Cisco Meeting Server

Cisco Meeting Server リリース 3.0

リリース ノート

2020 年 9 月 29 日

目次

変更事項

バージョン	変更
2020 年 9 月 16 日	フォーマット エラーを修正しました。
2020 年 9 月 8 日	新しいレコーダーまたはストリームを外部録音/ストリーミング サービスとして使用できないことを明確にするために軽微な編集を行いました。
2020 年 9 月 2 日	VM の最小要件が vCPU コア 4 基であることを明確にするために軽微な編集を行いました。
2020 年 8 月 27 日	以前は記載されていなかったスニペットを記載しました。
2020 年 8 月 12 日	Web アプリケーションのコール キャパシティの数値を編集しました。
2020 年 7 月 29 日	3.0 の最初のリリース。

1 はじめに

これらのリリース ノートでは、Cisco Meeting Server ソフトウェア リリース 3.0 の新機能、改善、および変更について説明します。

The Cisco Meeting Server ソフトウェアは以下でホストされる場合があります。

- Cisco Meeting Server 2000、B200 ブレード 8 枚を搭載した UCS 5108 シャーシ、および Meeting Server ソフトウェアをプレインストール。
- Cisco Meeting Server 1000、VMware を事前設定済みの Cisco UCS サーバ、および VMware 導入環境としてインストールされた Cisco Meeting Server。
- またはスペックベースの VM サーバ。

バージョン 3.0 では、Cisco Meeting Server の多数のコンポーネントが削除されます。3.0 での変更の一覧については、セクション 2.1を参照してください。

注：Meeting Server 3.0 では、Cisco Meeting Management 3.0（またはそれ以降）を使用するための必須の要件が導入されています。Meeting Management は、製品登録と、スマート ライセンスのサポートに関連するスマート アカウント（セットアップされている場合）とのやり取りを処理します。詳細については、セクション 2.2を参照してください。

Acano X シリーズに関する注：Cisco Meeting Server バージョン 3.0 以降では X シリーズ サーバはサポートされません。Meeting Server 3.0 で利用可能な Web Bridge 3、レコーダー、ストリーマなどの最新の Meeting Server サービスに対する旧バージョンの Call Bridge からの接続もサポートされません。

注：WebRTC 用 Cisco ミーティング アプリケーション（Web Bridge 2）は、Cisco Meeting Server version 3.0 で削除されています。WebRTC 用 Cisco ミーティング アプリケーションの代わりに、Cisco Meeting Server Web アプリケーションを使用する必要があります。それには、Web Bridge 3 を展開する必要があります。Web Bridge 3 の展開と設定の詳細については、バージョン 3.0 の導入ガイド [英語] を参照してください。

このリリースノートではこれ以降、Cisco Meetings Server ソフトウェアを Meeting Serverと呼びます。

これよりも前のバージョンからアップグレードする場合は、**backup snapshot <filename>** コマンドを使用して設定のバックアップを作成し、別のデバイスに安全に保存することを推奨します。詳細については、『MMP Command Reference（MMP コマンド リファレンス）』を参照してください。

Microsoft RTVideo **に関する注意：**Microsoft RTVideo および Windows 上の Lync 2010 および Mac OS 上の Lync 2011 は、Meeting Server ソフトウェアの将来のバージョンではサポートされません。ただし、Skype for Business と Office 365 のサポートは続行されます。

1.1 他のシスコ製品との相互運用性

この製品の相互運用性テストの結果は http://www.cisco.com/go/tp-interop に送信されます。ここでは、他のシスコ会議製品の相互運用性テストの結果も確認できます。

1.2 Cisco Meeting Server プラットフォームメンテナンス

Cisco Meeting Server ソフトウェアが実行されるプラットフォームを維持し、最新の更新プログラムでパッチを適用することが重要です。

1.2.1 Cisco Meeting Server 1000 およびその他の仮想化プラットフォーム

Cisco Meeting Server ソフトウェアは、次のプラットフォームで仮想化された導入として実行されます。

- Cisco Meeting Server 1000
- 仕様ベースの VM プラットフォーム

1.2.2 Cisco Meeting Server 2000

Cisco Meeting Server 2000 は、仮想化された導入としてではなく、物理的な展開としての Cisco Meeting Server ソフトウェアを実行する Cisco UCS テクノロジーに基づいています。

注意：プラットフォーム（UCS マネージャによって管理される UCS シャーシおよびモジュール）が最新のパッチで更新されていることを確認して、『Cisco UCS Manager ファームウェア管理ガイド』の指示に従ってください。プラットフォームが最新の状態に維持されていないと、Cisco Meeting Server のセキュリティが低下する場合があります。

1.2.3 コール キャパシティ

表 1 に、Cisco Meeting Server ソフトウェア バージョン 3.0 をホストしているプラットフォームのコール キャパシティの比較を示します。

表 1：Meeting Server プラットフォームのコール キャパシティ

コールのタイプ	Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5	Cisco Meeting Server 2000
フル HD コール 1080p60 ビデオ 720p30 コンテンツ	24	24	175
フル HD コール 1080p30 ビデオ 1080p30/4K7 コンテンツ	24	24	175
フル HD コール 1080p30 ビデオ 720p30 コンテンツ	48	48	350
HD コール 720p30 ビデオ 720p5 コンテンツ	96	96	700
SD コール 448p30 ビデオ 720p5 コンテンツ	192	192	1000
音声通話（G.711）	1700	2200	3,000

次の表 2 では、単一またはクラスタ構成の Meeting Server のコール キャパシティと、Call Bridge グループ内のコールのロード バランシングを比較しています。

表 2：Meeting Server ソフトウェア バージョン 3.0 のコール キャパシティ

Cisco Meeting Server プラットフォーム		Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5	Cisco Meeting Server 2000
個々の Meeting Server またはクラスタの Meeting Server（注 1、2、3、4）	1080p30 720p30 SD 音声通話	48 96 192 1700	48 96 192 2200	350 700 1000 3000
	サーバごとの会議あたりの HD 参加者数	96	96	450
	Web アプリケーションのコールキャパシティ（内部コール）： フル HD HD SD 音声通話	 48 96 192 500	 48 96 192 500	 350 700 1000 1000
Call Bridge グループ内の Meeting Server	サポートされるコール タイプ	インバウンド SIP アウトバウンド SIP		
	1080p30 720p30 SD 音声通話 負荷制限	48 96 192 1700 96,000	48 96 192 2200 96,000	350 700 1000 3000 700,000
	サーバごとの会議あたりのHD 参加者数	96	96	450
	Web アプリケーションのコールキャパシティ（内部コール）： フル HD HD SD 音声通話	 48 96 192 500	 48 96 192 500	 350 700 1000 1000

注 1：クラスタあたりの最大 24 個の Call Bridge ノード。ノード 8 個以上のクラスタ設計は、シスコによる承認が必要です。詳細については、シスコ サポートにお問い合わせください。

注 2：Call Bridge グループが設定されていないクラスタ Cisco Meeting Server 2000 では、最大コール数の整数倍（700 HD コールの整数倍など）をサポートします。

注 3：SIP コールまたは Web アプリケーション コールにクラスタあたり最大 16,800 の HD 同時コール（24 ノード X 700 HD コール）が適用されます。

注 4：クラスタ内の Meeting Server プラットフォームに応じて、1 つのクラスタの会議あたり最大 2600 の参加者。

注 5：表 2は、ビデオ通話で最大 2.5 Mbps-720p5 コンテンツ、音声通話で最大 G.711 のコール レートを想定しています。その他のコーデックや高いコンテンツ解像度/フレームレートは、容量の減少につながります。ミーティングが複数の Call Bridge にまたがる場合は、分散リンクが自動的に作成され、サーバのコール数とキャパシティに対してもカウントされます。負荷制限の数値は H.264 にのみ使用されます。

注 6：VMware が最近のバージョン（6.0 アップデート 3、6.5 アップデート 2、および 6.7）で実施した変更により、Cisco Meeting Server バージョン 3.0 での音声コールのスループットが低下しました（ビデオのキャパシティは影響を受けません）。

注 7：クラスタでサポートされるコール セットアップ レートは、SIP コールでは 1 秒あたり最大 40 コール、Cisco Meeting Server Web アプリケーションのコールでは 20 コールです。

1.2.4 Cisco Meeting Server Web アプリケーションのコール キャパシティ

このセクションでは、外部コールおよび混在コールに Web Bridge 3 と Web アプリケーションを使用する展開でのコール キャパシティの詳細について説明します。（内部コールのキャパシティについては、表 2 を参照してください。）

1.2.4.1 Cisco Meeting Server Web アプリケーションのコール キャパシティ：外部コール

外部コールとは、クライアントがリバース プロキシおよび TURN サーバとして Cisco Expressway を使用して、Web Bridge と Call Bridge に到達する場合を言います。

Web アプリケーションのコールのプロキシとして Expressway を使用する場合、表 3 に示すように、Expressway により最大コール数の制限が適用されます。

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

表 3：Cisco Meeting Server Web アプリケーションのコール キャパシティ：外部コール

セットアップ（Setup）	コール タイプ	CE1200 プラットフォーム	大規模 OVA Expressway
Cisco Expressway ペア（X12.6 以降）	フル HD	150	150
	その他	200	200

Expressway ペアをクラスタリングすることで、Expressway のキャパシティを増大させることができます。Expressway ペアのクラスタリングは、最大 6 ノードまで可能です（4 ノードは拡張のために使用され、2 ノードは冗長性のために使用されます）。その結果、1 ペアのキャパシティの 4 倍の合計コール キャパシティが得られます。

注：Cisco Meeting Server Web アプリケーションのコールについては、Expressway クラスタのコール セットアップ レートが 1 秒あたり 6 コールを超えることはできません。

1.2.4.2 Cisco Meeting Server Web アプリケーションのキャパシティ：混在（内部 + 外部）コール

スタンドアロンとクラスタのどちらの導入環境でも、内部と外部を組み合わせたコールの使用をサポートできます。内部参加者と外部参加者の混在をサポートする場合、Web アプリケーションの合計キャパシティは、内部コールについては表 2 のとおりですが、外部から接続できる合計の範囲内での参加者数は、表 3 の制限を受けます。

たとえば、1 つのスタンドアロン Meeting Server 2000 と 1 つの Expressway のペアでは、音声のみの Web アプリケーション コールであれば混在で 1,000 までサポートしますが、外部参加者の数は、合計 1,000 のうち最大 200 に制限されます。

1.3 Cisco Meeting Server Web アプリケーション重要事項

注：WebRTC 用 Cisco ミーティング アプリケーション（Web Bridge 2）は、Cisco Meeting Server version 3.0 で削除されています。WebRTC 用 Cisco ミーティング アプリケーションの代わりに、Cisco Meeting Server Web アプリケーションを使用する必要があります。それには、Web Bridge 3 を展開する必要があります。Web Bridge 3 の展開と設定の詳細については、バージョン 3.0 の導入ガイド [英語] を参照してください。

