dialTransforms を使用します。共有 coSpace データベースは、クラスター内のすべての Call Bridge に対して単一の設定場所なので、クラスターでは、各 Call Bridge でダイアル変換を個別に設定する必要はありません。クラスターのダイアル変換は、データベース クラスター内の最初の coSpace データベースと同じ場所にある Call Bridge ホスト サーバーで定義されたものです。

---

**メモ：** 同じダイアルトランスフォームがクラスター内のすべての Call Bridge に適用されますが、発信ダイアルプランルールは Call Bridge ごとに設定できます。

---

# 11 ダイアルプランの構成 - SIP エンドポイント

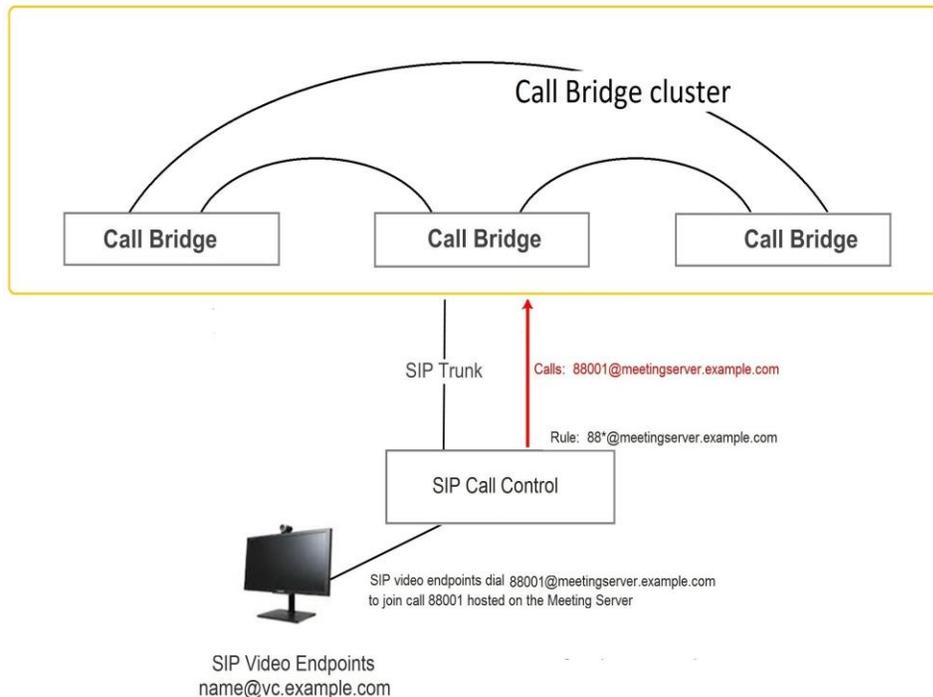
## 11.1 はじめに

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

## 11.2 クラスタ化された Meeting Server で主催されているミーティングにダイヤルする SIP ビデオエンドポイント

この最初のステップでは、クラスタ化された Meeting Server で主催されたミーティングに SIP ビデオ エンドポイントを転送するために、コール制御デバイスと Meeting Server で必要な構成を検討します。

図 33 : クラスタ化した Meeting Server がホストする通話に発信する SIP ビデオエンドポイントの例



### 11.2.1 SIP コール制御の構成

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

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

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

### 11.2.2 Meeting Server の設定

1. クラスタ内の Meeting Server の 1 つの API にサインインします。

2. エンドポイントがダイヤルインするためのスペースをMeeting Server上に作成することもできます：

- a. /coSpaces にパラメータとその値をPOSTする

- name=<string> 例 name="Call 001"
- uri=<URI のユーザ部分> 例：uri=88001

または既存のスペースを使用してください。

3. Meeting Server への着信通話用のインバウンドダイヤルプランルールを追加してください。

- a. POSTを/inboundDialPlanRules にこれらのパラメータとその値を：

- domain=<string> 例 domain="meetingserver.example.com"
- resolveTocoSpaces=true
- resolveToIvrs=true
- オプション resolveToUsers=true
- resolveToLyncConferences=true これは後ほど [セクション 12.1.2](#) で必要になります。

---

**注：** /inboundDialPlanRules の詳細については、[セクション 10.2.2](#) を参照してください。

---

4. VCS 経由で SIP エンドポイントへの発信通話のための発信ダイヤルプランルールを追加します。

- a. POSTを/outboundDialPlanRules にこれらのパラメータとその値を：

- domain=<string> ルールに一致させるドメインを使用します。例：  
domain="example.com"
- sipProxy=<string> where VCS の IP アドレスまたは FQDN が <string>です
- localFromDomain=<string> ここで、<string>はMeeting Serverクラスタの FQDN です
- trunkType=sip

---

**注：** Lync へのトランクをセットアップする場合を除き、[localContactDomain]を空のままにします ([セクション 12.1.2](#))。

---



---

**注：** /outboundDialPlanRules についての詳細情報は、[セクション 10.2.1](#) にあります。

---

SIP ビデオエンドポイントは、ダイヤルすることで Meeting Server でホストされる 88001 の通話にダイヤルすることができます。88001@meetingserver.example.com, Meeting Server が SIP エンドポイントをコールアウトできるようになります。

第 12 章の Lync のダイアルプランの作成に移る前に、次のことを検討してください：

- メディア暗号化設定を設定するには、第 11.3 項を参照してください。
- Cisco CTS エンドポイントの TIP サポートを有効にするには、項 11.4 を参照してください。
- 自動音声応答 (IVR) を設定するには、セクション 11.5 を参照してください。

### 11.3 SIP 通話のメディア暗号化

Meeting Serverは、Meeting Serverとの間で行われる、Lync 通話を含む SIP 接続のメディア暗号化をサポートしています。

SIP メディア暗号化は、進行中の SIP 通話 (アクティブな通話) または今後の SIP 通話に対して、任意、必須、または禁止に設定できます。

1. クラスタ内の Meeting Server の 1 つの API にログインします。
2. `sipMediaEncryption` パラメータを設定したコールログプロファイルを作成します。例えば、これらのパラメータを値とともに `/callLegProfiles` に POST します。
  - `name=<string>` 例えば `name="encrypt media"`
  - `sipMediaEncryption=必須`
3. 今後の SIP 通話にメディア暗号化を設定するには：
  - a. ステップ 2 で作成されたコール ログ プロファイルの ID を見つけます。  
GET `/callLegProfiles` はリストを返し、リストからコール ログ プロファイルの ID を特定してください。
  - b. コール ログ プロファイルを `coSpace`、`coSpaceUser`、`accessMethod`、または `tenant` に関連付けます。  
例えば、POST `/coSpaces/<coSpace id>/accessMethods` これらのパラメータに値を設定します。
    - `uri=<URI のユーザ部分>` 例 `uri=exec.reviews`
    - `callLegProfile=<step 3a からの ID>`
4. アクティブな SIP 通話のメディア暗号化を設定するには：
  - a. アクティブな通話を識別する  
GET `/calls` はアクティブな通話のリストを返します、通話の名前を使用して、このアクティブな通話に関連付けられている `coSpace` の ID を識別します。
  - b. ステップ 1 で作成したコール ログ プロファイルを、ステップ 3a の `coSpace ID` と関連付けます。PUT に `/coSpaces/<coSpace ID>` このパラメータには値があります
    - `callLegProfile=<step 3a からの ID>`

---

**注：** `/outboundDialPlanRule` オブジェクトには、`sipControlEncryption` パラメータがあります。発信 SIP 通話の暗号化の動作を制御します。コントロールとメディア暗号化を分離するこの機能により、メディア暗号化がない場合に TLS コントロール接続を使用できます。ウェブ管理インターフェイスからも動作を設定できます。

---

## 11.4 TIP サポートを有効にする

Cisco CTS 範囲のエンドポイントを使用する場合、TIP プロトコルサポートを選択する必要があります。API を次のように使用します。

1. クラスタ内の Meeting Server の 1 つの API にログインします。
2. コールレグのプロファイルを作成し、`telepresenceCallsAllowed` パラメータを「true」に設定します。これらのパラメータとその値を `/callLegProfiles` に POST します。
  - `name=<string>` 例えば、`name="TIP.endpoints"`
  - `telepresenceCallsAllowed=true`
3. ステップ 2 で作成されたコールレグプロファイルの ID を見つけます。  
GET `/callLegProfiles` はリストを返し、リストからコールレグプロファイルの ID を特定してください。
4. すべてのミーティングで TIP 通話を許可するには、ステップ 2 で作成したコールレグプロファイルを `/system/profiles` に関連付けます。  
たとえば、`/system/profiles` パラメータ `callLegProfile=<ID from setp 3>` に PUT を実行します。
5. TIP コールを特定の CoSpace、`coSpaceUser`、`accessMethod`、またはテナントに対してのみ許可する場合は、コールレグプロファイルを適切なオブジェクトに関連付けます。  
例：`/coSpaces/<coSpace id>/accessMethods` に POST し、`uri=TIP.meetings` とおよび `callLegProfile=<ステップ3からのID>`

---

**注意：**TIP通話では、RxおよびTx帯域幅設定を少なくとも4000000に設定する必要があります。  
`/calls/<call id>/callLegs` または `/calls/<call id>/participants` に POST して帯域幅設定を行い、**帯域幅=4000000** と指定します。

---

## 11.5 IVR 設定

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

IVR を使用する場合は、次の手順に従ってください：

1. クラスタ内の Meeting Server の 1 つの API にサインインします。
2. IVR を作成します。  
POST to `/ivr/s`、指定：`uri=<number>`、`<number>`ユーザーが IVR に到達するために発信する数字のコール ID です。

3. ユーザーが IVR に到達するために発信する必要がある外部電話番号で /accessQuery を作成します。

この IVR に連絡するための外線電話番号である <string> を ivr パラメータとして /accessQuery に POST します。

4. この IVR に着信をマッチさせる :

/inboundDialPlanRules に `resolveToIvrs=true` を使用して POST する

5. SIP 通話制御で適切なルーティングを設定し、前の手順で設定した番号への通話が Meeting Server にルーティングされるようにします。

## 11.6 次のステップ

第 12 章 の手順に従い、Meeting Server クラスタを Lync 導入と統合するためのダイアルプランを設定してください。

## 12 ダイアルプランの構成 – Lync/Skype for Business の統合

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

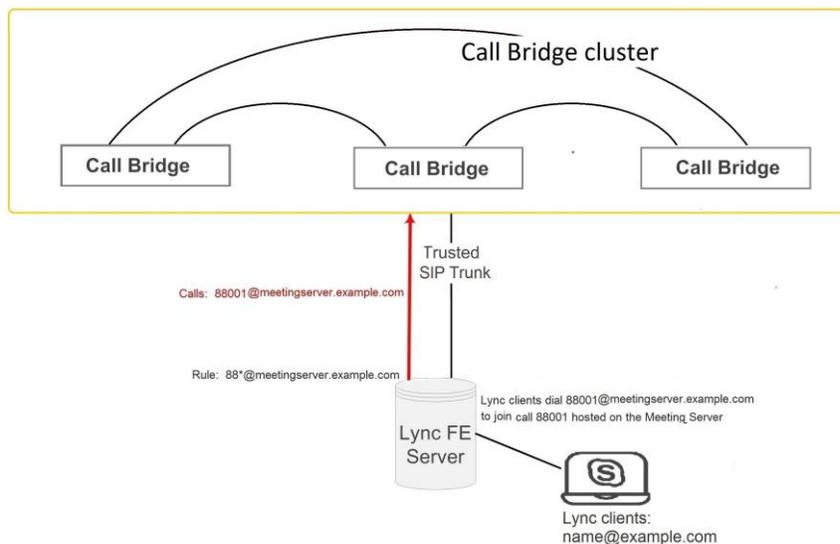
**注：** Call Bridge を Lync Edge と統合するには、Call Bridge 専用のログインアカウントが必要です。Call Bridge クラスタと Lync の統合の場合、クラスタ内の各 Call Bridge には、Lync Edge への独自の一意のログイン アカウントが必要です。

Call Bridge との間の Lync 通話ごとに、Meeting Server は Call Bridge アカウントを使用して、Lync Edge に TURN リソースを要求します。通話が切断されるまで、その TURN リソースは Lync の観点から「使用済み」と見なされます。Lync では、ユーザアカウントごとに最大 12 TURN の割り当てのみが許可されます。そのため、各 Call Bridge 登録に対して可能なのは 12 回の通話のみです。

### 12.1 Lync クライアントがクラスター化された Meeting Server 上の通話にダイヤルインする

この項では、前のセクションと同等の内容を提供しますが、Lync エンドポイントがクラスター化された Meeting Server で主催されるミーティングに参加する場合について説明します。同じ呼び出し番号/URI を使用します。必要に応じて例を変更してください。

図 34：クラスター化された Meeting Server で主催されているミーティングに参加する Lync クライアントの例



### 12.1.1 Lync フロントエンドサーバーの構成

---

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

---

**注：**Lync FE サーバからのスタティックルートを設定する前に、Lync FE サーバーが信頼するクラスタ Meeting Server に証明書がインストールされていることを確認してください。スケーラブルで復元力のある展開については、[証明書のガイドライン](#) を参照してください。

---

Lync クライアントからの発信を Meeting Server クラスタにルーティングするには、クラスタを指定する Lync スタティックルートを追加します。これには、Meeting Server クラスタを Lync FE サーバーの信頼できるアプリケーションとして設定し、スタティックルートを追加することが含まれます。設定の概要については、この [リンク](#) を参照してください。

1. Lync Server 管理シェルを開きます。
2. Meeting Server クラスタを含む新しいアプリケーションプールを信頼済みアプリケーションとして作成します。

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

置換する

`callbridgeclusterfqdn.meetingserver.com` を Meeting Server クラスタの FQDN に置き換えます。これは、すべての Call Bridge クラスタ ピアの IP を解決する A レコードであるべきです。

`callbridgelfqdn.meetingserver.com` を最初の Meeting Server の FQDN に置き換えます。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` をあなたの Lync FE サーバまたは FE プールの FQDN として使用します。

3. 他の Meeting Server をアプリケーションプールに追加します。ステップ 2 で指定した最初のを除く、クラスタ内の他のすべての Call Bridge に対してこの手順を繰り返します。

```
New-CsTrustedApplicationComputer -Identity callbridge2fqdn.meetingserver.com -pool
callbridgeclusterfqdn.meetingserver.com
```

置換：

`callbridgeclusterfqdn.meetingserver.com` を Meeting Server クラスタの FQDN に置き換えます。これは、すべての Call Bridge クラスタ ピアの IP を解決する A レコードである必要があります。

`callbridge2fqdn.meetingserver.com` をあなたの第二/第三/第四等の FQDN に置き換えます。Meeting Server。

- Meeting Server クラスタ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 callbridgeclusterfqdn.meetingserver.com -Port
5061
```

置換：

`callbridgeclusterfqdn.meetingserver.com` を Meeting Server クラスタの FQDN に置き換えます。これは、すべての Call Bridge クラスタ ピアの IP を解決する A レコードである必要があります。

- Meeting Server クラスタと Lync FE サーバ間のスタティックルートを作成します。

```
$x1=New-CsStaticRoute -TLSSRoute -Destination
"callbridgeclusterfqdn.meetingserver.com" -MatchUri
"meetingserver.example.com" -Port 5061 -UseDefaultCertificate $true
```

置換：

`callbridgeclusterfqdn.meetingserver.com` をクラスタの FQDN に置き換えます。これは、すべての Call Bridge クラスタ ピアの IP を解決する A レコードである必要があります。

`meetingserver.example.com` を、すべてのあなたのドメインに一致する URI に置き換えます。Meeting Server のコールに使用されるドメイン。

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

```
Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$x1}
```

- Meeting Server クラスタと Lync FE サーバーの各 Call Bridge の間に静的ルートを作成します。これにより、コンテンツまたはチャットを Lync から正しい Call Bridge 経由で共有できるようになります。

```
$x<n>=New-CsStaticRoute -TLSSRoute -Destination
"callbridgelfqdn.meetingserver.com" -MatchUri
"callbridgelfqdn.meetingserver.com" -Port 5061 -UseDefaultCertificate $true
```

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

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

- クラスタ内の各 Call Bridge に対して、ステップ 7 と 8 を繰り返します。

- これはオプションです。静的ルートを有効にする前に、Lync 通話の既定の画面解像度を既定の VGA から HD720p に変更することを検討してください。Lync で HD720p を有効にするには：

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

- 新しいスタティック ルートを有効にします。

```
Enable-CsTopology
```

---

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

---

### 12.1.2 クラスタ化された Meeting Server にダイアルプランルールを追加する

**注：**ウェブ管理を使用して発信ダイアルプランルールを作成すると、そのダイアルプランルールがクラスタ内のすべての Call Bridge に適用されます。発信ダイアルプランルールを特定の通話に適用するにはブリッジまたはコールブリッジグループの場合は、API を使用して `/outboundDialPlanRules` に POST する必要があります。スコープパラメータを適切に設定します。

**警告：**現在、Lync でクラスタ化された Meeting Server を展開すると、Lync クライアントは SIP エンドポイントからの着信通話を、実際の SIP ドメインではなく、Call Bridge FQDN からのものであるとして認識します。これにより、Lync デスクトップ共有がクラスタ内の別の Call Bridge に到達する際に問題が発生する可能性があります。この問題を回避するには、クラスタ内の各 Meeting Server に発信ダイアルプランルールを作成します。 `scope = callbridge` かつ `callBridge=<callbridge id>`。これにより、クラスタ内の各 Call Bridge が独自のサーバ FQDN を `localFromDomain` として使用できるようになります。

1. クラスタ内の Meeting Server の 1 つの API にサインインします。
2. アウトバウンドダイアルプランルールを Meeting Server に追加します。これは、Meeting Server クラスタ内のすべての Call Bridge に対して実行する必要があります。
  - a. POST を `/outboundDialPlanRules` にこれらのパラメータとその値を：
    - `domain=<string>` は `<string>` が Lync に送信する必要がある通話にマッチする Lync ドメインです。例えば `domain="example.com"`
    - `sipProxy=<string>` ここで、`<string>` が Lync FE プールまたはサーバーの IP アドレスまたは FQDN であるか、または空白のままにし、以下の注を参照してください。

**注：** について `sipProxy` パラメータ：

- `<string>` が空欄の場合、Meeting Server は `_sipinternaltls._tcp.<yourlyncdomain>.com` を使用してドメインの DNS SRV ルックアップを実行します
- `<string>` がフロントエンドプール (または Lync SIP ドメイン) を保持している場合、Meeting Server はまず `_sipinternaltls._tcp.<サーバアドレス>.com` を使用してその定義されたドメインの DNS SRV ルックアップを実行し、SRV ルックアップが解決に失敗した場合、ホストの DNS A レコードルックアップを実行します
- `localContactDomain=callbridgelfqdn.meetingserver.example.com`

**注：**ローカル連絡先ドメインフィールドには、Meeting Server の完全修飾ドメイン名 (FQDN) が含まれている必要があります。Lync へのトランクをセットアップする場合にのみ設定してください。

- `localFromDomain=<string>` これは、通話がどこから来たと見せたいドメイン (発信者ID) です。例：

```
localFromDomain="callbridgefqdn.meetingserver.example.com"
```

注：`localFromDomain` を空のままにしておくと、発信者番号 ID に使用されるドメインは、デフォルトで `localContactDomain` になります。

- `trunkType=Lync`
- `scope=callブリッジ` 発信ダイアルプランルールは、指定された Call Bridge に対してのみ有効です。
- `callBridge=<callbridge id>` これは、発信ダイアルプランルールが有効な Call Bridge の ID です。例、`callBridge=callbridge1` のようにします。

注：/outboundDialPlanRules についての詳細情報は、[セクション 10.2.1](#) にあります。

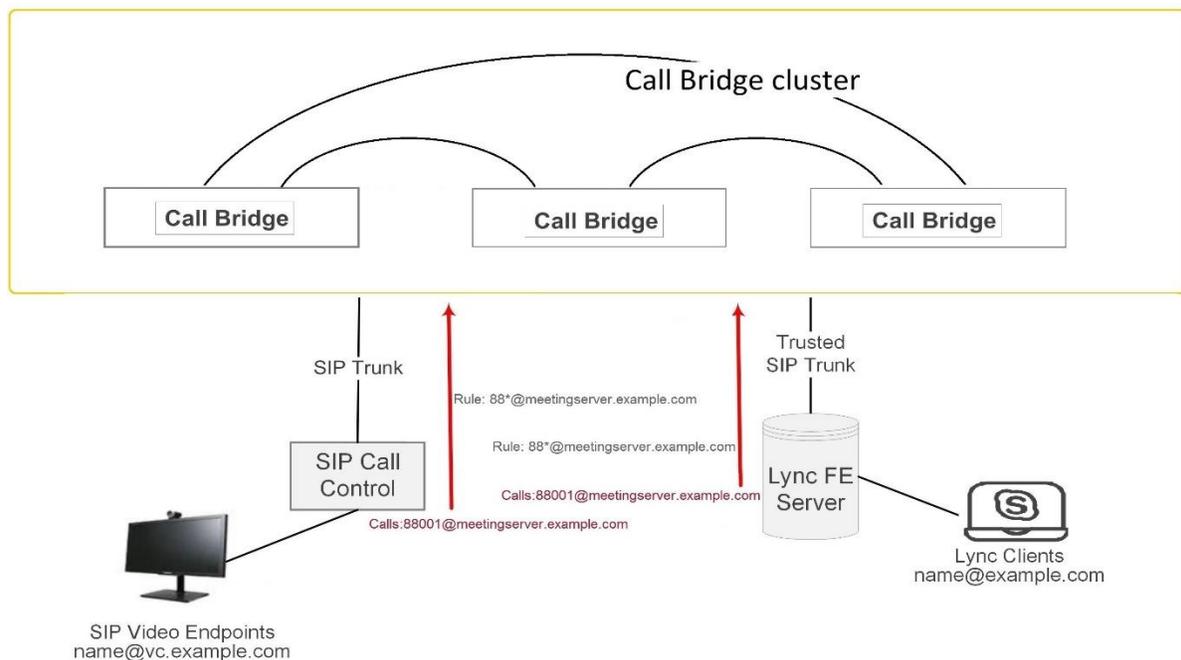
この例では、Lync クライアントは、88001@meetingserver.example.com をダイヤルすることで、クラスタ化した Meeting Server でホストされている通話 88001 に接続できます。

## 12.2 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、[項 11.2](#) の手順を実施します。Lync クライアントが Meeting Server スペースにダイヤルできるようにするには、[項 12.1](#) を実施します。

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

図 35 : Meeting Server がホストするミーティングに参加する SIP ビデオエンドポイントと Lync クライアントの例

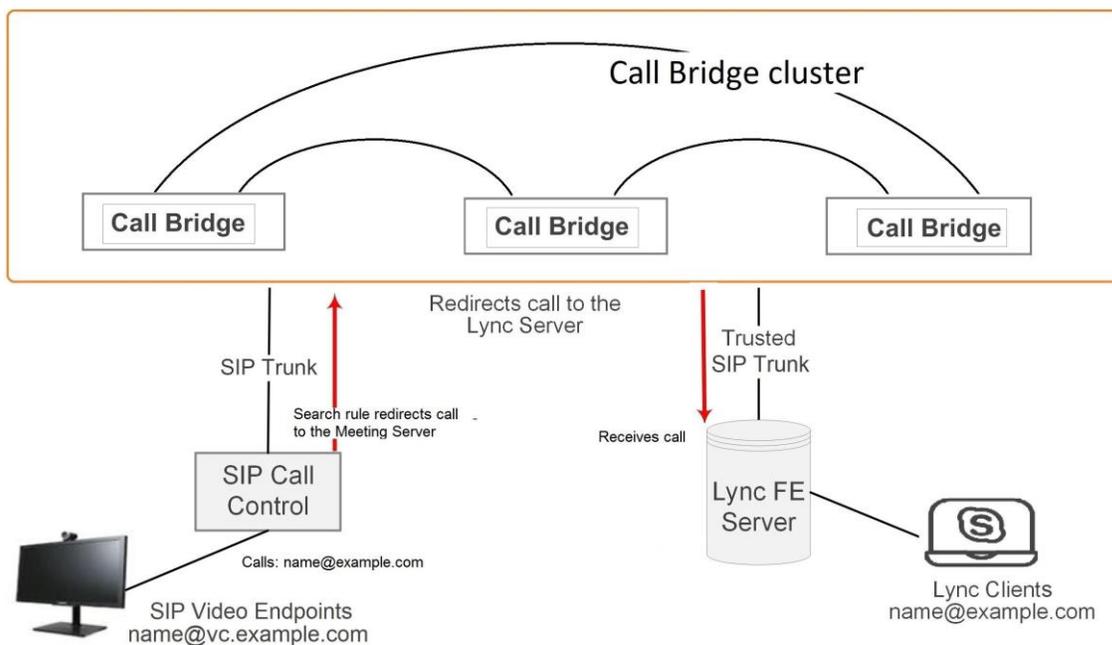


### 12.3 Lync クライアントと SIP ビデオエンドポイント間の通話を追加する

この項では、[発信](#) および [着信](#) の設定が完了していることを前提としています。例を拡張して、Lync および SIP ビデオエンドポイントが、ビデオと音声を変換するゲートウェイとして Meeting Server を使用して、通話で互いに発信できるようにします (下図を参照)。

**注：** /outboundDialPlanRule オブジェクトは、以前は Meeting Server から Cisco VCS への SIP トランクのセットアップに使用されていました。Lync 環境と SIP 環境の間の「ポイントツーポイントブリッジ」として機能するように Meeting Server を設定するには、この項で説明されているとおりに着信転送を設定し、さらに Meeting Server から他の SIP 環境への SIP トランクをセットアップする必要があります。使用している通話制御デバイス (Lync FE サーバ、Cisco VCS、CUCM、Avaya CM、Polycom DMA など)

図 36 : 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：

- Lync ユーザーは `<name>@vc.example.com` にダイヤルして、SIP ビデオエンドポイントとの通話をセットアップします `<name>@vc.example.com`。
- SIP ビデオエンドポイントは、`<name>@example.com` にダイヤルして、Lync エンドポイントとの通話をセットアップします `<name>@example.com`。

必要に応じて例を修正してください。

### 12.3.1 Lync フロントエンドサーバーの構成

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

- `vc.example.com` の Meeting Server クラスタに向けた Lync スタティックルートを追加してください。詳細については、[セクション 12.1.1](#) を参照してください。

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

### 12.3.2 VCS 構成

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

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

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

### 12.3.3 Meeting Server の設定

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

1. クラスタ内の Meeting Server の 1 つの API にログインします。
2. API オブジェクト / `forwardingDialPlanRules` を使用して、2 つの新しいルールを作成します：
  - a. SIP エンドポイントの `vc.example.com` への通話のための転送ダイヤル プラン ルールを /`forwardingDialPlanRules` に POST する。
    - `matchPattern=<string>`、ここで、`<string>` は、転送ダイヤル プラン ルールを適用するために一致させるドメインです。例：`matchPattern=vc.example.com`。ドメイン マッチング パターンのどの部分でもワイルドカードを使用できます。しかし、すべてに一致するように「`matchPattern=*`」を使用しないでください。呼び出しループが作成されてしまいます。
    - **優先順位** = number 他の転送ルールが設定されていない場合は 0 を含め、任意の値を使用できます。このルールが常に使用されるようにするには、設定したルールの中で最も高い優先順位を設定します。

---

**注：** `forwardingDialPlanRules` は優先順位に従って適用されます。優先順位の高いものから順に適用されます。2 つの `matchingPatterns` が接続先ドメインに一致する場合、高い優先順位のルールが使用されます。

---

- **action=forward** に設定すると、一致するコールレックが新しい接続先とのポイントツーポイント コールになります。注：**action=reject** を設定すると、着信コールレックが終了します。
- **callerIdMode=regenerate** これにより、発信ダイアルプランのドメインが使用されます。
- **destinationDomain=<string>** このルールで転送される通話の接続先ドメインをこの文字列の値でリライトする場合にのみ、このパラメータを指定します。

- b. Meeting Server クラスタ内の各 Call Bridge について、POST を `/forwardingDialPlanRules` Lync クライアントの `example.com` への通話の転送ダイアルプランルールです。

callBridge1 の場合：

- **matchPattern=<string>**、ここで、`<string>`は、転送ダイアルプランルールを適用するために一致させるドメインです。例：**matchPattern=vc.example.com**。
- **優先順位 = number** 他の転送ルールが設定されていない場合は 0 を含め、任意の値を使用できます。このルールが常に使用されるようにするには、設定したルールの中で最も高い優先順位を設定します。

---

注：`forwardingDialPlanRules` は優先順位に従って適用されます。優先順位の高いものから順に適用されます。2 つの `matchingPatterns` が接続先ドメインに一致する場合、高い優先順位のルールが使用されます。

---

- **action=forward** に設定すると、一致するコールレックが新しい接続先とのポイントツーポイント コールになります。注：**action=reject** を設定すると、着信コールレックが終了します。
- **callerIdMode=regenerate** これにより、発信ダイアルプランのドメインが使用されます。これにより、Lync クライアントが不在着信にコールバックできるようになります。
- **destinationDomain=<string>** このルールで転送される通話の接続先ドメインをこの文字列の値でリライトする場合にのみ、このパラメータを指定します。

3. API オブジェクト `/outboundDialPlanRules` を使用して、2 つの新しいルールを作成します：

- a. クラスタ化された Meeting Server の 1 つで、SIP エンドポイントへのコールのためのダイアルプランを作成します。POST を `//outboundDialPlanRules` にこれらのパラメータとその値を：

- **domain=<string>** 例 **domain="meetingserver.example.com"**
- **sipProxy=<string>** where VCS の IP アドレスまたは FQDN が `<string>` です

- `localFromDomain=<string>` ここで `<string>` は Meeting Server クラスタの FQDN です
  - `trunkType=sip`
  - `scope=global` クラスタ内のすべての Call Bridge がこのダイアルプランを使用します
- b. Meeting Server クラスタ内の各 Call Bridge について、Lync クライアントの `example.com` への通話のダイアルプランを `/outboundDialPlanRules` に POST します。これは、[セクション 12.1.2](#) のステップ2の繰り返しです。

callbridge1 の場合：

- `domain=<string>` ここで、`<string>` 通話を Lync に送信するために照合する Lync ドメインです。例：`domain="lync.example.com"`
- `sipProxy=<string>` ここで、`<string>` が Lync FE プールまたはサーバーの IP アドレスまたは FQDN であるか、または空白のままにし、以下の注を参照してください。

---

注：について `sipProxy` パラメータ：

- `<string>` が空欄の場合、Meeting Server は `_sipinternaltls._tcp.<yourlyncdomain>.com` を使用してドメインの DNS SRV ルックアップを実行します
- `<string>` がフロントエンドプール (または Lync SIP ドメイン) を保持している場合、Meeting Server はまず `_sipinternaltls._tcp.<yourlyncdomain>.com` を使用してその定義されたドメインの DNS SRV ルックアップを実行し、SRV ルックアップが解決に失敗した場合、ホストの DNS A レコードルックアップを実行します

- 
- `localContactDomain=callbridgelfqdn.meetingserver.example.com`

---

注：ローカル連絡先ドメインフィールドには、Meeting Server の完全修飾ドメイン名 (FQDN) が含まれている必要があります。Lync へのトランクをセットアップする場合にのみ設定してください。

- 
- `localFromDomain=<string>` これは、通話がどこから来たと見せたいドメイン (発信者 ID) です。例：  
`localFromDomain="callbridgelfqdn.meetingserver.example.com"`

---

注：`localFromDomain` を空のままにしておくと、発信者番号 ID に使用されるドメインは、デフォルトで `localContactDomain` になります。

- 
- `trunkType=Lync`
  - `scope=callブリッジ` 発信ダイアルプランルールは、指定された Call Bridge に対してのみ有効です。
  - `callBridge=<callbridge id>` これは、発信ダイアルプランルールが有効な Call Bridge の ID です。

クラスタの各 Call Bridge で繰り返します

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

## 12.4 Lync Edge サービスを使用した Lync の統合

Lync Edge サーバーを使用する NAT トラバーサルについては、この項の構成手順に従い、Meeting Server で Lync Edge 設定を構成します。これは、[デュアルホーム](#)をサポートするために必要です。会議 または、Lync 通話の TURN/ICE の役割を Lync Edge が実行する場合、Meeting Server ではなく

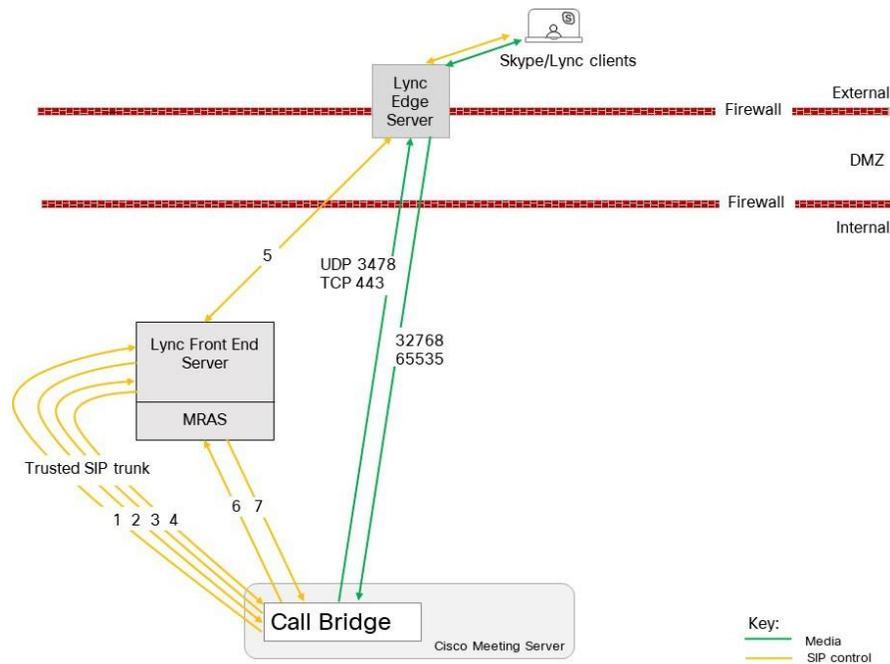
### 12.4.1 Lync Edge 通話フロー

Meeting Server から Lync Edge サーバーへの通話を確立するには (次の 図 37 を参照) :

1. Call Bridge は、Lync フロントエンドサーバーへの「登録」 SIP 通話を発信します。
2. 「登録」が承認されます。
3. Call Bridge は「サービス」を Lync フロントエンドサーバーに送信します。
4. フロントエンドサーバーは、メディアリレー認証サーバー (MRAS) の URI を返します。(Lync Edge サーバーは MRAS として機能します。)
5. Lync クライアントが着信を受け取ります。
6. Call Bridge は「サービス」メッセージを Lync フロントエンド サーバーに送信し、Lync Edge MRAS サービスを使用するための MRAS 資格情報を要求します
7. Lync フロント エンド サーバーは、Call Bridge が使用する資格情報、UDP および TCP ポート、および MRAS URI を再度返します
8. Call Bridge は、DNS を使用してこの MRAS URI を解決し、Lync Edge サーバーへの直接 STUN メッセージの送信を開始します。
9. 通話メディアは、Call Bridge と Lync Edge の TURN サーバーの間を UDP ポート 3478 で直接流れ、上記の一時的な範囲のポートで Lync Edge サーバーから Call Bridge に返されます。

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

図 37 : Call Bridge から Lync Edge サーバーへの通話フロー



### 12.4.2 Lync Edge を使用するための Meeting Server の構成

Lync Edge サーバーを使用するには、API ではなく、Meeting Server クラスター内の各 Call Bridge のウェブ管理インターフェイスを通じて Lync Edge 設定を構成する必要があります。

Lync Edge サーバーが構成されると、Lync 通話の TURN / ICE の役割を担うため、あるレベルでは、Meeting Server の TURN サーバ設定の代わりにになります。

また、Meeting Server - Lync Edge サーバ構成をセットアップするために、Lync ユーザクライアントアカウントを作成する必要があります。クラスター内の各 Call Bridge には異なる Lync ユーザクライアントアカウントが必要です。ウェブ管理インターフェイスではなく、Meeting Server API が以下のステップ 4 で使用される場合、Lync ユーザアカウントは、各 Call Bridge が独自のアカウントを持つのではなく、クラスター内の Call Bridge によって共有されます。

クラスター内の各 Meeting Server に対して、これらの手順に従い、Lync Edge サーバーを使用するために Meeting Server をセットアップします：

1. 適切な DNS レコードが設定されていることを確認してください。スケーラブルで回復力のあるサーバタイプの展開に必要な DNS レコードの一覧については、[付録 A](#) を参照してください。
2. ディレクトリ内の他のユーザーと同様に、LDAP ディレクトリ内に新しいユーザーを作成します。例えば、`firstname="edge"`, `second name = "user"` です。
3. Lync FE サーバーのユーザマネージャーにログインし、前のステップで作成したユーザから Lync クライアントユーザーを作成します。他のユーザーと同じように、Lync を使用できる

ようにします。上記の例の名前を使用して、`edge.user@lync.example.com` という名前の Lync クライアントユーザーを作成します。

4. Meeting Serverのウェブ管理インターフェイスにログインし、**構成>全般** に移動して、Lync Edge 設定を構成します。
  - **サーバアドレス** このフィールドには Lync フロントエンドサーバーのアドレスを入力します (またはそれを解決する主催者名を入力します)
  - **ユーザ名** このフィールドは手順 3 で作成した Lync クライアントのユーザ名です
  - **登録数** このフィールドは、1 つの登録済みデバイスに対して実行される同時通話の数を制限する Lync Edge サーバーの機能を克服します。1 より大きい数字を入力することで、Call Bridge は指定された数の登録を行います。これにより、Meeting Serverが Lync Edge Server 経由で発信できる同時通話の数が増えます。

1 より大きい数字を入力すると、Lync Edge ユーザ名の末尾に数字が追加され、そのユーザ名で登録されます。例えば、ユーザー名を `edge.user@lync.example.com` として設定し、**登録数** を 3 に設定した場合、Edge サーバーで使用するために Lync 環境で次のユーザーを作成します：`edge.user1@lync.example.com`

`edge.user1@lync.example.com`

`edge.user2@lync.example.com`

`edge.user3@lync.example.com`

例えば、単一の登録のみを行う場合は、**登録数** を空白にしてください。

`edge.user@lync.example.com.`

---

**注：** **レジストレーション数** を使用して同時コール数を増やすには、いくらかの管理オーバーヘッドが必要です。ただし、上記で説明したように、Lync Edge サーバーの制限によるものです。

---



---

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

---

Lync Edge の構成に関する注意事項：

- Meeting Serverは、Lync Edge サーバ経由で到着するメディアを持つ外部の Lync クライアントからの Lync コンテンツ (RDP 経由で提供されるプレゼンテーション) をサポートします。さらに、スペース (URI) は現在スペースにいる参加者の数に基づいて、使用中または利用可能としてレポートされるようになったため、お気に入りにスペースがある Lync クライアントはスペースの状況を確認できます。
- Lync AVMCU を使用している場合、Lync フロントエンドサーバーに登録するには、Lync エッジ設定を構成する必要があります。
- ウェブアプリは、Lync Edge サーバーが構成されている場合でも、Meeting Serverの TURN サーバーを使用し続けます。注：ウェブ アプリ ユーザーは、Lync クライアントによってのみ Lync ミーティングに追加され、Lync ミーティングに直接ダイヤルインできません。
- Lync Edge サーバーが構成されている場合、すべての Lync 通話で ICE 候補の収集と外部メディア接続にそのサーバーが使用されます。Lync Edge サーバーが構成されていないが、

展開で Cisco Expressway が構成されている場合、Lync 通話は Expressway の構成された TURN サーバーによって処理されます。

- 通常の Lync Edge 導入では、Lync Edge サーバーの内部インターフェイスにはデフォルトゲートウェイが定義されません。外部インターフェイスのみにデフォルトゲートウェイが定義されます。Lync Edge サーバーの内部インターフェイスと同じローカルサブネット上にない場合、内部インターフェイスを使用して Meeting Server にパケットを正しくルーティングできるように、Lync Edge サーバーへの静的で永続的なネットワークルートを定義する必要があります。静的で永続的なネットワークルートを Lync Edge サーバーに追加するには、CMD を開いて以下のコマンドを発行し、サンプルデータを実際の IP 情報で置き換えます。

コマンド例：

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

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

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

## 12.5 Microsoft Lync および Skype for Business 通話で共有コンテンツの帯域幅を制御する

**注：** Microsoft Lync および Skype for Business 通話の共有コンテンツの帯域幅の制御は、Meeting Server クラスターの各 Call Bridge に対して実行する必要があります。ウェブ管理インターフェイス経由でのみ実行できます。API 経由では実行できません。

Call Bridge は、発信 Lync プレゼンテーションメディアに使用される帯域幅の総量に制限を課します。主催者コンピュータが直接接続されている通話の場合、LAN 帯域幅の制限が適用されます。それ以外のすべてのケース、例えば接続に DMZ を越えたトラバーサルが含まれる場合、リモート Lync クライアントに関しては、WAN 帯域幅制限が適用されます。デフォルトの制限は、LAN 帯域幅に 8MB、WAN 帯域幅に 2MB です。

Lync 通話とのコンテンツ共有に使用される帯域幅は、ウェブ管理インターフェイスから変更できます。に移動します [構成] > [通話設定] Lync コンテンツの LAN および WAN 帯域幅制限を設定してください。[送信] ボタンをクリックし、必要に応じて [アクティブな通話に適用] ボタンをクリックします。

図 38 : Lync コンテンツ共有の帯域幅の設定

Bandwidth settings (Lync content)

LAN bandwidth limit	8000000
WAN bandwidth limit	2000000

Submit Apply to active calls

## 12.6 Lync 直接フェデレーション

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

着信通話を許可するには：

1. Meeting Server の FQDN を指定する DNS SRV レコード `_sipfederationtls._tcp.domain.com` を作成します。Call Bridge はパブリック IP を持つ必要があり、NAT はこのシナリオではサポートされないため、この手順が必要です。
2. Meeting Server の FQDN をパブリック IP アドレスに解決する DNS A レコードを追加します。
3. 以下の要件を満たす証明書と証明書バンドルを Meeting Server にアップロードします。
  - a. 証明書は、CN として FQDN を持つ必要があります。または、SAN リストで証明書を使用する場合は、FQDN が SAN リストにもあることを確認します。注：証明書に SAN リストが含まれている場合、Lync は CN フィールドを無視し、SAN リストのみを使用します。
  - b. 証明書はパブリック CA によって署名されている必要があります。

---

**注：** Lync フロントエンドサーバーが信頼している認証局 (CA) と同じものを使用してください。CA の詳細および Meeting Server と Lync の統合に関するサポートについては、Lync アドバイザに問い合わせてください。

---

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

---

**注：** 証明書の詳細は、[Cisco ミーティング サーバ証明書のガイドラインの概要を参照してください](#)。

---

- d. **付録 1** に従い、適切なファイアウォールポートを開きます。例：TCP 5061, UDP 3478, UDP 32768-65535, TCP 32768-65535

Meeting Server からの発信通話の場合：

1. 発信ダイヤルルールを作成します。[domain] と [sipProxy] のフィールドを空白のままにして、[trunk] タイプを Lync として設定します。また、適切な [localContactDomain] および [localFromDomain] フィールドを設定します。

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

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

Lync 展開の前提条件：この機能を使うには、電話ダイヤルイン機能が有効な Lync 展開が必要です。Lync 展開では、1 つ以上のオンプレミス Lync フロントエンドサーバーを構成する必要があります。

---

**注：**Lync 展開が外部の Lync または Skype for Business クライアントをサポートしていない場合でも、オンプレミスの Lync フロントエンドサーバーを設定する必要があります。

---

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

---

**注：**Lync ミーティング解決のために、Meeting Server は発信ルールではなく、Lync ミーティング ID と `_sipinternaltls._tcp.lync-domain` の DNS ルックアップを使用します。DNS サーバーに DNS SRV レコード `_sipinternaltls._tcp.lync-domain` を設定するか、DNS SRV レコードを使用しない場合は、コマンド `dns app add rr` で Meeting Server のレコードをセットアップします。<DNS RR>. Dns app コマンドの使用に関する詳細は、[MMP コマンドライン リファレンス](#)を参照してください。スケーラブルで復元力のある展開に必要な 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。

---

Lync フロントエンドサーバーを設定し、次の表 7 のタスクシーケンスに従います：

表 7 : Lync フロントエンドサーバーを構成するための一連のタスク

シーケンス	タスク	API 経由	ウェブ管理インタフェース上 - クラスタ Meeting Server には使用しないでください
1	Lync 会議 ID の入力を許可するように Call Bridge IVR を設定する。	API を通じて IVR をセットアップしている場合：  設定済み IVR の <code>resolveLyncConferenceIds</code> を <code>true</code> に設定します。	ウェブ管理インタフェース経由で IVR をセットアップしている場合：  [設定] に移動します。全般 IVR 項で、[ID でスケジュール済みの Lync 会議に参加する] を許可します。
2	標準 SIP システムから Lync 会議 ID への直通ダイヤルを許可します。注：既存の構成済みドメインを拡張して Lync 電話会議へのアクセスを許可するか、この目的のために新しくドメインを作成することを選択できます。	設定 受信するダイヤル プランルールで、 <code>resolveToLyncConferences</code> を <code>true</code> に設定します。	[設定 (Configuration)] > [着信コール (Incoming calls)] に移動します。そして、1 つ以上の設定されたコールマッチングドメインに対して、[ターゲット Lync (Targets Lync)] を [yes] に設定します。
3	Web Bridgeの通話参加インタフェース経由で Lync 会議 ID 入力を許可する。	API を通じて Web Bridge をセットアップしている場合：  Web Bridge で <code>resolveLyncConferenceIds</code> を <code>true</code> に設定します。	Web 管理インタフェース経由で Web Bridge をセットアップしている場合：  Web Bridge 設定項で、[設定 (Configuration)] > [全般 (General)] にして、[ID によるスケジュール済み Lync 電話会議への参加 (Joining scheduled Lync conferences by ID)] が [許可 (Allowed)] になっていることを確認します。

コールが Lync conference IDs に対して照合される場合、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、適用されない場合、設定された、アドバタイズされた Lync フロントエンドサーバーを特定します ID を解決する機能を持つものとして、Call Bridge は Lync フロント エンド サーバーにクエリを実行し、問題のコール ID が Lync 電話会議に対応するかどうかを判断します。一致する場合、ルックアップが成功したと見なされ、通話は Lync 通話に参加します。通話 ID が Lync 会議に対応していると認識されない場合、Lync フロントエンドサーバーへの照会は行われません。

注：異なる Lync 展開環境にある複数の Lync フロントエンドサーバーの設定を追加すると、予期しない結果となる場合があります。たとえば、異なる Lync 展開の複数の Lync 電話会議が同じコール ID を使用する場合、複数の Lync フロントエンドサーバーがルックアップに対して積極的に応答する可能性があります。この場合、「最初に」成功した Lync の解決が使用されます。

---

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

---

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

# 13 OBTP スケジュールでの Office 365 デュアル ホーム エクスペリエンス

## 13.1 概要

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

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

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

---

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

---

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

---

## 13.2 構成

---

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

---

Meeting Serverを構成します。この Office 365 ミーティングへの参加方法をセットアップするには、リクエストパラメータ `resolveToLyncSimpleJoin` を true に設定した着信ダイヤルプランルールを使用します。これにより、Office 365 招待で送信された Lync Simple Meet URL を解決する方法が Meeting Serverに通知されます。

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

### 13.3 会議中の体験

「OBTP スケジュールを使用した Office 365 デュアル ホーム エクスペリエンス」は、双方向の音声、ビデオ、コンテンツ共有による「デュアル ホーム エクスペリエンス」を提供します。Office 365 クライアントには、使い慣れた会議中の体験は Lync AVMCU により決定され、OBTPを有効にしたエンドポイントを使用する参加者は Meeting Server によりビデオ会議体験が決定されます。全員に統合参加者リストが表示されます。

---

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

---

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

---

## 14 Web Bridge 3 の設定

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

ウェブ アプリをテストしている場合、Meeting Server の初期設定が完了した後はいつでも、[項 14.2](#) の手順をこの順番で実行してください。ウェブ アプリを使用していない場合は、この章をスキップしてください。

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

### 14.1 Web Bridge 3 接続

表 8 にウェブ アプリの接続に使用されるポートを示します。[項 14.1.1](#) では、ウェブ アプリと Meeting Server のコンポーネント間の通話フローについて説明しています。

図 39：ウェブ アプリのポートの使用状況

表 8：ウェブ アプリの接続に必要なポート

コンポーネント	接続先	開く接続先ポート	トラフィックタイプ	コンポーネントに対するトラフィックの方向	追加情報
Web Bridge 3	web app	443 (メモ 1)	TCP (HTTPS)	着信	
Web Bridge 3	web app	80	TCP (HTTP)	着信	
Call Bridge	Web Bridge 3				

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

#### 14.1.1 Web Bridge 3 の通話フロー

この項では、ウェブ アプリと Meeting Server のコンポーネント間の通話フローについて説明します。

1. ウェブブラウザが HTTPS 接続を開きます。
2. ユーザーには **ミーティングに参加** (手順 3 を参照) または **ログイン** (手順 4 を参照) の選択が提示されます。

3. [ミーティングに参加] が選択されている場合、ユーザーは呼び出し ID/URI とパスコードを入力し、名前を設定するように求められます。
  - a. 通話の詳細は、HTTPS 経由で Web Bridge 3 に送信されます。Web Bridge 3 は、通話の詳細を検証するために、C2W 接続を介して Call Bridge にクエリを実行します。
  - b. 成功した場合、ユーザーはメディア設定を選択するように求められます。
  - c. メディア設定を選択した後、通話の詳細と希望の名前が HTTPS 経由で Web Bridge 3 に送信されます。C2W 経由で Call Bridge に転送されます。Call Bridge は、ブラウザに返される通話アクセストークンで応答します。このトークンは、ブラウザが使用する TURN サーバーの詳細を示します。
  - d. Call Bridge は、設定された TURN サーバからの割り当てを要求します。
  - e. ウェブアプリは、指定された TURN サーバーに割り当てを要求します。
  - f. ブラウザが Web Bridge 3 へのウェブソケット接続を開きます。この接続は、C2W 接続経由で Call Bridge に転送されます。呼び出しアクセストークンはこのウェブソケット経由で送信されます。
  - g. ブラウザと Call Bridge は、ローカル メディア IP アドレス/ポートおよびメディア リレー アドレス/ポートを含むウェブソケット上の SDP を交換します。
  - h. ICE ネゴシエーションは、すべてのブラウザメディア IP アドレス/ポートの組み合わせと、すべての Call Bridge アドレス/ポートの組み合わせの間で UDP パケットを送信し、TCP メディアリレーアドレス/ポートに TCP 接続を試みます。
  - i. ブラウザと Call Bridge の間のメディア転送には成功した最短メディア パスを使用され、これは直接、TURN UDP リレーを経由、または TURN サーバーが TCP ストリームと UDP の間でメディアパケットを変換する TURN TCP リレーを経由します。
4. ログイン が選択されている場合、ユーザーはユーザ名とパスワードの入力を求められます。
  - a. HTTPS 経由で Web Bridge に送信され、成功した場合、ポータルアクセストークンを取得するために Call Bridge に転送されます。
  - b. ユーザーのポータルサイトに入ると、すべてのリクエストが HTTPS 経由で送信され、ポータル アクセストークンがヘッダーとして送信されます。
  - c. 通話参加リクエストが行われた場合、フローはステップ 3c 以降と同じですが、通話の詳細と希望する名前を送信して通話アクセストークンを取得する代わりに、ブラウザは代わりに通話の詳細とポータルアクセストークンを送信します。

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

## 14.2 Web Bridge 3 の設定

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

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

Web Bridge 3 の設定の詳細については、「[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。

### 14.2.1 Web Bridge プロファイルを作成して適用する方法の例

開始する前に、Web Bridge 3 証明書をインストールし、Web Bridge 3 を [セクション 4.6](#) に記載の通りに設定していることを確認してください。その後、次の手順に従って操作してください：

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

- i. allowUnauthenticatedGuests フィールドを true または false に設定してください。true に設定した場合、このWeb Bridgeのプロファイルを使用するWeb Bridgeのランディング画面からのゲストアクセスが許可されます。False に設定すると、訪問者アクセスは、ユーザーがユーザポータルにログインした後にのみ許可されます。このパラメータが指定されていない場合、デフォルトで [true] に設定されます。
  - j. resolveCoSpaceCallIds フィールドを true または false に設定してください。このフィールドは、このWeb Bridge プロファイルを使用するWeb Bridgeが、coSpace および coSpace アクセス メソッド コール ID を受け入れ、訪問者が cospace ミーティングに参加できるようにするかどうかを決定します。このパラメータが指定されていない場合、デフォルトで [true] に設定されます。
  - k. resolveCoSpaceUri フィールドを **オフ**、domainSuggestionDisabled または domainSuggestionEnabledに設定してください。このフィールドは、このWeb Bridgeが、coSpace および coSpace アクセス方式 SIP URI を、訪問者が cospace ミーティングに参加できるようにする目的で受け入れるかどうかを決定します。[off] に設定すると、URI による参加は無効になります。[domainSuggestionDisabled] に設定すると、URI による参加は有効になり、しかし、このWeb Bridgeでは URI のドメインは自動補完または検証されません。[domainSuggestionEnabled] に設定すると、URI による参加は有効になり、そして、このWeb Bridgeで URI のドメインが自動補完され、検証されます。このパラメータが指定されていない場合、デフォルトで [off] に設定されます。
  - l. **[作成 (Create) ]** をクリックします。
2. プロファイルを作成したら、アドレスを追加できます。これはミーティング招待状を生成するために使用されるWeb Bridge URI であり、ウェブ アプリのクロス起動 URL です。

---

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

---

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

- a. API オブジェクトのリストで、/api/v1/webBridgeProfiles 後の ▶ をタップします。
- b. **[表示または編集]** をクリックします。
- c. 結果の"webBridgeProfile オブジェクト選択ウィンドウ"から、**ステップ 1 で作成し、Web Bridge URI および IVR 番号を割り当てたい webBridgeProfile の オブジェクト ID を選択します。** Web Bridgeの **ラベル** および **URL アドレス** を入力し、必要に応じて IVR の **ラベル** および **番号** を入力します。

« return to object list

/api/v1/webBridgeProfiles/410c2b53-3135-4f58-8742-08e5b025675a/webBridgeAddresses

Related objects: [/api/v1/webBridgeProfiles](#)  
[/api/v1/webBridgeProfiles/410c2b53-3135-4f58-8742-08e5b025675a](#)

« start < prev **1 - 1** (of 1) next » [Table view](#) [XML view](#)

object id	label
<a href="#">b4311cfb-6071-4fe9-b684-f55c197e4681</a>	Pre-A

---

/api/v1/webBridgeProfiles/410c2b53-3135-4f58-8742-08e5b025675a/webBridgeAddresses

label

address   (URL)

---

« return to object list

/api/v1/webBridgeProfiles/410c2b53-3135-4f58-8742-08e5b025675a/ivrNumbers

Related objects: [/api/v1/webBridgeProfiles](#)  
[/api/v1/webBridgeProfiles/410c2b53-3135-4f58-8742-08e5b025675a](#)

« start < prev **none** next » [Table view](#) [XML view](#)