Cisco Meeting Server Web アプリケーションを使用している場合（Web Bridge 3 を展開している場合）、Web アプリケーションに関連する機能のリリース時期および解決済みの問題の詳細については、『Cisco Meeting Server web app Important Information（Cisco Meeting Server Web アプリケーション重要事項）』[英語] を参照してください。

Web アプリケーションに関連するすべての情報は、この別個のドキュメントに記載され、Meeting Server のリリース ノートには含まれません。

重要事項ガイドでは、以下のことを説明しています。

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

1.4 ソフトウェアメンテナンスの終了

Cisco Meeting Server ソフトウェア バージョン 3.0 のリリースにあたり、シスコは、表 4 に示すソフトウェアのソフトウェア メンテナンス終了予定を発表しています。

表 4：Cisco Meeting Server のバージョンのソフトウェア メンテナンス終了予定

Cisco Meeting Server **ソフトウェアバージョン**	**ソフトウェアメンテナンス終了の通知機関**
Cisco Meeting Server バージョン 2.8.x	Cisco Meeting Server バージョン 3.0 の最初のリリースの 4 ヵ月後。

Cisco Meeting Server の Cisco のソフトウェア メンテナンス終了ポリシーの詳細については、ここをクリックしてください。

2 バージョン 3.0 の新機能と変更点

Meeting Server ソフトウェア バージョン 3.0 では、以下の新機能と変更が導入されています。

- レガシーの Meeting Server コンポーネントの削除およびその他の変更。
- ライセンスの購入、登録、ソフトウェア管理におけるユーザ エクスペリエンス向上を目的としたスマート ライセンスのサポート。
- Cisco Meeting Server のアップグレード時に Image Signing を使用することによるセキュリティの向上。
- 管理者が設定可能な最小パスコード長による、ミーティングのダイヤル方法すべてに共通するセキュリティ強化。
- XMPP 内部レコーダーおよびストリーマ コンポーネントを置き換える新しい内部 SIP レコーダーおよびストリーマ コンポーネント。新しいレコーダーおよびストリーマはレイアウト変更をサポートしており、新しいストリーマは最大 1080p の解像度をサポートします。
- Web Bridge の設定は、API 内の Web Bridge プロファイルとの設定に移動しました。
- Cisco Meeting Server Web アプリケーションでは、廃止された WebRTC 用 Cisco ミーティング アプリケーションと同等の機能を提供するため、3.0 で多数の新機能が導入されています。3.0 で導入された Web アプリケーションの機能の完全なリストについては、『Cisco Meeting Server 3.0 web app Important Information（Cisco Meeting Server 3.0 Web アプリケーション重要事項）』を参照してください。Meeting Server 側で設定が必要な Web アプリケーションの機能の一覧を以下に示します。
  - ビデオ アドレス（URI）を使用したミーティングへの参加。
  - Web アプリケーションからの参加者のアクセス許可の変更。
  - ビデオ会議における Web アプリケーションからの参加者に対する名前ラベルの表示。
  - 録音/ストリーミング、ミーティングのロック/ロック解除、重要度に関する Web アプリケーションの制御。
  - 中間/エンドエンティティ（root 以外）の証明書を受け入れるように、C2W 接続を変更。

  - Web アプリケーションのサインイン ページを独自のブランディングを使用してカスタマイズ可能。
- オートゲインコントロール(AGC)は、デフォルトでは有効になっています。
- ESXi7.0 のサポート。
- 割り当て済みの PMP ライセンス数のレコードの履歴を表示可能。

Acano X **シリーズに関する注**：Cisco Meeting Server バージョン 3.0 以降では X シリーズサーバはサポートされません。Meeting Server 3.0 で利用可能な Web Bridge 3、レコーダー、ストリーマなどの最新の Meeting Server サービスに対する旧バージョンの Call Bridge からの接続もサポートされません。

実稼働環境でベータ（またはプレビュー）機能を使用しないことをお勧めします。完全にリリースされるまでテスト環境でのみ使用してください。

注：シスコは、ベータ版（またはプレビュー）機能が将来完全にサポートされる機能になると保証していません。ベータ機能はフィードバックを基に変更される可能性があり、今後、機能性が変更または削除される場合があります。

2.1 3.0 で削除または変更された Meeting Server コンポーネント

Meeting Server 3.0 以降では、以下の機能とサービスが提供終了またはサポート終了となります。

- ACU：ACU を使用しているユーザは SMP+ ライセンスに移行する必要があります。詳細については、シスコのリセラーにお問い合わせください。
- Web Bridge 2：Web Bridge 2 は 3.0 で削除されたため、Web アプリケーションをサポートするためには、Web Bridge 2 のユーザは Web Bridge を展開し直して Web Bridge 3 を使用する必要があります。Web Bridge 2 から Web Bridge 3 への自動アップグレードによる移行はありません。バージョン 2.9 の Web Bridge 3 をすでに展開している場合は、Web 管理または /webBridges/<webbridge id> の設定から引き継がれないため、アップグレード後に設定を確認する必要があります。
  - デスクトップ版、iOS 版、および WebRTC 用 Cisco ミーティング アプリケーションはサポート終了となりました。

- XMPP：XMPP に依存する従来のレコーダーとストリーマは、3.0 で新しい内部 SIP レコーダーおよびストリーマ コンポーネントに置き換えられました。3.0 にアップグレードする際に、レコーダーとストリーマを展開し直す必要があります。
- H.323 ゲートウェイ
- ロード バランサ
- SIP エッジ
- トランク
- X シリーズ サーバ

関連するすべての MMP コマンド、API オブジェクト、およびパラメータが、廃止または削除されています。特定の情報については、セクション 2.11 とセクション 2.13 を参照してください。

2.2 スマート ライセンス

バージョン 3.0 では、Cisco Meeting Management バージョン 3.0 以降を使用した Cisco Meeting Server でのスマート ライセンスのサポートが導入されています。今回のソフトウェア ライセンス モデルへの移行、つまり従来の製品アクティベーション キー（PAK）ライセンスからスマート ライセンスへの移行により、ライセンスの購入、登録、ソフトウェア管理のユーザ エクスペリエンスが向上します。また、Meeting Server でも、他のシスコ製品におけるソフトウェア ライセンスの方法と同様に Cisco スマート アカウントを利用します。これは、組織全体でライセンスの表示、格納、管理ができる一元的なリポジトリです。

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

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

注：「超過（overage）」という言葉は、ライセンスの使用数が使用権を超えている状態を表します。

Meeting Server 3.0 でのライセンスの変更と動作は次のとおりです。

- バージョン 3.0 では Cisco Meeting Management バージョン 3.0 以降が必須です。Meeting Management は Meeting Server ライセンス ファイルを読み取り、製品登録と、スマート アカウント（セットアップされている場合）とのやり取りを処理することができます。
- スマート アカウントに存在する 1 セットの Meeting Server ライセンスを使用して、複数のクラスタにライセンスを付与できるようになり、3.0 より前のバージョンでのように個々の Meeting Server インスタンスにライセンス ファイルをロードする必要がなくなります。
- スマート ライセンスを使用した Meeting Management では、クラスタあたりいくつの Call Bridge が使用されているかをトラッキングできるため、R-CMS-K9 アクティベーション ライセンスは不要になります。
- 既存のライセンスがない新規の展開の場合は、次のようになります。
    - 新規購入のライセンスはデフォルトでスマート対応になっておりスマート アカウントが必要な場合があります。Meeting Management にライセンスの詳細情報を入力すると、スマート アカウントで保有されているライセンスに対してライセンスの詳細情報が検証されます。
- 各 Call Bridge にローカルのライセンス ファイルがある既存の環境の場合は、次のようになります。
    - スマート アカウントを使用せずに 3.0 にアップグレードできます。その場合、従来のライセンス方法に従って Meeting Management が既存のライセンス ファイルを読み取ります。
    - Cisco Smart Software Manager（CSSM）ポータルを使用してスマート アカウントに移行し、既存のライセンスをスマートに変換するオプションを選択することができます。

  SMP および PMP のライセンス使用状況が合算され、ある特定の 1 日の使用数が超過であるかどうか判別されます（いずれかのライセンスが超過した場合、その日は終日、使用数が使用権を超えていると見なされます）。他の機能のライセンス（録音やカスタム レイアウトなど）は個別に評価され、（スマート アカウントにライセンスが存在する前提で）Meeting Management を通じて有効化されます。

注：3.0 のすべての展開で Meeting Management が必須であるため、大規模な導入環境の場合は、アクティブな Meeting Management を使用せずに、新規ライセンス専用モードで Meeting Management を導入できます。

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

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

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

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

Meeting Server 3.0 以降でライセンスが機能するためには Meeting Management が必須です。バージョン 3.0 では、スマートを使用した新規ライセンス、または既存ユーザの場合はインストール済みライセンス ファイルをサポートするために、Meeting Server と Meeting Management の間の新しい信頼とやり取りが導入されています。Meeting Management が Meeting Server にライセンスを付与できるようにする仕組みが、この信頼リンクです。
スマート ライセンスを実装するための概要レベルのワークフローを以下に示します。

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

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

3. スマート ライセンスを管理するためにセットアップされた Meeting Management インスタンスに Meeting Server が初めて接続すると、その Meeting Server に以前にライセンスが適用されていたかどうかがチェックされます。適用されていなかった場合は、ライセンス有効期限が 90 日後に設定されます。

   セクション 2.2.4 に示すように、ライセンスの有効期限は Meeting Management に表示され、clusterLicensing API でも返されます

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

4. Meeting Management は、Meeting Server の遵守状態を確保するのに必要なライセンスがあることをチェックするために、毎日、クラスタの Meeting Server ライセンス使用状況を照合し、スマート アカウントに対してレポートします。スマート アカウントは Meeting Management に応答し、Meeting Server が遵守状態であるかどうかを提示します。その後、Meeting Management は、次のようにして有効期限を適切に設定します。
   a. Meeting Management は、ライセンスが存在しており特定の機能の使用権があることを特定すると、有効期限が 90 日後に延長されます。

> 注：Meeting Server が Meeting Management に接続して 90日間の使用状況データを送信しないと、Meeting Server のライセンスは更新されず、期限切れになります。ライセンスの有効期限が切れた場合の強制アクションの詳細については、セクション 2.2.2 を参照してください。