```
<?xml version="1.0"?>
<ivrNumbers total="0"></ivrNumbers>
```

---

/api/v1/webBridgeProfiles/410c2b53-3135-4f58-8742-08e5b025675a/ivrNumbers

label

number

d. [作成 (Create) ] をクリックします。

3. 必要に応じて、新しく作成された webBridgeProfile の ID を次のいずれかまたはすべてに割り当てます。
  - 最上位 (グローバル) プロファイル (/api/v1/system/profiles)
  - テナント (/api/v1/tenants/<id>)
  - WebBridges (/api/v1/webBridges/<id>)

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

- a. API オブジェクトのリストで、/api/v1/system/profiles 後の ▶ をタップします。
- b. [表示または編集] をクリックします。
- c. パラメータを下にスクロールして webBridgeProfile を選択し、[選択 (Choose) ] をクリックします。
- d. 結果の "webBridgeProfile オブジェクト選択ウィンドウ" から、**ステップ1で作成した、最上位のグローバルプロファイルに割り当てたい webBridgeProfile のオブジェクトIDを 選択** をクリックします。
- e. [変更 (Modify) ] をクリックします。
- f. 新しく割り当てられた webBridgeProfile オブジェクト ID が、**オブジェクトの設定** の下に表示されます。

---

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

---

## 15 ミーティングの録画とストリーミング

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

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

### 15.1 新しい内部 SIP レコーダーとストリーマの機能の利点

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

### 15.2 新しい内部 SIP レコーダーとストリーマを実装する際の注意事項

---

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

---

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

表 9 : 内部 SIP レコーダーのパフォーマンスとリソース使用率

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

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

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

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

表 10 : 内部 SIP ストリーマの推奨仕様

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

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

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

### 15.3 録画の概要

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

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

### 15.3.1 サードパーティの外部 SIP レコーダーのサポート

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

---

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

---

サードパーティの外部 SIP レコーダー機能：

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

---

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

---

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

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

レコーダーは、電話会議を主催するサーバーとは別のMeeting Server上で有効にしてください。図 40 を参照してください。レコーダーは、導入をテストする目的で、電話会議（ローカル）を主催している Call Bridge と同じ Meeting Server 上にのみ配置します。

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

---

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

---



---

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

---

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

次の図は、許可されているさまざまなレコーディング導入を示しています。スケーラブルで復元力のある展開についての詳細は、[セクション 15.3.3](#) を参照してください。

図 40 : 録画のデプロイメントで許可されている：リモートモード

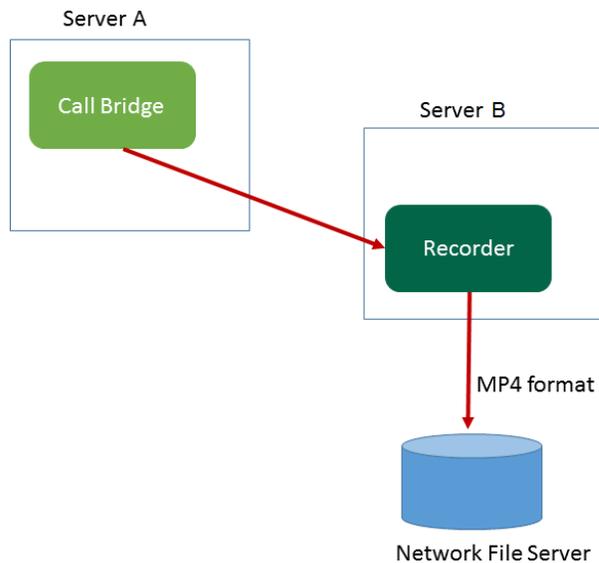
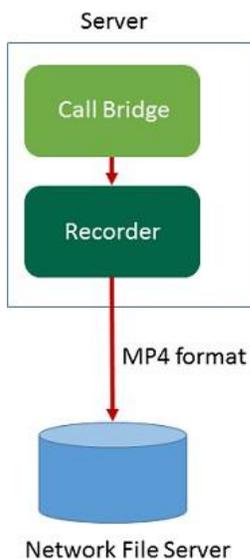


図 41 : テスト目的でのみ許可された展開：ローカルモード

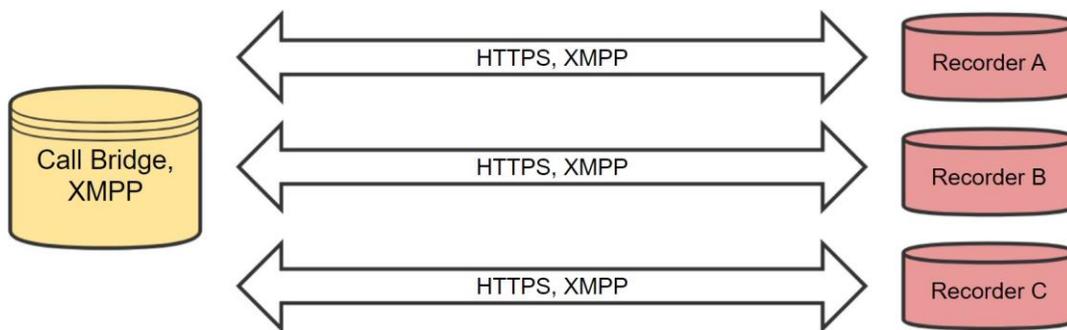


### 15.3.3 スケーラビリティとレジリエンスのためのレコーダー/ストリーマを導入する

複数のレコーダーまたはストリーマを展開する場合、コールコントロールプロバイダーの背後に展開し、コールコントロールプロバイダーがロードバランシングとフェイルオーバーをサポートできるようにすることを推奨します。sipRecorderUri API パラメータを設定して、プロキシに通話を転送できるダイヤルプランルールを指定する必要があります。

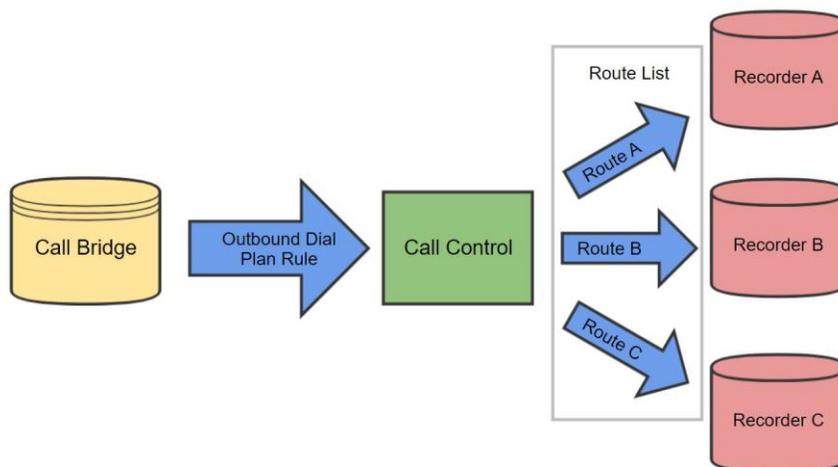
新しいレコーダーの通話制御フローの動作は、古い XMPP レコーダーの動作とは異なります。以前は、レコーダーは XMPP クライアントとして Call Bridge に直接接続し、利用可能性の情報を HTTPS リンク経由で送信していました。図 42 に示されています。

図 42 : 古い XMPP レコーダーの通話制御フロー



新しい内部 SIP レコーダー コンポーネントでは、通話制御は通話制御プロバイダーを通じてフローしますが、メディアはほとんどの場合、Call Bridge とレコーダーの間で直接フローします。場合によっては、通話制御プロバイダの設定によっては、メディアが通話制御プロバイダを経由することもあります。この新しいレコーダーの通話制御フローは 図 43 に示されています。

図 43 : 新しい内部 SIP レコーダーの通話制御フロー



### 15.3.3.1 サポートされている通話制御方法

- Cisco Unified Communications Manager : クラスタ内の各レコーダーは SIP トランクの背後に展開されるべきで、クラスタ内の各レコーダーは同じルートリストに関連付けられるべきです。
- Cisco Expressway –各レコーダーは、クラスタ内のすべてのレコーダーにマッピングされるルートパターンで、独自のゾーンを持つように構成されるべきです。
- **ダイレクト フロー** : レコーダー/ストリーマのアドレス/FQDN になるようにダイヤル プラン ルールのプロキシを設定できますが、これは 1 つのインスタンスを展開する場合にのみ推奨されます。

詳細については、[Cisco Meeting Server 2.x、ホワイトペーパー「Cisco Meeting Server 間での通話の負荷分散」](#)を参照してください。

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

**注** : Windows 2008 R2 SP1 を実行している NFS サーバーに録画を保存する予定の場合は、権限の問題を修正するために Windows hotfix を適用する必要があります。  
<https://support.microsoft.com/en-us/kb/2485529> この修正を適用する前に、Microsoft Windows 管理者に問い合わせてください。

これは 2 段階のプロセスです。

- [MMP 経由での Meeting Server レコーダーの設定](#)
- [API 経由でレコーダー URI を設定する](#)

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

1. バージョン 3.0 にアップグレードします。
2. MMP に SSH で接続し、ログインしてレコーダーを設定します (MMP コマンド、レコーダー すべての利用可能なコマンドのリストを見るために)。
3. `recorder nfs <hostname/IP> : <directory>` を入力し、NFS ロケーションを設定します。
4. `recorder resolution <audio|720p|1080p>` を入力し、目的の解像度に設定します (または通話の音声のみを録音します)。
5. MMP コマンド `recorder sip listen <interface> <tcp-port|none>` を使用して、レコーダーをリスンするインターフェイスと、リスンする SIP TCP および TLS ポートを設定します。<tls-port|none>。サービスを無効にするには、それぞれのポートを **なし** に設定します :
  - a. たとえば、TCP ポートではなく、TLS ポートでのみリスンする場合、次を入力します。

`recorder sip listen a none 6000`を設定します

- b. 構成したポートが既定の TCP/TLS ポート (5060/5061) ではない場合、後で必要になるため、メモしておきます。

---

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

---

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

---

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

---

- 7. オプションで、TLS が構成されている場合、レコーダーの SIP の TLS 検証を次のように実行できます。
  - a. MMP コマンド `tls sip trust [<crt-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 接続を安全なものにするために、TLS 検証を有効にすることをお勧めします。

---

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

## タスク 2：API 経由でレコーダー URI を設定する

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

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

---

**注：**設定された URI のユーザ部分 ('@' 記号の前の部分) には特別な意味がありません。新しい内部 SIP レコーダー コンポーネントでは必須ですが、通常は何でもかまいません例：`"recording@recorder.com"`。しかし、これはユーザ資格情報の URI のユーザ部分を使用する可

性能があるサードパーティの SIP レコーダーには当てはまらない場合があります。URI の重要な部分はドメイン部分です。

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

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

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

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

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

1. Web 管理インターフェースを使用して、**[設定 (Configuration)]** > **[API]** の順に選択します。
  - a. API オブジェクトのリストで、`/api/v1/system/profiles` 後の ▶ をタップします。
  - b. **[表示または編集]** をクリックします。
  - c. パラメータを `callProfile` まで下にスクロールし、**[Choose]** をクリックします。
  - d. 表示された「`callProfile` オブジェクト選択ウィンドウ」から、**オブジェクト ID** を選択し、**最上位のグローバルプロファイル**に割り当てられる `callProfile` を選択します。
  - e. **[変更 (Modify)]** をクリックします。
  - f. 新しく割り当てられた `callProfile` オブジェクト ID が、**[オブジェクトの構成]** の下に表示されます。

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

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

Object configuration	
<code>recordingMode</code>	<code>automatic</code>
<code>sipRecorderUri</code>	<code>recording@recorder.com</code>

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

Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption	Tenant
recorder.com	10.209.131.45		<use local contact domain>	Standard SIP	Stop	0	Unencrypted	no
				Standard SIP ▼	Stop ▼	0	Auto ▼	

デフォルトの標準ポート (5060/5061) とは異なる SIP TCP/TLS ポートを使用するように MMP レコーダーを設定した場合、sipRecorderUri フィールドまたは一致する発信ダイヤルプランルールを使用している場合はそのルールに追加します、以下に示すようにリスニングポートを指定しなければなりません。

Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption	Tenant
recorder.com	10.209.131.45:5000		<use local contact domain>	Standard SIP	Stop	0	Unencrypted	no
				Standard SIP ▼	Stop ▼	0	Auto ▼	

発信ダイヤルプランルールを使用している場合は、指定されたポートのサービスが暗号化タイプと一致していることを確認してください。例えば、SIP TLS ポートを使用している場合、暗号化 モードを 暗号化 に設定します。

## 15.5 外部のサードパーティ SIP レコーダーの設定

- SIP レコーダーを指定します – /callProfile オブジェクトの sipRecorderUri API パラメータを使用します。設定されている場合、このURIは録画が有効な場合にダイヤルアウトするために使用されます。設定されていない場合、Meeting Serverのレコーダーコンポーネント (/recorders で設定されている場合) が使用されます。
  - a. Meeting Server のWeb 管理インタフェースを使用して、[設定 (Configuration) ] > [API] の順に選択します。
  - b. API オブジェクトのリストで、/callProfiles の後ろの ▶ をタップします。
  - c. 既存の通話プロファイルの オブジェクト ID をクリックするか、新しいプロファイルを作成する。
  - d. sipRecorderUri パラメータを設定します。
- API オブジェクト /callProfiles または /callProfiles/<call profile id>の recordingMode パラメータを使用して、ミーティングを録画できるかどうかを選択します。このためのオプションは次のとおりです。
  - **自動** – ユーザーの介入なしで録画が行われます。録画ができない場合でもミーティングは行われます。
  - **手動** – ユーザーは DTMF を使用して手動で録画を開始および停止できます。
  - **無効** – どのユーザも録画できません。
- callLegProfiles の RecordingControlAllowed パラメータを設定することで、どのユーザが録画を開始および停止する権限を持つかを制御します。

- /dtmfProfiles に対して startRecording および stopRecording パラメータを使用します。  
/dtmfProfiles/<dtmf profile id> をマッピングするために、録音を開始および停止する DTMF トーンを使用します。

注：追加の API オブジェクトについては、[Cisco Meeting Server API リファレンス ガイド](#)に記載されています。

## 15.6 レコーディングの状況を確認する

録画の状況を確認するには：

- Meeting Server のWeb 管理インターフェースを使用して、[設定 (Configuration) ] > [API] の順に選択します。
- API オブジェクトのリストで、/callLegs の後ろの ▶ をタップします。
- 既存のコールレグのオブジェクト ID をクリックしてください。

callLegs/<call leg id> で GET を実行します。録音 のステータス 出力は、この callLeg が録音されているか (true)、否か (false) を示します。

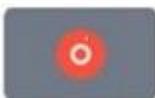
## 15.7 デュアル ホーム会議の録画インジケータ

デュアルホーム電話会議の場合、録画は Lync/Skype エンドポイントで Microsoft 録画メソッドを使用して実行する必要があります。デュアルホーム電話会議の録画に Cisco Meeting Server の使用はお勧めしません。

録画アイコンは、Meeting Server に接続している SIP 参加者に、Lync/Skype エンドポイントが Lync/Skype 側で電話会議を録画していることを示します。

Meeting Server は、ActiveControl 以外のエンドポイント用に作成されたビデオペインに録画アイコンを追加します。表 11 は、デュアルホームド会議が録画されていることを示すために Meeting Server が表示するアイコンを示しています。

表 11：録画インジケータ

表示されるアイコン	説明
	ミーティングは Meeting Server 経由で録画されています。
	ミーティングが Lync/Skype エンドポイントにより録画されています。
	ミーティングが Meeting Server 経由、および Lync/Skype エンドポイント経由で録画されています。
	ミーティングは録画されていません (アイコンは表示されていません)。

---

**注：**ウェブ アプリは独自のアイコンを使用して録画の状態を表示しますが、ローカルとリモートの録画を区別しません。Meeting Serverのアイコンがウェブ アプリのビデオ ペインにオーバーレイ表示されません。

---

## 15.8 Vbrick で録画する

---

**注：**この項は、Meeting Serverの内部レコーダーコンポーネントにのみ適用されます。

---

アップローダコンポーネントは、Meeting Serverに設定された NFS 接続からビデオコンテンツ マネージャ Vbrick にMeeting Server録画をアップロードするためのワークフローを簡素化します。録画を手動でインポートする必要はありません。

アップローダ コンポーネントが構成され、有効になると、録画が NFS から Vbrick にプッシュされ、録画に所有者が割り当てられます。Rev ポータルはビデオコンテンツに管理者が設定したセキュリティを適用し、ユーザーがアクセスできるのは、許可されたコンテンツのみです。所有者の Rev ポータルで録画が利用可能になると、Vbrick から所有者にメールが届きます。録画の所有者は Rev ポータルからビデオ コンテンツにアクセスし、必要に応じて編集して配信できます。

---

**注：**ファイルがスペースディレクトリ内の NFS 共有に追加される場合、ファイルは有効な録画であるかのように Vbrick にアップロードされます。レコーダーだけが書き込みできるように、NFS 共有に権限を適用するように注意してください。

---

---

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

---

---

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

---

### 15.8.1 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ーにインストールすることも、別のサーバーにインストールすることもできます。レコーダーと同じサーバーにインストールされている場合、使用する vCPU をいくつか追加します。別のサーバーで実行する場合、レコーダーと同じサーバ仕様、つまり最小 4 つの物理コアと 4GB の RAM を備えた専用 VM を使用します。

---

**警告：**アップローダは、電話会議を主催する Call Bridge とは別のMeeting Server 上で実行する必要があります。

---

NFS 共有への読み取りおよび書き込みアクセス権。アップローダを実行している Meeting Server には、NFS の読み取りおよび書き込み権限が必要です。アップロードが完了したときにアップローダが mp4 ファイルの名前を再書き込みできるようにするには、書き込み権限が必要です。

**注：**NFS が設定されているか、読み取り専用になっている場合、アップローダコンポーネントは同じビデオ録画を Vbrick にアップロードし続けます。このエラーは、アップローダがファイルにアップロード完了のマークを付けることができないことが原因です。これを回避するには、NFS が読み取り/書き込みアクセスを提供していることを確認してください。

**Vbrick RevへのAPIアクセス** Vbrick Revのユーザーの API アクセスを設定します。

**Call Bridge への API アクセス。** Call Bridge を実行している Meeting Server で、ユーザーの API アクセスを設定する。

**トラストストア** Vbrick Rev サーバからの証明書チェーン、および Call Bridge の Web 管理インターフェイスを実行している Meeting Server を保存する。アップローダは Vbrick Rev と Call Bridge の両方を信頼する必要があります。

**ビデオ録画にアクセスできるユーザーを決定する。** アップロードされたビデオ録画へのアクセスは、[すべてのユーザ]、[プライベート]、[スペースの所有者とメンバーのみ] に設定できます。

**ビデオ録画のデフォルト状態。** アップロード後すぐにビデオ録画を利用可能にするか (アクティブ)、またはビデオ録画の所有者が公開する必要があるか (非アクティブ) を決定します。

表 12 : ポート要件

コンポーネント	接続先	開く接続先ポート
Call Bridge	NFS (バージョン 3)	2049
アップローダー	Call Bridge の Web 管理	443 またはアップローダ設定で指定されたポート
アップローダー	Vbrick Rev サーバ	443 ビデオ アップロードおよび Vbrick Rev サーバへの API アクセス

## 15.8.2 Vbrick で動作するように Meeting Server を設定する

これらの手順は録画を保存するための NFS のセットアップが完了していることを前提としています。

- 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。
- 新しい Vbrick インストールの場合、この手順は無視してください。Vbrick インストールを再設定する場合、まず Meeting Server への Vbrick アクセスを無効にします。  
**アップローダの無効化**
- アップローダが監視する NFS を指定します。  
`uploader nfs <ホスト名/IP> : <ディレクトリ>`

4. アップローダが録画に関連するスペースをホストしているMeeting Server の名前などの録画情報を照会するMeeting Server を指定します  
`uploader cms host <hostname>`
5. Call Bridge を実行しているMeeting Serverのウェブ管理ポートを指定します。ポートが指定されていない場合、デフォルトでポート 443 になります。  
`uploader cms port <port>`
6. Call Bridge を実行しているMeeting Server上で API アクセスを持つユーザーを指定します。パスワードは別に入力します。  
`uploader cms user <username>`
7. ステップ 6 で指定したユーザーのパスワードを設定します。次を入力します。  
`uploader cms password`  
 パスワードの入力が求められます。
8. ルート CA の証明書のコピーを保持する証明書バンドル (crt-バンドル) を作成し、Call Bridgeを実行しているMeeting Server のWeb 管理用のチェーンにあるすべての中間証明書のコピーを保持します。
9. 手順 8 で作成した証明書バンドルをMeeting Server の信頼ストアに追加します。  
`uploader cms trust <crt-bundle>`
10. アップローダが接続するVbrick ホストとポートを設定します。  
`uploader rev host <hostname>`  
`uploader rev port <port>`

---

**注：**特に指定がない限り、ポートのデフォルトは 443 です。

---

11. ビデオ録画をアップロードするための API 権限を持つ Vbrick Rev ユーザーを追加します。  
`uploader rev user <username>`
12. ステップ 11 で指定したユーザーのパスワードを設定します。  
`uploader rev password`  
 パスワードの入力が求められます。
13. ルート CA の証明書と Vbrick Rev サーバーのチェーンにあるすべての中間証明書のコピーを保持する証明書バンドル (crt-バンドル) を作成します。
14. 手順 13 で作成した証明書バンドルを Vbrick Rev の信頼ストアに追加します。  
`uploader rev trust <crt-bundle>`
15. ビデオ録画へのアクセスを設定します。  
`uploader access <Private|Public|AllUsers>`
16. 録画を表示または編集する権限をスペースのメンバーに付与します。  
`uploader cospace_member_access <view|edit|none>`

---

**注：**このステップでは、リスト中のメンバーが Vbrick のアカウントに関連付けられた有効なメールアドレスを持っている必要があります。For example `user1@example.com`

---

17. 会議スペースの所有者がビデオ記録の単独の所有者であるかどうかを決定します。  
`uploader recording_owned_by_cospace_owner <true|false>`

---

**注：**また、このステップでは、ビデオ録画の所有者が Vbrick のアカウントに関連付けられた有効なメールアドレスを持っている必要があります。

---

18. 会議スペースの所有者が Vbrick リビジョンにリストされていない場合、代替所有者のユーザ名を設定します。フォールバック所有者が指定されていない場合、MMP で設定されたユーザーがデフォルトで所有者になります。  
アップローダーフォールバック所有者<vbrick-user>
19. ビデオ録画へのコメントを有効にします。  
uploader comments enable
20. 録画のレーティングを有効にします。  
uploader ratings enable
21. ビデオ録画のダウンロード権限を設定します。  
uploader downloads enable
22. Vbrick Rev に最初にアップロードされたビデオ録画のデフォルト状態を設定します。  
uploader initial\_state <active|inactive>
23. アップロード完了後に NFS から録画を削除するかどうかを決定する  
uploader delete\_after\_upload <true|false>
24. アップローダが Meeting Server にアクセスできるようにする  
アップローダの有効化

---

**注：**messageBoardEnabled を true に設定します。これにより、録画が利用可能であることを示すメッセージがスペースに表示されるようにします。

---

## 15.9 ミーティングのストリーミング

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

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

---

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

---



---

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

---



---

**注：**ストリーミングの接続先 RTMP URL がファイアウォールの外側にある場合は、ファイアウォールのポートを開く必要があります。

---

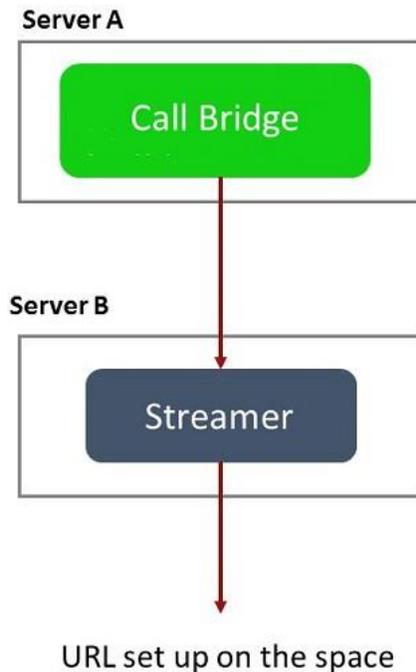
バージョン 3.1 では、内部 SIP ストリーマアプリケーションの RTMP サポートを RTMPS に拡張します。本質的には TLS 接続上の RTMP です。これまでは、ストリーマと RTMP サーバ間

のすべてのトラフィックは暗号化されていませんでした。3.1 RTMPS のサポートにより、このトラフィックを暗号化することができます。

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

次の図は、許可されているストリーマ導入を示しています。スケーラブルで復元力のある展開についての詳細は、[セクション 15.3.3](#) を参照してください。

図 44 : ストリーミングで許可されている展開 : リモートモード



テスト目的でのみ、ストリーマを Call Bridge と同じサーバ上に共存させることができます。これは 1 から 2 の同時ストリーミングをサポートします。

## 15.10 VM サーバーに新しい SIP ストリーマ コンポーネントを展開する

これは 2 段階のプロセスです。

- [MMP 経由で Meeting Server のストリーマを設定する](#)
- [API 経由でストリーマ URI を設定する](#)

### タスク 1 : MMP 経由で Meeting Server のストリーマを設定する

1. バージョン 3.0 にアップグレードします。
2. MMP に SSH で接続し、ログインしてレコーダーを設定します (MMP コマンド、`streamer help` で、使用可能なすべてのコマンドのリストを表示します)。

3. MMP コマンド `streamer sip listen <interface> <tcp-port|none>` を使用して、ストリーマをリッスンするインターフェイスと、リッスンする SIP TCP および TLS ポートを設定します。<tls-port|none>。サービスを無効にするには、それぞれのポートを `なし` に設定します：
  - a. たとえば、TCP ポートではなく、TLS ポートでのみリッスンする場合、次を入力します。 `streamer sip listen a none 6000`
  - b. 設定したポートが既定の TCP/TLS ポート (5060/5061) ではない場合、後で必要になるため、メモしておいてください
4. 必要に応じて、MMP コマンドを使用して、ストリーマが使用する(または通話の音声のみをストリーミングさせたい)最大解像度を設定することができます。 `streamer sip resolution <audio|720p|1080p>` です。指定しない場合、720pがデフォルトになります。
  - a. たとえば、1080p に設定する場合は、 `streamer sip 解像度 1080p` と入力します。

---

**注意：** 1080p を使用する場合は、送信 SIP 通話帯域幅を 3,500,000 ビット/秒に増やしてビデオ品質を最適化することをお勧めします。これを行うには、Web 管理 UI で [Configuration] に移動します。 [Call settings] > 帯域幅の設定 (SIP) および必要に応じて設定します。

---

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

---

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

---

6. TLS が設定されている場合、オプションとして、以下のようにストリーマの SIP (または LDAP または RTMPS) の TLS 検証を実行できます。
  - a. MMP コマンド `tls sip trust [<cert-バンドル>]` を入力します
  - b. MMP コマンド `tls sip verify enable` を入力します

---

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

---

7. 構成が正しいことを確認してください。構成を表示するには、MMP コマンド `streamer` を入力します。
8. MMP コマンド `ストリーマ エネーブル` を入力してストリーマサービスを有効にします。

## タスク 2：API 経由でストリーマ URI を設定する

新しい SIP ストリーマーが有効になると、コールブリッジで設定して使用できるようになります。 `sipStreamerUri` API 呼び出しプロファイル オブジェクトで指定された API パラメータ。

希望する場合は、out バウンドダイヤルプランルールにマッピングするカスタム URI を構成することもできます (ドメインは自由に選択できます。例、「streaming.com」)。sipStreamerUri で使用されるドメインをストリーマにルーティングする方法を Meeting Server に指示する、outboundDialPlan ルールを設定する必要があります。これにより、優先順位の値、暗号化などを制御することができます。/outboundDialPlanRules の設定の詳細については、[導入ガイド](#)の「ダイヤル プランの設定 - 概要」の章を参照してください。

---

**注：**設定された URI のユーザ部分 ('@' 記号の前の部分) には特別な意味がありません。新しい内部 SIP ストリーマコンポーネントでは必須ですが、通常は何でもかまいません例："streaming@streamer.com"。URI の重要な部分はドメイン部分です。

---

Meeting Server のウェブ管理インターフェースを使用して sipStreamerUri パラメータを設定するには：

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

---

**注：**新しい SIP ストリーマを使用する場合、1 つの SIP URI のみを使用する必要があります。例：streaming@streamer.com、異なるプロファイルで異なる SIP URI を持つ必要はありません。

---

4. まだ設定していない場合は、streamingMode パラメータを manual または自動 (ミーティングをどのようにストリーム配信するかによります)
5. [**変更 (Modify)**] をクリックします。

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

1. Web 管理インターフェースを使用して、[**設定 (Configuration)**] > [API] の順に選択します。
  - a. API オブジェクトのリストで、/api/v1/system/profiles 後の ▶ をタップします。
  - b. [**表示または編集**] をクリックします。
  - c. パラメータを callProfile まで下にスクロールし、[Choose] をクリックします。
  - d. 表示された「callProfile オブジェクト選択ウィンドウ」から、**オブジェクト ID** を選択し、**最上位のグローバルプロファイル**に割り当てられる callProfile を選択します。
  - e. [**変更 (Modify)**] をクリックします。
  - f. 新しく割り当てられた callProfile オブジェクト ID が、[**オブジェクトの構成**] の下に表示されます。

ストリーミングを有効にする API の各 coSpace について、`streamUrl` coSpace API フィールドに、ストリーミング先の RTMPS ストリーム URL を設定する必要があります (例: "rtmps://mystream.com/live/app"). これを構成するには :

1. Meeting Serverのウェブ管理インタフェースにログインして **設定 (Configuration)** >API を選択します。
2. API オブジェクトのリストで、`/api/v1/coSpaces` の後ろの ▶ をタップします。
3. 既存の共有スペースを設定または変更するには、必要な共有スペースのオブジェクト ID を選択します `streamUrl` フィールドにストリーミング先の RTMPS ストリーム URL を入力します。
4. [**変更 (Modify)**] をクリックします。

### 15.10.1 既知の制限事項

---

**警告 :** ストリーム URL は SIP ヘッダーで送信されるため、ログイン資格情報を含むすべての RTMP ストリーム URL は、ログを記録する可能性のあるコールコントロールプロバイダに露出される可能性があることに注意してください。

---

## 16 LDAP 設定

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

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

---

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

---

**注：** バージョン 2.1 から、Meeting Server は Oracle Internet Directory (LDAP バージョン 3) をサポートします。これは、Web 管理インターフェースではなく、API を通じて構成する必要があります。Oracle Internet Directory をサポートするように Meeting Server を構成するには、LDAP 同期中の検索操作で Meeting Server が LDAP ページ結果コントロールを使用しないようにする必要があります。`/ldapServers` に POST するか、`/ldapServers/<ldap server id>` に PUT し、リクエストパラメータ `usePagedResults` を `false` に設定します。

---

### 16.1 LDAP を使用する理由は何ですか？

LDAP を使用して Meeting Server を構成することは、環境を設定するための強力なスケラブルな方法です。LDAP 構造内で組織の通話要件を定義すると、Meeting Server で必要な構成の量が最小限に抑えられます。

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

- 人事部門の全員
- グレード 11 以上の職員
- 職名 = 'ディレクター'
- 姓が「B」で始まる人

### 16.2 Meeting Server の設定

この項の例では、Meeting Server の Web 管理インターフェースを使用して、単一の LDAP サーバー (この場合は Active Directory) を設定する方法について説明します。しかし、Meeting

Serverは API 経由で設定できる複数の LDAP サーバーをサポートしています。詳細は、『[API リファレンスガイド](#)』の LDAP メソッドのセクションを参照してください。

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

---

**注：**ウェブ管理インターフェイスでは、1 つの LDAP サーバーのみ設定できます。

---

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

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

例：

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

---

**注：**ユーザ名とパスワードの証明書に必要な権限の詳細は、[セクション 16.4](#) を参照してください。

---

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

---

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

---

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

- ベース識別名 = ユーザーをインポートする LDAP ツリー内のノード。以下は、ユーザーをインポートするベース DN の賢明な選択です  
`cn=Users,dc=sales,dc=YourCompany,dc=com`
- フィルター = ユーザーの LDAP レコードの属性値を満たす必要があるフィルター式。フィルター フィールドの構文は rfc4515 で説明されています。

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

```
mail=*
```

テスト目的で、指定ユーザ (例 fred.bloggs) と、メールアドレスが「test」で始まるテストユーザ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*))
```

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

```
(!(mail=fred.bloggs*))
```

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

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

これにより、APAC グループのメンバーであるグループとユーザーの両方がインポートされます。

ユーザーに制限 (およびグループを除外) するには、次を使用します：

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

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

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

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

!で定義されたものを除くフィルターが含まれます。

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

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

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

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

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

このフィルタは、(|( ツリー内の指定されたユーザーのみをインポートします

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

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

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

#### 4. フィールド マッピング式のセットアップ

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

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

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

\$<LDAP フィールド名>\$

一例として、表現

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

生成する：

```
fred@example.com
```

詳細については、次を参照してください。「LDAP フィールドのマッピングの詳細」(178 ページ)。

---

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

---

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

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

- Active Directory と同期するには、[今すぐ同期] を選択するか、適切な API 呼び出しを使用して同期を有効にします（「[Cisco Meeting Server API リファレンスガイド](#)」を参照）。

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

- 同期の結果を確認するには、[ステータス > ユーザ] に移動します。

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

## 16.3 例

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

- LDAP 構造に「スペース」と呼ばれるグループを作成し、そのグループに必要なメンバーを割り当てます。
- 拡張可能なマッチングルール (LDAP\_MATCHING\_RULE\_IN\_CHAIN / 1.2.840.113556.1.4.1941) を使用する次のフィルターを使用して、「スペース」グループのメンバーであるすべてのユーザーを検索します。

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

3. 次に、次のディレクトリで特定のユーザーを同期します。

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

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

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

次に示すスペースは、**設定 > スペース** ページを参照してください。

名前	URI ユーザ部分
fred.blogs	fred.blogs.space

## 16.4 LDAP フィールド マッピングの詳細

この項では、Meeting Server用にセットアップする LDAP フィールドマッピングについての追加情報を提供します。

LDAP フィールド値の一部は、以下のように、sed に似た構文で置換できます。

```
$<LDAP フィールド名>|'|<regex>/<置換形式>/<オプション>|'$
```

引数の説明

<option> を g に指定すると、<regex> で <replacement format>、または空白にする場合は最初のみ一致

の一部 <regex> を使用するためにタグをつけることができます。<replacement format> には、それらを丸括弧でくくります

タグ付けされたマッチは、<replacement format> で \x として参照でき、xは0から9までの数字です。マッチ0は全体マッチに対応し、マッチ1-9は1番目から9番目のタグ付けされた部分表現に対応します

置換式の中の一重引用符は、バックスラッシュ文字自体と同様に、バックスラッシュでエスケープする必要があります

一重引用符、バックスラッシュ、または 0-9 の数字以外の任意の文字は、置換式のコンポーネントを区切るスラッシュの代わりに使用できます

式の中で区切り文字をリテラルとして使用する場合は、バックスラッシュでエスケープする必要があります

一例として、以下はアドレスの形式を変換します：

```
firstname.lastname@test.example.com
```

以下の形式に変換します：

```
firstname.lastname@example.com JIDたち
```

```
$mail|'|/@test/@xmpp/'$
```

次の例では、ユーザーのフルネームからすべての小文字の「a」を削除することができます。

```
$cn|'/a//g'$
```

使用に理にかなった式のセットは次のとおりです。

```
氏名：                $cn$
JID：                $mail|'/@test/'$
space URI：          $mail|'/@.*//'$ .space
space dial-in number： $ipPhone$
```

---

**注：**LDAP サーバ資格情報は次のフィールドの読み取りに使用されます (セキュリティ上の理由から、これらの資格情報を使用して利用できるフィールドや権限を制限することもできます)：

- メール
  - objectGUID
  - entryUUID
  - nsuniqueid
  - telephoneNumber
  - モバイル
  - sn
  - givenName
- 

## 16.5 すべてのユーザスペースへの非メンバーアクセスにパスワード保護を適用する

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

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

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

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

---

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

---

## 17 Cisco Meeting Server web app のシングルサインオン (SSO)

この機能により、ウェブ アプリ ユーザーは SSO プロバイダーを使用してログインし、ID を確認できます。

SSO は、ウェブアプリのユーザーが、ログインするたびにパスワードを入力する必要がないことを意味します。これは、例えば、OAuth、Gmailなどのアイデンティティプロバイダーとの単一のセッションを持つことができるためです。

これにより、ウェブ アプリ ユーザーは異なる SSO プロバイダを使用して同じWeb Bridgeにログインできます。

この SSO メカニズムでは、オープン標準で業界標準プロトコルとして広く使用されている SAML (Security Assertion Markup Language) 2.0 を使用しています。

---

**注：**現在、Meeting Serverは SAML 2.0 プロトコルでの HTTP-POST バインディングのみをサポートしています。これは、HTTP-POST AssertionConsumerService でのみメッセージを受け入れ、HTTP-POST バインディングが利用できない ID プロバイダを拒否することを意味します。

---



---

**注：**SSO ログインを有効にすると、LDAP ログインは使用できなくなります。

---

### 17.1 Meeting Server web app で使用する SSO を設定する

SSO を使用するには、ID プロバイダとMeeting Server (SAML 2.0 交換でサービスプロバイダと見なされる) で、以下に示すいくつかの設定が必要です。

#### タスク 1 : ID プロバイダとMeeting Serverユーザー間のマッピング

Meeting Serverが ID プロバイダのユーザーを適切なユーザーにマッピングできるように、SSO 経由で認証されるすべてのユーザーに対し、authenticationId をセットアップする必要があります。これは、標準 LDAP 同期プロセスの一部として実行できます。このフィールドのコンテンツは、成功の応答でアイデンティティ プロバイダから渡されたカスタム パラメータに対して検証されます (タスク 2 を参照)。

各ユーザーに一意的識別子を選択することをお勧めします (例 : \$sAMAccountName\$)。authenticationId の空の値は受け入れられません。

ldapSync の一部として authenticationId をセットアップするには、新しい ldapSync を作成するか、既存のものを変更します。

次に、ldapマッピングを作成/変更し、authenticationIdマッピング パラメータに適切な値を入力する必要があります (例、\$sAMAccountName\$)。

Meeting Server のWeb 管理インターフェースを使用する：

- Meeting Serverのウェブ管理インターフェースにログインして **設定 (Configuration)** >API を選択します。
- API オブジェクトのリストで、/api/v1/ldapMappings の後ろの ▶ をタップします。
- [**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。

The screenshot shows the Cisco Meeting Server web management interface. At the top, there is a navigation bar with 'Status', 'Configuration', and 'Logs' tabs, and a user dropdown menu showing 'User: testadmin'. Below the navigation bar, there is a link to 'return to object list'. The main content area is titled '/api/v1/ldapMappings' and contains a form with several input fields, each with a checkbox to its left. The fields are: 'jidMapping', 'nameMapping', 'cdrTagMapping', 'coSpaceUriMapping', 'coSpaceSecondaryUriMapping', 'coSpaceNameMapping', 'coSpaceCallIdMapping', and 'authenticationIdMapping'. A 'Create' button is located at the bottom right of the form.