ライセンスの使用数が使用権を超えている場合、またはライセンスが見つからない場合は、次の強制措置が発生します。

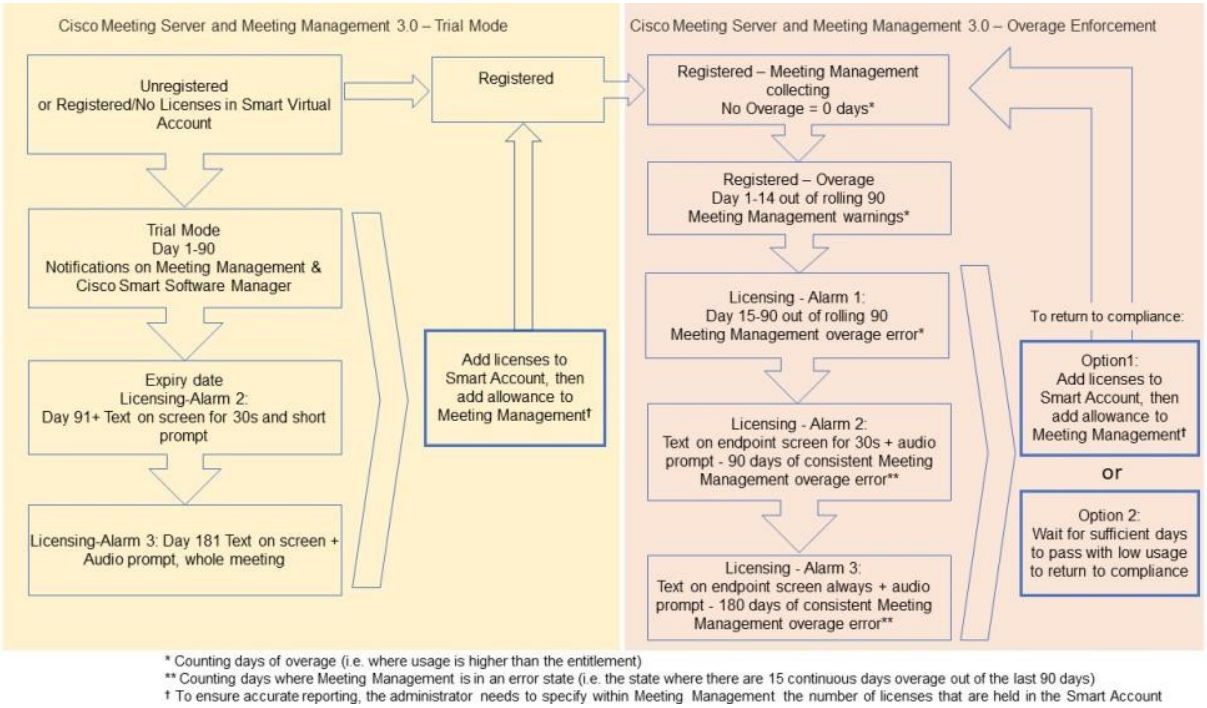
b. 遵守状態でなかったのが過去 90 日間のうち 15 日未満であることを Meeting Management が特定した場合、これを許容して Meeting Server の有効期限をその時点から 90 日後に再設定します。管理者に、ライセンス不足を通知するビジュアル警告が表示されます。

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

d. 超過使用が続く場合、Meeting Management は 90 日間の計算をリセットせず、新規ライセンスの追加期限までの日数がカウントダウンされます。ライセンスが追加されない場合、図 1 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 1 に、左側に示したトライアル モードでの初回起動から、右側に示した超過使用による強制までの、強制フローを示します。

図 1：Cisco Meeting Server と Cisco Meeting Management スマート ライセンスの強制フロー



注：すべての展開タイプでライセンスを有効化して管理する方法の詳細については、Cisco Meeting Management 3.0 のリリース ノートを参照してください。

2.2.2 機能ライセンスの有効期限切れによる強制アクション

従来は、Meeting Server は再起動時にのみライセンス ファイルを評価していました。3.0 以降では、機能にライセンスが付与されているかどうかの現在のステータスは動的に変化する可能性があります。たとえば、機能ライセンスの有効期限が切れた（従来はこれは再起動されるまで明らかになりませんでした）、API の変更があったなどの理由によるものです。Meeting Management は、スマート ライセンスまたは従来のライセンス ファイル モードを使用して強制アクションを計算します。

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

機能ライセンスが期限切れになると、表 5 に示したアクションが発生します。

表 5：期限切れライセンスの強制アクション

機能	操作
callBridge callBridgeNoEncryption PMP/SMP	期限切れの場合：すべての参加者およびすべてのミーティングに対し、ミーティング参加時にビジュアルなテキスト メッセージが画面に 30 秒間表示され、音声プロンプトが再生されます。（アラーム レベル 2） 90 日以上前に期限切れとなりライセンスが存在しない場合：それ以前と同様ですが、メッセージは永続的に表示されます。「Your deployment is out of licensing compliance, please contact your administrator（ライセンスが遵守されていません。管理者に連絡してください）」という音声プロンプトが再生されます。（アラーム レベル 3） 注：前述のアクションを回避するために必要なのは callBridge または callBridgeNoEncryption のみです。
customizations	期限切れであるかライセンスが存在しない場合、カスタマイズ機能はミーティング中にアクティブになりません。
録音	期限切れまたはライセンスが存在しない場合、（サードパーティのレコーダーであるかどうかにかかわらず）新規の録音を開始できなくなります。 このライセンスは録音とストリーミングに該当するため、ストリーミングにも同じ制限が適用されます。

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

2.2.3 スマート ライセンシング API の追加

この機能では、バージョン 3.0 で以下の API が追加されています。

新しい API オブジェクト：

- **`/clusterLicensing`**
- **`/clusterLicensing/raw`**

新しい API 応答値：

- **`clusterId`** が /system/status の応答値に追加されています。これは、Meeting Server が含まれるクラスタを識別する ID です。この ID は、クラスタが存続する間は変わりません。クラスタに新しい Call Bridge を割り当てると、それぞれに同じ clusterId が割り当てられます。クラスタ化されていない Meeting Server はメンバーが 1 つのクラスタと見なされるため、この応答パラメータには同様に 1 つの Meeting Server インスタンスに対応する値が設定されます。

従来は、既存の **/system/licensing** API がライセンス ファイルの内容を返していました。つまり、Meeting Server の機能コンポーネントが、各コンポーネントのライセンス ステータスと有効期限（該当する場合）と共に表示されていました。たとえば、Meeting Server で callbridge ライセンスがアクティブ化されているかどうか、また、ライセンスが付与されている場合はその有効期限が表示されていました。

3.0 以降では、既存の **/system/licensing** API ではライセンス ファイルの内容（つまり機能コンポーネント）だけが Meeting Server インスタンス単位で返され、新しく導入された API オブジェクト /clusterLicensing で、Meeting Server クラスタのライセンス ステータスと有効期限（該当する場合）が返されます。

注：新しい **/clusterLicensing** API はクラスタを表します（単独の Meeting Server の導入はメンバーが 1 つのクラスタと見なされます）。ライセンス ファイルの内容を表す **/system/licensing** API は、引き続き Meeting Server インスタンス単位での処理となります。

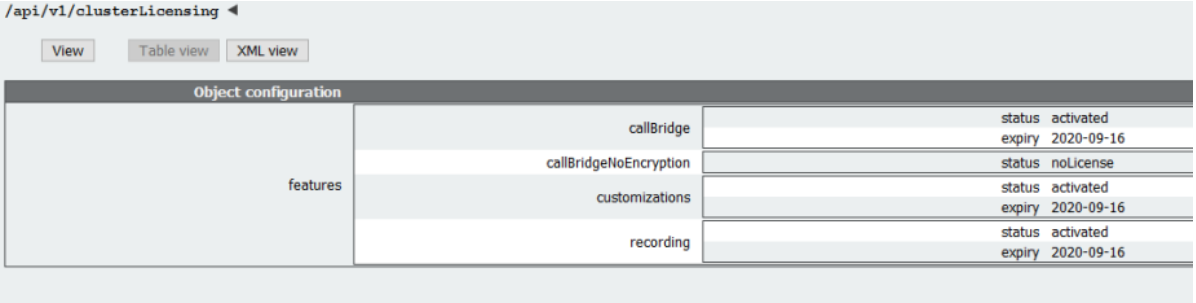
Meeting Server は新しい **/clusterLicensing/raw** API オブジェクトをサポートします。このオブジェクトは、ライセンス データを JSON フォーマットで書き込みます。必須のパラメータとして **data** と **signature** の 2 つがあり、信頼リンクの作成と Meeting Server ライセンスの発行のために Meeting Management によって使用されます。

2.2.4 ライセンス情報の取得方法

Meeting Server Web 管理インターフェイスを使用してクラスタのライセンス情報を取得するには、次の手順を実行します。

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

図 2：clusterLicensing API：ライセンス ステータス



2.2.5 MMP license コマンド

MMP コマンド **`license`** を使用すると、（/clusterLicensing API で実装されているように）クラスタにどのようなライセンスが付与されているかではなく、単一の Meeting Server インスタンスのローカルにある cms.lic 内のライセンスが表示されます。

2.3 Image Signing

Meeting Server バージョン 3.0 では、デバイスをアップグレードする際のセキュリティを向上するために、Image Signing が導入されています。この新機能では、Meeting Server のアップグレード イメージに署名が導入され、アップグレード イメージの検証（署名と完全性）が実行されます。Meeting Server は、これらの署名を使用して、アップグレード前にアップグレード イメージの真偽を検証します。

注：Meeting Server はセキュア ブートをサポートしていません。署名の検証は、アップグレード中にのみ実行されます。

従来は、すべてのアップグレード イメージの SHA-256 ハッシュを表示する MMP コマンド **`upgrade list`** を使用して、アップグレード イメージの完全性を検証することを管理者に推奨していました。この場合、管理者は、アップグレードを続行する前に、リリース ノートで公開されているハッシュと照合して手動で検証する必要がありました。

この新機能では、アップグレード イメージに署名を埋め込み、Meeting Server はその署名を使用してイメージが本物かどうかを確認します。改変されたイメージは Meeting Server によって拒否されます。このプロセスは、署名付きイメージにアップグレードする際に自動的に実行されるため、手動検証が不要になります。この方法によって、管理者は、Meeting Server にインストールして実行するイメージがシスコ提供の本物のイメージであり改変されていないことを確認できます。

イメージの署名は、署名付きイメージからアップグレードする場合にのみ検証されます。このため、署名されていないイメージから署名付きイメージにアップグレードする場合、つまり、2.9 から 3.0 へのアップグレード、または旧バージョンへのダウングレードでは、引き続き手動でハッシュを検証することを推奨します。この機能は、3.0 以降からアップグレードするときに完全に有効になります。