- authenticationIdMapping パラメータに適切な値を入力します (例：\$sAMAccountName\$) を選択し、必要に応じて [**作成 (Create)**] または [**変更 (Modify)**] をクリックします。
- Meeting Serverで変更を有効にするには、ldapSync をトリガーする必要があります。API オブジェクトのリストから、▶ /api/v1/ldapSyncs の後] をクリックしてオブジェクト ID を選択するか、**新規作成** を選択します。ldapSync が完了したら、Meeting Serverユーザーの 1 人を調べることで、プロセスが成功したことを確認できます。
- まず、API オブジェクトのリストから、▶ /api/v1/users の後でタップして、次の例のようにユーザーのリストを表示します。

The screenshot shows the Cisco Meeting Server web management interface displaying a list of users. The breadcrumb navigation shows: /api/v1/userProfiles ▶ /api/v1/userProfiles/<id> /api/v1/users ◀. Below the breadcrumb, there are navigation links: < start < prev 1 - 20 (of 24) next >. There is also a search filter box and buttons for 'Table view' and 'XML view'. The main content is a table with two columns: 'object id' and 'userId'.

object id	userId
<a href="#">a474c231-bc85-48cf-99c7-30357800a9bc</a>	baylee.moss@example.com
<a href="#">f2406d37-862d-4ca1-9ad4-5f5799128810</a>	byron.bell@example.com
<a href="#">8ede7b2f-3472-4f08-8114-60ad834586df</a>	davis.walker@example.com
<a href="#">dfe720d2-b2b3-4d27-b0d9-97556bb051bc</a>	diamond.conley@example.com
<a href="#">bffc08e-0e23-4c2e-869b-f48059e62785</a>	edith.lamb@example.com
<a href="#">e4a417d0-55f3-4cc3-839d-6a8f7ec482e6</a>	esmeralda.coughlin@example.com
<a href="#">76b732d1-b012-49d2-b2bc-4b3902b52ddc</a>	frank.crowley@example.com
<a href="#">e3f6cbf3-2089-4705-8b7f-1670c67baf64</a>	gia.mahoney@example.com
<a href="#">5b29f430-ab0b-457a-a322-573967dc47a5</a>	janessa.cardenas@example.com
<a href="#">71e3e16a-1adc-47e1-9f71-e1f1e99ae6ff</a>	keagan.christie@example.com
<a href="#">48a6640b-e913-464f-ac13-b60324613417</a>	london.cowan@example.com
<a href="#">55bf73f6-7d40-4666-bb8a-3b32a80b4c95</a>	marely.fitzgerald@example.com
<a href="#">9e6cca5a-2dd1-46dd-979a-16ce2b43e1f8</a>	melissa.gleason@example.com
<a href="#">061b08ff-f6d1-447d-0e61-b0-473942465b</a>	melly.meredith@example.com

- g. authenticationId をセットアップするユーザーの 1 人を選択します (場合によっては [フィルター] フィールドを使用します)。ユーザエントリには、次の例に示すように、ldapSync からの正しい値を持つ authenticationId フィールドが含まれます。

/api/v1/users/a474c231-bc85-48cf-99c7-30357800a9bc

Related objects: </api/v1/users>

</api/v1/users/a474c231-bc85-48cf-99c7-30357800a9bc/usercoSpaces>

</api/v1/users/a474c231-bc85-48cf-99c7-30357800a9bc/userCoSpaceTemplates>

</api/v1/users/a474c231-bc85-48cf-99c7-30357800a9bc/userProvisionedCoSpaces>

Table view XML view

Object configuration	
userJid	baylee.moss@example.com
name	Baylee Moss
email	baylee.moss@autotest.com
authenticationId	baylee.moss

## タスク 2 : ID プロバイダの構成

- すべての ID プロバイダで、登録されているサービスプロバイダ (このインスタンスの場合は Meeting Server) を表すメタデータ xml ファイルをアップロードできます。一部の ID プロバイダーでは、最も重要な情報を設定できるため、プロセスが簡素化されます。メタデータ xml ファイルの例は [ここで確認できます](#)。

ID プロバイダにアップロードされるメタデータ xml ファイルに含まれる値 :

- entityID – Web Bridge 3 アドレスです (例、https://<domain>:port)。このアドレスは、ウェブ アプリ ユーザーのブラウザから到達可能な有効な Web Bridge 3 アドレスである必要があります。

**注 :** 展開に複数の Web Bridge 3 がある場合、これは負荷分散されたアドレスである必要があります。

- 「https://<domain>:<port>/api/auth/sso/idpResponse」形式に従い、entityId として定義された Web Bridge アドレスの HTTP-POST AssertionConsumerService。
- これはオプションです。ID プロバイダが AuthnRequest 署名を確認するために使用する署名用の公開鍵。
- これはオプションです。ID プロバイダが上記で提供されたアドレス経由でルーティング可能ないずれかの Web Bridge に送り返される情報を暗号化の際に使用する公開鍵です。

**注 :** Meeting Server に送信するメッセージは、ID プロバイダによりレスポンスおよび/またはアサーションレベルで署名されている必要があります。署名されていない通信は破棄されます。

- 成功の応答で ID プロバイダから渡されたカスタム パラメータを設定する必要があります。各ユーザーのコンテンツは、その Meeting Server ユーザーの authenticationId として設定済みの値と一致する必要があります (例、\$sAMAccountName\$)。通常、ID プロバイダは、サービスプロバイダエントリを作成する一環として、専用のフォームまたはダイアログを持ちます。このパラメータには任意の名前を付けることができますが、「uid」など、覚えやすい名前を付けることをおすすめします ([タスク 3](#) で名前が必要になります)。

### タスク 3 : SSO アーカイブ zip ファイルを作成する

- Meeting Server を設定するには、sso\_ という名前のアーカイブ zip ファイルを作成する必要があります。<name>.zip を、その Meeting Server 上の Web Bridge 3 に設定する各 SSO 用に作成します。「sso\_」で始まり、その後自分で選んだ意味のある名前を付ける必要があります。

これらのファイルを含む zip アーカイブファイルを作成します。

- idp\_config.xml – 管理者が ID プロバイダから受け取るファイルです。
- config.json – 含む :
  - supportedDomains (文字列の配列) – この ID プロバイダに対して認証される Meeting Server ユーザーのすべてのドメインのリストです。つまり、[タスク 1](#) の例を使うと、supportedDomains には "example.com" という単一のエントリが含まれることになります。
  - authenticationIdMapping (文字列) – Meeting Server の authenticationIds に一致する、[タスク 2](#) の一部として設定された ID プロバイダの応答のパラメータ (例、「uid」) の名前。SSO のウェブアプリユーザーは、authenticationIds をセットアップする必要があります ([タスク 1](#) を参照してください。)
  - ssoServiceProviderAddress (文字列) – アイデンティティ プロバイダが応答を送信するアドレスです。これは [タスク 2](#) の entityID で指定された Web Bridge 3 と一致します。
- 任意です。sso\_sign.key – ID プロバイダ側で設定された公開署名用の秘密鍵です。これは、Meeting Server からの発信 AuthnRequest に署名するために使用され、アイデンティティプロバイダ側で公開鍵を使用して確認されます。
- 任意です。sso\_encrypt.key – ID プロバイダ側で設定された公開暗号化キーの秘密鍵です。これは、アイデンティティプロバイダ側で公開鍵で暗号化されたメッセージを Meeting Server 上で復号化するために使用されます。

---

**注意 :** ID プロバイダごとに異なる名前付き zip ファイルが必要です。

---

- SSO ファイルを含むアーカイブ (zip) ファイルを作成します。

---

**注 :** ファイルを圧縮する場合、SSO ファイルを含むフォルダは圧縮しないでください。これが行われると、フォルダの追加レイヤーが作成されます (zip 形式のファイル > フォルダ > SSO ファイル)。代わりに、SSO ファイルをハイライトし、それらを右クリックして圧縮してください (または、zip アプリケーションを開き、ファイルをまとめて圧縮します)。これにより、追加のフォルダ レイヤーを作成することなく、SSO ファイルを含む zip ファイルが作成されます (例 : zip ファイル > SSO ファイル)。

---

#### タスク 4 : SSO アーカイブ zip をアップロードする

SSO アーカイブの zip はアップロードされ、ローカルの Web Bridge 3 でホストされる必要があります。

---

**注 :** 次の手順で使用するコマンドは、コンソール/ターミナル環境 (コマンドプロンプトまたはターミナル) を対象としたものであり、WinSCP などの SFTP クライアントを対象としたものではありません。

---

1. この zip アーカイブをローカルでホストする、有効になっている Web Bridge 3 を持つ各 Meeting Server について、
2.
  - a. SFTP クライアントを MMP の IP アドレスに接続します。
  - b. MMP 管理者ユーザーの資格情報を使用してログインします。
  - c. zip ファイル `sso_<name>.zip` をアップロードしてください。次に例を示します。  
`PUT sso_<name>.zip`
  - d. SSH クライアントを MMP の IP アドレスに接続します。
  - e. MMP 管理者ユーザーの資格情報を使用してログインします。
  - f. Web Bridge 3 を再起動します。

##### WebBridge3 再起動

3. 新しい SSO アーカイブファイルは再起動後に反映されます。

---

**注 :** ウェブアプリユーザーがログインすると、ウェブアプリアプリケーションで、ID プロバイダとのセッションとは別のセッションを持つこととなります。これは、同じユーザー名を入力した後に ID プロバイダではなく、Web アプリケーションからログアウトやサインアウトしても、Web アプリケーションに自動的に再許可されることを意味します。ただし、ID プロバイダからサインアウトする場合は、ウェブ アプリ アプリケーションからはサインアウトしないため、ウェブ アプリ アプリケーションからもサインアウトする必要があります。このブラウザセッションで再度ログインできないようにするには、web app application と ID プロバイダーの両方からサインアウトする必要があります。

---

#### 17.1.1 例 1 config.json ファイル

これは config.JSON ファイルの例です。

```
{
  "authenticationIdMapping" : "<parameter_from_task_2>",
  "ssoServiceProviderAddress" : "https://<domain>:<port>",
  "supportedDomains" : ["<domain1>","<domain2>"]
}
```

### 17.1.2 例 2 単純なサービスプロバイダメタデータファイル

これは、サービスプロバイダの簡単なメタデータファイルの例です。管理者は、<domain>および<port>をそれぞれの適切な値に変更する必要があります。

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="https://<domain>:<port>" entityID="https://<domain>:<port>">
  <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</md:NameIDFormat>
    <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://<domain>:<port>/api/auth/sso/idpResponse" index="0"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

### 17.1.3 例 3 詳細なサービスプロバイダメタデータファイル

これは、署名および暗号化キーの xml を含む包括的なメタデータ ファイルの例です。

---

**注：**鍵は、使用パラメータ（「暗号化」または「署名」）に従って、対応する KeyDescriptor 要素の X509Certificate サブ要素に配置する必要があります。「...」をキーのテキストコンテンツに置換する必要があります（例：ds:X509CertificateMIID\*\*<omitted\_key\_text>\*\*+gb</ds:X509Certificate>）

---

**注：**署名証明書を含める場合、AuthnRequestsSigned の値は「true」に設定されます（例 2 の簡単なメタデータファイルでは「false」に設定されています）。

---

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="https://<domain>:<port>" entityID="https://<domain>:<port>">
  <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>...</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>...</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</md:NameIDFormat>
```

```
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://<domain>:<port>/api/auth/sso/idpResponse" index="0"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

## 18 ActiveControl のサポート

Meeting Serverは、主催された通話に対して ActiveControl をサポートしています。CE 8.3+ ソフトウェアがインストールされた Cisco SX、MX または DX エンドポイントを使用する参加者の場合、ActiveControl によりミーティングの詳細を受け取り、ミーティング中にエンドポイント インターフェイスを使用していくつかの管理タスクを実行することができます。

### 18.1 Meeting Server の ActiveControl

Meeting Server は、ActiveControl が有効なエンドポイントへの次のミーティング情報の送信をサポートしています。

- 参加者リスト (参加者リストとも呼ばれます) : 通話の参加者の名前と参加者の合計数を確認することができます、
- 発言中の参加者の音声アクティビティのインジケータ、
- 現在プレゼンテーションを行っている参加者を示すインジケータ、
- ミーティングが録画されているか、ストリーミングされているか、および通話中にセキュアではないエンドポイントが含まれているかどうかを示すインジケータ、
- すべての参加者に表示されるオンスクリーンメッセージ、

また、ActiveControl が有効なエンドポイントでこれらの管理タスクをサポートしています。

- エンドポイントに使用するレイアウトを選択し、
- ミーティングの他の参加者を切断します。

### 18.2 制約事項

- ActiveControl が有効な通話が、9.1 (2) より古い Unified CM バージョンの Unified CM トランクを通過する場合、通話は失敗する場合があります。ActiveControl は、古い Unified CM トランク (Unified CM 8.x 以前) では有効にしないでください。
- ActiveControl は SIP のみの機能です。H.323 インターワーキングシナリオはサポートされていません。

### 18.3 ActiveControl と iX プロトコルの概要

ActiveControl は、SIP セッション記述プロトコル (SDP) のアプリケーション回線として通知される iX プロトコルを使用します。Meeting Server 自動的に ActiveControl をサポートしますが、この機能は無効にできます。セクション第 18.4 項を参照してください。遠端ネットワークが不明であるか、iX プロトコルをサポートしないデバイスがあることがわかっている状況では、Meeting Server と他のコール制御またはビデオ会議デバイス間の SIP トランクで iX を無効にするのが最も安全です。例：

- Unified CM 8.x 以前のシステムへの接続では、古い Unified CM システムは ActiveControl 対応デバイスからの発信を拒否します。これらの通話の失敗を回避するには、ネットワーク内の Unified CM 8.x デバイスに向かうトランクで iX を無効のままにしておきます。SIP プロキシ経由で 8.x デバイスに到達する場合、iX がプロキシへのトランクで無効になっていることを確認します。
- サードパーティネットワークへの接続用。このような場合、サードパーティのネットワークが ActiveControl 対応デバイスからの呼び出しをどのように処理するかはわからず、処理システムによっては拒否される場合があります。このような通話の失敗を避けるには、サードパーティネットワークへのすべてのトランクで iX を無効のままにします。
- 外部ネットワークに接続する、または内部で古い Unified CM バージョンに接続する、Cisco VCS 中心の導入用。Cisco VCS X8.1 から、ゾーン フィルターをオンにして、外部ネットワークまたは古い Unified CM システムに送信される INVITE 要求の iX を無効にすることができます。(既定では、このフィルターはオフになっています。)

## 18.4 SIP 通話内の UDT を無効にする

ActiveControl は、エンドポイントへの参加者リストの送信、通話中の他の参加者の切断、導入間の参加者リストなど、特定の機能に UDT トランスポートプロトコルを使用します。UDT はデフォルトで有効になっています。診断の目的で UDT を無効にすることができます。例えば、コールコントロールが UDT を使用しない場合で、これがコールコントロールが Meeting Server からのコールを受けない原因であると考えられる場合です。

Meeting Server の Web 管理インターフェイスを使用して、**[設定 (Configuration)]** > **[API]** の順に選択します。

1. API オブジェクトのリストで、/compatibilityProfiles の後の ▶ をタップします。
2. 既存の互換性プロファイルの object id をクリックするか、または新しい互換性プロファイルを作成します。
3. パラメータ sipUDT = false を設定します。**[変更 (Modify)]** をクリックします。
4. API オブジェクトのリストで、/system/profiles の後の ▶ をタップします。
5. **[表示または編集]** ボタンをクリックします。
6. **[選択 (Choose)]** をクリックし、パラメータ compatibilityProfile の右側を選択します。上記のステップ 3 で作成した互換性プロファイルの **オブジェクト ID** を選択します。
7. **[変更 (Modify)]** をクリックします。

## 18.5 Cisco Unified Communications Manager で iX サポートを有効にする

iX プロトコルのサポートは、Cisco Unified Communications Manager で一部の SIP プロファイルに対してデフォルトで無効になっています。Unified CM で iX サポートを有効にするには、まず SIP プロファイルのサポートを設定し、それから SIP プロファイルを SIP トランクに適用します。

### SIP プロファイルでの iX サポートの設定

1. [デバイス (Device) ] > [デバイス設定 (Device Settings) ] > [SIP プロファイル (SIP Profile) ] を選択します。[SIP プロファイルの検索と一覧表示] ウィンドウが表示されます。
2. 次のいずれかを実行します。
  - a. 新しい SIP プロファイルを追加するには、**新規追加** をクリックします。
  - b. 既存の SIP プロファイルを変更するには、検索条件を入力して [検索 (Find) ] をクリックします。更新する SIP プロファイルの名前をクリックします。

[SIP プロファイル設定] ウィンドウが表示されます。
3. [iX アプリケーションメディアを許可 (Allow iX Application Media) ] のチェックボックスを選択します。
4. 追加の設定変更を加えます。
5. [保存] をクリックします。

### SIP トランクへの SIP プロファイルの適用

1. [デバイス (Device) ] > [トランク (Trunk) ] を選択します。  
[トランクの検索と一覧表示] ウィンドウが表示されます。
2. 次のいずれかを実行します。
  - a. 新しいトランクを追加するには、[**新規追加**] をクリックします。
  - b. トランクを変更するには、検索条件を入力して、[**検索**] をクリックします。更新するトランクの名前をクリックします。

[トランク設定] ウィンドウが表示されます。
3. [SIP プロファイル] ドロップダウンリストから、適切な SIP プロファイルを選択します。
4. [保存] をクリックします。
5. 既存のトランクを更新するには、[**設定の適用 (Apply Config)** ] をクリックして新しい設定を適用します。

## 18.6 Cisco VCS で iX をフィルタリングする

プロトコルをサポートしない近隣ゾーンの iX アプリケーション回線をフィルタリングするように Cisco VCS を設定するには、SIP UDP/iX フィルターモードの詳細設定オプションがオンに設定されているカスタムゾーンプロファイルでゾーンを設定する必要があります。

アドバンスドゾーンプロファイルのオプション設定を更新するには：

1. 新しい近隣ゾーンを作成するか、既存のゾーンを選択します (**設定 > ゾーン > ゾーン**)。

2. [ゾーンプロファイル (Zone profile) ]の詳細設定のパラメータ項で、まだ選択されていない場合は、[カスタム (Custom) ]を選択します。ゾーンプロファイルの詳細設定オプションが表示されます。
3. SIP UDP/IX フィルタモード ドロップダウンリストから オンを選択します。
4. [保存] をクリックします。

## 18.7 iX のトラブルシューティング

表 13 : iX ヘッダーを含む通話の通話処理の概要

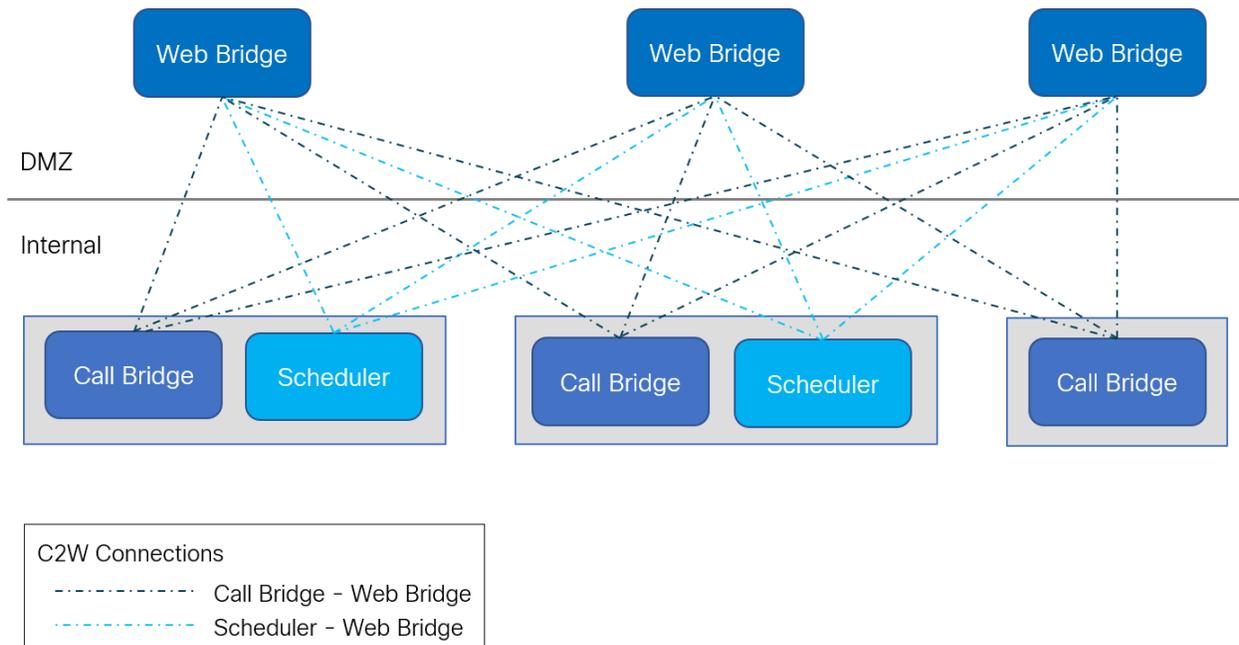
シナリオ	結果
Unified CM 8.x またはそれ以前	通話が失敗する
Unified CM 9.x 9.1(2) 以前	通話は正常に処理されるが、ActiveControl はなし
Unified CM 9.1(2)	通話は正常に処理され、ActiveControl もある
エンドポイント - iX および SDP 実装のサポートなし	エンドポイントが再起動する可能性があるか、通話が失敗する可能性がある

## 19 スケジューラ - 導入

スケジューラは、Meeting Server MMP を使用して、新しいコンポーネントとして導入されます。スケジューラが有効になると、スケジューラはループバック インターフェイスを介して Call Bridge に API 要求を行います。そのため、スケジューラは、Call Bridge もホストしている Meeting Server に導入する必要があります。スケジューラがリモート Call Bridge を使用するよう設定することはできません。

設定済みの Web Bridge のリストは、Call Bridge API を使用してスケジューラによって取得されます。持続的な C2W 接続は、Call Bridge が各 Web Bridge への C2W 接続を確立する方法と同様に、各 Web Bridge へ確立されます。これはループバック インターフェイス経由で自動的に行われるため、スケジューラと Call Bridge 間の接続を有効にするために、明示的な設定は必要ありません。同様に、C2W 接続はすべて自動ですが、スケジューラと Web Bridge の間で [信頼バンドル](#) を構成する必要があります。

**注意：**スケジューラは、クラスタ内のすべてのウェブブリッジへの C2W 接続を確立できる必要があります。大規模なデータベースを含む Call Bridge の導入では、サーバーを再起動する前にスケジューラを無効にし、データベースの同期が完了した後にのみ再度有効にします。これには最大 30 分かかります。



すべての Call Bridge と一緒にスケジューラを導入する必要はありません。Meeting Server 1000 と VM 導入上の Meeting Server のスケジューラは、合わせて 150,000 のミーティングをサポートし、Meeting Server 2000 のスケジューラは 200,000 のミーティングをサポートします。2 つまたは 3 つのスケジューラを追加して、レジリエンスを提供できます。スケジュー

ル済みミーティングのデータはMeeting Server のデータベースに保存され、クラスター化およびシングルボックスデータベース導入の両方がサポートされています。

Call Bridge は、スケジューラからの API リクエストをユーザーの「スケジューラ」としてログ記録する場合があります。これはログのみを目的としており、実際のアカウントではありません。ビルトインアカウントはなく、スケジューラのユーザは明示的にアカウントを作成する必要はありません。スケジューラは、ループバック インターフェイス経由で Call Bridge API を使用し、自動的に API コマンドを発行する信頼できるソースになります。

## 19.1 スケジューラを導入する

スケジューラと Call Bridge の間の接続を有効にするために、明示的な設定は必要ありません。これはループバック インターフェイスで自動的に行われます。同様に、C2W 接続はすべて自動ですが、sスケジューラとWeb Bridgeの間で信頼関係バンドルを設定する必要があります。

### 1. C2W トラストを設定します。

C2W は、スケジューラから各Web Bridgeに確立される TLS ベースの WebSocket 接続です。各スケジューラは、クラスタ内の各Web Bridgeに接続できる必要があります。スケジューラは、この接続に使用されるクライアント証明書とキーの設定を要求します。これを行うには、証明書を作成し、SFTP 経由でMeeting Serverにアップロードするか、`pki MMP` コマンドを使用して証明書を作成します。

スケジューラが証明書を使用するように設定します。

```
scheduler c2w certs <key-file> <crt- fullchain-file>
```

次に例を示します。

```
scheduler c2w certs scheduler_c2w.key scheduler.cer
```

スケジューラは、接続する各Web Bridgeを信頼できる必要があります。SFTP 経由で、各Web Bridgeの証明書を含む信頼バンドルをアップロードします。

次のコマンドを使用して、スケジューラを設定します。

```
scheduler c2w trust webbridge_bundle.cer
```

Web Bridgeがスケジューラを信頼できることも必要です。そのため、次のコマンドを使用して設定されたバンドルにスケジューラ証明書を含めることが重要です。

```
webbridge3 c2w trust <crt-bundle>
```

スケジューラと Call Bridge の両方に必要なすべての証明書は、<crt-bundle> に含める必要があります。

### 2. (オプション) スケジューラの HTTPS インターフェイスを設定します。

スケジューラには独自の HTTPS インターフェイスがあり、これを有効にすると、スケジューラ API を使用してスケジューラ ミーティングを設定することができます。ただし、Web Bridgeは管理 API を使用してスケジューラと通信することはありません。HTTPS サーバーの有効化は必須ではありませんが、診断およびトラブルシューティングの機能が提供されるため、有効にすることをお勧めします。

次のコマンドを使用して、HTTPS サーバ リッスン インターフェイスを設定します。

```
scheduler https listen <interface> <port>
```

次に例を示します。

```
scheduler https listen a 8443
```

コマンド `scheduler https certs <key-file> <crt-fullchain-file>` を使用して、サーバーの証明書キーペアを設定します。例：

```
scheduler https certs scheduler_https.key scheduler_https.cer
```

3. (オプション) メールサーバーを設定します。

メールサーバーの設定およびメール設定の種類の詳細については、[「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、メールプロトコルの有効化、認証のためのユーザー名の設定は、次のスケジューラ MMP コマンドで指定します。

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

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

4. メールサーバーを設定したら、次のコマンドを使ってスケジューラを有効にします。

```
scheduler enable
```

5. 次のコマンドを使用して、サービスの設定とステータスを確認します。

```
scheduler status
```

正常な構成のサンプル出力：

```
1 | cms> scheduler status
2 | Status:enabled
3 | 実行中 (Running)
4 | 開始時にデータベースが反応する
5 | HTTPS が設定されました
6 | C2W が設定されました
7 | メールサーバーが設定されました
```

```
8
9 スケジューラ アプリケーションのステータス :
10 {
11   "status" : "UP",
12   "コンポーネント" : {
13     "c2w" : {
14       "status" : "UP",
15       "詳細" : {
16         "guid" : "dc06c10f-a220-42d8-b4eb-f9be3d07faf4",
17         "webbridges" : "webbridge1.mycompany.com : 4443 : CONNECTED,
webbridge1.mycompany.com : 8443 : CONNECTED,
webbridge3.mycompany.com : 8443 : CONNECTED"
18       }
19     },
20     "db" : {
21       "status" : "UP"
22     },
23     "メール" : {
24       "status" : "UP",
25       "詳細" : {
26         "location" : "smtp.mycompany.com : 25"
27       }
28     },
29     "ping" : {
30       "status" : "UP"
31     }
32   }
33 }
```

## 20 セキュリティに関するその他の考慮事項と QoS

この章では、X.509 証明書と公開鍵による認証に加えて、Meeting Serverで利用できるその他のセキュリティ機能について説明します。

注：この章に記載されているコマンドは、[MMP コマンドリファレンス](#) ガイドにも記載されています。

### 20.1 Common Access Card (CAC) 統合

Common Access カード (CAC) は、コンピュータ施設にアクセスするための認証トークンとして使用されます。CAC には抽出できない秘密鍵が含まれていますが、カード上の暗号ハードウェアで使用してカード所有者の身元を証明することができます。

Meeting Server は、CAC を使用した SSH および Web 管理インターフェースへの管理ログインをサポートしています。表 14 の MMP コマンドを使用して、あなたのデプロイメントのために CAC を設定します。

表 14 : CAC ログインを設定する MMP コマンド

MMP コマンド	説明
<code>cac enable disable [strict]</code>	すべてのパスワードベースのログインを削除するオプションのストリクトモードで CAC モードを有効/無効にします
<code>cac issuer &lt;ca cert-bundle&gt;</code>	CAC 証明書を確認するための信頼できる証明書バンドルを識別します
<code>cac ocsp certs &lt;keyfile&gt; &lt;certificatefile&gt;</code>	使用されている場合、OCSP サーバーとの TLS 通信のための証明書と秘密鍵を識別します
<code>cac ocsp responder &lt;URL&gt;</code>	OCSP サーバーの URL を識別します
<code>cac ocsp 有効化 無効化</code>	CAC OCSP 検証を有効/無効にします

### 20.2 Online Certificate Status Protocol (OCSP)

OCSP は、証明書の有効性と失効状況を確認するためのメカニズムです。MMP は OCSP を使用して、ログインに使用された CAC が有効かどうか、特に失効していないかどうかを確認できます。

### 20.3 FIPS

FIPS 140-2 レベル 1 認定のソフトウェア暗号モジュールを有効にすると、暗号操作はこのモジュールを使用して実行され、暗号操作は FIPS 承認済み暗号アルゴリズムに制限されます。

表 15 : FIPS を設定する MMP コマンド

MMP コマンド	説明
<code>fips enable disable</code>	ネットワークトラフィックのすべての暗号化操作で FIPS-140-2 モード暗号化を有効または無効にします。FIPS モードの有効化または無効化後は、再起動が必要です
<code>fips</code>	FIPS モードが有効かどうかを表示します
<b>FIPS テスト</b>	組み込みの FIPS テストを実行します

## 20.4 TLS 証明書の検証

リモート証明書が信頼できるものであることを確認するために、SIP および LDAP の相互認証を有効にすることができます。有効にすると、Call Bridge は常にどちらの側で接続を開始したかに関係なく、リモート証明書を要求し、提示された証明書を、アップロードされ、サーバーに定義されている信頼ストアと比較します。

表 16 : TLS を設定する MMP コマンド

MMP コマンド	説明
<code>tls &lt;sip ldap&gt; trust &lt;cert bundle&gt;</code>	信頼できる認証局を定義します
<code>tls &lt;sip ldap&gt; verify enable disable ocsp</code>	証明書の検証を有効/無効にするか、検証に OCSP を使用するかを指定します
<code>tls&lt;sip ldap&gt;</code>	現在の構成を表示します

## 20.5 ユーザ コントロール

MMP 管理ユーザーは次のことができます。

- 別の管理ユーザーのパスワードをリセットする
- ユーザーのパスワードで繰り返し使用できる最大文字数を設定する - その他にも多くのユーザーパスワード ルールが追加されています
- IP アドレスで MMP アクセスを制限する
- 設定可能なアイドル期間の後に MMP アカウントを無効にする

## 20.6 ファイアウォールルール

MMP は、メディア インターフェイスと管理インターフェイスの両方に対して、簡単なファイアウォール ルールの作成をサポートします。これは完全なスタンドアロン ファイアウォール ソリューションの代替を意図したものではないため、ここでは詳細を説明しません。

ファイアウォールルールは各インターフェイスに個別に指定する必要があります。インターフェイスにファイアウォールルールを設定したら、必ずそのインターフェイスのファイアウォールを有効にしてください。詳細と例については、[MMP コマンド リファレンス](#) を参照してください。

**警告：**ファイアウォールの設定には、シリアルコンソールを使用することを推奨します。SSH を使用する場合、ルールのエラーにより SSH ポートがアクセス不能になるからです。SSH を使用する必要がある場合は、ファイアウォールを有効にする前に、許可 `ssh` ルール が管理者インターフェースに対して作成されていることを確認してください。

## 20.7 DSCP

ミーティングサーバ上のさまざまなトラフィックタイプに対して DSCP タグを有効にすることができます ([MMP コマンドリファレンス](#))。

1. MMP にログインします。
2. 必要に応じて、`dscp (4|6) <traffic type> (<DSCP value>|none)` を使用して DSCP を設定します。例：`dscp 4 oa&m 0x22` これは IPv4 の運用、管理、およびメンテナンスを設定します。
3. 代わりに、`dscp Assured (true|false)` コマンドを使用して、「音声」および「マルチメディア」トラフィックタイプに対して保証または非保証 DSCP 値の使用を強制します。  
例：`dscp assured true`

**注：**DSCP タグは、Meeting Serverから送信されるすべてのパケットにのみ適用されます。PC クライアント DSCP タギングの場合、グループポリシーを使用して希望の DSCP 値を定義する必要があります。これは Windows が制御し、通常のユーザアカウントには DSCP を設定する権限がないためです。

## 20.8 SSH 指紋を確認する

初めて SSH または SFTP 経由で Meeting Server に接続する管理者は、ログインする前に Meeting Server にインストールされたキーの指紋を取得することで、Meeting Server がプロンプトするキーを確認することができます。

表 17：キーを取得する MMP コマンド

MMP コマンド	説明
<code>ssh_server_key</code> リスト	出力には、Meeting Server ホスト内のすべての既存キーのサイズ、タイプ、フィンガープリントのキーのリストおよび以下のキーが表示されます。 <ul style="list-style-type: none"> <li>• <code>ssh_host_dsa_key.pub</code></li> <li>• <code>ssh_host_ecdsa_key.pub</code></li> <li>• <code>ssh_host_ed25519_key.pub</code></li> <li>• <code>ssh_host_key.pub</code></li> <li>• <code>ssh_host_rsa_key.pub</code></li> </ul>

## 21 問題をトラブルシューティングするのに役立つ Cisco サポートの診断ツール

Syslog レコードを使用することに加えて ([セクション 3.1.4](#)) 展開の問題の診断を支援するために、Meeting Serverで以下の機能を利用できます。

- [SIP トレース](#)
- [ログバンドル](#)
- [特定のコールレグのキーフレームを生成する](#)
- [登録済みメディア モジュールの定期的なレポート](#)

### 21.1 SIP トレース

Web管理者インタフェースの [ログ] > [詳細トレース] ページを使用して、追加のSIPトレースを有効にすることができます。これらのログは、SIP エンドポイントの通話セットアップの失敗問題を調査する場合に役立ち、それ以外の場合は無効にする必要があります。冗長ログが必要以上に長く有効になることを防ぐために、1分、10分、30分、または24時間の選択後に自動的にオフになります。トラブルシューティングの詳細については、Cisco ウェブサイトの「Meeting Serverのサポートに関するFAQ」を参照してください。

失敗したログイン試行の診断には以下が含まれます。

- ログインに関連するイベントログメッセージに含まれる遠端の IP アドレス
- ユーザ名を除く失敗したログインおよびログイン セッションのタイムアウトに対して生成された監査メッセージ。成功したログインに対しても生成されます。

### 21.2 ログバンドル

Meeting Serverは、Meeting Serverの様々なコンポーネントの構成と状態を含むログバンドルを生成することができます。このログバンドルには、syslog および live.JSON ファイルが含まれます。問題に関して Cisco サポートに連絡する際は、これらのファイルをご提供いただくと、早く分析ができます。

Meeting Serverのログバンドルは以下の方法で生成されます：

- Meeting Server管理者は、MMP 管理者ユーザ資格情報を使用して SFTP クライアントを MMP IP アドレスに接続することにより、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 というファイル名でログバンドルを生成しダウンロードします。
- 代わりに、管理者は、`generate_logbundle` コマンドを使用してダウンロードプロセスを開始する前に、ログバンドルを生成できます。generatedlogbundle.tar.gz という名前のログバンドルが生成されます。

コマンド/例	説明/メモ
<code>generate_logbundle</code>	それぞれの Meeting Server で <code>generatedlogbundle.tar.gz</code> というファイル名のログバンドルを生成します。  注：このコマンドが実行されるたびに、前に生成されたログバンドルが最新のログバンドルで置換されます。

以下の手順でログバンドルをダウンロードします。

1. SFTP クライアントを MMP の IP アドレスに接続します。
2. MMP 管理者ユーザーの資格情報を使用してログインします。
3. ログバンドルをダウンロードする場所でこれらのコマンドを実行します。
  - a. `sftp get logbundle.tar.gz`
  - b. `sftp get generatedlogbundle.tar.gz`
4. `logbundle.tar.gz/generatedlogbundle.tar.gz` ファイルをローカルフォルダにコピーします。
5. ファイル名を変更し、ファイル名の `logbundle` の箇所を変更し、ファイルを生成するサーバーを特定します。これは複数サーバーの展開では重要です。
6. 名前を変更したファイルを分析のために Cisco サポート担当者に送信します。