Meeting Server では、署名されていないイメージにアップグレードする前に次のプロンプトを表示し、確認を要求するようになりました。

アップグレード イメージの完全性を検証できません。（`The integrity of the upgrade image cannot be verified.`）

続行しますか。`(Y/n)`

注意：信頼されていないイメージにアップグレードすると、システムのセキュリティが侵害される可能性があります。署名されていないイメージにアップグレードする前に、必ずハッシュを手動で検証してください。

2.3.1 Image Signing の仕組み

アップグレード イメージには、秘密キーへのアクセスを制限するセキュアなシスコの内部サーバによって生成された署名が含まれます。公開キーは、実行中の Meeting Server のイメージ内に格納され、署名の検証に使用されます。この署名は、イメージ全体の真偽を検証するために使用されます。

2.3.2 アップグレード プロセスに導入された変更点

この新機能は、管理者に対してほとんど透過的です。Meeting Server は、従来と同じ方法でアップグレードできますが、次のような違いがあります。

- 署名されていないイメージにアップグレードすると、警告が表示され、続行するかどうかの確認を求められます（この動作はダウングレードのために必要です）。
- イメージが改変されている場合は、アップグレードが防止されます。
- 新しい MMP コマンドである **`upgrade <name> verify`** は、アップグレードを続行せずに、イメージのステータス（署名されているかどうか、改変されているかどうか）を検証します。アップグレード時には常に検証が実行されるため、このコマンドの使用は任意です。

- 新しい MMP コマンドである **authenticity** は、実行中のイメージのステータスを表示し、イメージの署名キーを管理します。キーの管理は、エンジニアリング用の特別なイメージを実行するために必要な場合にのみ、TAC の監督の下で実行してください。

  注：このソフトウェア バージョンにアップグレードするときに MMP コマンド **authenticity** を実行すると、[実行中のイメージの完全性を検証できませんでした（The integrity of the running image could not be verified）] と表示されます。これは、Image Signing をサポートしていないイメージから Meeting Server がアップグレードされ、新しいイメージの署名を検証できなかったことを示しているだけであり、問題ありません。

2.3.3 イメージの検証プロセス

管理者向けの新しいアップグレード プロセスは次のとおりです。

1. SFTP でアップグレード イメージを Meeting Server にアップロードします。Meeting Server は、この段階ではイメージの署名を検証しません。
2. MMP コンソールで、使用するイメージ名を指定してアップグレードを開始します。

   ```
   MMP> upgrade <upgrade_file.img>
   ```

Meeting Server は以下のように検証プロセスを実行します。

1. アップグレード パッケージを解凍します。
2. イメージの署名に使用されたキーのバージョンとキーのタイプを取得し、一致する公開キーが保持されていることを確認します。
3. 特別なキーを使用してイメージが署名されている場合は、インポートされたキーの署名を検証します。マスター キーはこのステップで使用されます。これは、EFT またはエンジニアリング用の特別なイメージのみに適用されます。
4. 署名を使用してイメージ全体の完全性を検証します。

上記のいずれかのステップが失敗した場合、Meeting Server は、拒否理由を示してそのイメージを拒否します。

2.3.4 署名付きイメージ ファイルの命名規則

イメージ ファイル名には次の規則が使用されます。

- ***[release_name]_s<s/p><a/b/…>.img***

値は次のとおりです。

- ***[release_name]***：リリース名
- ***_s***：ファイルが署名済みかどうかを示します
- ***<s/p>***：イメージが特別なものか実稼働環境用かを示します
- ***<a/b/…>***：キーのバージョンを示します

注：アップグレード イメージは Meeting Server にアップロードする前に名前を変更可能なため、名前に基づいてイメージ タイプを判別することはできません。イメージ タイプは、MMP コマンド **upgrade <name> verify** を使用して取得できます。

2.3.5 キー ファイルの命名規則

キー ファイル名には次の規則が使用されます。

- **CMS_[key identifier]_key_<a/b/...>_SPECIAL.pem**

説明：

- ***[key identifier]***：このキーを使用して署名された特別なアップグレード イメージがどれであるかを識別する情報
- ***<a/b/…>***：このキーが署名されたマスター キー バージョンを示します

注：キー ファイルの名前は変更できません。名前を変更したキーは Meeting Server によって拒否されます。

2.3.6 ファイル名の例

次の例では、バージョン「a」のキーを想定しています。

リリース イメージ	説明
upgrade_spa.img	内部リリース キーを使用して署名されたイメージ
vm_upgrade-3.0_spa.img	内部リリース キーを使用して署名されたイメージ

注意点：

- _spa サフィックスは、Meeting Server 内部のキーを使用して検証される実稼働環境用のイメージであることを意味します。
- キーをローテーションする必要がある場合は、キー バージョンが変わる可能性があります。

特別なキーを使用して署名されるのは、ベータまたはエンジニアリング用の特別なリリース ビルドのみです。実稼働用のビルドは、常にリリース キーを使用して署名されます。
特別なキーを使用して署名されたビルドに関する有用な情報を以下に示します。

- 典型的なファイル名の例：upgrade_ssa.img
- このタイプのアップグレードを実行する前に、特別なキーを Meeting Server にアップロードする必要があります。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。
- 特別なキーを使用して署名されたリリースから 3.0 以降にアップグレードする場合は、管理者による特別な操作は必要ありません。

2.4 最小パスコード長ポリシー

バージョン 3.0 では、最小パスコード長の機能が導入されました。これは、セキュリティを強化し個別の企業のセキュリティ ポリシーを遵守するために、管理者が設定できます。
最小パスコード長は、IVR、直接 SIP ダイヤル、Web アプリケーションなど、さまざまなダイヤルインの方法すべてに適用できます。

最小パスコード長は、新しい API オブジェクト **/dialInSecurityProfiles** で定義されます。新規に定義されたセキュリティ プロファイルは、最上位レベル（グローバル）のプロファイル、テナント、coSpace、accessMethods のいずれかに割り当てることができます。このプロファイルは、coSpaceTemplates および /coSpaceTemplates/<coSpace template id>/accessMethodTemplates にも割り当てることができます。

プロファイルには階層があり、階層の下位にあるプロファイルの値が上位の値より優先されます。また、パラメータが設定されていない場合やダイヤルイン セキュリティ プロファイルが設定されていない場合は、階層内で次に上位にあたるプロファイルから継承されます。

dialInSecurityProfile の階層は次のとおりです。

- 最上位レベル（グローバル）プロファイル（**/system/profiles**）
- テナント（**/tenants/<tenant id>**）
- coSpace（**/coSpaces/<cospace id>**）
- accessMethod（**/coSpaces/<cospace id>/accessMethods/<access method id>**）

ダイヤルイン セキュリティ プロファイルは、次の coSpace テンプレートおよび coSpace アクセス方式テンプレートにも適用できます。

- coSpaceTemplates（**/coSpaceTemplates/<coSpace template id>**）
- accessMethodTemplates（**/coSpaceTemplates/<coSpace template id>/accessMethodTemplates/<access method template id>**）

coSpaces および関連するアクセス方式がテンプレートからインスタンス化されるときに、テンプレートからダイヤルイン セキュリティ プロファイルが対応するインスタンス化されたオブジェクトに割り当てられます。

プロファイルの使用の詳細については、『API Reference Guide（API リファレンス ガイド）』[英語] の 14 章を参照してください。

注：スケジュールされたミーティングでバージョン 15.12.0 より前の TMS を使用する場合、CUCM アドホック会議コールではシステム レベルまたはテナント レベルでセキュリティ プロファイルが設定されません。

注：パラメータ **minPasscodeLength** が 0 に設定されている場合、パスコード長は適用されません。

この機能では、バージョン 3.0 で以下の API が追加されています。

新しい API オブジェクト：

- **/dialInSecurityProfiles**
- **/dialInSecurityProfiles/<dial in security profile id>**

新しい API 要求と応答パラメータ：

- **dialInSecurityProfile**

新しいエラー コード：

- **dialInSecurityProfileDoesNotExist**
- **passcodeTooShort**

2.4.1 Meeting Server がパスコードの変更を検証する仕組み

API、Web 管理インターフェイス（[設定（Configuration）]> [スペース（Spaces）]））、または Web アプリケーションを使用して coSpace または accessMethod のパスコードを変更するときに、coSpace または accessMethod がコール可能である場合、つまり URI またはコール ID、または coSpace の場合はセカンダリ URI が設定されている場合、新しいパスコードがポリシーに従っているかどうかが検証されます。つまり、パスコード長が coSpace または accessMethod の有効な minPasscodeLength 以上であるかどうかが検証されます。

新しいパスコードがポリシーに従っている場合は、変更は正常に受け付けられます。新しいパスコードが短すぎる場合は、変更は拒否されます。その場合、API は、HTTP 応答コード「403 Forbidden」（理由 **passcodeTooShort**）を使用して変更を拒否します。Web アプリケーションのユーザには、[パスコードは n 桁以上で指定してください（Passcode requires at least n digits）]（n は最小パスコード長）というメッセージが表示されます。

注：coSpace テンプレートから coSpace を作成するときは、ダイヤルイン セキュリティ プロファイルがグローバル、テナント レベル、coSpace テンプレート レベルのいずれで設定されているかにかかわらず、作成される coSpace には URI、コール ID、またはパスコードは設定されません。この coSpace はコール可能ではないため、Meeting Server では、設定されている既存のダイヤルイン セキュリティ プロファイルに従っていることを必要としません。それよりも後の段階で coSpace に URI またはコール ID（またはセカ

ンダリ URI）が割り当てられ、パスコードが更新されていない場合に、minPasscodeLength の有効な値が 0 よりも大きく、allowOutOfPolicy の有効な値が false であると、その coSpace に参加しようとすると失敗します。テンプレートから作成されるアクセス方式には常に URI が設定されるため、ダイヤルイン セキュリティ プロファイルの階層に基づいてパスコードが自動生成されます。

パスコードを使用してミーティングに参加する場合（SIP または Web アプリケーション）、Meeting Server は、入力されたパスコードがポリシーに従っているかどうかをチェックしますが、現在設定されているパスコードがポリシーに従っていない場合（つまり minPasscodeLength 設定に対してパスコードが短すぎる場合）にも追加のアクションも実行します。この動作は次のようになります。

- **`allowOutOfPolicy=true`** である場合は、パスコードが短すぎる場合に Meeting Server は追加のアクションを実行しません。ただし、ミーティングに参加するためには正しいパスコードが必要です。
- **`allowOutOfPolicy=false`** である場合、パスコードが正しい場合でもミーティングに参加できません。このとき、パスコードが正しいがポリシーに従っていない場合には、管理者がアクションを実行するためのメッセージが syslog に記録されます。

注：ユーザからは、ポリシー違反による拒否は、パスワードが正しくない場合と同じように見えます。

2.4.2 最小パスコード長の作成と適用の方法

1. Meeting Server Web 管理インターフェイスを使用して dialInSecurityProfile を作成するには、次の手順を実行します。
    a. Meeting Server Web 管理インターフェイスにログインし、[設定（Configuration）] > [API]を選択します。
    b. API オブジェクトのリストから、/api/v1/dialInSecurityProfiles の後ろにある ► をタップします。
    c. [新規作成（Create new）]をクリックします。

d. [名前（name）]フィールドに、セキュリティ プロファイルに付ける名前を設定します。

e. [minPasscodeLength]フィールドに、許可する最小パスコード長を 0 ～ 200（0 と 200 を含む）の範囲で設定します。

f. [allowOutOfPolicy]フィールドを true または false のいずれかに設定します。このフィールドによって決定されるのは、ダイヤルイン セキュリティ プロファイルが適用される前に設定され、新たに定義されたパスコード長を遵守しなくなった古いパスコードを、ユーザが使用してコールに参加することを許可するかどうかです。このパラメータが指定されていない場合、デフォルトは true になります。

g. [作成（Create）]をクリックします。

2. 必要に応じて、新しく作成された dialInSecurityProfile を以下のいずれかまたはすべてに割り当てます。

- 最上位レベル（グローバル）プロファイル/api/v1/system/profiles）
- テナント（/api/v1/tenants/<*id*>）
- coSpace（/api/v1/coSpaces/<*id*>）
- accessMethod（/api/v1/coSpaces/<*id*>/accessMethods/<*id*>）
- coSpaceTemplates（/api/v1/coSpaceTemplates/<*id*>）
- accessMethodTemplates（/api/v1/coSpaceTemplates/<*id*>/accessMethodTemplates/<*id*>）

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

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

b. [表示（View）]または [Edit（編集）] をクリックします。

c. パラメータ dialInSecurityProfile まで下にスクロールし、[選択（Choose）]をクリックします。

d. 結果として表示される dialInSecurityProfile オブジェクト セレクタ ウィンドウで、最上位レベルのグローバル プロファイルに割り当てる、ステップ 1 で作成した dialInSecurityProfile の**オブジェクト** ID に対して [選択（Select）]をクリックします。

e. [変更（Modify）]をクリックします。

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

2.5 SIP レコーダおよびストリーマ

従来、Meeting Server の内部レコーダおよびストリーマ コンポーネントは Meeting Server の内部 XMPP サーバ コンポーネントに依存していました。3.0 では、この XMPP サーバが削除されています。バージョン 3.0 では、SIP ベースの新しい内部レコーダーおよびストリーマが導入されています。

この新しい内部レコーダおよびストリーマ コンポーネントと、サードパーティの SIP レコーダーへのダイヤルアウトはすべて、SIP URI を使用して設定されます。このため、録音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。

2.5.1 新しいレコーダーおよびストリーマ機能の利点

- 新しいレコーダーとストリーマは、レイアウトの変更をサポートしています。レコーダーおよびストリーマは他の SIP コールと同様の方法で、つまり callLegProfile 階層または coSpace オブジェクトの defaultLayout パラメータからレイアウトを取得します。また、callLeg のレイアウト パラメータを変更することもできます。
- カスタム レイアウトは、layoutTemplate パラメータを使用して設定できます（カスタム レイアウトを実装するには、カスタマイズ ライセンスが必要です）。
- callLegProfiles および callLegs の qualityMain パラメータを使用して、最大解像度を callLeg 単位で制御できます。
- 従来の XMPP ストリーマは 720p の解像度のみをサポートしていましたが、新しいストリーマは最大 1080p の解像度をサポートします。また、3.0 では、MMP コマンド **`streamer sip resolution`** を使用してストリーマの解像度を選択できます。

- callLegProfile の presentationViewingAllowed パラメータ設定を変更することで、ストリーマまたはレコーダーでプレゼンテーションを受信するかどうかを選択できます。
- 新しい MMP コマンド **`recorder limit`** と **`streamer limit`** が導入され、拡張性が向上しました。

2.5.2 新しい内部レコーダおよびストリーマを実装する際の注意点

- 新しいストリーマおよびレコーダーのサポート、およびサードパーティの外部 SIP レコーダーの使用には、引き続き Meeting Server の録音ライセンスが必要です。
- レコーダーおよびストリーマ アプリケーションは、仮想化された展開（Meeting Server 1000 を含む）でのみサポートされます。
- Meeting Server 2000 ではレコーダーまたはストリーマの実行はサポートされません。
- 3.0 にアップグレードする際に、MMP インターフェイスを使用してレコーダーとストリーマを展開し直す必要があります。新しいレコーダーおよびストリーマで使用する MMP コマンドは、従来使用されていたものと異なります。（詳細については、後述するレコーダーおよびストリーマーの展開に関するセクションを参照してください）。
- レコーダーおよびストリーマを Call Bridge と同じ場所に配置して実行することは推奨しません。このような構成は、テスト目的でのラボ シナリオ以外ではサポートされません。レコーダーおよびストリーマは、Call Bridge とは別の VM に構成する必要があります。
- レコーダーとストリーマの両方を同じ VM 上で実行することは推奨しません。
- 3.0 より前のバージョンでレコーダーおよびストリーマ用に使用されていた API オブジェクト **`/recorders`** と **`/streamers`** は削除されています。

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

2.5.2.1 新しい内部 SIP レコーダー コンポーネント用の VM のサイジング

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

表 6：内部 SIP レコーダーのパフォーマンスとリソース使用率

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

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

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

2.5.2.2 新しい内部 SIP ストリーマ コンポーネント用の VM のサイジング

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

表 7：内部 SIP ストリーマの推奨仕様

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

注意すべき重要事項（新しい内部レコーダー コンポーネントとストリーマ コンポーネントの両方に適用されます）：

- vCPU 数が物理コア数をオーバーサブスクライブすることは避けるべきです。

- サポートされる 720p ストリームの最大数は、vCPU の増設に関係なく 200 です。
- サポートされる 1080p ストリームの最大数は、vCPU の増設に関係なく 150 です。
- サポートされるオーディオ専用ストリームの最大数は、vCPU の増設に関係なく 200 です。

2.5.3 SIP ストリーマを指定するための新しい API コマンド

/callProfiles オブジェクト用の新しい API パラメータが導入され、SIP ストリーマの URI を指定するための文字列を値として取ります。GET、PUT、および POST をサポートしており、次のように定義されます。

- **sipStreamerUri**：これを設定した場合、ストリーミングがオンになると、ダイヤルアウトするためにこの URI が使用されます。

注：API パラメータ **sipRecorderUri** はバージョン 2.9 で導入され、API コール プロファイル オブジェクトでも指定されます。

2.5.4 新しい MMP コマンド

3.0 より前のバージョンでは、証明書と信頼に関するコマンドで、Call Bridge とレコーダーおよびストリーマー コンポーネントとの間の https リンクを参照していました。これらは、3.0 の新しいレコーダーおよびストリーマ コンポーネントでは不要になりました。その代わりに、Meeting Server では、新しい MMP コマンド **recorder sip certs** と **streamer sip certs** を使用して SIP 証明書を設定できます。

3.0 より前のバージョンでの listen コマンドは、Call Bridge からの https 接続のリッスンを参照していました。新しいレコーダーおよびストリーマ コンポーネントでは、https 接続をリッスンする必要はなくなりましたが、SIP 接続をリッスンする必要があります。このために、TCP と TLS の両方を設定する次の新しい MMP コマンドが導入されました。**recorder sip listen <interface> <tcp-port|none> <tls-port|none>**

ストリーマまたはレコーダー上のすべての SIP メッセージのロギングを有効にするために、ストリーマおよびレコーダーの新しいコマンド **sip trace** が導入されました。

すべての新しい MMP コマンドと廃止の詳細については、該当するセクションを参照してください。

2.5.5 VM サーバでの新しいレコーダー コンポーネントの展開

これは 2 段階からなるプロセスです。

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

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

1. バージョン 3.0 にアップグレードします。
2. MMP に SSH 接続し、ログインしてレコーダーを設定します（MMP コマンド **recorder** を入力すると、使用可能なすべてのコマンドのリストが表示されます）。
3. **recorder nfs <hostname/IP>:<directory>** と入力し、NFS のロケーションを設定します。
4. **recorder resolution <audio|720p|1080p>**と入力し、希望の解像度を設定します（またはコールの音声のみの録音に設定します）。
5. MMP コマンド **recorder sip listen <interface> <tcp-port|none> <tls-port|none>** を使用して、レコーダーのリスニング インターフェイスと、リッスンする SIP TCP ポートおよび TLS ポートを設定します。サービスを無効にするには、該当するポートを **none** に設定します。
   a. たとえば、TLS ポートのみをリッスンし、TCP ポートはリッスンしない場合は、**recorder sip listen a none 6000** と入力します。
   b. デフォルトの TCP/TLS ポート（5060/5061）以外を指定する場合は、後で必要になるため、ポートを書き留めておきます。

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

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

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

7. TLS を設定した場合は、必要に応じて、レコーダーでの SIP の TLS 検証を次のように実行できます。
   a. MMP 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 接続をセキュアにするためには、TLS 検証を有効にすることを推奨します。

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

タスク 2：API を使用したレコーダー URI の設定

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

必要に応じて、outboundDialPlan ルールにマップされるカスタム URI を設定することもできます（ドメインは、「recording.com」のように任意に指定できます）。**`sipRecorderUri`** で使用されるドメインをレコーダーにルーティングする方法を Meeting Server に指示するために、outboundDialPlan ルールを設定する 必要があります。これにより、優先度の値、暗号化などを制御できます。outboundDialPlan ルール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：設定される URI のユーザ 部分（@ 記号より前の部分）は特に意味を持ちませんが、新しい内部 SIP レコーダー コンポーネントの場合は必須であるため、「recording@recorder.com」のように任意の値を設定できます。ただし、サードパーティの SIP レコーダーでは、たとえば URI のユーザ部分をユーザのログイン上方として使用する可能性があるため、このことが該当しない場合があります。URI で重要なのはドメインの部分です。

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

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

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

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

必要に応じて、更新された callProfile を、coSpace、テナント、または最上位レベル（グローバル）プロファイルに割り当てることができます。この例では、以下の手順で、更新された callProfile をグローバル レベルに割り当てます。