`log bundle.tar.gz` の初期ファイルサイズは、1 KB です、SFTP 経由で転送した場合、サイズは、ファイル数とそのサイズに応じて大きくなります。

**メモ：**お使いのコンピューターと Meeting Server 間でネットワーク接続が遅いなどの原因で `logbundle` がダウンロードできない場合は、ログファイルと `live.json` ファイルをダウンロードして、Cisco サポートにご送信ください。

### 21.3 特定のコールレグのキーフレームを生成する機能

`generateKeyframe` オブジェクトが `/callLegs/<callleg id>` に追加されました。これはデバッグ機能です。Cisco サポートは、問題を診断する際に、この機能の使用をお願いする場合があります。

Web 管理インターフェースを使用して、[設定 > API] を選択し、

1. API オブジェクトのリストで、`/callLegs` の後ろの ▶ をタップします。
2. コールレグの オブジェクト ID をクリックします。
3. ページ上部にある 関連オブジェクトのリスト で、`/callLegs/<callleg id>/generateKeyframe` をクリックします。
4. [作成 (Create) ] をクリックします。

これにより、問題のコールレグの発信ビデオ ストリームに新しいキーフレームが生成されます。

## 21.4 syslog に登録されたメディアモジュールを報告する

syslog では、15 分ごとにメッセージを出力することができるため、すべてのメディアモジュールが稼働しているかどうかを監視できます。

Meeting Server 2000 の例：

```
2020-08-06T13:21:39.316Z user.info cms2kapp host:server INFO:media module
status 1111111 (1111111/1111111) 7/7 (full media capacity)
```

## 22 追加のライセンス情報

Meeting Management はライセンスの目的で、Meeting Server 3.0 以降では必須です。Smart Licensing を使用している場合は、Cisco Smart Software Manager に接続する必要があります。ローカル ライセンス ファイル (従来のライセンス モード) のサポートが廃止され、ライセンス予約が導入されました。

---

**注：**セキュリティ上の理由から Meeting Management を使用できない、またはインターネットに接続できない環境では、担当の Cisco アカウントチームに連絡して代替オプションを入手してください。

---

### 22.1 ライセンス

この章では以下の情報を確認できます：

- Meeting Server でのスマートライセンスの仕組み
- 期限切れライセンス機能の強制アクション
- ライセンス情報を取得する方法 (Smart Licensing)
- Smart Licensing 登録プロセス
- ユーザーに Personal Multiparty ライセンスを指定する
- 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を確認する
- SMP Plus ライセンスの使用数を計算する
- Meeting Serverからライセンス使用状況のスナップショットを取得する
- ライセンスレポート

#### 22.1.1 Meeting Server でのスマートライセンスの仕組み - 概要

ライセンスが Meeting Server 3.0 以降で動作するためには、Meeting Management が必須です。Meeting Server と Meeting Management の間の信頼と相互作用は、Smart を使用した新しいライセンシングをサポートするために、または既存の顧客がインストール済みのライセンスファイルを使用するために導入されています。この信頼されたリンクにより、ミーティング管理は Meeting Server にライセンスを付与します。

---

**メモ：** Cisco Meeting 管理を使った Smart Licensing の管理の詳細は、[『ミーティング管理管理者ガイド』](#)を参照してください。

---

Smart Licensing を実装するためのワークフローの概要は以下の通りです。

1. ミーティング管理を Smart Licensing バーチャルアカウントに登録します。

2. Meeting Server が最初に起動したとき、ライセンス状況の値は定義されていません。

---

**メモ：** トライアルモードは、90 日間のフル機能の期間、ライセンスなしで使用できます。

---

3. Meeting Server は、Smart Licensing を管理するためにセットアップされたミーティング管理インスタンスに最初に接続するときに、Meeting Server にライセンスが以前に適用されているかどうかを確認します。有効になっていない場合、ライセンスの有効期限が 90 日後に設定されます。

ライセンスの有効期限はミーティング管理に表示され、また付録 B.5 に示すように clusterLicensing API にも返されます。

---

**メモ：** 機能ライセンスの有効期限は、最大で 90 日後になります。

---

4. Meeting Management は、Meeting Server が準拠していることを確認するために必要なライセンスがあるかどうかを確認するために、クラスターの Meeting Server ライセンスの使用状況を照合し、スマートアカウントに日単位でレポートを行います。スマートアカウントはミーティング管理に応答し、Meeting Server が準拠しているかどうかを示します。ミーティング管理では、有効期限を次のように適切に設定します。

- a. ミーティング管理が、ライセンスが存在し、特定の機能の利用権限を下回っていることを確認した場合、有効期限は 90 日後に延長されます。

---

**メモ：** Meeting Server がミーティング管理に接続せず、90 日間の使用状況データを送信しない場合、Meeting Server のライセンスは更新されず、期限切れになります。ライセンス期限切れ時の強制措置についての情報は、[セクション 22.1.2](#) を参照してください。

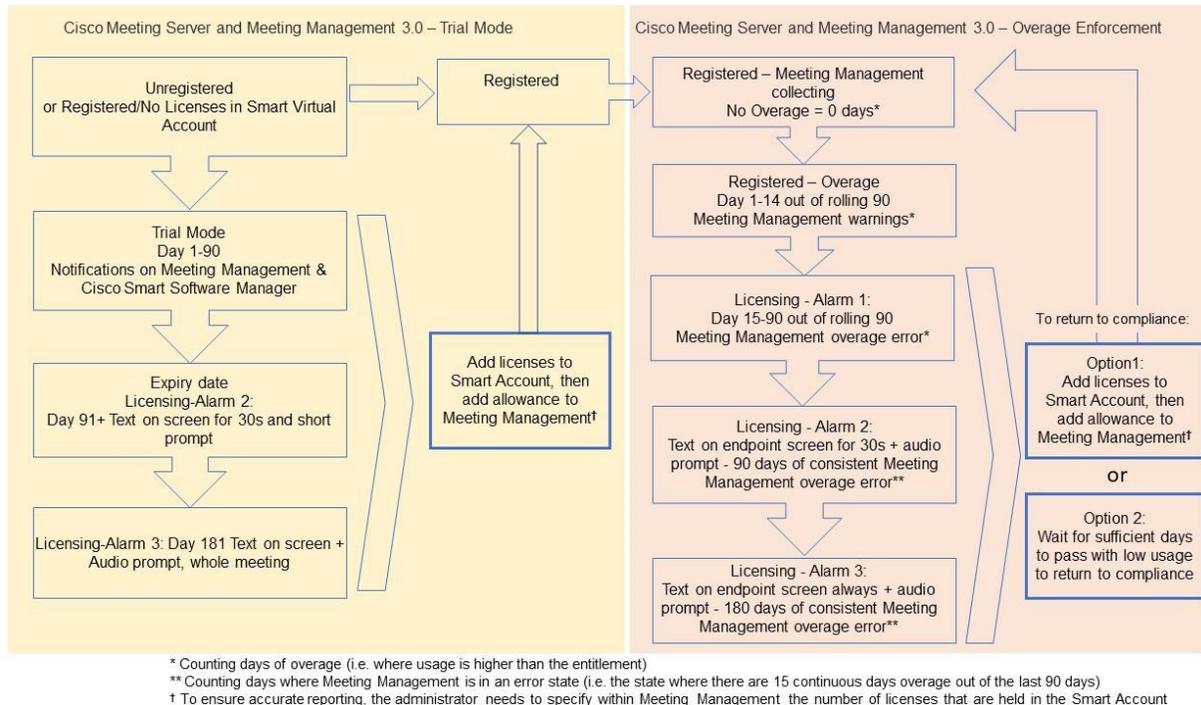
---

ライセンスの使用数が資格を超える場合、またはライセンスが見つからない場合、施行は次のように行われます。

- b. ミーティング管理が過去 90 日間のうち 15 日間未満が非準拠であると特定した場合、これを許可し、Meeting Server の有効期限日をその時点から 90 日後の将来にリセットします。管理者は「ライセンスが不十分」を通知する視覚的な警告を受け取ります。
- c. ミーティング管理で過去 90 日間のうち 15 日間以上で準拠していないことが確認された場合、第 1 レベルの強制（アラーム 1）が発生します。つまり、ミーティング管理インターフェイスに準拠していないことが通知されます。
- d. 超過が続く場合、Meeting Management は 90 日のクロックをリセットしません。新しいライセンスを追加するための xx 日間のカウントダウンが表示されます。そうしないと、図 45 に示すように、ミーティングに参加するすべての参加者に対して、アラームレベル 2 と 3 が有効になります。

図 45 では、左側のトライアルモードでの初回起動から、右側の超過数の強制までの強制フローを示します。

図 45 : Cisco Meeting Server および Cisco Meeting Management Smart Licensing の強制フロー



### 22.1.2 期限切れライセンス機能の強制アクション

以前は、Meeting Server は再起動時にのみライセンスファイルを評価していました。3.0 から、機能がライセンスされているかどうかの現在のステータスが動的に変更される可能性があります。これは、機能ライセンスの有効期限が切れている場合や（以前は再起動するまで確認できなかった場合）、または API が変更された場合などです。ミーティング管理で強制措置が Smart Licensing で計算されます。

**メモ** : Smart Licensing ポータルを使用して、「不十分なライセンス」のメール通知を有効にできます。

ライセンス機能の有効期限が切れると、表 18 に記載のアクションが行われます。

表 18 : 期限切れライセンスの強制アクション

機能	アクション
callBridge	有効期限が切れた場合：すべての参加者/すべてのミーティングのミーティングに参加するときに、視覚的なテキストメッセージが画面に 30 秒間表示され、音声プロンプトが再生されます。（アラームレベル 2）
callBridgeNoEncryption	90 日以上前に期限切れになった場合、またはライセンスが存在しない場合：以前と同じですが、ビジュアルメッセージは永久的なものです。音声プロンプトにより、「展開はライセンスに準拠していません。管理者に連絡してください」が再生されます。（アラームレベル 3）
PMP/SMP	ただし、ライセンスのない状態では暗号化された通話は処理されません。  メモ：上記のアクションを防ぐには、callBridge または callBridgeNoEncryption のみが必要です。
customizations	期限が切れているか存在しない場合、会議中にカスタマイズ機能はアクティブになりません。
recording	有効期限が切れているか、出席していない場合、新しい録画を開始することはできません（サードパーティのレコーダーかどうかは関係ありません）。  このライセンスは録画とストリーミングを表すため、同じ制限がストリーミングにも適用されます。

アラーム 2 および 3 をオフにするには、スマートアカウントにライセンスを追加するだけです。

### 22.1.3 ライセンス情報を取得する方法（Smart Licensing）

Meeting Serverのウェブ管理インターフェイスを使用してクラスタのライセンス情報を取得するには、

1. Meeting Serverのウェブ管理インターフェイスにログインして **設定（Configuration）** >API を選択します。
2. API オブジェクトのリストで、/api/v1/clusterLicensing **後にタップ**します。
3. クラスタの現在のライセンス状況は、次の例のように表示されます。

図 46 : clusterLicensing API - ライセンスステータス

The screenshot shows the API endpoint /api/v1/clusterLicensing with three view options: View, Table view, and XML view. The 'Table view' is selected, displaying the following data:

Object configuration		
features	callBridge	status activated expiry 2020-09-16
	callBridgeNoEncryption	status noLicense
	customizations	status activated expiry 2020-09-16
	recording	status activated expiry 2020-09-16

## 22.1.4 Smart Licensing 登録プロセス

### Smart Licensing の有効化

1. Cisco Smart Software Manager (CSSM) ポータル にログインし、[Meeting Server ライセンスを持つバーチャル アカウント] 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ミーティング管理のインスタンスを開きます。
5. **設定** ページの [ライセンス] タブに移動します。
6. [変更] をクリックします。
7. [Smart Licensing] を選択し、[保存] を選択します。
8. [登録 (Register) ] をクリックします。
9. 登録トークンを貼り付けます (これにより、ミーティング管理を Smart Licensing ポータルに接続できます)。
10. [登録 (Register) ] をクリックします。
11. 登録が済んだら、バーチャルアカウントにあるライセンス数を確認してください。
12. ミーティング管理で、**ライセンス** ページに移動します。
13. バーチャルアカウントで所有するライセンスのライセンス情報を入力します。

バーチャルアカウントに表示されていないライセンスがある場合は、[ライセンスの変換] タブを使用し、PAK で検索し、[ライセンスの変換] を選択します。追加 図 47 に従います。(ライセンスが見つからない場合は、licensing@cisco.com にメールを送信してケースを開きます。)

図 47 : Smart Licensing のライセンス変換

Cisco Software Central > Smart Software Licensing BU Production Test 1

Smart Software Licensing Feedback Support Help

Alerts | Inventory | **Convert to Smart Licensing** | Reports | Preferences | On-Prem Accounts | Activity

License Conversion

Convert PAKs | Convert Licenses | Conversion History | Event Log

The Product Activation Keys (PAKs) below contain licenses that can be used for traditional licensing or Smart Software Licensing. To add some or all of them to a Virtual Account as Smart Software Licenses, use the 'Convert to Smart Licenses' action in the table below.

If you do not see a PAK you expect to see in the table, ensure that it has been assigned to your Smart Account in the [Product License Registration Portal](#).

**The Smart Account administrator may be able to more easily convert the licenses based on the automatic conversion settings.**

Last Updated : 2020-Jul-20 16:30:09

Search PAK, SKU, Virtual Account or Order Number

PAK	SKUs	Order Number	Order Date	Virtual Account	Status	Actions
-----	------	--------------	------------	-----------------	--------	---------

## 22.1.5 マルチパーティライセンス

### 22.1.5.1 パーソナル Multiparty Plus ライセンス

Personal Multiparty Plus (PMP Plus) は、頻繁にビデオミーティングを主催する特定のユーザーに割り当てられた指名主催者ライセンスを提供します。これは、Cisco UWL Meeting を通じて購入できますまたは Flex Meetings (PMP Plusを含む)。Personal Multiparty Plus は、ビデオ会議のためのオールインワンのライセンス製品です。これにより、ユーザーはあらゆるサイズの電話会議を開催できます（導入された Cisco Meeting Server ハードウェアの制限内）。誰でもどのエンドポイントからでもミーティングに参加でき、このライセンスは最大 HD 1080p60 品質のビデオ、音声、コンテンツ共有に対応します。

---

**メモ：** Unified Communications Manager を使用すると、アドホック電話会議の開始者を識別することができます。PMP Plus ライセンスが割り当てられている場合は、それが電話会議で使用されます。

---

**メモ：** 個人の PMP Plus ライセンスを使用するアクティブな通話数を確認するには、パラメータ `callsActive` を API オブジェクトで使用します。

`/system/multipartyLicensing/activePersonalLicenses`. 通常、2 つのコールをアクティブにできるため、1 つは開始、もう 1 つは終了とします。通話が Call Bridge のクラスターで発生する場合、パラメータ `weightedCallsActive` を API オブジェクトで使用します。

`/system/multipartyLicensing/activePersonalLicenses` for each Call Bridge in the cluster. クラスター全体の `weightedCallsActive` の合計は、個人の PMP Plus ライセンスを使用するクラスター上の個別の通話数と一致します。PMP Plus ライセンスの上限を超えた場合は、SMP Plus ライセンスが割り当てられます。[項 22.1.1](#) を参照してください。

---

### 22.1.5.2 Shared Multiparty Plus ライセンス

Shared Multiparty Plus (SMP Plus) は、まれにビデオミーティングを主催する複数のユーザーによって共有される同時ライセンスを提供します。Shared Multiparty Plus は、PMP Plus 主催者ライセンスを持たないすべての従業員がビデオ会議にアクセスできるようにします。これは、多くの従業員が共有する会議室システムを展開している顧客に最適です。PMP Plus を持つユーザまたは SMP Plus ライセンスを使用するユーザーは、同じように優れたエクスペリエンスを得ることができます。スペースでミーティングを主催したり、アドホック ミーティングを開始したり、今後のミーティングをスケジュールしたりできます。各共有主催者ライセンスは、任意のサイズ (展開されたハードウェアの制限内) の 1 つの同時ビデオ ミーティングをサポートします。

---

**注：** 必要な SMP Plus ライセンスの数を確認するには、パラメータ `callsWithoutPersonalLicense` を使用します。API `/system/multipartyLicensing`. 通話が Call Bridge のクラスター上にある場合は、パラメータ `weightedCallsWithoutPersonalLicense` を API object `/system/multipartyLicensing` で使用します。> クラスター内の各 Call Bridge に対して。クラスター全体の `weightedCallsWithoutPersonalLicense` の合計は、SMP Plus ライセンスを必要とするクラスター上の個別の通話の数と一致します。

---

### 22.1.6 ユーザーに Personal Multiparty ライセンスを指定する

このプロセスでは、ユーザーが単一の LDAP ソースからインポートされる必要があります。詳細については、「[プロビジョニング – ユーザーをインポート](#)」を参照してください。これは、[「会議管理管理者ガイド」](#)にあります。

#### 22.1.6.1 特定のユーザーがライセンスを持っているかどうかを確認するには：

1. API オブジェクトのリストで、[/users 回の後] の [] をタップします
  - a. 特定のユーザーの **オブジェクト ID** を選択します
  - b. このユーザーに関連付けられた userProfile の **オブジェクト ID** を特定する
2. API オブジェクトのリストで、[/users 回の後] の [] をタップします
  - a. 特定のユーザーの **オブジェクト ID** を選択します
  - b. パラメータ hasLicenceの設定を確認してください。true に設定すると、ステップ 1 で特定されたユーザーが Cisco Multiparty ユーザライセンスに関連付けられます。false に設定すると、ユーザーに Cisco Multiparty ユーザライセンスは関連付けられません。

---

**注：** userProfile が削除されると、ldapSource およびインポートされたユーザーの userProfile の設定が解除されます。

---

### 22.1.7 Cisco Multiparty ライセンスの割り当て方法

スペースでミーティングが開始されると、Cisco ライセンスがスペースに割り当てられます。Cisco Meeting Serverにより割り当てられるライセンスは、以下のルールにより決定されます。

- スペース所有者が定義されており、Cisco PMP Plus ライセンスが割り当てられている、Meeting Serverからインポートされた LDAP ユーザーに対応する場合、その所有者のライセンスは、その人物が電話会議でアクティブであるかどうかに関係なく割り当てられます。
- ミーティングが Cisco Unified Communications Manager からのアドホック エスカレーションで作成された場合、Cisco Unified Communications Manager はミーティングをエスカレートするユーザーの GUID を提供します。その GUID が、Meeting Serverからインポートされた Cisco PMP Plus ライセンスを持つ LDAP ユーザーに対応する場合、そのユーザーのライセンスが割り当てられます。そうでない場合は、
- ミーティングが Cisco TMS バージョン 15.6 以降からスケジュールされた場合、TMS はミーティングの所有者に情報を提供します。そのユーザーが、Cisco PMP Plus ライセンスが割り当てられたユーザ ID/メールアドレスで、Meeting Serverからインポートされた LDAP ユーザーに対応する場合、そのユーザーのライセンスがミーティングに割り当てられます。そうでない場合は、次に、
- Cisco SMP Plus ライセンスが割り当てられている。

### 22.1.8 Cisco Multiparty ライセンスの使用状況を確認する

マルチパーティライセンスの使用状況を表示するには、ミーティング管理を使用することをお勧めします。ただし、API は使用できません。

表 19 は、Multiparty ライセンスの消費量を決定するために使用できる API オブジェクトとパラメータの一覧です。

表 19 : マルチパーティライセンスの使用に関連するオブジェクトとパラメータ

API オブジェクト :	パラメータ	使用目的...
/system/license	個人用、共有	Cisco Meeting Server のコンポーネントが Multiparty ライセンスを持ち、アクティベートされているかどうかを判別します。値は次のとおりです：noLicense、アクティブ化、猶予、期限切れ。 有効期限日と上限数も表示されます。
/system/multipartyLicensing	personalLicenseLimit, sharedLicenseLimit, personalLicenses, callsWithoutPersonalLicense, weightedCallsWithoutPersonalLicense	利用可能で使用中のライセンスの数を示します。
/system/multipartyLicensing/activePersonalLicenses	CallsActive, weightedCallsActive	パーソナルマルチパーティプラスユーザーライセンスを使用しているアクティブ通話の数を示します。
/userProfiles	hasLicense	ユーザーが Cisco Multiparty ユーザーライセンスに関連付けられているかどうかを示します。

Cisco Multiparty ライセンスをサポートするための、これらの追加のオブジェクトとフィールドの詳細については、『[Cisco Meeting Server API リファレンスガイド](#)』を参照してください。

### 22.1.9 SMP Plus ライセンスの使用数を計算する

次の特定のシナリオにおいて、ミーティングで使用される SMP Plus ライセンスは、フルライセンスの 1/6 に減らされます。

- 出席者がビデオを使用していない音声のみの電話会議
- Lync ゲートウェイ通話 (Meeting Serverが記録またはストリーミングを行っている場合を除く)
- ウェブアプリと 1 つの SIP エンドポイント、または 2 つのウェブアプリが関係する二地点間コール Meeting Serverが録画またはストリーミング中の場合を除き、録画中またはストリーミング中は完全な電話会議と見なされ、SMP Plus ライセンスが消費されます

フル SMP Plus ライセンスは、所有者のプロパティが未定義のスペースからインスタンス化された音声/ビデオ会議、PMP Plus ライセンスを持たないインポートされた LDAP ユーザーが所有、または PMP Plus ライセンスがすでに使用されているインポートされた LDAP ユーザーが所有する音声ビデオ会議です。で参加する場合、これは参加者数に関係ありません。

---

**注：**ポイントツーポイント通話は次のように定義されます：

- Meeting Server上に永久スペースがない
- レコーダーまたはストリーマを含めて 2 人未満の参加者
- Lync AVMCU で主催されている参加者がいない、

これには、Lync ゲートウェイ通話だけでなく、他のタイプの通話 (ポイントツーポイント ウェブ アプリからウェブ アプリ、ウェブ アプリから SIP、および SIP から SIP) が含まれます。

---

### 22.1.10 ミーティングサーバーからライセンス使用状況のスナップショットを取得する

管理者は Meeting Server からライセンスの使用状況を取得できます。これらにはウェブ管理インターフェイスからはアクセスできません。代わりに、POSTMAN：

展開内の Meeting Server の主催者 ID を取得するには、`/system/MPLicenseUsage/knownHosts` で GET を使用します。リストの最初のページ以外の主催者 ID を取得するために必要な場合は、オフセットと制限を指定します。

`/system/MPLicenseUsage` で GET を使用して、指定された主催者 ID を持つ Meeting Server の Call Bridge からライセンスの使用状況を取得します。スナップショットの開始時刻と終了時刻を指定します。使用中のパーソナルライセンス数、使用中の音声のみ、ポイントツーポイント、または音声でもポイントツーポイントでもないライセンスの数、記録されている通話の数、ストリーミングされた通話の数に関する情報を提供します。

---

**注：**注：個人ライセンスと共有ライセンスは、通話がスパンする Call Bridge の数で正規化されます。

---

### 22.1.11 ライセンスレポート

ミーティング管理には、過去 90 日間のライセンスレポート/使用情報があります。Cisco Smart Software Manager にはライセンスレポート情報も含まれます。録画ライセンスの使用は同時に録画する会議の数を示し、同様にストリーミング ライセンスの使用は同時にストリーミングする会議の数を示します。

### 22.1.12 レガシーライセンスファイルによる方法

この項は、従来のライセンス方法を使用している場合にのみ適用されます。バージョン 3.4 から、従来のライセンスのサポートは廃止されました。既存のローカルライセンスは、ライセンスの有効期限が切れるまで引き続きサポートされます。

### 22.1.12.1 従来のライセンス方法を使用して Cisco ユーザライセンスを取得する

この項は、あなたがすでに Meeting Server に必要なライセンスを Cisco パートナーから購入しており、PAK コードを受け取っていることを前提としています。

これらの手順に従い、次のアドレスを使用して、Meeting Server の MAC アドレスに PAK コードを登録します。[Cisco ライセンス登録ポータルサイト](#)。

---

**注：**個々の Call Bridge に対してライセンス ファイルが必要です。ライセンスは、同じクラスター内のサーバ間でのみ共有できます。各ライセンスファイルには、そのクラスター用に購入した必須機能がすべて含まれている必要があります。PMP Plus、SMP Plus、録画、ストリーミングなど。

---

1. サーバーの MMP にログインして Meeting Server の MAC アドレスを取得し、MMP コマンドを入力します：**a** の場合

---

**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プラットフォームの MAC アドレスではありません。

---

2. [Cisco ライセンス登録ポータルサイト](#) そして Meeting Server の PAK コードと MAC アドレスを登録してください。
3. PAK に R-CMS-K9 アクティベーション ライセンスがない場合、機能ライセンスに加えてこの PAK が必要になります。
4. ライセンスポータルからライセンスファイルの zip 圧縮されたコピーがメールで送信されます。Zip ファイルを解凍し、結果として得られた xxxxx.lic ファイルの名前を **cms.lic**。
5. SFTP クライアントを使用して Meeting Server にログインし、**cms.lic** ファイルを Meeting Server ファイルシステムにコピーする必要があります。
6. MMP コマンドを使用して Call Bridge を再起動する **callbridge restart**。
7. Call Bridge を再起動したら、MMP コマンドを入力してライセンスのステータスを確認します。

**license**

アクティブ化された機能と有効期限が表示されます。

## 23 ホストされた会議の情報を取得する

Meeting Server で主催されている電話会議の情報を取得するための 2 つのメカニズムにより、API を頻繁にポーリングする必要性を減らします。通話詳細レコードとイベントです。

---

**注：** Cisco ミーティング管理を CDR (通話詳細レコード) レシーバーとして、および各 Call Bridge のイベント クライアントとして設定し、API 要求、CDR、および Meeting Server イベント経由でアクティブなミーティングに関する情報を取得することができます。詳細については、『[管理者向け Meeting Management ユーザー ガイド](#)』を参照してください。

---

### 23.1 コール詳細レコード (CDR)

Meeting Server は、サーバーに到達する新しい SIP 接続、または通話のアクティブ化または非アクティブ化など、主要な通話関連イベントに対して、内部で通話詳細レコード (CDR) を生成します。

サーバーは、これらの記録を収集および分析するためにリモートシステムに送信するように設定することができます。Meeting Server 上に記録を長期間保存するための規定はなく、Meeting Server 自体の CDR を参照する方法もありません。

CDR システムは Meeting Server API と組み合わせて使用できます。コール ID とコール レッグ ID の値は 2 つのシステム間で一貫しているため、イベントと診断の相互参照が可能になります。

Meeting Server は最大 4 つの CDR 受信者をサポートするため、Cisco Meeting Management など、異なる管理ツールまたは同じ管理ツールの複数のインスタンスを展開することができます。詳細は、『[Cisco Meeting Server 通話詳細記録ガイド](#)』を参照してください。

### 23.2 イベント

Meeting Server は、Meeting Server 上で発生する変更をリアルタイムで「イベントクライアント」に通知することができます。Meeting Server は、イベントのためのサーバーとして機能し、イベントクライアントは、例えば、ウェブベースの管理アプリケーションである場合があります。Cisco Meeting Management はイベントクライアントとして機能します。

---

**注：** 独自のイベントクライアントを構築することができます。これは API クライアントの構築と似ています。イベント クライアントは、HTTP および WebSocket ライブラリをサポートする必要があり、どちらも Python 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ウェブ管理で設定したものと同じです。通常はインタフェース A の TCP ポート 443 です。

---

Meeting Server の API リソースを継続的にポーリングする代わりに、イベントクライアントはイベントリソースをサブスクライブして更新を受け取ることができます。たとえば、イベントクライアントとミーティングサーバ間の WebSocket 接続を確立した後、イベントクライアン

トはイベントリソース `callRoster` をサブスクライブし、アクティブなミーティングの参加者リストの更新を受け取ることができます会議で、新しい参加者が参加したときや、既存の参加者のレイアウトが変更されたときなどを確認します。

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 導入に必要な DNS レコード

注：外部 DNS サーバーで設定されていない、または上書きする必要がある値を返すように DNS リゾルバを設定することができます。外部 DNS サーバーに照会する代わりに返されるカスタム リソース レコード (RR) を設定することができます。(クライアントは RR を利用できません。) 詳細は「[MMP コマンドリファレンス](#)」を参照してください。

注：レコードを以下に定義する前に、Meeting Serverに A または SRV レコードがないことを確認してください。

表 20：展開に必要な DNS レコード

Type	例、説明、レジリエンスの考慮事項
A / AAAA	<p><b>ukedge1.example.com</b></p> <p>解決先： Web Bridgeの IP アドレス。</p> <p>説明： このレコードは、Meeting ServerがWeb Bridgeに接続するために使用されます。</p>
A / AAAA	<p><b>join.example.com</b></p> <p>解決先： 1) Web Bridgeの単一のDNSエントリ (使用している場合)、または 2) DNS でネットワーク負荷分散を行う場合、IP またはロケーションに基づいた単一の DNS エントリ、または 3) ネットワークロードバランサーの単一の IP、または 4) Cisco Expressways の 1 つ以上の IP アドレス</p> <p>説明： このレコードに解決されるブラウザに入力するための FQDN をエンドユーザーに提供するのが一般的な方法です。</p>
A / AAAA	<p><b>ukedges.example.com</b> <b>nyedges.example.com</b></p> <p>解決先： Web Bridgeの IP アドレス。</p> <p>説明： Web Bridge 3 (c2w 用) に接続するために、Call Bridge で使用されます。</p>

Type	例、説明、レジリエンスの考慮事項
A / AAAA	<p><b>ukcore1.example.com</b> <b>nycore1.example.com</b></p> <p>解決先： Call Bridge の IP アドレス。</p> <p>説明： Lync FE サーバーが Call Bridge に接続するために使用します。</p> <p>復元性の考慮事項： Call Bridge ごとに 1 つのレコードが必要です。各 Call Bridge は一意の FQDN を持つ必要があります。</p>
A / AAAA	<p><b>ukcoreladmin.example.com</b> <b>ukedge1admin.example.com</b> <b>ukcoreadmin.example.com</b></p> <p>解決先： MMP インターフェ이스の IP アドレス。</p> <p>説明： このレコードは管理目的でのみ使用されます。システム管理者が各 MMP インターフェ이스に対して覚えやすい FQDN を好む場合です。</p> <p>復元性の考慮事項： ウェブ管理インターフェースごとに 1 つのレコードが必要です。各 MMP インターフェ이스は固有の FQDN を持つ必要があります。</p>
SRV(*)	<p><b>_sipinternaltls._tcp.&lt;yourLyncdomain&gt;</b></p> <p>解決先： Lync FE サーバまたは FE プールの A レコード。</p> <p>説明： FE プールがある場合、プール内の個々の FE サーバーをポイントする複数の FE レコードを持つことができます。Meeting Serverに Lync ミーティング ID によって Lync ミーティングを解決させたい場合にもこのレコードが必要です。</p>
A / AAAA	<p><b>fe.&lt;yourLyncdomain&gt;</b></p> <p>解決先： Lync FE サーバーの IP アドレス。</p> <p>説明： 個々の FE サーバごとに 1 つのレコードが必要です。</p>
SRV(*)	<p><b>_sipfederationtls._tcp.&lt;yourSIPdomain&gt;</b></p> <p>解決先： Meeting Serverの FQDN です。</p> <p>説明： このレコードは Lync フェデレーションに必要です。</p>

Type	例、説明、レジリエンスの考慮事項
A	<b>callbridge.example.com</b> 解決先： Call Bridge の IP アドレス。 説明： Lync フェデレーションで必須。Call Bridge はパブリック IP アドレスを持つ必要があり、NAT はこのシナリオではサポートされません。

(\*) SRV レコードは IP アドレスを直接解決しません。SRV 要件を満たすために、関連する A または AAAA 名レコードを作成する必要があります。

## 付録 B 導入に必要なポート

以下の図は、スケーラブルで復元力のあるサーバ展開におけるMeeting Serverへの接続とファイアウォールの場所を示しています。図の下の表を使用して、開くポートを特定します。