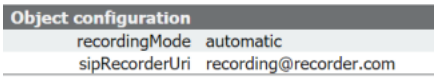
1. Web 管理インターフェイスを使用して、[設定（Configuration）] > [API]を選択します。
   a. API オブジェクトのリストから、/api/v1/system/profiles の後ろにある ► をタップします。
   b. [表示（View）]または [Edit（編集）] をクリックします。
   c. パラメータ callProfile まで下にスクロールし、[選択（Choose）]をクリックします。
   d. 結果として表示される callProfile オブジェクト セレクタ ウィンドウで、最上位レベルのグローバル プロファイルに割り当てる callProfile の**オブジェクト** ID に対して [選択（Select）]をクリックします。

e. [変更（Modify）]をクリックします。

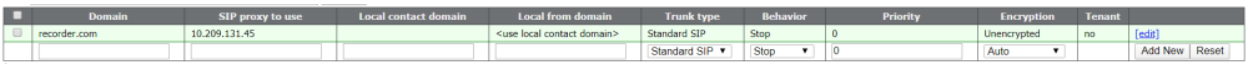
f. 新たに割り当てた callProfile オブジェクトの ID が、[オブジェクトコンフィギュレーション（Object configuration）]の下にリストされます。

2.5.5.1 callProfile の設定例（一致するアウトバウンド ダイヤル プラン ルールを使用している場合）

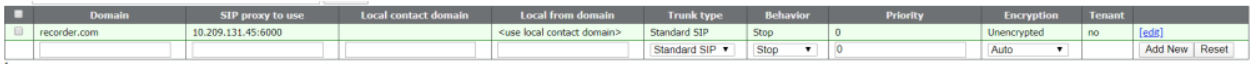
この例では、前述の手順を使用して recordingMode は automatic に設定され、sipRecorderUri は recording@recorder.com に設定されています。



Meeting Server Web 管理インターフェイスから [設定（Configuration）] > [アウトバウンドコール（Outbound calls）]を選択して、一致するアウトバウンド ダイヤル プラン ルールを表示します。



デフォルトの標準ポート（5060/5061）と異なる SIP TCP/TLS ポートを使用するようにレコーダーを MMP で設定した場合は、次のように、リスニング ポートを [sipRecorderUri] フィールドで指定するか、アウトバウンド ダイヤル プラン ルールを使用している場合は一致するルールで指定する必要があります。



アウトバウンド ダイヤル プラン ルールを使用している場合は、指定されたポートのサービスが暗号化タイプと一致している必要があります。たとえば、SIP TLS ポートを使用する場合は、[暗号化（Encryption）]モードを Encrypted に設定します。

2.5.6 VM サーバでの新しいストリーマ コンポーネントの展開

これは 2 段階からなるプロセスです。

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

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

1. バージョン 3.0 にアップグレードします。
2. MMP に SSH 接続し、ログインしてレコーダーを設定します（MMP コマンド **streamer help** を入力すると、使用可能なすべてのコマンドのリストが表示されます）。
3. MMP コマンド **streamer sip listen <interface> <tcp-port|none> <tls-port|none>** を使用して、ストリーマのリスニング インターフェイスと、リッスンする SIP TCP ポートおよび TLS ポートを設定します。サービスを無効にするには、該当するポートを **none** に設定します。
   a. たとえば、TLS ポートのみをリッスンし、TCP ポートはリッスンしない場合は、streamer sip listen a none 6000 と入力します。
   b. デフォルトの TCP/TLS ポート（5060/5061）以外を指定する場合は、後で必要になるため、ポートを書き留めておきます。
4. 必要に応じて、MMP コマンド **streamer sip resolution <audio|720p|1080p>** を使用して、ストリーマで使用する最大解像度を設定できます（またはコールの音声のみをストリームするように設定できます）。設定しない場合、デフォルトで 720p になります。
   a. たとえば、1080p に設定する場合は **streamer sip resolution 1080p** と入力します。

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

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

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

6. TLS を設定した場合は、必要に応じて、ストリーマでの 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 接続をセキュアにするためには、TLS 検証を有効にすることを推奨します。

7. 設定が正しいことを確認します。MMP コマンド **`streamer`** を入力して、設定を表示します。
8. MMP コマンド **`streamer enable`** を入力して、ストリーマ サービスを有効にします。

タスク 2：API を使用したストリーマ URI の設定

新しい SIP ストリーマが有効になると、API コール プロファイル オブジェクトで指定する API パラメータ **`sipStreamerUri`** を使用して、Call Bridge で設定して使用することができます。

必要に応じて、outboundDialPlan ルールにマップされるカスタム URI を設定することもできます（ドメインは、「streaming.com」のように任意に指定できます）。**`sipStreamerUri`** で使用されるドメインをストリーマにルーティングする方法を Meeting Server に指示するために、outboundDialPlan ルールを設定する 必要があります。これにより、優先度の値、暗号化などを制御できます。**`outboundDialPlanRules`** の設定の詳細については、導入ガイドの「ダイヤル プランの設定：概要」の章を参照してください。

注：設定される URI のユーザ 部分（@ 記号より前の部分）は特に意味を持ちませんが、新しい内部 SIP ストリーマ コンポーネントの場合は必須であるため、「streaming@streamer.com」のように任意の値を設定できます。URI で重要なのはドメインの部分です。

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

1. Meeting Server Web 管理インターフェイスにログインし、[設定（Configuration）] > [API]を選択します。
2. API オブジェクトのリストから、/api/v1/callProfiles の後ろにある ▶ をタップします。

3. 既存のコール プロファイルを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、[sipStreamerUri] フィールドに希望の URI を入力します。

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

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

必要に応じて、更新された callProfile を、coSpace、テナント、または最上位レベル（グローバル）プロファイルに割り当てることができます。この例では、以下の手順で、更新された callProfile をグローバル レベルに割り当てます。

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

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

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

2.5.7 既知の制限事項

注意：ストリーム URL は SIP ヘッダーを使用して送信されるため、ログイン情報を含む RTMP ストリーム URL はコール制御プロバイダーに公開され記録される可能性があることに注意してください。

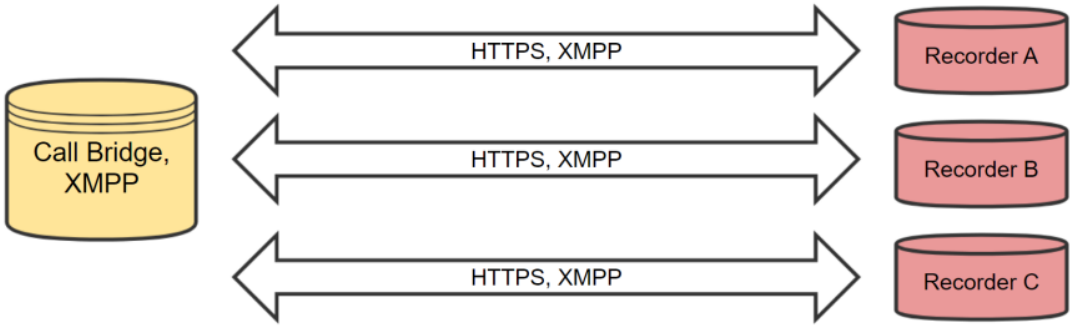
新しい SIP ストリーマ コンポーネントは RTMPS をサポートしていません。

2.5.8 拡張性と復元力を重視したレコーダーとストリームの展開

複数のレコーダーまたはストリーマを展開する場合は、コール制御プロバイダーの背後に配置し、コール制御プロバイダーがロード バランシングとフェールオーバーのサポートを提供できるようにすることを推奨します。コールをプロキシに転送することが可能なダイヤル プランルールをポイントするように、API パラメータ **`sipRecorderUri`** を設定する必要があります。

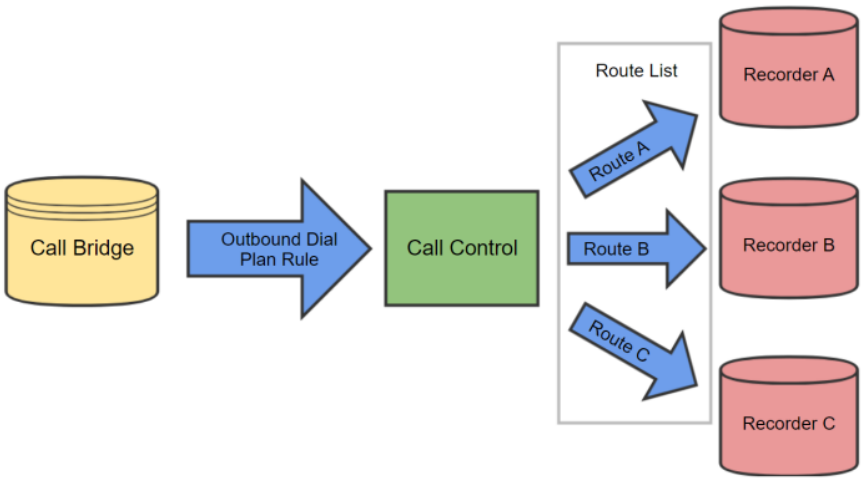
新しいレコーダーのコール制御フローの動作は、従来の XMPP レコーダーでの動作とは異なります。従来は、図 3 に示すように、レコーダーは XMPP クライアントとして Call Bridge に直接接続し、HTTPS リンクを介して可用性の情報を送信していました。

図 3：従来の XMPP レコーダーのコール制御フロー



新しい内部 SIP レコーダー コンポーネントの場合、コール制御はコール制御プロバイダーを経由します。その間、ほとんどの場合、メディアは Call Bridge とレコーダーの間を直接流れます。コール制御プロバイダーの設定によっては、メディアがコール制御プロバイダーを経由することもあります。図 4 に、この新しいレコーダーのコール制御フローを示します。

図 4：新しい内部 SIP レコーダーのコール制御フロー



2.5.8.1 サポートされるコール制御方式

- Cisco Unified Communications Manager：クラスタ内のレコーダーをそれぞれ SIP トランクの背後に展開し、クラスタ内の各レコーダーを同じルート リストに関連付ける必要があります。

- Cisco Expressway：1 つのルート パターンをクラスタ内のすべてのレコーダーにマッピングして、各レコーダーが独自のゾーンを持つように設定する必要があります。
- **ダイレクト フロー**：ダイヤル プラン ルールのプロキシをレコーダーまたはストリーマのアドレス/FQDN に設定できますが、これはインスタンスを 1 つだけ展開する場合にのみ推奨します。

詳細については、Cisco Meeting Server 2.x の『Cisco Meeting Server 間でのコールのロードバランシング ホワイト ペーパー』を参照してください。

2.6 API での Web Bridge のプロファイルと設定

バージョン 3.0 では、Web 管理ユーザ インターフェイスの [設定（Configuration）] > [一般（General）]ページから [Web Bridgeの設定（Web bridge settings）]オプションが削除されています。この Web Bridge の設定は API に移動され、重複していた一部の設定オプションが削除されました。Web Bridge の設定は API から実行しますが、主に Web 管理インターフェイスの [設定（Configuration）] > [API] ページを使用します。

注：[Web Bridge URI]フィールドと [IVR電話番号（IVR telephone number）]フィールドは、現在も Web 管理ユーザ インターフェイスの [設定（Configuration）] > [一般（General）] ページの [外部アクセス（External access）]の下で設定します。これらの設定フィールドは、将来のリリースで Web Bridge プロファイルに移動される可能性があります。

新しく導入されたこれらの変更により、Web Bridge 単位で個別に設定するのではなく、いくつかの Web Bridge 設定オプションを使用して、同じ設定をすべての Web Bridge または指定した Web Bridge のグループに適用できるようになります。

この変更をサポートするために、Web Bridge のさまざまな設定オプションを含む API オブジェクト /webBridgeProfiles が導入されました。新しく定義した Web Bridge プロファイルは、個別の webBridge オブジェクト、トップ レベル（グローバル）プロファイル、テナントのいずれかに割り当てることができます。

プロファイルには階層があり、階層の下位にあるプロファイルの値が上位の値より優先されます。また、パラメータが設定されていない場合や Web Bridge プロファイルが設定されていない場合は、階層内で次に上位にあたるプロファイルから継承されます。

webBridgeProfiles の階層は次のとおりです。

- 最上位レベル（グローバル）プロファイル（**/system/profiles**）
- テナント（**/tenants/<tenant id>**）
- webBridges（**/webBridges/<webbridge id>**）

2.6.1 Web 管理ユーザ インターフェイスの変更

従来は、図 5 に示すように [設定（Configuration）] > [一般（General）]ページに Web Bridge の設定オプションが含まれていました。これらのオプションは、このページから削除されています。

図 5：3.0 の Web 管理ユーザ インターフェイスから削除された Web Bridge の設定

[Web Bridge の設定（Web bridge settings）]の下にあったフィールド は、3.0 では以下のような扱いになります。

- [ゲストアカウントクライアントURI（Guest account client URI）]：Web アプリケーションの展開には不要であるため削除されました
- [ゲストアカウントJIDドメイン（Guest account JID domain）]：Web アプリケーションの展開には不要であるため削除されました
- [ハイパーリンク経由のゲストアクセス（Guest access via hyperlinks）]：allowSecrets の下の webBridgeProfiles に移動しました
- [ユーザサインイン（User sign in）]：webBridgeProfiles の下の userPortalEnabled で置き換えられました
- [スケジュールされたLync会議にIDを使用して参加（Joining scheduled lync conferences by ID）]：resolveLyncConferenceIds として webBridgeProfiles に移動されました

2.6.2 API の追加と変更

この機能では、バージョン 3.0 で以下の API が追加されています。

新しい API オブジェクト：

- **/webBridgeProfiles**
- **/webBridgeProfiles/<web bridge profile id>**
- **/webBridges/<web bridge id>/effectiveWebBridgeProfile**
- **/tenants/<tenant id>/effectiveWebBridgeProfile**
- **/system/profiles/effectiveWebBridgeProfile**

新しい API 要求と応答パラメータ：

- **webBridgeProfile**

新しいエラー コード：

- **webBridgeProfileDoesNotExist**

移動された API 要求と応答パラメータ：

従来は、resolveCoSpaceUris パラメータは API オブジェクト /webBridges/<web bridge id> に存在していました。バージョン 3.0 以降では、このパラメータは以下の API オブジェクトに存在します。

- **/webBridgeProfiles**
- **/webBridgeProfiles/<web bridge profile id>**
- **/webBridges/<web bridge id>/effectiveWebBridgeProfile**
- **/tenants/<tenant id>/effectiveWebBridgeProfile**
- **/system/profiles/effectiveWebBridgeProfile**

API オブジェクト **/webBridges/<web bridge id>** に存在していたその他のパラメータは、3.0 で移動されたか削除されました。

- **resourceArchive**：webBridgeProfiles に移動されました
- **idEntryMode**：廃止されました
- **allowWeblinkAccess**：**allowSecrets** として **webBridgeProfiles** に存在します
- **showSignIn**：**userPortalEnabled** として **webBridgeProfiles** に存在します

- **resolveCoSpaceCallIds**：webBridgeProfiles に移動しました
- **resolveLyncConferenceIds**：webBridgeProfiles に移動しました

2.6.3 Web Bridge プロファイルの作成と適用の方法

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

h. [userPortalEnabled]フィールドを true または false のいずれかに設定します。このフィールドによって決定されるのは、この Web Bridge プロファイルを使用する Web Bridge で、インデックス ページにサインイン タブを表示するかどうかです。このパラメータが指定されていない場合、デフォルトは true になります。

i. [allowUnauthenticatedGuests]フィールドを true または false のいずれかに設定します。true に設定した場合、この Web Bridge プロファイルを使用するWeb Bridge でランディング画面からのゲスト アクセスが許可されます。false に設定した場合、ゲスト アクセスは、ユーザ ポータルへのログイン後にのみ許可されます。このパラメータが指定されていない場合、デフォルトは true になります。

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

k. [resolveLyncConferenceIds]フィールドを true または false のいずれかに設定します。このフィールドによって決定されるのは、この Web Bridge プロファイルを使用する Web Bridge で、スケジュールされた Lync 会議 ID に解決される ID を受け付けるかどうかです。このパラメータが指定されていない場合、デフォルトは false になります。（このフィールドは表示されますが、3.0 では機能しません）。

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

m. [作成（Create）]をクリックします。

2. 必要に応じて、新しく作成された webBridgeProfile を以下のいずれかまたはすべてに割り当てます。

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

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

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

    b. [表示（View）]または [Edit（編集）] をクリックします。

    c. パラメータ webBridgeProfile まで下にスクロールし、[選択（Choose）] をクリックします。

    d. 結果として表示される webBridgeProfile オブジェクト セレクタ ウィンドウで、最上位レベルのグローバル プロファイルに割り当てる、ステップ 1 で作成した webBridgeProfile の**オブジェクト** ID に対して [選択（Select）]をクリックします。

    e. [変更（Modify）]をクリックします。

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

2.7 Cisco Meeting Server Web アプリケーションの新機能と変更

バージョン 3.0 では、Cisco Meeting Server Web アプリケーションにいくつかの新機能と変更が導入されています。また、Web アプリケーションの拡張性が向上しています。コールキャパシティの詳細については、「はじめに」を参照してください。

注：3.0 の Web アプリケーションのすべての新機能の詳細については、『Cisco Meeting Server 3.0 web app Important Information（Cisco Meeting Server 3.0 Web アプリケーション重要事項）』を参照してください。以下に示す Web アプリケーションの新機能では、サーバ側の設定が必要な場合があります。

2.7.1 Cisco Meeting Server Web アプリケーションでのビデオ アドレス（URI）によるミーティングへの参加

バージョン 3.0 では、参加者がビデオ アドレス（URI）を入力することで Web アプリケーション上でミーティングに参加できます。

この機能は 3.0 で実行可能であり、インバウンド ダイヤル プラン ルールが適切に設定されていることを前提として、管理者による設定は不要です。具体的には、（当該の Web Bridge 3 と同じテナント下にある）インバウンド ダイヤル プラン ルールで、coSpace へのダイヤルインを許可するように設定されている、つまり [ターゲットスペース（Targets spaces）]が [はい（yes）]に設定されている、いずれかのドメインである場合です。

ドメイン名は、Meeting Server Web 管理インターフェイスの [設定（Configuration）] > [着信コール（Incoming Calls）] > [コールマッチング（Call Matching）]で設定します。

2.7.2 Web アプリケーションからの参加者のアクセス許可の変更

3.0 では、Web アプリケーション（Web Bridge 3）からの参加者に対するアクセス許可が、従来の WebRTC 用ミーティング アプリケーション（Web Bridge 2）の動作とは変更されています。

従来は、参加者がスペースのメンバーであるかどうかに基づいて、参加者を追加または削除することができました。3.0 以降では、Web アプリケーションについては、たとえば SIP の参加者に対して想定されるのと同様に、CallLeg に関連付けられた CallLegProfile によって制御されます。

Web アプリケーションからの参加者向けに実装された **`/CallLeg/CallLegProfile`** プロパティは、**`disconnectOthersAllowed`**、**`endCallAllowed`**、**`addParticipantAllowed`** です。

詳細については、『API Reference Guide（API リファレンス ガイド）』[英語] を参照してください。

2.7.3 ビデオ会議で Web アプリケーションからの参加者に表示される名前ラベルの動作の変更

ビデオ会議で Web アプリケーションからの参加者に表示される名前ラベルの動作は、SIP コールでの表示と同じになりました。つまり、汎用的な callLegProfile の participantLabels 設定によって指定されるのではなく、SIP の名前ラベルに従って表示されます。

2.7.4 Web アプリケーションのその他の機能の追加

バージョン 3.0 では、Web アプリケーション インターフェイスに次の機能に対する制御が導入されています。

- 録画とストリーミング
- ミーティングのロック/ロック解除
- 重要度

Web Bridge 3 でこれらの機能を使用するためのアクセス許可はすべて API の CallLegProfile 設定で定義されるため、Web Bridge 2 でのこれらの機能の実装と変わりありません。

2.7.5 C2W 接続の証明書の変更

3.0 では、Web Bridge 3 での C2W 接続用の証明書が変更され、信頼ストアでルート証明書が不要になりました。これにより、管理者は、どの証明書を信頼するかをより柔軟に選択できます。たとえば、管理者が社内のポリシーに従って C2W 接続を保護するために公開証明書を使用する必要がある場合でも、その公開 CA によって署名されたすべての証明書を信頼することなく、接続先で使用されるクライアントまたはサーバの C2W 証明書だけを信頼することができます。これは、証明書のピンニングと呼ばれます。

2.7.6 Web アプリケーションのサインイン ページのカスタマイズ

バージョン 3.0 では、Cisco Meeting Server Web アプリケーションのサインイン ページのカスタマイズとブランディングが導入されました。

注：以前の WebRTC 用 Cisco ミーティング アプリケーションでのブランディング zip ファイルを使用することはできません。Web アプリケーション専用の新しいブランディング zip ファイルを作成する必要があります。ただし、ブランディング zip ファイルは、従来の WebRTC アプリケーションと同じ方法で Web アプリケーション用に展開されます。（resourceArchive は webBridgeProfiles API の下に移動されたことに注意してください）。