図 48 : スケーラブルでレジリエントなサーバデプロイメントにおいて、DMZ内のExpresswayを使用した場合に開く必要があるポート

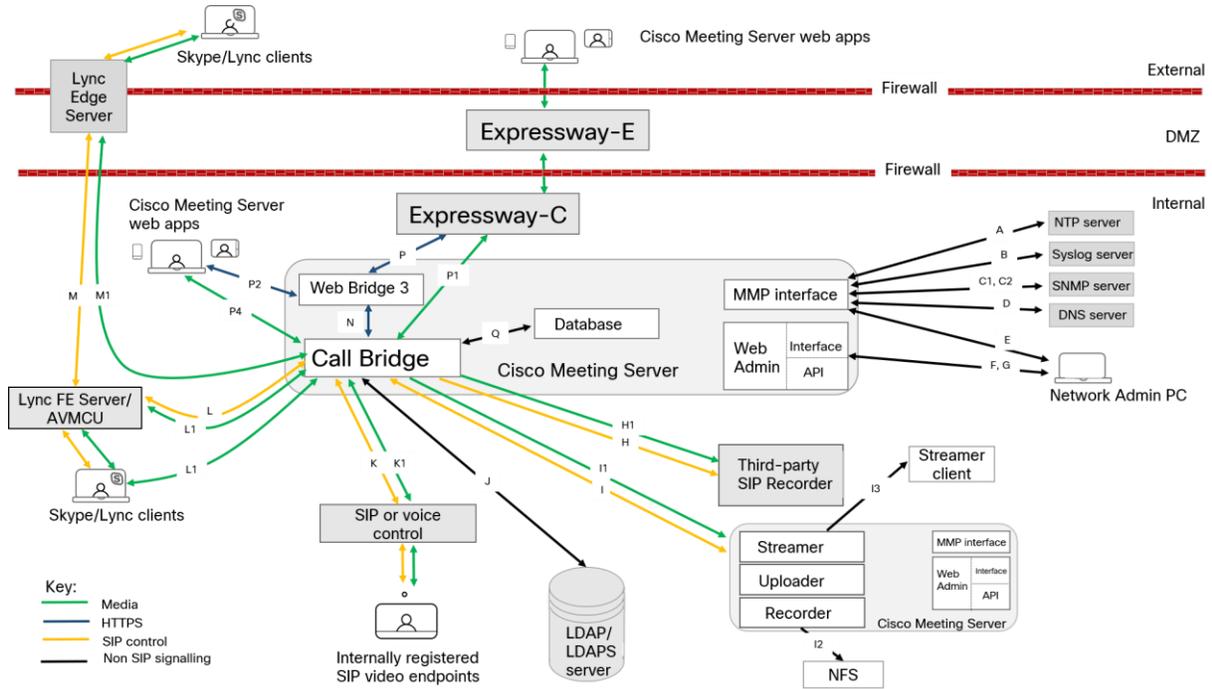
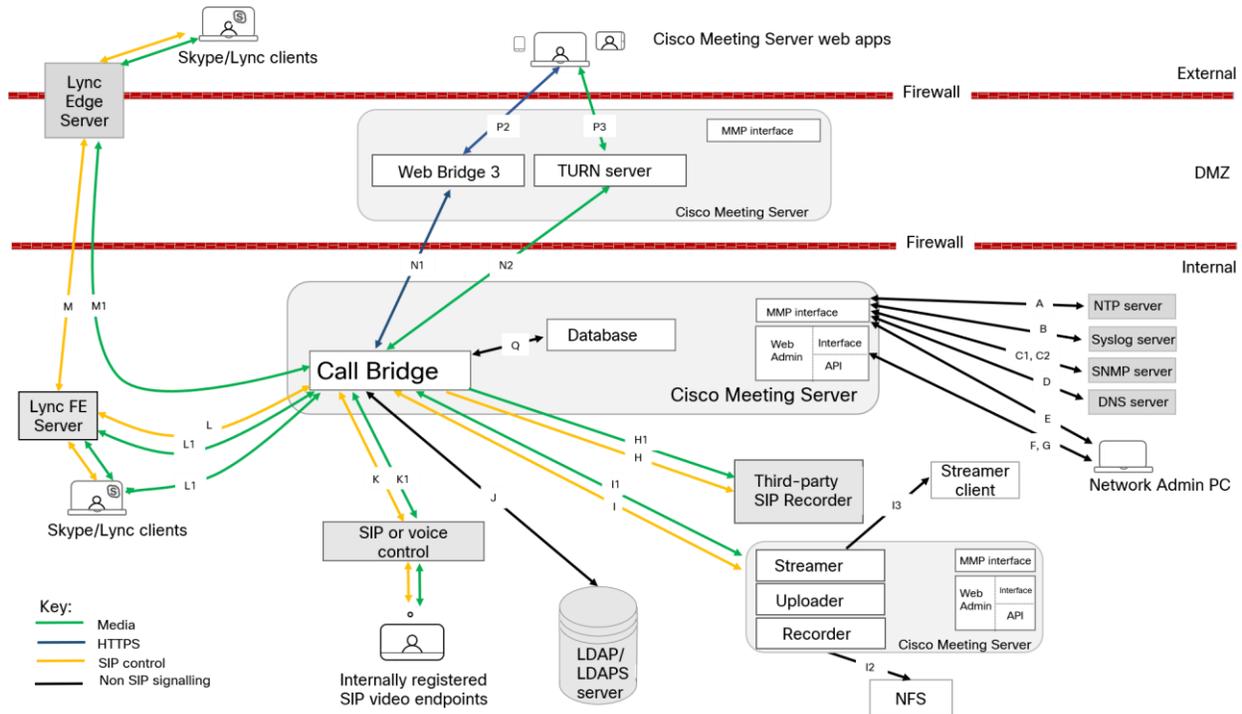


図 49 : DMZ で TURN サーバーと Web Bridge 3 コンポーネントを使用するスケーラブルでレジリエントなサーバー導入で開く必要があるポート



## B.1 Meeting Server を設定する

表 21 に、Meeting Serverの設定に使用するポートを示します。

表 21 : Meeting Server管理用のポート

code	接続先	開く接続先ポート	方法	トラフィックタイプ	Meeting Server に対するトラフィックの方向	追加情報
E	MMP	22	SSH	TCP	着信	MMP への安全なログイン
F	API または Web 管理者	80	HTTP	TCP	着信	MMP を通じて有効化/無効化されたポート
G	API または Web 管理者	443	HTTPS	TCP	着信	MMP を通じて構成可能なポート

## B.2 サービスへの接続

さまざまなサービスをウェブアプリに接続するために使用されるポートを特定するために表 22 を使用します。

表 22 : サービスに接続するために開くポート

code	コンポーネント	接続先	開く接続先ポート	トラフィックタイプ	コンポーネントに対するトラフィックの方向	追加情報
A	MMP	NTP サーバ	123	TCP または UDP	発信	
B	MMP	Syslog サーバ	514	TCP	発信	デフォルトのポート、MMP で別のポートを設定可能
C1	MMP	SNMP サーバ	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	53	TCP または UDP	発信	
	Call Bridge	CDR 受信デバイス		TCP	発信	Web 管理インターフェイスで CDR 受信者の URI を設定するか、 /system/cdrReceivers/ の API オブジェクトを使用して API

### B.3 Meeting Serverのコンポーネントを使用する

表 23 を使用して、Meeting Serverのコンポーネントに接続するために使用するポートと、ファイアウォールを通して開く必要があるポートを特定します。

表 23 : Meeting Serverコンポーネントを使用するために開くポート

code	コンポーネント	接続先	開く接続先ポート	トラフィックタイプ	コンポーネントに対するトラフィックの方向	追加情報
H	Call Bridge	サードパーティ SIP レコーダー	5060	TCP (SIP)	発信	
			5060	UDP (SIP)		
			5061	TLS (SIP)		
H1	Call Bridge	サードパーティ SIP レコーダー		Media	発信	サードパーティ SIP レコーダーにより決定されるポート
			32768-65535	UDP (STUN, RTP, BFCP)	着信	

code	コンポーネント	接続先	開く接続先ポート	トラフィックタイプ	コンポーネントに対するトラフィックの方向	追加情報
I	Call Bridge	レコーダー/ ストリーマー	5060	TCP (SIP)	発信	MMP を通じて構成可能なポート。ローカルレコーダーの場合は、ループバック インターフェイスを使用しません。例えば、lo : 8443
			5061	TLS (SIP)		
			5060	TCP (SIP)	着信	
			5061	TLS (SIP)		
I1	Call Bridge	レコーダー/ ストリーマー	32768- 65535	Media	発信	
			32768- 65535	UDP (STUN, RTP, BFCP)	着信	
I2	レコーダ	ネットワーク ファイルサー バー NFS				MMP コマンドレコー ダー nfs <host- name/IP<directory> を 使用して、NFS 上のど こに録画を保存するか を指定します。
I3	ストリーマ ー	ストリーマク ライアント	1935	RTMP	発信	
J	Call Bridge	LDAP/LDAPS (アクティブデ ィレクトリ)	389/636 (メモ 1)	TCP/TCP (SIP TLS)	発信	ポート設定可能 Web 管理インターフェース を通じて
K	Call Bridge	内部の登録済 み SIP エンド ポイントまた は音声コール 制御	5060	UDP (SIP), TCP (SIP)	着信および発信	
			5061	TCP (SIP TLS)		
K1	Call Bridge	内部の登録済 み SIP エンド ポイントまた は音声コール 制御	32768- 65535	UDP (STUN, RTP, BFCP)	着信	
L	Call Bridge	Lync FE サーバ/ AVMCU	5061	TCP (SIP TLS)	着信および発信	

code	コンポーネント	接続先	開く接続先ポート	トラフィックタイプ	コンポーネントに対するトラフィックの方向	追加情報
L1	Call Bridge	Lync クライアント、Lync FE サーバ /AVMCU	1024-65535 (メモ 2)	UDP (STUN, RTP)	発信	
			32768-65535	UDP (STUN, RTP)	着信	
			1024-65535 (メモ 2)	TCP (RDP)	発信	
			32768-65535	TCP (RDP)	着信	
M	Call Bridge	Lync Edge サーバ	3478	UDP	発信	
			443	TCP	発信	
M1	Call Bridge	Lync Edge サーバ	32768-65535	UDP (STUN, RTP)	着信	
N	Call Bridge	Web Bridge 3		TCP (C2W)	双方向データフロー	注：クラスタ内のすべての Call Bridge が、すべての Web Bridge に接続する必要があります。
N1	Call Bridge	Web Bridge 3	9999	TCP (C2W)	双方向データフロー	
N2	Call Bridge	[TURN Server]	50000-62000 (メモ 4)	UDP (RTP, STUN)	発信	ファイアウォールはリターン UDP トラフィックを許可する必要があります
P	Web Bridge 3	Expressway	443	TCP (HTTPS)	着信および発信	
			80	TCP (HTTP)	着信	HTTP 用のオプションポート 80 > HTTPS リダイレクト
P1	Call Bridge	Expressway	1024-65535	UDP (STUN, RTP)	着信および発信	ポート 3478 は常に使用されており、エフェメラルポートは通話ごとの必要に応じて範囲内で割り当てられます
P2	Web Bridge 3	Cisco Meeting Server web app	443	TCP (HTTPS)	着信および発信	HTTP 用のオプションポート 80 > HTTPS リダイレクト
P3	TURN サーバ	Cisco Meeting Server web app	3478 (メモ 3)	UDP (RTP, STUN)	着信	ファイアウォールはリターン UDP トラフィ

code	コンポーネント	接続先	開く接続先ポート	トラフィックタイプ	コンポーネントに対するトラフィックの方向	追加情報
			(メモ 4)			ックを許可する必要があります
P4	Call Bridge	Cisco Meeting Server web app	1024-65535	メディア TCP/UDP (STUN RTP)	着信および発信	
Q	Call Bridge	データベース				ミーティングサーバ内部で、ファイアウォールのポートを開放する必要はありません

## 注：

メモ 1：この機能ではポート 636 (セキュア) および 389 (非セキュア) が一般的に使用されますが、ポートはウェブ管理インターフェイスから設定することができます。同じことが 3268 および 3269 (非セキュアおよびセキュア) グローバル カタログ LDAP 要求にも適用されます。

メモ 2：正確な範囲は Lync サーバーの構成により異なります。

メモ 3：管理者はオプションで、TURN に対して 3478 TCP または別の TCP ポートを有効にすることができます。

メモ 4：TURN とメディアの範囲は、ウェブ アプリが TURN リレーを割り当て、このガイドに記載されているように、Call Bridge が TURN リレーを作成しないことを想定しています。

## B.4 スケーラビリティとレジリエンスに必要な追加ポート

図 50：スケーラブルでレジリエンスのある複数サーバーの展開には、開く必要がある追加のポート

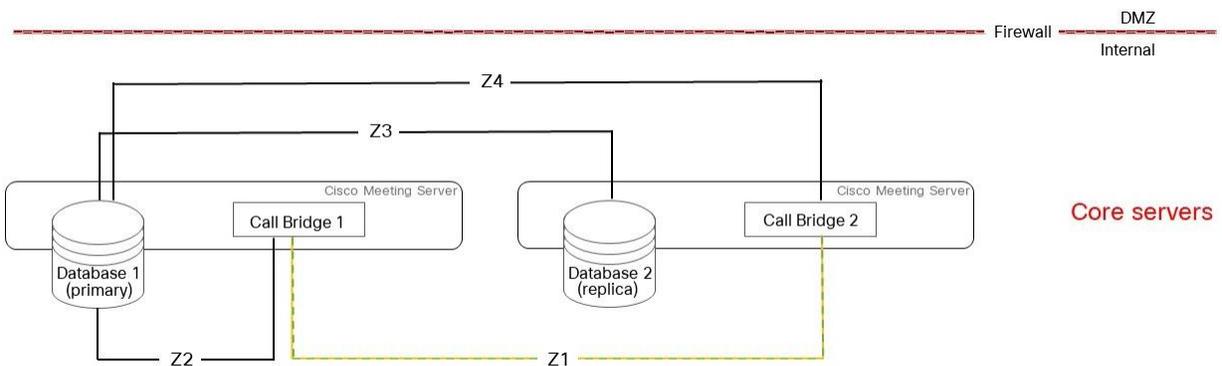


表 24 : スケーラブルでレジリエンスのある複数サーバーの導入で開く必要がある追加のポート

code	コンポーネント	接続先	開く接続先ポート	トラフィックタイプ	コンポーネントを基準にしたトラフィックの方向	追加情報
Z1	Call Bridge 1	Call Bridge 2	443	TCP	着信および発信	Call Bridge クラスタリング用
Z1	Call Bridge 1	Call Bridge 2	5060	TCP/UDP (SIP)	着信および発信	図 50 は、Call Bridge 間の SIP のダイレクトフローとメディアトラフィックを示します。すべての SIP 通話は、コール制御 (CUCM または VCS) を介して実行できることに注意してください。また、メディアは、展開内の Turn サーバを含む他のデバイスを通じて流れることもできます。
Z1	Call Bridge 1	Call Bridge 2	5061	TCP (SIP) TLS	着信および発信	
Z1	Call Bridge 1	Call Bridge 2	32768-65535	UDP (SIP) BFCP	着信	
Z1	Call Bridge 1	Call Bridge 2	1024-65535 (メモ 1)	UDP (SIP) BFCP	発信	
Z1	Call Bridge 1	Call Bridge 2	32768-65535	UDP STUN/RTP	着信および発信	
Z2	Call Bridge 1	データベース 1 (プライマリ)	該当なし	TCP		
Z3	データベース 1 (プライマリ)	データベース 2 (複製)	5432	TCP	着信および発信	データベースクラスタ / レプリケーションポート
Z4	Call Bridge 2	データベース 1 (主要な)	5432	TCP	着信および発信	

注 :

1) 正確な範囲は遠端によって異なります

## B.5 ループバック上の開放ポート

表 25 に記載されているポートは、ループバック インターフェイスで開いています。

表 25 : ループバックのポート

Port	使用法	注意事項
53	DNS	
123	NTP	
1234	HTTP	Cisco Meeting Server 2000 には適用されません

Port	使用法	注意事項
2829, 2830	サーバからメディアへの内部接続	
3521	configd	
5432	postgres	
5060	SIP	常に開いている
5061	暗号化された SIP	証明書が Call Bridge に適用されている場合のみ
5070	BFCP	IPv6 のみ
8080	HTTP	常に開いている
8081	HTTP	Webadmin が有効な場合
3478	STUN	

# 付録 C クラスタ内で Call Bridge ライセンスを共有する

---

**注：**この項は従来のライセンス方法にのみ適用されます。

---

この項では、Call Bridge クラスタに必要なライセンスをすでに購入しており、PAK コードを受け取っていることを前提としています。

---

**注：**個々の Call Bridge に対してライセンス ファイルが必要です。ライセンスは、同じクラスタ内のサーバ間でのみ共有できます。各ライセンスファイルには、そのクラスター用に購入した必須機能がすべて含まれている必要があります。PMP Plus、SMP Plus、録画、ストリーミングなど。

---

**注：**ACU は、Meeting Serverバージョン 3.0 以降でサポートされていません。

---

## C.1 Cisco Meeting Serverのアクティベーション PAK コードの登録

次の手順に従って、Call Bridge クラスタを登録し、ライセンスを取得します。[Cisco License 登録ポータルを使用する](#)：

1. Call Bridge クラスタで使用される Meeting Server ノードの 1 つの MAC アドレスに対して、Meeting Server アクティベーション PAK コードを登録してください。このプライマリノード用の Call Bridge、TURN サーバ、および Web Bridge のライセンスが含まれた単一の cms.lic ファイルを受け取ります。
2. ステップ 1 で使用したのと同じ MAC アドレスに対して、残りの PAK コードをクラスターに登録してください。PAK コードは、クラスター用に購入した機能 (ブランディング、SMP Plus、PMP Plus、録画、ストリーミングなど) に関連付けられます。複数の PAK コードがある場合、PAK コードを登録するたびに、新しい cms.lic ファイルを受け取るようになります。この新しいファイルは、以前のファイルを集約したものです。

---

**注：**cms.lic をテキストエディタで開いて、購入した機能を確認できます。

---

3. すべての機能を登録したら、クラスタ内の他の Call Bridge を登録する必要があります。Call Bridge クラスタで使用される Meeting Server ノードの各 MAC アドレスに対して、Meeting Server アクティベーション PAK コードを登録してください。各セカンダリノードの cms.lic ファイルを受け取ります。

### C.1.1 クラスター全体で機能ライセンスを共有する

4. プライマリ ノードに登録された機能ライセンスを他のセカンダリ ノードと共有する必要があります。ステップ 3 で登録した Meeting Server の各ノードについて、以下のステップ a から k を実行します。
  - a. ライセンス登録ポータルで、[ライセンス] タブを選択し、[ライセンスの移動] > [ライセンスの共有] > [アクティベーションコードの取得] に移動します。

PAKs or Tokens | Licenses | Devices | Transactions History

Get Licenses ▾ | Move Licenses ▾ | Download Licenses | Email Selected Licenses | Export to CSV | Show Filters

<input type="checkbox"/>	License	Type	Device	Quantity
<input type="checkbox"/>	Cisco Meeting Server (CMS) PAK SKU:LIC-CMS-PAK PAK:FPPAIT	Perpetual Created: 03/02/2018	MAC Address:00:11:22:33:44:AB Family:Cisco Meeting Server (Acano)	1
<input type="checkbox"/>	Cisco Meeting Server (CMS) PAK SKU:LIC-CMS-PAK PAK:FP98BRTCLOUD	Perpetual Created: 03/02/2018	MAC Address:00:11:22:33:44:AB Family:Cisco Meeting Server (Acano)	1
<input type="checkbox"/>	SKU:LIC-TP-SMP-DEMO-10	Demo 03/28/2017-06/26/2017	Serial Number:09BF8838 Family:TelePresence Conferencing D...	3
<input type="checkbox"/>	SKU:L-5300-4PL-DEMO	Demo 10/28/2015-01/26/2016	Serial Number:FOC1841P1UN Family:TelePresence Conferencing D...	10

- b. Cisco Meeting Server を選択し、ソースデバイス MAC アドレス : フィールドに最初のノードの MAC アドレスを入力します。
- c. ターゲットデバイス MAC アドレス : フィールドに他のノードの MAC アドレスを入力します。送信先 フィールドにメールアドレスを入力します。

Show: All Licenses for Rory Betteridge ▾

PAKs or Tokens | Licenses | Devices | Transactions History

Get Licenses ▾ Move

<input type="checkbox"/>	License
<input type="checkbox"/>	Cisco Meeting S SKU:LIC-CMS-PA PAK:FP998RTCL
<input type="checkbox"/>	Cisco Meeting S SKU:LIC-CMS-PA PAK:FP998RTCL
<input type="checkbox"/>	SKU:LIC-TP-SMP
<input type="checkbox"/>	SKU:L-5300-4PL-I

### Share License Process

Apply the licensed features of an existing device to additional devices. If intending to use an activation code but find it has expired, request another code.

- Product: Cisco Meeting Server (Acano) ▾
- Source Device MAC Address: 00:11:22:33:44:AB
- Target Device MAC Address: 11:22:33:44:55:AB
- Send to:

d. 共有ライセンス アクティベーション コードの確認メッセージが表示されます。

**Shared License Activation Code Confirmation**

The request for an activation code has been successfully submitted.  
Email confirmation will be sent to these email addresses - rorbette@cisco.com  
[Please provide feedback...](#)Let Cisco know how to improve this experience.

- e. ステップ c で入力したターゲット ノードのアクティベーション コードをメールで受信します。

PLEASE DO NOT DISCARD THIS EMAIL.

You have received this email because your email address was provided to Cisco Systems during the registration pr

Below, you will find the Activation Code:  
Activation Code : 8NF7R5E1

Here is the device registration information:  
Existing Device Serial # : 00:11:22:33:44:AB  
New Device Serial # : 11:22:33:44:55:AB

Please click the below link and follow the instructions given below to continue the registration process:

<https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Quickstart>

- 1) Click on Other Licenses drop down and Select 'Share License Process' option.
- 2) Select 'Use Activation code' option and Enter the above activation code in 'Specify Activation Code' tab and

- f. [ライセンス] タブに戻り、[ライセンス共有] > 移動ライセンス > アクティベーションコードを使用します。
- g. e で受け取ったアクティベーションコードを入力して、[次へ] をクリックします。

**Share License Process**

1. Specify Activation Code | 2. Select SKU Options | 3. Review

**Recipient and Owner Information**

Enter multiple email addresses separated by commas. Your License Key will be emailed within the hour to the specified email addresses.

Add...

Send To:

End User:  Edit..

**License Request**

Apply the licensed features of an existing device to additional devices. If intending to use an activation code but find it has expired, request another code. The license information that will be submitted.

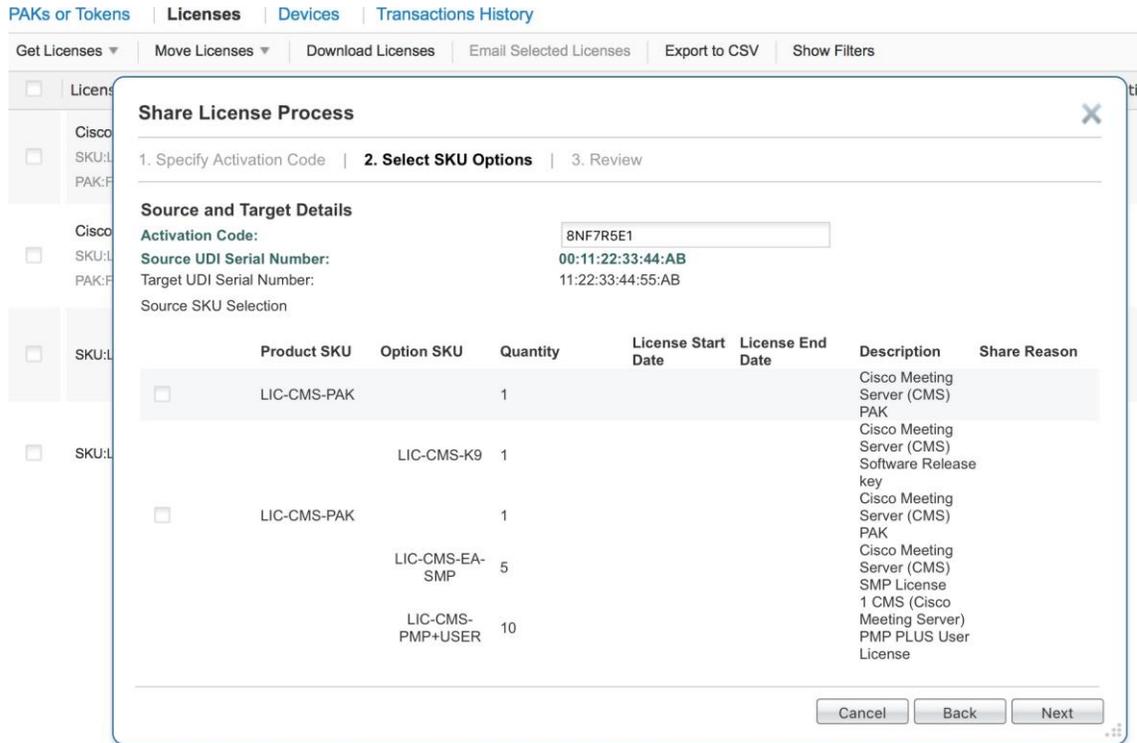
SKU	Feature	Description	License Start Date	License End Date	Quantity
LIC-CMS-PAK		Cisco Meeting Server (CMS) PAK			1
LIC-CMS-PAK		Cisco Meeting Server (CMS) PAK			1

I Agree with the [Terms of the License Agreement](#)

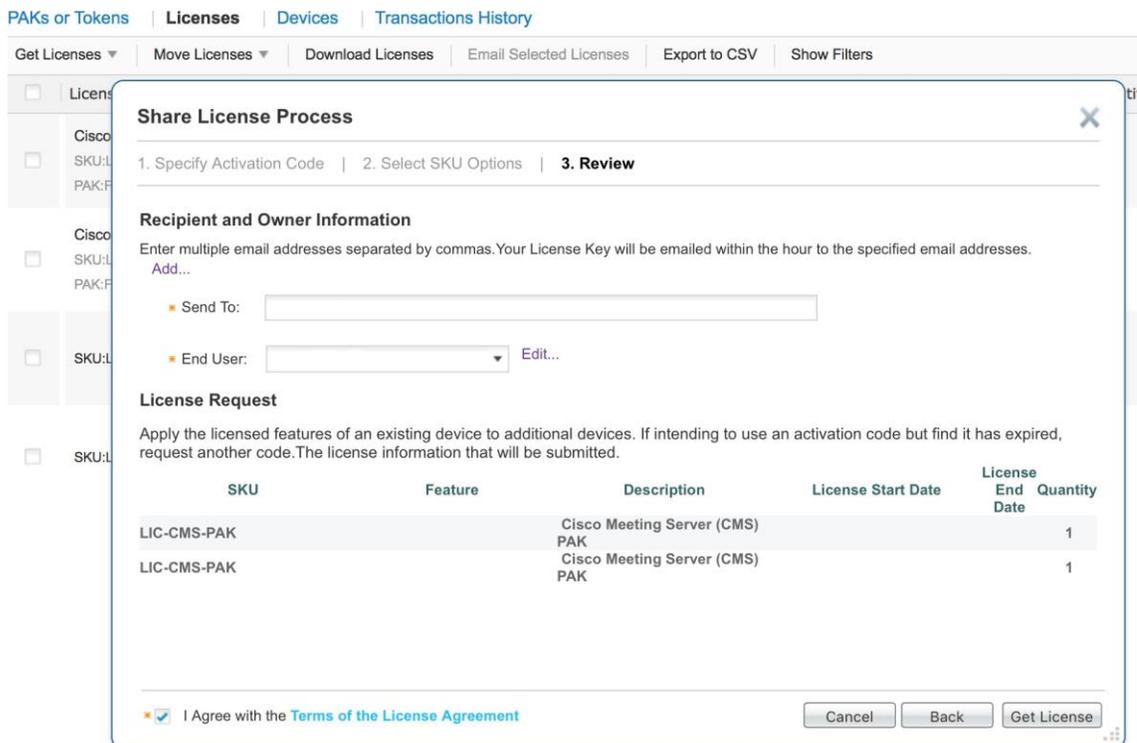
Cancel Back Get License

- h. ステップ 2 で登録した機能のボックスにチェックを入れ、[次へ] をクリックします。

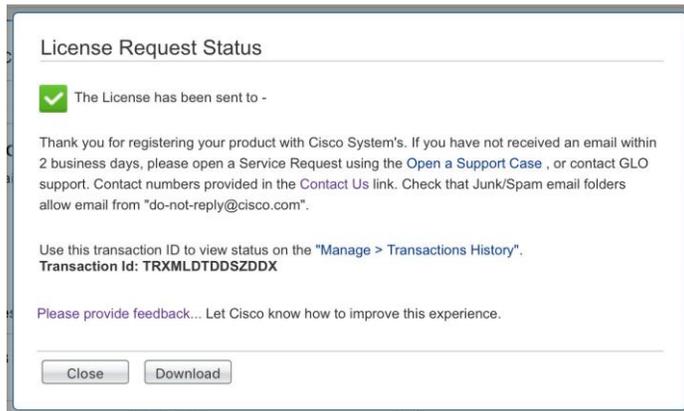
**注意：**このセカンダリノードはすでに登録されているため、ソフトウェアリリースキーのボックスにチェックを入れる必要はありません。



- i. このセカンダリノードのライセンスを受け取るメールアドレスを入力します。画面下部の [使用許諾契約 に同意する] にチェックを入れます。[ライセンスを取得] をクリックします。



- j. ライセンスのリリースに問題がある場合に備えて、「トランザクション ID」をメモするようにしてください。



- k. このセカンダリノード用の新しい cms.lic ファイルがメールで送信されます。このファイルには、この Meeting Server 上の Call Bridge、TURN サーバ、および Web Bridge のライセンス、および登録された機能が含まれています。
5. **オプションの手順**：各セカンダリノードで手順 4a から 4k を完了した後、ライセンスをスマートアカウントに割り当てることができます。これにより、組織全体で Cisco ライセンスを簡単に管理、コントロールできます。スマートアカウントには、Cisco ライセンス登録ポータル の **デバイス** タブからアクセスできます。

PAKs or Tokens		Licenses	Devices	Transactions History	
Get Licenses ▾	Move Licenses ▾	Add Devices	Download Licenses	Email Selected Licenses	
		Smart Accounts ▾	Export to CSV	Show Filters	
<input type="checkbox"/>	Device	Smart Account	Family	Features	Quantity
<input type="checkbox"/>	MAC Address: [redacted]	[redacted]	Cisco Meeting Server (Acano)	webbridge	1
				turn	1
				recording	+4 1
<input type="checkbox"/>	MAC Address: [redacted]	-	Cisco Meeting Server (Acano)	recording	1
				shared	5
				branding	+1 1
<input type="checkbox"/>	MAC Address: [redacted]		g Server (Acano)	webbridge	1
				recording	1

## C.2 既存の Call Bridge クラスタへのライセンスの追加

新しく取得した PAK コードを、ステップ 1 で詳述したように、Meeting Server の MAC アドレスの 1 つに登録します。これは任意のノードで行うことができます。この操作により、新しいライセンスが既存のライセンスに追加されます。その後、ステップ 4 を繰り返して、クラスタ全体で新しいライセンスを共有する必要があります。

## 付録 D クラスタリング解除

### D.1 Call Bridge のアンクラスタリング

一部の Call Bridge をクラスタ化して、データベース クラスタにアクセスすることができます。ただし、Call Bridge クラスタにない Call Bridge はクラスタ データベースにアクセスできず、ローカル データベースを使用します。

1. クラスタから Call Bridge を削除します。
  - a. その Call Bridge のコアサーバーでウェブ管理インターフェイスにログインし、次の場所へ移動します。**構成 > クラスタ**。
  - b. Call Bridge のエントリの隣にあるチェックボックスを選択し、**削除する**。  
これにより、その Call Bridge が Call Bridge クラスタから外されます。
2. 次に、データベースクラスタから共有データベースを削除します（ある場合）。
  - a. Call Bridge サーバーの MMP にログインします。
  - b. **データベースクラスタを削除する** コマンドを入力してください。

データベースはデータベース クラスタから切断されており、スペース データベース クラスタのコンテンツには、このコア サーバ上の Call Bridge はアクセスできません。ただし、元のデータベースのコンテンツには再びアクセス可能になります。（クラスタ化されたデータベースのコンテンツと比較すると古い場合があることに注意してください。）

## 付録 E Cisco Meeting Server プラットフォーム別の通話容量

表 26 以下では、後のソフトウェアバージョンにアップグレードすることで Meeting Server の最大コールキャパシティの詳細を示しています。Call Bridge グループ内の負荷分散コールと比較して、単一またはクラスターの Meeting Server には異なる容量があることに注意してください。

表 26 : クラスターと Call Bridge グループの Meeting Server の通話キャパシティ

Cisco Meeting Server プラットフォーム		Cisco Meeting Server 1000 M5v2 (ノードあたり)	Cisco Meeting Server 1000 M6 (ノードあたり)	Cisco Meeting Server 1000 M7 (ノードあたり)	Cisco Meeting Server 2000 M5v2 (ノードあたり)	Cisco Meeting Server 2000 M6 (ノードあたり)
個人 Meeting Server または会議サーバはクラスター (注 1、2、3、4) および	1080p30	60	80	120	437	648
	720p30	120	160	240	875	1296
Call Bridge グループの Meeting Server	SD	240	320	480	1250	1875
	音声通話	2200	3000	3000	3000	3200
Call Bridge グループの Meeting Server	会議あたりサーバあたり HD 参加者数	120			450	
	web app のコールキャパシティ (内部通話 外線通話 (CMS ウェブ上) エッジ):					
Call Bridge グループの Meeting Server	フル HD	60	80		437	648
	HD	120	160		875	1296
	SD	240	320		1250	1875
	音声通話	500	500		1250	1875
Call Bridge グループの Meeting Server	サポートされているコールタイプ					
	読み込み制限	120,000	160,000		875,000	1,296,000

**注意点：**

- クラスタあたり最大 24 個の Call Bridge ノード。8 個以上の Call Bridge ノードのクラスタ設計はシスコによる承認が必要です。詳細についてはシスコ サポートにお問い合わせください。
- Call Bridge グループが設定されていないクラスタ化された Cisco Meeting Server 2000 は、最大通話数の整数倍（たとえば、700 HD 通話の整数倍）をサポートします。
- クラスタあたり最大 21,000 HD 同時通話（24 ノード x 875 HD 通話）は、SIP またはウェブアプリの通話に適用されます。
- クラスタ内の Meeting Servers プラットフォームに応じて、クラスタあたり会議あたり最大 2600 人の参加者。
- 表 26 では、ビデオコールについては最大 2.5 Mbps-720p5 コンテンツ、音声コールについては G.711 のコールレートを想定しています。他のコーデックおよび高いコンテンツ解像度/フレームレートを使用すると、容量が減ります。ミーティングが複数の Call Bridge にまたがる場合、分散リンクが自動的に作成され、サーバーの呼び出しカウントとキャパシティに対してカウントされます。読み込み制限値は H.264 のみに対するものです。
- クラスタでサポートされている通話セットアップレートは、SIP 通話で 1 秒あたり最大 40 通話、Cisco Meeting Server web app 通話で 1 秒あたり最大 20 通話です。
- クラスタあたり最大 16,800 HD 同時通話（24 ノード x 700 HD 通話）は、SIP またはウェブアプリの通話に適用されます。
- バージョン 3.2 以降、Meeting Server は、Meeting Server 1000 M5v2 および Meeting Server 2000 M5v2 ハードウェア バリエーションでの通話容量の増加をサポートします。
  - Meeting Server 1000 M5v2 の負荷制限が 96,000 から 120,000 に増加しました。720p ビデオコールに対する Meeting Server 1000 のコールキャパシティは、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 の負荷制限が 700,000 から 875,000 に増加しました。720p ビデオコールに対する Meeting Server 2000 のコールキャパシティは、新しいプラットフォームで 700 から 875 に増加しました。
- 表 26 では、ビデオコールについては最大 2.5 Mbps-720p5 コンテンツ、音声コールについては G.711 のコールレートを想定しています。他のコーデックおよび高いコンテンツ解像度/フレームレートを使用すると、容量が減ります。ミーティングが複数の Call Bridge にまたがる場合、分散リンクが自動的に作成され、サーバーの呼び出しカウントとキャパシティに対してカウントされます。読み込み制限値は H.264 のみに対するものです。
- Meeting Server 1000 M7 バリエーションは、最大 94 個の vCPU と 128 GB の RAM をサポートします。

## E.1 Cisco Meeting Server web app のコールキャパシティ

この項では、外線および混合通話に Web Bridge 3 とウェブ アプリを使用した展開の通話容量について詳しく説明します。(内線通話容量については、表 26 を参照してください。)

### E.1.1 Cisco Meeting Server web app のコールキャパシティ - 外線通話

Expressway (Large OVA または CE1200) は、中規模のウェブ アプリのスケール要件を持つ展開 (つまり、800 コール以下) に推奨されるソリューションです。Expressway (中規模 OVA) は、小規模なウェブ アプリスケール要件を持つ導入 (つまり、200 コール以下) に推奨されるソリューションです。ただし、より大きなウェブ アプリのスケールが必要な導入では、バージョン 3.1 以降、SIP 容量にスケールアップする必須のソリューションとして、Cisco Meeting Server ウェブエッジを推奨します (表 26 を参照)。

外部発信では、クライアントが Cisco Expressway をリバースプロキシと TURN サーバーとして使用して、Web Bridge と Call Bridge に到達します。

Expressway を使用してウェブ アプリの通話をプロキシする場合、Expressway は、表 27 に示すように、最大通話数制限をかけます。

---

**注：** Web Bridge 3 およびウェブ アプリを導入する場合、Expressway バージョン X14.3 以降を使用する必要があります。以前の Expressway バージョンは Web Bridge 3 ではサポートされません。

---

表 27 : Cisco Meeting Server web app 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 Platform	大規模 OVA Expressway	中規模 OVA Expressway
Cisco Expressway ごと ( X14.3 以降)	フル HD	150	150	50
	その他	200	200	50

Expressway 容量は、Expressway ペアをクラスタ化することで増やすことができます。Expressway ペア クラスタリングは最大 6 ノードまで可能で (4 はスケーリングに、2 は冗長性に使用されます)、合計コール キャパシティはシングル ペア キャパシティの 4 倍になります。

---

**注：** Expressway クラスタの通話セットアップ レートは、Cisco Meeting Server web app の通話で 1 秒あたり 6 通話を超えてはなりません。

---

### E.1.2 Cisco Meeting Server web app の容量 - 混合 (内部 + 外部) 通話

スタンドアロン導入とクラスタ導入の両方で、組み合わせた内部と外部の通話使用をサポートできます。内部と外部の参加者が混在する場合、ウェブ アプリの合計容量は内線通話については付録 E に従いますが、外部から接続できる合計内の参加者数は表 27 の制限を受けます。

例えば、単一の大規模 OVA Expressway ペアを持つ単一のスタンドアロン Meeting Server 2000 は、1000 の音声のみのウェブアプリ コールの混在をサポートしますが、外部の参加者の数は、合計 1000 のうちの最大 200 に制限されます。

## E.2 Cisco Meeting Server でサポートされるユーザー数

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に応じて最大 300,000 人のユーザをサポートできます。クラスタ中のすべてのデータベースは、同じスペックサーバ上になければなりません。

表 28 : Cisco Meeting Server でサポートされるユーザー数

Cisco Meeting Server	ユーザーの発信者最大数
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

**メモ：**多数のユーザーを LDAP 同期すると、通話参加時間が長くなる可能性があります。メンテナンス期間中またはオフピーク時に、Meeting Serverに新しいユーザー/スペースを追加することをお勧めします。

# 付録 F 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、および VM ソフトウェアイメージ用のアクティベーションキーを購入するときは、SIP メディア暗号化を有効にするか無効にするか（暗号化されていない SIP メディア）から選択できます。ソフトウェア PID R-CMS-K9 および R-CMS-2K-K9 の下で、暗号化または非暗号化オプションのいずれかを選択します。メディアには、音声、ビデオ、コンテンツビデオ、および ActiveControl データが含まれます。

---

**注：** SIP メディア暗号化を無効にしてアクティベーション キーをアップロードしない限り、現在の Call Bridge アクティベーションは影響を受けません。

---

## F.1 非暗号化 SIP メディア モード

「SIP メディア暗号化が無効」のアクティベーションキーが Meeting Server にアップロードされると、以下のことが起こります。

- Meeting Server と SIP デバイス間で送信されるメディアは暗号化されていません
- クラスタ化された Call Bridge 間の配信リンクを介して送信されるメディアは暗号化されていません
- コールシグナリングは暗号化されたままです
- プラットフォームを問わず、Meeting Server とウェブアプリ間の通話のメディアは暗号化されたままです
- 次の API オブジェクトで、sipMediaEncryption パラメータが **許可しない** 以外に設定されている場合、エラーメッセージが返されます

/calls/<call id>/participants

/calls/<call id>/callLegs

/callLegs/<call leg id>

/callLegProfiles および /callLegProfiles/<call leg profile id>

/callLegs/<call leg id>/callLegProfileTrace

- エラーメッセージが表示されます、SIP **メディア暗号化** フィールドが **設定>Web 管理インタフェースの通話設定** ウェブページで、**無効**以外に設定されている。

---

**注：** SIP メディア暗号化が無効になっている場合でも、必要に応じて sipControlEncryption パラメータを設定することで、発信通話で暗号化することができます。/**アウトバウンドダイヤルプランルール**。

---

## F.2 Call Bridge メディア モードの決定

Call Bridge が暗号化または非暗号化 SIP メディア使用のどちらを使用するかを決定するには、Web 管理インターフェイスを使用し、**設定** を選択し、次に API を選択します：

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

**機能オブジェクト** callBridgeNoEncryption のステータスが **アクティベート済み** に設定されている場合、非暗号化メディア用のアクティベーション キーが Call Bridge にロードされます。callBridgeNoEncryption のステータスに対する他の有効な設定は **ライセンスなし**、**猶予期間**、**または期限切れ** です。

callBridgeNoEncryption にも、文字列形式の expiry フィールドがあります。

## 付録 G デュアルホーム電話会議

### G.1 概要

デュアルホーム電話会議は、Lync でスケジュールされたミーティングおよび Lync のドラッグアンドドロップスタイルのミーティング (アドホック コールとも呼ばれる) で、Lync クライアント ユーザーとウェブ アプリ ユーザーの両方のユーザーエクスペリエンスも改善します。Lync 参加者は、ドラッグアンドドロップを使用してウェブ アプリ ユーザーを Lync ミーティングに追加でき、電話会議コントロールを使用してウェブ アプリ ユーザーをミュートまたは切断できます。Lync でスケジュールされた電話会議に参加するウェブ アプリ ユーザーには、ウェブ アプリ ユーザーからのビデオだけでなく、最大 5 人の Lync 参加者からのビデオが表示されます。Lync ユーザーには、すべてのウェブ アプリ ユーザーおよびミーティングの Lync ユーザーのビデオがギャラリー形式で表示されます。Lync ユーザーとウェブ アプリ ユーザーの両方が、ミーティングの参加者を組み合わせた完全なリストを受け取ります。

---

**注：**アドホックのデュアルホーム電話会議では、Lync/Skype for Business クライアントの [参加者の追加] ボタンは機能しません。回避策として [今すぐミーティング] ボタンを使用しないでください。これにより、Meeting Server と AVMCU 間のアクティブな通話が残ることになります。

---

Lync の参加者は、Meeting Server スペースに直接ダイヤルするか、またはドラッグアンドドロップを使用して Meeting Server スペースを Lync ミーティングに追加できます。これらは、Lync ユーザーが参加したい Cisco Meeting Server スペースで大規模なミーティングが開催されている場合に便利です。1 つ目のケースでは、複数の参加者で設定されたレイアウトを受信します。Lync ミーティングに完全なスペースを追加すると、Lync ユーザーはスペース (主発言者) から 1 つのビデオ ストリームのみを受信し、完全に統合された参加者リストを受信しません。通常どおり、Lync 参加者を追加できます。

---

**注：**Expressway X8.11 を Meeting Server のエッジとして使用する場合、少なくとも一部の Microsoft トラフィックがクラスタ内の Meeting Server と Microsoft インフラストラクチャとの間で直接流れない限り (かつ Expressway を経由しない)、Meeting Server クラスタを持つデュアルホーム電話会議は現在サポートされていません。デュアルホーミングは、スタンドアロン Meeting Server のエッジとして Expressway X8.11 でサポートされます。

---

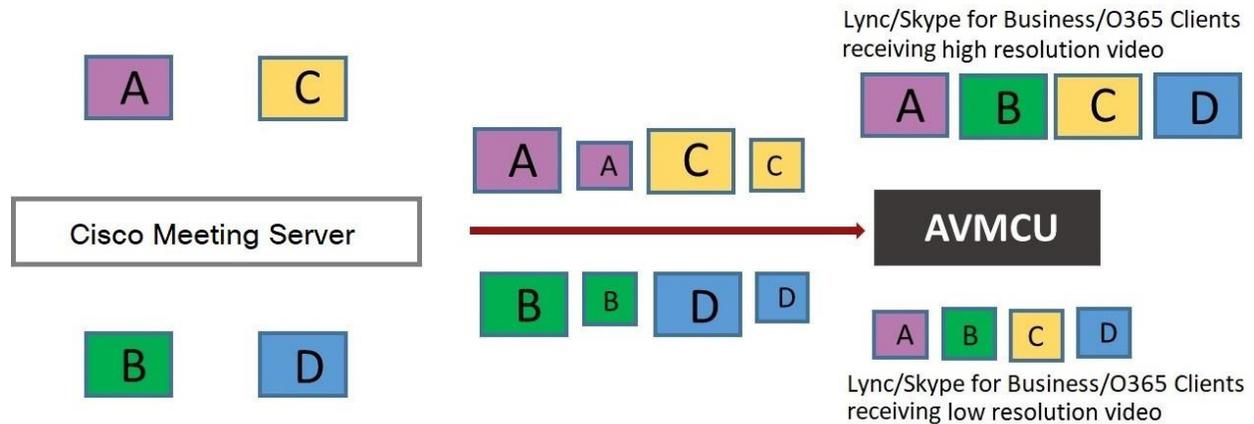
### G.2 デュアルホーム会議で一貫したミーティング エクスペリエンス

Meeting Server は、ビデオ参加者ごとに 2 つの H.264 ビデオストリームを AVMCU に送信します。高解像度ビデオストリームと低解像度ビデオストリームです。図 25 を参照してください。Lync、Skype for Business、および O365 クライアントは高解像度をサポートし、高品質ビデオ ストリームをサブスクライブし、受信します。帯域幅制限、ウィンドウ サイズ、レイ

アウト、CPU 性能、またはモバイル デバイスを使用しているために、より低い品質を選択するクライアントは、より低い品質のストリームをサブスクライブおよび受信し、ビデオ品質を低下させたり、他の参加者のビデオ エクスペリエンスを低下させたりしません。

**注：** SIP トランクの帯域幅は、2 つのビデオストリームを配信するのに十分に高く設定してください。LAN には 8MB、WAN には 2.5MB を推奨します。

図 51 : AVMCU へのデュアルメディアストリーム



**注：** Microsoft RTVideo を使用する端末ではこの機能から利益を得ることはありません。

### G.2.1 ユーザエクスペリエンスの要約

デュアル ホーム電話会議と RDP および複数のビデオ エンコーダーのサポートを組み合わせることで、Lync とウェブ アプリ ユーザーの両方によりリッチなミーティング エクスペリエンスを提供します。

- Lync クライアント ユーザーとウェブ アプリ ユーザーの両方に、使い慣れた画面レイアウトが表示されます。
- Lync クライアント ユーザーとウェブ アプリ ユーザーの両方は、接続している場所に関係なく、ミーティングのすべての参加者をまとめた完全なリストを受け取ります。
- Lync クライアントのユーザーには、SIP エンドポイントとウェブ アプリからのビデオで非正方形のアスペクト比が表示されます。
- Lync クライアントのユーザーには、メインのビデオ領域ではなく、画面の別の領域にコンテンツが表示されます。
- Meeting Serverは、Lync ミーティングの各参加者がサポートする最高品質のコーデックを使用してビデオを送信します。これにより、参加者が複数の Lync クライアントバージョンを使用する場合に、ミーティングのすべての Lync クライアントユーザーのエクスペリエンスが最適化されます。

- Meeting Server は、高解像度ビデオストリームと低解像度ビデオストリームの 2 つの H.264 ビデオストリームをビデオ参加者ごとに AVMCU に送信します。これは、低解像度しかサポートできないクライアントがミーティングに参加した場合でも、高解像度をサポートするクライアントに対する高解像度体験を維持するためです。
- チャットは、スペースのウェブアプリユーザーとの Lync AVMCU 電話会議、およびウェブアプリユーザーと Lync クライアント間の直接通話で機能します。

---

**注：**ミーティング中に最高のユーザエクスペリエンスを得るには、Lync 2013、Skype for Business 2015 以降を使用してください。これらのバージョンでは、複数のビデオストリームを Meeting Server に送信できます。これにより、Meeting Server に接続しているエンドポイントまたはウェブアプリユーザーが複数の Lync 参加者を表示できます。Lync 2010 は単一の最大発言者ストリームのみを提供します。最大発言者がすでに電話会議の Meeting Server 側にいる場合、ウェブアプリユーザーおよび SIP エンドポイントユーザーは Lync 参加者を表示しません。

---

RDP および複数ビデオエンコーダサポートの詳細については、これらの FAQ を参照してください。

- [RDP サポート](#)、
- [複数のビデオエンコーダのサポート](#)。

### G.3 デュアルホーム会議のミーティングコントロールをミュート/ミュート解除する

Meeting Server ソフトウェアのバージョン 2.4 では、以下のデュアルホーム電話会議でのミーティングコントロールのミュート/ミュート解除が改善されました。

- オンプレミスおよび Office 365 Lync/Skype for Business クライアント、
- エンドポイントユーザ、
- ウェブアプリユーザー。

---

**注：**この項では、Meeting Server の API を使用してミュートおよびミュート解除が有効になっていることを想定しています。

---

#### ミュート/ミュート解除：

- Lync クライアントは、デュアルホーム電話会議では自分自身と他の参加者を含め誰でもミュートおよびミュート解除できます。また、オーディエンスをミュートおよびミュート解除することもできます。
- すべてのエンドポイントユーザーは Lync クライアントをミュートできます。
- AVMCU の Lync 側のエンドポイントユーザーは、自分自身および他のエンドポイント (AVMCU に接続された Lync クライアント/エンドポイントまたは Meeting Server 側)

をミュートおよびミュート解除できます。バージョン 2.4 以前は、AVMCU の Meeting Server 側のエンドポイントユーザーのみが、自分自身と他のユーザーをミュートおよびミュート解除できました。

- 非 ActiveControl エンドポイントの場合、Meeting Server はミュートおよびミュート解除するたびに DTMF キーシーケンスを送信し、エンドポイントへのメディアストリーム上にアイコンをオーバーレイして、エンドポイントがミュートまたはミュート解除されているかどうかを示します。
- CE 9.2.1 以降のソフトウェアを実行している ActiveControl エンドポイントの場合、エンドポイントはアイコンとメッセージを処理します (Meeting Server はアイコンをオーバーレイしません)。
- ActiveControl エンドポイントがミュートされると、ローカルでの会話のプライバシーを確保するために、ローカルでミュート解除する必要があります。たとえば、リモートの参加者が ActiveControl エンドポイントをミュートしてからミュート解除しようとする、ActiveControl エンドポイントはローカルでミュート解除されるまで、自分自身をミュートし続けます。
- リモート参加者が ActiveControl 以外のエンドポイントのミュートを解除しようとする、ActiveControl 以外のエンドポイントのミュートが解除されます。
- ウェブ アプリ ユーザーと Cisco ミーティング管理ユーザーは Lync クライアントをミュートおよびミュート解除できます。また、ミーティングのすべての参加者の正しいミュート状態も表示されます。

#### ミュート/ミュート解除 ウェブ アプリ ユーザー :

- ウェブアプリユーザーのローカルのミュートおよびミュート解除に関する情報は、デュアルホームの電話会議では Lync クライアントに渡されません。しかし、Lync クライアントがウェブアプリのユーザーをリモートでミュートし、ウェブアプリがそれ自体をミュート解除する場合、Meeting Server は Lync クライアントにミュート解除について通知します。
- リモートの参加者がウェブ アプリ ユーザーのミュートを解除しようとする、ウェブ アプリ ユーザーはローカルでミュートされたままになります。注：他の参加者は実際にはミュートされていますが、ミュートされていないように見えます。
- ウェブ アプリは独自のアイコンを使用してミュート/ミュート解除の状態を示します。Meeting Server のアイコンがウェブ アプリのビデオ ペインにオーバーレイ表示されません。

## G.4 デュアルホームの Lync 機能の設定

すでにオンプレミスの Lync 展開または Lync フェデレーションの展開が Meeting Server の展開と連携している場合、Meeting Server で追加の構成を行う必要はありません。

これが新規の導入である場合、Meeting Server 上で Lync Edge 設定を設定していることを確認してください。 [項 1.5](#) を参照してください。

### G.4.1 トラブルシューティング

ユーザーが IVR または「Lync」を解決するダイヤルプランルールを使用して Lync 電話会議に参加できない場合、最初に行うべきことは、「Lync Edge」設定がセットアップされていることを確認することです。Lync 電話会議を解決し、Edge サーバーを見つけるために同じメカニズムが使用されます。Meeting Serverは Lync FE サーバーにクエリを行い、これらの両方を見つける必要があります。

これに失敗した場合、電話会議 ID が見つからないというメッセージがイベントログに記録されます。

#### **lync 電話会議の解決：電話会議 "1234" が見つかりません**

これは、電話会議が存在しないことを意味する場合がありますが、他の原因も考えられます。

SIP トラフィックのトレースが有効な場合、上記のメッセージがログに記録される直前に「SERVICE」メッセージが Lync FE サーバーに送信され、その応答に対して 200 OK が返されます。このメッセージが正しい IP (Lync FE サーバーのものである必要があります) に送信されていることを確認してください。

このメッセージが送信されない場合 (ログに表示されない場合)、Call Bridgeがどこに送信すべきかわからない可能性があります。これは、`_sipinternaltls._tcp.lyncdomain` レコードの DNS SRV ルックアップを使用して Lync サーバーを見つけられないからです。DNS トレースを有効にして再試行することでこれを確認する必要があります。しかし、これは Lync Edge 設定が Meeting Server で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ものの、Lync サーバーが「403 未承認」と応答する場合、最も可能性の高い原因は、この Lync ドメインの発信ダイヤル プラン ルールのローカル連絡先ドメインが正しく設定されていないことです。Meeting Server の FQDN に設定する必要があります。これは、Call Bridge の証明書の CN で提供される FQDN と同じである必要があります。

## 付録 H NAT の背後で TURN サーバーを使用する

TURN サーバーは NAT の背後に導入でき、NAT アドレスは MMP コマンド `turn public-ip` を使用して指定されます。ただし、Interactive Connectivity Establishment (ICE) の仕組みにより、接続が常に機能することを保証するには、NAT の慎重な設定が必要です。

この付録では、ICE の動作原理について説明します。以下の内容について説明しています。

- 候補者を特定する方法、
- 接続性を確認する方法、
- TURN サーバーの前での NAT の影響、
- NAT が外部ウェブ アプリ ユーザーに与える影響。

---

**注：**両方のリレー候補が利用可能なパスにしか含まれていない場合、問題が発生する可能性があります。これにはファイアウォールが正しく設定され、すべてのクライアントがビデオと音声を送受信できるようにする必要があります。

---

### H.1 候補を特定する

ICE は、アドレスとポートの候補のリストを収集し、これらの候補のどのペアがメディアの交換を可能にするかを見つけることによって機能します。複数のペアの候補がある場合、どのペアが使用されるかを決定するために、優先順位スキームが使用されます。

通常、3 つの候補が存在します。

1. ホスト候補
2. サーバリフレクシブ候補
3. リレー候補

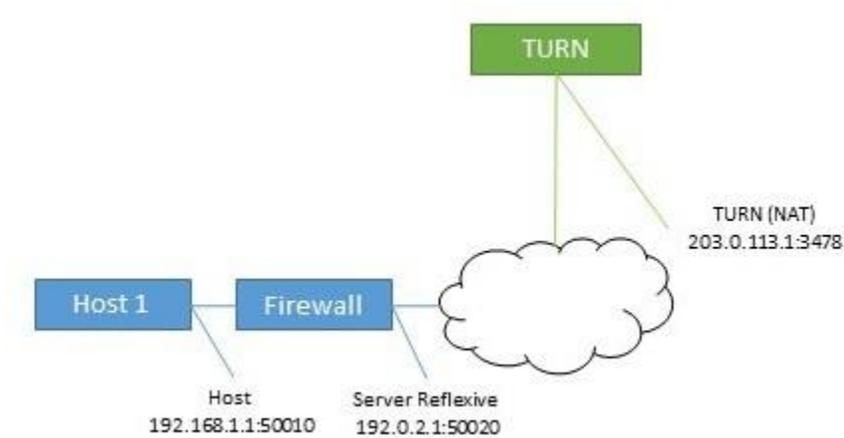
#### H.1.1 ホスト候補

最も単純な候補はホスト候補です。これは、ホスト インターフェイスによって使用されるアドレスです。これは多くの場合、ローカル ネットワーク上にあり、ルーティングできません。

#### H.1.2 サーバリフレクシブ候補

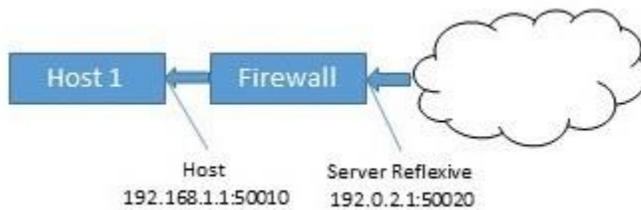
サーバー反射候補は、TURN サーバーが受信パケットが来ると見るアドレスです。これを確認するために、ホストは TURN サーバーの定義されたポート（通常はポート 3478）にパケットを送信し、TURN サーバーはパケットの送信元に関する情報を返信します。

図 52 : Server Reflexive 候補



ホストが NAT を実行するファイアウォールの背後にいる場合、これはホスト候補とは異なります。多くの場合、このポートとアドレスに送信されたパケットはホストに戻されます。

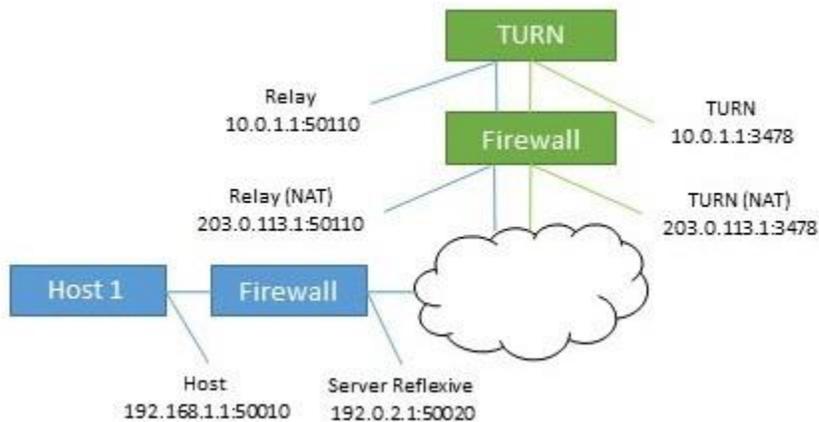
図 53 : ファイアウォールの背後で NAT を実行するホストの影響



### H.1.3 リレー候補

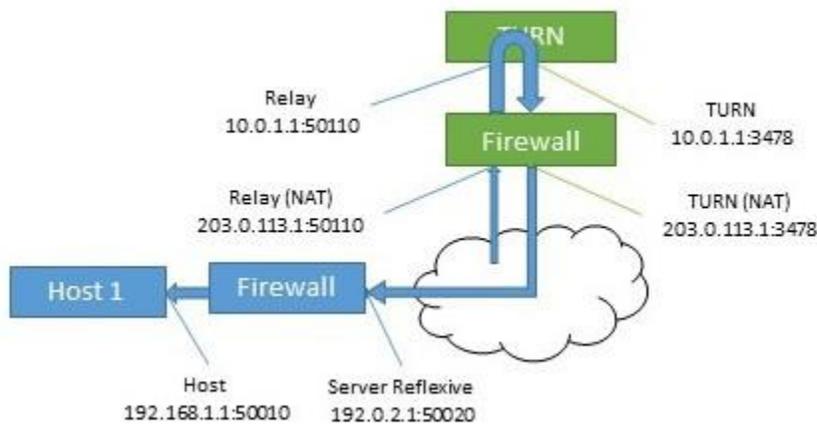
最終的な候補はリレーカンディデートです。この候補は、主催者の要求に応じて TURN サーバーによって作成されます。この候補者の中継アドレスは TURN サーバー インタフェース アドレスです。NAT が使用される場合、中継アドレスは NAT のアドレスに変更されます。

図 54 : リレー候補者



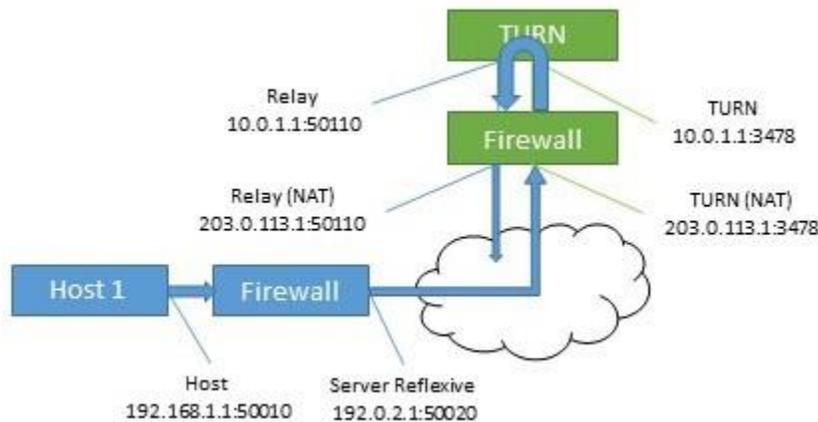
このリレーアドレスに送信されたデータは、TURN サーバ経由で主催者に返されます。

図 55 : TURN サーバーがホストにリレーアドレスを返す



このリレー候補には 2 番目の用途があります。また、遠端にパケットを送信するために、ホストが使用することもできます。これは、他のパスが利用できない場合に発生します。これらのパケットは TURN サーバから送られてくることに注意してください。そのため、ファイアウォールによって書き換えられると、それらは NAT アドレスのみを取得します。

図 56 : 遠端にパケットを送信するホスト



## H.2 接続を確認しています

候補が特定されると、接続性チェックが行われます。各ホストは、遠端のホスト、サーバ反射とリレーアドレスに直接接続しようとします。また、リレーを使用して、同じ遠端候補への接続を試みます。

表 29 : 2 人のホストの候補 (同じ TURN サーバーを使用)

ホスト	Type	アドレス : ポート
1	ホスト	192.168.1.1 : 50010
1	サーバリフレクシブ	192.0.2.1 : 50020
1	リレー	203.0.113.1 : 50110
2	ホスト	172.16.1.1 : 50100
2	サーバリフレクシブ	198.51.100.1 : 50040
2	リレー	203.0.113.1 : 50510

表 30 : ホスト 1 により形成された候補のペア

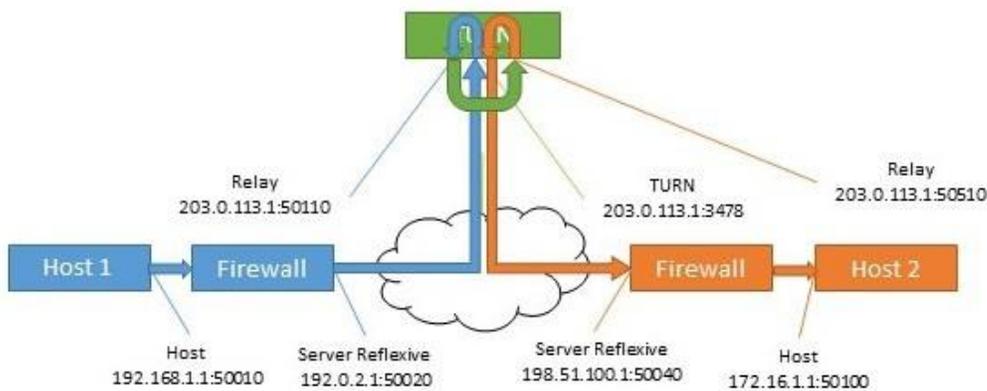
ソース (Source)	接続先タイプ	接続先アドレス
ホスト (192.168.1.1:50010)	ホスト	172.16.1.1:50100
ホスト (192.168.1.1:50010)	サーバリフレクシブ	198.51.100.1:50040
ホスト (192.168.1.1:50010)	リレー	203.0.113.1:50510
リレー (10.0.1.1:50110)	ホスト	172.16.1.1:50100

ソース (Source)	接続先タイプ	接続先アドレス
リレー (10.0.1.1:50110)	サーバリフレキシブ	198.51.100.1:50040
リレー (10.0.1.1:50110)	リレー	203.0.113.1:50510

通常、リレーアドレスはホストのネットワークアクセスが制限されている場合にのみ必要です。例えば、コーヒーショップやホテルのユーザーは、これより大きな番号のポートにはアクセスできない場合があります。

両方のホストがアクセスを制限されている場合、両方のリレー候補を含むパスが形成されます。この場合、トラフィックは一方のリレー候補からもう一方のリレー候補に流れ込んでから、遠端に転送されます。

図 57 : ホスト間のメディアパス (リレー間パスを使用、NATなし)



### H.3 TURN サーバーの前の NAT

NAT が TURN サーバーの前に存在する場合、フローはより複雑になります。リレー候補は、他のホスト候補の 1 つからトラフィックを受信することを期待しています。パケットが TURN サーバーのインターフェースから送信され、ファイアウォールによってリライトされない場合、未知のアドレスから送信されたように見えます。これにより、接続性チェックの成功が妨げられ、他のパスが利用できない場合、メディアがたどるルートがなくなります。

図 58 : ホスト間のメディアパス (リレー間パスを使用、NATあり)

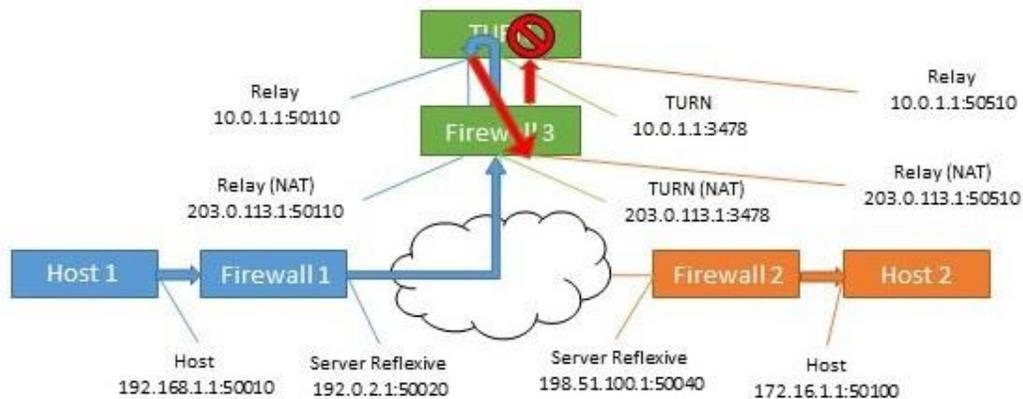


表 31 : ホスト間のメディアパス (リレー間パスを使用、NATあり)

送信元アドレス (パケット単位)	Destination	接続先でのアクション
192.168.1.1 : 50010	203.0.113.1 : 3478 経由 [ファイアウォール(Firewall)]	ファイアウォール 1 が送信元アドレスを書き直す
192.0.2.1 : 50020	203.0.113.1 : 3478	ファイアウォール 3 は接続先アドレスを書き換え、TURN サーバーに転送する
192.0.2.1 : 50020	10.0.1.1 : 3478	TURN サーバーは内部的にこれをこのソースのリレーアドレスにマッピングし、遠端のリレーに送信します
10.0.1.1 : 50110	203.0.113.1 : 50510 ファイアウォール経由	Firewall 3 が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 サーバーが予期せぬ送信元アドレスを検出し、トラフィックをドロップします

これに対するソリューションは、ヘアピン NAT、ループバック NAT、または NAT リフレクションとして知られています。この場合、トラフィックの送信元アドレスと接続先が書き換えられます。この場合、ソースアドレスはファイアウォールのアドレスになります。これは、候補の 1 つと一致することを意味します。

表 32 : ホスト間のメディアパス (リレー間パスを使用、ヘアピン NATあり)

送信元アドレス (パケット単位)	Destination	接続先でのアクション
192.168.1.1 : 50010	203.0.113.1 : 3478 via Firewall	ファイアウォール 1 が送信元アドレスを書き直す。
192.0.2.1 : 50020	203.0.113.1 : 3478	ファイアウォール 3 は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 (パケット単位)	Destination	接続先でのアクション
192.0.2.1 : 50020	10.0.1.1 : 3478	TURN サーバーは内部的にこれをこのソースのリレーアドレスにマッピングし、遠端のリレーに送信します。
10.0.1.1 : 50110	203.0.113.1 : 50510 ファイアウォール経由	Firewall 3 は送信元と送信先の両方のアドレスを書き換えます。
203.0.113.1 : 50110	10.0.1.1 : 50510	TURN サーバーは、リレーから指定された主催者へのトラフィックを内部的にマッピングします。
10.0.1.1 : 3478	198.51.100.1 : 50040 ファイアウォール経由	Firewall 3 が送信元アドレスを書き換えます。
203.0.113.1 : 3478	198.51.100.1 : 50040	Firewall 2 が送信先アドレスを書き換える。
203.0.113.1 : 3478	172.16.1.1 : 50100	最終目的地に到着します。

この機能を有効にする方法の詳細については、ファイアウォールのドキュメントを参照してください。

# 付録I ウェブ管理インタフェース – 設定メニューオプション

Call Bridge のWeb 管理インタフェースにある [設定] タブでは、次のオプションを設定することができます。

- [全般](#)
- [Active Directory](#)
- [通話設定](#)
- [発信通話と着信通話](#)
- [CDR 設定](#)
- [スペース](#)
- [クラスタ](#)
- [API](#)

## I.1 全般

を使用して[設定] >全般 ページ セットアップと設定：

- **TURN サーバ設定**。これらの設定を使用して、Call Bridge および外部クライアントによる TURN サーバへのアクセスを許可します。MMP コマンドを使用して、TURN サーバ自体を設定します。ウェブ管理インタフェースから単一の TURN サーバを設定することもできますが、複数の TURN サーバがある場合は、[セクション 8.1](#) で説明されているように、API のみを使って設定することを強くお勧めします。
- **Lync Edge 設定**。Call Bridge を Lync Edge と統合する場合は、これらの設定を使用します。[Lync Edge を使用するための Meeting Server の設定](#) を参照してください。
- **IVR**。音声自動応答 (IVR) を使用して事前設定された通話を手動でルーティングする場合、これらの設定を使用します。こうすることで、参加する通話またはスペースの ID 番号を入力するように促す事前に録音されたボイスメッセージで発信者が挨拶されます。[IVR 設定](#) を参照してください。

## I.2 Active Directory

ユーザーがウェブアプリを使って Meeting Server に接続するようになるには、LDAP サーバが必要です。Meeting Server が 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) を使用できます。しかし、これは API 経由で設定する必要があります。ウェブ管理インタフェース経由では設定できません。

---

[設定 (Configuration) ] > [Active Directory] ページを使用して、Active Directory と連携するように Meeting Server をセットアップします。LDAP 設定を参照してください。

### 1.3 通話設定

設定 > 通話設定ページで行うこと：

- SIP 通話 (Lync を含む) のメディア暗号化を許可する。
- SIP 通話で参加者ラベルのオーバーレイを表示するかどうかを指定します。
- 発信する音声パケットのサイズをミリ秒で指定します。10ms、20ms、または 40ms。
- TIP サポートを有効にします。(Cisco CTS などのエンドポイントを使用する場合は、TIP サポートを有効にする必要があります。)
- プレゼンテーションビデオチャネルの操作を許可する **禁止** に設定された場合、コンテンツチャネルビデオまたは BFCP 機能は遠端にアダプタサイズされません。
- プレゼンテーション ビデオ チャネル操作が SIP 通話に許可されている場合、この設定により、次のいずれかの Call Bridge の BFCP 動作が決定されます。
  - **サーバロールのみ**—これは電話会議デバイスの通常のオプションであり、BFCP クライアントモードデバイス (SIP エンドポイントなど) での使用を想定しています。または
  - **サーバーとクライアントの役割**—このオプションを選択すると、リモート デバイスとの通話で、Call Bridge が BFCP クライアントまたは BFCP サーバ モードのいずれかで動作できるようになります。

この設定により、リモートの電話会議主催デバイスとのプレゼンテーションビデオ共有が改善されます。

- 発信 SIP コールの Resource-プライオリティ ヘッダー フィールドの値を設定します。この設定により、Meeting Server に対し、帯域幅をプレゼンテーションに割り当てる優先順位を指定します。これは、ネットワーク環境の帯域幅容量と、例えばHDをプッシュするイマーシブ システムがあるかどうかなど、他の要因によって異なります。
- SIP の UDP シグナリングを有効または無効にします。次のいずれかに設定します：
  - **無効|有効** SIP over TCP を使用する場合、またはすべてのネットワークトラフィックを暗号化する必要がある場合に無効にします。
  - **有効な場合、単一アドレス** モードは 2.2 以前のバージョンでの SIP over UDP の動作に対応し、既定値になります。
  - **有効で**、Call Bridge が複数のインターフェイスでリッスンするように設定されている場合は、マルチアドレスモードを使用します。
- Lync プレゼンスサポートを有効にします。この設定では、この Call Bridge が Lync プレゼンスのサブスクリバに提供する接続先 URI に関する情報を提供する必要があるかどうかを決定します。

- Lync パケットペーシングモードは **デフォルト**のままにします。Cisco サポートからの指示がない限り、設定を 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、カーソルを合わせると各フィールドに表示されるテキストを使用するか、または「[ダイヤルプラン設定-SIP エンドポイント](#)」を参照してください。

**通話設定** ページでは、SIP、Cisco Meeting Server (ウェブ アプリ)、Server Reflexive、Relay、VPN、および Lync コンテンツの帯域幅設定を変更することもできます。設定は bps で測定されます。たとえば、2000000 は 2Mbps です。少なくとも 64kbps を音声専用に割り当てます。720p30 通話には 2Mbps、1080p30 通話には約 3.5Mbps を推奨します。60fps ではより多くの帯域幅が必要になります。

SIP メディア暗号化を許可したり、TIP サポートを有効にしたりする場合、帯域幅設定の一部を変更する必要がある場合があります。3 スクリーン TIP コールの場合、**通話設定** ページに表示される帯域幅の数値は自動的に 3 倍になります。そのため、たとえば手動で 6Mbps に設定する必要はありません。ただし、ほとんどの CTS 通話では通常、3 倍の 4Mbps を推奨しています。

## 1.4 発信通話と着信通話

[**設定 (Configuration)**] > [**発信コール (Outbound calls)**] / [**着信コール (Incoming calls)**] ページを使用して、Meeting Server が各通話をどのように処理するかを決定します。

**発信通話** ページでは、発信通話の処理方法を管理します。**着信** ページでは、着信を拒否するか、照会および転送するかを指定します。それらが一致して転送される場合、転送方法に関する情報が必要です。**着信コール** ページには 2 つのテーブルがあります。1 つはマッチング/リジェクションを設定し、もう 1 つは転送動作を設定します。

これらのフィールドへの入力に関する詳細は、通話を処理する [Web 管理者インターフェイスの設定ページ](#) を参照してください。

## 1.5 CDR 設定

**設定** > **CDR 設定** ページをクリックして CDR 受信者の URI を入力します。

Meeting Server は、サーバーに到達する新しい SIP 接続、または通話のアクティブ化または非アクティブ化など、主要な通話関連イベントに対して、内部で通話詳細レコード (CDR) を生成します。これらの CDR をリモートシステムに送信して収集および分析するように設定できます。Meeting Server 上に長期のレコードを保存したり、Meeting Server 上の CDR を参照することはできません。

これらのフィールドへの入力方法の詳細は、「[通話詳細記録サポート](#)」および「[通話詳細記録ガイド](#)」を参照してください。

API を使用して、CDR 受信者の URI で Meeting Server を設定することもできます。「[API リファレンスガイド](#)」を参照してください。

## 1.6 スペース

[設定 (Configuration) ] > [スペース (Spaces) ] ページを使用して、ダイヤルインする Meeting Server 上のスペースを作成します。これにより、たとえば、エンドポイントとウェブアプリがダイヤルインすることができます。

スペースを追加する方法：

- Name の例：001 に発信する
- URI などです。88001

このページでは、オプションで、セカンダリ URI ユーザパート、コール ID、パスコード、デフォルトレイアウトも指定できます。

API を使用してスペースを作成することもできます。詳細については、[API リファレンス ガイドを参照してください](#)。

---

注：通話 ID パラメーターは数値のみをサポートするため、数値で構成する必要があります。

---

## 1.7 クラスタ

---

注：設定>クラスタ ページは、すべてのデータベースがクラスタとして実行中で、すべての Call Bridge がデータベースクラスタに接続されている場合にのみ、ウェブ管理インターフェイスに表示されます。

---

Meeting Server 展開内で、Call Bridge クラスタリングを有効にできます。これにより、複数の Call Bridge が単一のエンティティとして動作し、単一の Call Bridge のキャパシティを超えてスケールすることができます。

クラスタ内の Call Bridge をピアツーピアでリンクするように設定するか、クラスタ化された Call Bridge 間で通話コントロールデバイスを介して通話をルーティングするかを選択できます。

詳細については、[Call Bridge のクラスタリング](#) を参照してください。

## 1.8 API

バージョン 2.9 から、API には API メソッドおよびサードパーティアプリケーションではなく、Meeting Server の Web 管理インターフェイスを使用してアクセスできます。Web 管理インターフェイスにログインした後、[設定 (Configuration) ] タブを選択し、[API] プルダウンリストから選択します。図 59 を参照。

図 59 : Meeting Serverのウェブ管理インターフェイス経由で API にアクセス

The screenshot displays the Cisco Meeting Server web management interface. At the top left is the Cisco logo. Below it, there are navigation tabs: Status, Configuration (selected), Logs, and Debug. The user is identified as 'admin'. The main content area is titled 'API object' and contains a list of configuration options under the 'Configuration' tab. The options include: General, Active Directory, Call settings, Outbound calls, Incoming calls, Interactive Voice Response, CDR settings, and Spaces. The 'API' option is highlighted. Below the list, there is a text block that reads: 'by the API. Where you see a ▶ control, you can expand that section to either show a list of objects of that specific type or the details of one specific'. To the right of this text are two buttons: 'Allow delete' and 'Disallow delete', and a checked checkbox labeled 'Require delete confirmation'. At the bottom of the interface, there is a list of API endpoints, including: /api/v1/ac, /api/v1/ca, /api/v1/callBrandingProfiles/<id>, /api/v1/callBridgeGroups ▶, /api/v1/callBridgeGroups/<id>, /api/v1/callBridges ▶, /api/v1/callBridges/<id>, /api/v1/callLegProfiles ▶, /api/v1/callLegProfiles/<id>, /api/v1/callLegProfiles/<id>/usage, /api/v1/callLegs ▶, /api/v1/callLegs/<id>, /api/v1/callLegs/<id>/callLegProfileTrace, /api/v1/callLegs/<id>/cameraControl, /api/v1/callLegs/<id>/generateKeyframe, /api/v1/callProfiles ▶, /api/v1/callProfiles/<id>, /api/v1/calls ▶, /api/v1/calls/<id>, /api/v1/calls/<id>/callLegs, /api/v1/calls/<id>/callLegs/<id>, and /api/v1/calls/<id>/diagnostics.

**注 :** Web インターフェイスから API にアクセスするには、サードパーティアプリケーションを使用する場合と同様に、Meeting Server の初期設定と MMP を使用した認証を行う必要があります。

ウェブ管理インターフェイスを通じた API ツールの使用例については、[付録 J](#) を参照してください。

## 付録 J API の例

この付録の例では、ウェブ管理インターフェースを通じて API を使用方法を示しますが、POSTMAN などの API ツールを使用することも可能です。例は、これらの API メソッドで可能なすべてのパラメータを使用しているわけではありません。詳細については、[API リファレンスガイド](#) を参照してください。

以下に例を示します。

- [クラスタ内の特定の Call Bridge のための発信ダイヤルプランルールを作成する](#)
- [Meeting Server に Web Bridge を設定する](#)
- [Call Bridge 上に Web Bridge のカスタマイズを作成する](#)
- [Turn サーバーをセットアップして Call Bridge に接続する](#)
- [スペースを作成してメンバーを追加する](#)
- [主催者およびゲストアクセス用の Call Leg Profiles を作成する](#)
- [アクセス方法をスペースに適用する](#)

### J.1 クラスタ内の特定の Call Bridge のための発信ダイヤルプランルールを作成する

クラスタ内の Meeting Server のウェブ管理インターフェースを使用して、[設定] > [API] を選択します：

1. API オブジェクトのリストで、/outboundDialPlanRules の後の ▶ をタップします。
2. [新規作成] ボタンをクリックします。
3. 適用するダイヤル プラン ルールに一致する **ドメイン** を入力します。次の例では `example.com` を使用しています。
4. scope = callBridge を設定します。発信ダイヤル プラン ルールは、手順 4 で選択した Call Bridge に対してのみ有効になります。
5. callBridge パラメータの隣にある **選択** ボタンをクリックし、ルールが有効な Call Bridge の隣にある **選択** をクリックします。
6. [作成 (Create) ] をクリックします。

[« return to object list](#)

### /api/v1/outboundDialPlanRules

domain *	<input checked="" type="checkbox"/>	example.com	- required
priority	<input checked="" type="checkbox"/>	50	
localContactDomain	<input type="checkbox"/>		
localFromDomain	<input type="checkbox"/>		
sipProxy	<input checked="" type="checkbox"/>	198.51.100.0	
trunkType	<input checked="" type="checkbox"/>	sip	
failureAction	<input checked="" type="checkbox"/>	stop	
sipControlEncryption	<input checked="" type="checkbox"/>	auto	
scope	<input checked="" type="checkbox"/>	callBridge	
callBridge	<input checked="" type="checkbox"/>	34603cb3-2adb-47d3-bc95-1a27d83aa7db	Choose
callBridgeGroup	<input type="checkbox"/>		Choose
tenant	<input type="checkbox"/>		Choose
callRouting	<input type="checkbox"/>	<unset>	
Create			

上の例では、**優先度 = 50** も設定しています。優先順位が 50 を超えるダイヤルプランは、この前に適用されます。sipProxy をプロキシ デバイスの IP アドレスに設定し、このデバイスを経由して通話を行います。**トランクタイプ = sip**, **失敗時のアクション = 停止** このダイヤルプランが通話の接続に失敗した場合、次の発信ダイヤルプラン規則が試行されるのを防ぐために、さらに **SIPコントロール暗号化 = auto** を許可する暗号化されたコントロール接続が失敗した場合に、暗号化されていないコントロールトラフィックにフォールバックします。

7. ページ上部の [オブジェクトリストに戻る] ボタンをクリックする前に、発信ダイヤルプランルールのパラメータを確認してください。

## J.2 Meeting ServerにWeb Bridgeを設定する

Meeting Server の Web 管理インターフェイスを使用して、[設定 (Configuration)]>[API] の順に選択します。

1. API オブジェクトのリストで、/webBridges の後の ▶ をタップします。
2. [新規作成] ボタンをクリックします。
3. Web Bridgeの url を入力します。ここで、[ukedge1join.example.com](https://ukedge1join.example.com) は、Web Bridge に到達するためにCall Bridgeによって使用されるFQDNです。

また、以下の例では、通話 ID とパスコードの両方の入力を要求するように idEntryMode = **セキュア** を設定しています。Space を使用して allowWebLinkAccess = true に変更し、Web Bridgeがゲストにウェブリンクをたどることでスペースにアクセスすることを許可します。showSignIn = true これにより、Web Bridgeはログインボタンを表示します。resolveCoSpaceCallIds = true ビジターがスペースに参加できるようにする目的で、Web Bridgeがスペースのコール ID とスペースアクセス方法を受け入れることを許可します。また、resolve LyncConferencelds = false、通話 ID がスケジュールされた Lync/Skype for Business 通話 ID に解決されることを防ぎます。

[« return to object list](#)

/api/v1/webBridges

url	<input checked="" type="checkbox"/>	<input type="text" value="https://ukedge1join.example.com"/>	(URL)
resourceArchive	<input type="checkbox"/>	<input type="text"/>	(URL)
tenant	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Choose"/>
tenantGroup	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Choose"/>
idEntryMode	<input checked="" type="checkbox"/>	<input type="text" value="secure"/>	
allowWeblinkAccess	<input checked="" type="checkbox"/>	<input type="text" value="true"/>	
showSignIn	<input checked="" type="checkbox"/>	<input type="text" value="true"/>	
resolveCoSpaceCallIds	<input checked="" type="checkbox"/>	<input type="text" value="true"/>	
resolveLyncConferenceIds	<input checked="" type="checkbox"/>	<input type="text" value="false"/>	
callBridge	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Choose"/>
callBridgeGroup	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Choose"/>
<input type="button" value="Create"/>			

4. [作成 (Create) ] をクリックします。

### J.3 Call Bridge 上に Web Bridge のカスタマイズを作成する

前の例で設定された WebBridge を使用します。

1. [変更 (Modify) ] をクリックして、[resourceArchive] の URL を入力します。URL はカスタマイズファイルを保存した場所を指します。Call Bridge は、ウェブアプリの要素（サインインの背景画像、アイコンの表示、アイコンの下のテキスト、ブラウザ タブ上のテキスト）をカスタマイズするために使用します。

Object configuration	
url	https://ukedge1join.example.com
resolveCoSpaceCallIds	true
resolveLyncConferenceIds	false
idEntryMode	secure
allowWeblinkAccess	true
showSignIn	true

/api/v1/webBridges/b88a4de8-bb89-4e7a-9fad-4cf6eb763a4d

url	<input type="checkbox"/>	<input type="text" value="https://ukedge1join.example.com"/>	(URL) - <b>present</b>
resourceArchive	<input checked="" type="checkbox"/>	<input type="text" value="https://203.0.113.24/branding/web_app.zip"/>	(URL)
tenant	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Choose"/>
tenantGroup	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Choose"/>
idEntryMode	<input type="checkbox"/>	<input type="text" value="secure"/>	- <b>present</b>
allowWeblinkAccess	<input type="checkbox"/>	<input type="text" value="true"/>	- <b>present</b>
showSignIn	<input type="checkbox"/>	<input type="text" value="true"/>	- <b>present</b>
resolveCoSpaceCallIds	<input type="checkbox"/>	<input type="text" value="true"/>	- <b>present</b>
resolveLyncConferenceIds	<input type="checkbox"/>	<input type="text" value="false"/>	- <b>present</b>
callBridge	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Choose"/>
callBridgeGroup	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Choose"/>
<input type="button" value="Modify"/>			

注：ウェブアプリのカスタマイズの詳細については、「Cisco Meeting Server のカスタマイズガイドライン」を参照してください。

## J.4 TURN サーバーをセットアップして Call Bridge に接続する

**注：**TURN Server は、Cisco Meeting Server 2000 では利用できません。TURN Serverは、小容量の Cisco Meeting Server 1000 および仕様ベースの VM サーバーにより適しています。

Meeting Server の Web 管理インターフェイスを使用して、**[設定 (Configuration)]** > API の順に選択します。

1. API オブジェクトのリストで、/turnServers の後ろの ▶ をタップします。
2. **[新規作成]** ボタンをクリックします。
3. **サーバアドレス、ユーザ名、パスワード、タイプ、クライアントアドレス**、および必要に応じて他のパラメータを指定します。

server address = この TURN サーバーに到達するために Call Bridge が使用するアドレス  
 username = この TURN サーバーで割り当てを行う際に使用するユーザ名、  
**パスワード** = この TURN サーバーで割り当てを行う際に使用するパスワード、  
 type = cms、サーバーに接続する UDP/TCP ポート 3478 を選択します。  
 client address = ウェブアプリがこの TURN サーバーに到達するために使用するアドレス。

### /api/v1/turnServers

serverAddress	<input checked="" type="checkbox"/>	<input type="text" value="192.0.2.0"/>	
clientAddress	<input checked="" type="checkbox"/>	<input type="text" value="203.0.113.0"/>	
username	<input checked="" type="checkbox"/>	<input type="text" value="turn server"/>	
password	<input checked="" type="checkbox"/>	<input type="text" value="turn"/>	
type	<input checked="" type="checkbox"/>	<input type="text" value="cms"/>	
numRegistrations	<input type="checkbox"/>	<input type="text"/>	
tcpPortNumberOverride	<input type="checkbox"/>	<input type="text"/>	
callBridge	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Choose"/>
callBridgeGroup	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Choose"/>
<input type="button" value="Create"/>			

4. **[作成 (Create)]** をクリックします。
5. ページ上部にある **[オブジェクトリストに戻る]** ボタンをクリックする前に TURN サーバーのパラメータを確認してください。

## J.5 スペースを作成してメンバーを追加する

Meeting Server の Web 管理インターフェイスを使用して、**[設定 (Configuration)]** > [API] の順に選択します。

1. API オブジェクトのリストで、/coSpaces の後ろの ▶ をタップします。
2. **新規作成** ボタンをクリックします。

3. を入力します名前、 uri、 セカンダリ URI、 コールID、 パスコード およびその他の適切なパラメータ。

[← return to object list](#)

/api/v1/coSpaces

name	<input type="text"/>
uri	<input type="text"/> (URI user part)
secondaryUri	<input type="text"/> (URI user part)
callId	<input type="text"/>
cdtTag	<input type="text"/>
passcode	<input type="text"/>
defaultLayout	<unset>
tenant	<input type="text"/> Choose
callLegProfile	<input type="text"/> Choose
callProfile	<input type="text"/> Choose
callBrandingProfile	<input type="text"/> Choose
dialInSecurityProfile	<input type="text"/> Choose
requireCallId	<unset>
secret	<input type="text"/>
regenerateSecret	<unset>
nonMemberAccess	<unset>
ownerJid	<input type="text"/>
streamUrl	<input type="text"/> (URL)
ownerAdGuid	<input type="text"/> GUID (none available)
meetingScheduler	<input type="text"/>
panePlacementHighestImportance	<input type="text"/>
panePlacementSelfPaneMode	<unset>

Create

4. [作成 (Create) ] をクリックします。

### J.5.1 スペースにメンバーを追加する

1. ページ上部にある **関連オブジェクト** のリストから、[ここ]をクリックします。  
/api/v1/coSpaces/...../coSpaceUsers
2. userJid をと必要に応じて他のパラメータを入力します。userJid はユーザーの識別子です (例 : first.last@example.com)。

[← return to object list](#)

/api/v1/coSpaces/88e83395-a61b-48df-b7a1-bab787800216/coSpaceUsers

Related objects: [/api/v1/coSpaces](#)  
[/api/v1/coSpaces/88e83395-a61b-48df-b7a1-bab787800216](#)

« start « prev none next »  Filter

object id	userJid	userId	autoGenerated
no objects of this type are present, or none match any filters that may be in use			

---

/api/v1/coSpaces/88e83395-a61b-48df-b7a1-bab787800216/coSpaceUsers

userJid *	<input type="text"/>	- required
callLegProfile	<input type="text"/> Choose	
canDestroy	<unset>	
canAddRemoveMember	<unset>	
canChangeName	<unset>	
canChangeNonMemberAccessAllowed	<unset>	
canChangeUri	<unset>	
canChangeCallId	<unset>	
canChangePasscode	<unset>	
canPostMessage	<unset>	
canRemoveSelf	<unset>	
canDeleteAllMessages	<unset>	

Create

3. [作成 (Create) ] をクリックします。
4. スペースに追加する必要がある他のすべてのメンバーに対して繰り返します。

## J.6 コールレグ プロファイルの作成

この例では、主催者用とゲスト用の 2 つの callLegProfiles を作成します。

Meeting Server の Web 管理インターフェイスを使用して、[設定 (Configuration) ]>[API] の順に選択します。

1. API オブジェクトのリストで、/callLegProfiles の後ろの ▶ をタップします。
2. 主催者の callLegProfile を作成する。
  - a. **新規作成** ボタンをクリックします
  - b. パラメータ needsActivation = **false**、および **デフォルトレイアウト=すべて等しい**

[← return to object list](#)

/api/v1/callLegProfiles

needsActivation	<input type="checkbox"/>	<unset> ▼
defaultLayout	<input type="checkbox"/>	<unset> ▼
participantLabels	<input type="checkbox"/>	<unset> ▼
presentationDisplayMode	<input type="checkbox"/>	<unset> ▼
presentationContributionAllowed	<input type="checkbox"/>	<unset> ▼
presentationViewingAllowed	<input type="checkbox"/>	<unset> ▼
endCallAllowed	<input type="checkbox"/>	<unset> ▼
disconnectOthersAllowed	<input type="checkbox"/>	<unset> ▼
addParticipantAllowed	<input type="checkbox"/>	<unset> ▼
muteOthersAllowed	<input type="checkbox"/>	<unset> ▼
videoMuteOthersAllowed	<input type="checkbox"/>	<unset> ▼
muteSelfAllowed	<input type="checkbox"/>	<unset> ▼
videoMuteSelfAllowed	<input type="checkbox"/>	<unset> ▼
changeLayoutAllowed	<input type="checkbox"/>	<unset> ▼
joinToneParticipantThreshold	<input type="checkbox"/>	<input type="text"/>
leaveToneParticipantThreshold	<input type="checkbox"/>	<input type="text"/>
videoMode	<input type="checkbox"/>	<unset> ▼
rxAudioMute	<input type="checkbox"/>	<unset> ▼
txAudioMute	<input type="checkbox"/>	<unset> ▼
rxVideoMute	<input type="checkbox"/>	<unset> ▼
txVideoMute	<input type="checkbox"/>	<unset> ▼
sipMediaEncryption	<input type="checkbox"/>	<unset> ▼
audioPacketSizeMs	<input type="checkbox"/>	<input type="text"/>
deactivationMode	<input type="checkbox"/>	<unset> ▼
deactivationModeTime	<input type="checkbox"/>	<input type="text"/>
telepresenceCallsAllowed	<input type="checkbox"/>	<unset> ▼
sipPresentationChannelEnabled	<input type="checkbox"/>	<unset> ▼
bfcplMode	<input type="checkbox"/>	<unset> ▼
callLockAllowed	<input type="checkbox"/>	<unset> ▼
setImportanceAllowed	<input type="checkbox"/>	<unset> ▼
allowAllMuteSelfAllowed	<input type="checkbox"/>	<unset> ▼
allowAllPresentationContributionAllowed	<input type="checkbox"/>	<unset> ▼
changeJoinAudioMuteOverrideAllowed	<input type="checkbox"/>	<unset> ▼
recordingControlAllowed	<input type="checkbox"/>	<unset> ▼
streamingControlAllowed	<input type="checkbox"/>	<unset> ▼
name	<input type="checkbox"/>	<input type="text"/>
maxCallDurationTime	<input type="checkbox"/>	<input type="text"/>
qualityMain	<input type="checkbox"/>	<unset> ▼
qualityPresentation	<input type="checkbox"/>	<unset> ▼
participantCounter	<input type="checkbox"/>	<unset> ▼
layoutTemplate	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Choose"/>
controlRemoteCameraAllowed	<input type="checkbox"/>	<unset> ▼
audioGainMode	<input type="checkbox"/>	<unset> ▼
<input type="button" value="Create"/>		

- c. [作成 (Create) ] をクリックします。

### 3. ゲスト用にコールレグプロファイルを作成する

- a. **新規作成** ボタンをクリックします
- b. パラメータ `needsActivation = true`, `defaultLayout = speakerOnly`, `deactivationMode = 切断` および `deactivationModeTime = 10` を設定します

---

**注：**主催者がミーティングを退出してから 10 秒後に、ゲストは自動的に切断されます。

---

これらの主催者およびゲストのコールレグプロファイルは、スペースのアクセス方法を作成するときに適用できます。次の例を参照してください。

## J.7 アクセス方法をスペースに適用する

この例では、主催者アクセスとゲストアクセスのスペースに異なるアクセス方法を適用する方法を説明しています。

Meeting Server の Web 管理インターフェイスを使用して、**[設定 (Configuration)]** > **[API]** の順に選択します。

1. API オブジェクトのリストで、`/coSpaces` の後ろの ▶ をタップします。
2. 既存のスペースの `[object id]` をクリックするか、新しいプロファイルを作成する。
3. ページ上部にある **関連オブジェクト** のリストから、**[ここ]** をクリックします。  
`/api/v1/coSpaces/...../accessMethods`
4. このスペースを使用するホストのアクセス方法を作成する
  - a. パラメータを設定 `name = ホスト`、`callID = 12345678`、**選択ボタン** をクリックし、コールレグプロファイル **パラメータの横にある** ボタンをクリックし、前の例のステップ2で作成したコールレグプロファイルを選択します。
  - b. 必要に応じて他のパラメータを入力します。
  - c. **[作成 (Create)]** をクリックします。
5. このスペースを使用するゲストのアクセス方法を作成する。
  - a. パラメータを設定 `name = ホスト`、`callID = 87654321`、**選択ボタン** をクリックし、コールレグプロファイル **パラメータの横にある** ボタンをクリックし、前の例のステップ3で作成したコールレグプロファイルを選択します。
  - b. 必要に応じて他のパラメータを入力します。
  - c. **[作成 (Create)]** をクリックします。
6. この構成をテストします。次の動作が表示されます。
  - すべてのゲストは、87654321 にダイヤルしてスペースに参加します。
  - 主催者は 12345678 にダイヤルしてスペースに参加できます。

- 主催者が参加するまで、すべてのゲストはビデオストリームを見たり、音声を聞いたりすることはできません。
- 最後の主催者がミーティングを退出してから 10 秒後に、すべてのゲストの接続が切断されます。

## Cisco の法的情報

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

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

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

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

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

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

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

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

© 2025 Cisco Systems, Inc. All rights reserved.

## Cisco の商標または登録商標

Cisco および Cisco ロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、[www.cisco.com/jp/go/trademarks](http://www.cisco.com/jp/go/trademarks) をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1721R)