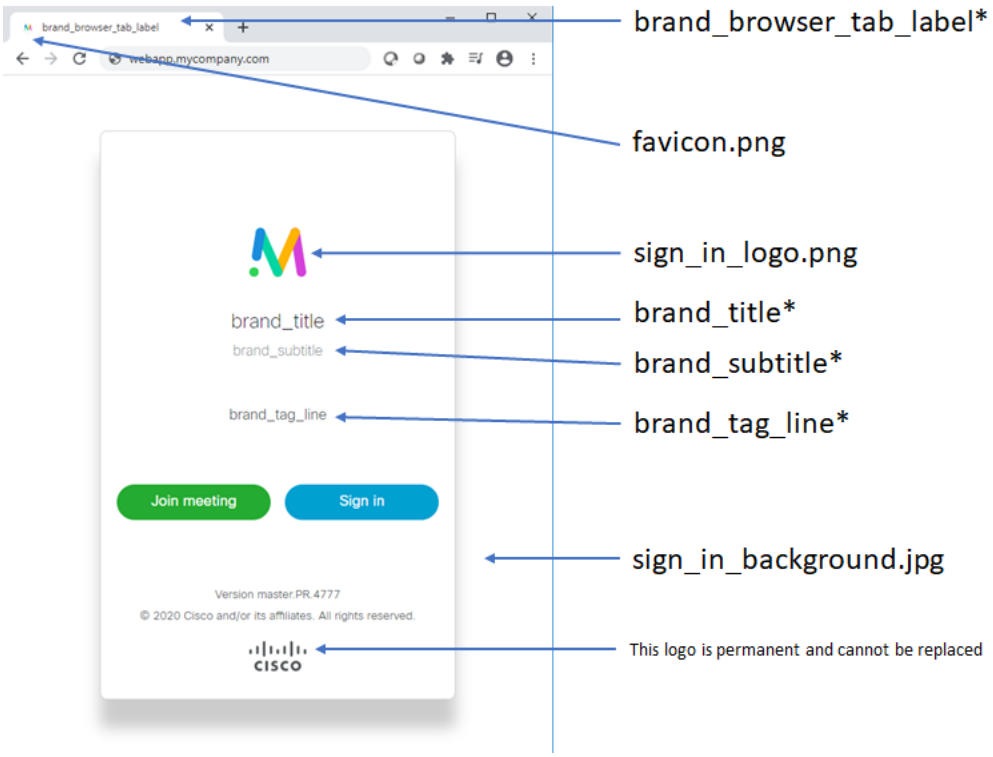
API を使用して、Web アプリケーションの以下の要素をカスタマイズできます。

- ブラウザ タブの横、およびブックマーク/ショートカットに表示されるアイコン

- ブラウザ タブのテキスト
- サインインの背景画像
- サインイン ダイアログ ボックス：表示されるロゴ
- サインイン ダイアログ ボックス：ロゴの下のテキスト

図 6 に、これらの要素の配置と場所を示します。

図 6：Web アプリケーションのアセット



** これらの文字列はすべて単一の single text_strings.json ファイルに格納されます（表 8 を参照）。*

表 8 に、図 6 のように Web アプリケーションをカスタマイズするためにアップロードできるファイルと、推奨されるサイズを示します。

注：すべてのファイルを、指定されたファイル形式（.png、.jpg、.json など）で指定する必要があります。すべてのファイル名で大文字と小文字が区別されます。また、表 8 で使用されているファイルの命名規則に従う必要があります。

表 8：Web アプリケーションのアセットの説明と仕様

ファイル名	説明	最大ファイルサイズ	推奨されるサイズ、形式、縦横比
favicon.png	ブラウザ タブのラベルの横、およびブックマーク/ショートカットに表示されるアイコン	128 KB	• 推奨される解像度：16 X 16 ピクセルまたは 32 X 32 ピクセル • 推奨される縦横比：1:1（正方形）
sign_in_logo.png	ランディング ページ、スプラッシュ画面、およびユーザ ポータルに表示されるロゴ	250 KB	• 推奨される解像度：128 X 128 ピクセル • 推奨される縦横比：可能であれば 1:1（正方形） • その他の推奨事項：透過的な背景
sign_in_background .jpg	ランディング ページに表示される背景	500 KB	• 推奨される解像度：1920 X 1080 ピクセル • 推奨される縦横比：可能であれば 16:9
text_strings.json	上書き可能なテキスト文字列で構成される JSON 形式のファイル。サポートされる文字列： • brand_title：メインのブランド名 • brand_subtitle：下に表示する 2 番目のテキスト • brand_title brand_tag_line：下に表示する 3 番目のテキスト • brand_subtitle brand_browser_tab_label：ブラウザのタブの名前	16 KB	推奨される長さ： • brand_title：最大 24 文字（1 行に表示）、または最大 48 文字（2 行に表示）。 • brand_subtitle：最大 24 文字（1 行に表示）、または最大 48 文字（2 行に表示）。 • brand_tag_line：最大 100 文字 • brand_browser_tab_label：最大 64 文字

図 7 の例に示すように、これらの各テキスト文字列をカスタマイズできます。

図 7：text_strings.json の内容の例

```
{
"brand_title": "Cisco Meeting Server",
"brand_subtitle": "Web アプリケーション",
 "brand_tag_line": "いつでもどこでもミーティングに参加",
"brand_browser_tab_label": "Cisco Meeting Server Web アプリケーション"
}
```

このレベルのカスタマイズの実装の詳細については、Cisco Meeting Server 3.0の『Customization Guidelines（カスタマイズ ガイドライン）』[英語] を参照してください。

2.8 デフォルトで有効化されているオート ゲイン コントロール（AGC）

注：この機能は、バージョン 2.8 でベータ版機能として導入され、バージョン 2.9 で完全にサポートされました。2.8 と 2.9 では、どちらもデフォルトで無効になっていました。バージョン 3.0 AGC 以降は、デフォルトで有効になっています。

サードパーティ クライアントによって設定されるオーディオ レベルはさまざまであり、ヘッドセットによってオーディオ レベルにも差があることから、会議では、参加者に届く音が大きすぎたり小さすぎたりすることがよくあります。Meeting Server では、オート ゲイン コントロール（AGC）を使用して、個々の参加者から受信するオーディオ レベルを調整し、会議全体で可能な限り一貫したオーディオ レベルを提供しています。

バージョン 2.8 以降では、Meeting Server で受信される音声についてはオート ゲイン コントロール（AGC）が導入されています（Meeting Server によって送信される音声ではありません）。

AGC は、Meeting Server に直接接続されているすべてのエンドポイント（物理エンドポイントまたはソフト クライアント）に適用されます。これは、混合オーディオ ストリームであるため、TIP コールや AVMCU には適用されません。

注：

- AVMCU に接続されている Skype 参加者は、AVMCU が音声を制御するので、AGC の対象となりません。
- AGC は混合オーディオ ストリームであるため、Meeting Server 間の分散リンクには適用されません。

AGC はデフォルトで有効になり、無効化するにはパラメータ **audioGainMode** を使用する必要があります。このパラメータが取ることのできる値は agc（デフォルト）と **disabled** の 2 つです。パラメータ **audioGainMode** は以下の API でサポートされます。

- **/callLegProfiles/<call leg profile id>** での GET 操作と PUT 操作、および **/callLegProfiles** での POST 操作
- **/callLegs/<call leg id>** での GET 操作と PUT 操作、および **/callLegs** での POST 操作
- **/calls/<call id>/callLegs** での GET および PUT 操作

AGC が有効である場合、適用されたゲインは、Web 管理ユーザ インターフェイス ページの [ステータス（Status）] > [コール（Calls）]で表示できます。API パラメータ **gainApplied** は、**rxAudio** セクションの下の **/callLegs/<call leg id>** での GET 操作に対する応答でも返されます。

2.9 ESXi のサポート

バージョン 3.0 では、Meeting Server 1000 M4、M5、および仕様ベースのサーバでの次のサポートが追加されています。

- ESXi7.0 と仮想ハードウェア バージョン 17

これ以前の ESXi バージョンも、ESXi6.0、6.5u2、6.7 を含め、バージョン 3.0 でサポートされています。

2.10 PMP ライセンス割り当ての履歴レコード

Meeting Server 3.0 では、割り当て済みの PMP ライセンス数の履歴レコードを定期的に表示できます。これをサポートするために、Meeting Server では、**/system/MPLicenseUsage** での GET 操作で取得可能な各ライセンス使用イベントに対応する、新しい **pmpAssigned** 応答パラメータが導入されています。この応答値は、PMP ライセンスが割り当てられたユーザ数を示します。

PMP ライセンスは、従来どおり LDAP 同期を介してユーザに割り当てられます。Meeting Server は、PMP ライセンスが割り当てられたユーザ数を、**/system/multipartyLicensing** API で **personalLicenses** パラメータの応答値を使用して表示します。

従来のリリースと同様に、Meeting Server はライセンスの使用状況のスナップショットを定期的に作成します。履歴レコードは、**/system/MPLicenseUsage** での GET 操作で取得できます。ただし、ライセンス使用イベントごとに、クラスタ内で PMP ライセンスが割り当てられたユーザ数が新しいパラメータ **pmpAssigned** により提供されます。一方で、既存のパラメータ **pmp** は、利用可能な PMP ライセンスのうち現在使用中のものがいくつあるかをトラッキングします。

2.11 3.0 の API の追加および変更の概要

Meeting Server 3.0 の新しい API 機能には次のものが含まれます。

- スマート ライセンスをサポートするための新しい API オブジェクトとパラメータ
- 新しい SIP ストリーマをサポートするための新しい API パラメータ
- ダイヤルイン セキュリティ プロファイルをサポートするための新しい API オブジェクトとパラメータ
- Web Bridge プロファイルをサポートするための新しい API オブジェクトとパラメータ

2.11.1 API の追加

バージョン 3.0 では、次の新しい API オブジェクトが導入されました。

- **/clusterLicensing**
- **/clusterLicensing/raw**
- **/dialInSecurityProfiles**
- **/dialInSecurityProfiles/<dial in security profile id>**
- **/webBridgeProfiles**
- **/webBridgeProfiles/<web bridge profile id>**
- **/system/profiles/effectiveWebBridgeProfile**
- **/tenants/<tenant id>/effectiveWebBridgeProfile**
- **/webBridges/<web bridge id>/effectiveWebBridgeProfile**

バージョン 3.0 の新しい API パラメータ：

- **sipStreamerUri**：/callProfiles API objects に追加されました
- **dialInSecurityProfile**：以下の API オブジェクトに追加されました
  - **/system/profiles**
  - **/tenants**
  - **/coSpaces**
  - **/coSpaces/<cospace id>/accessMethods**
  - **/coSpaceTemplates**
  - **/coSpaceTemplates/<coSpace template id>/accessMethodTemplates**

- **webBridgeProfile**：以下の API オブジェクトに追加されました
  - **/webBridges**
  - **/system/profiles**
  - **/tenants**

バージョン 3.0 の新しい API 応答パラメータ：

- **clusterId**：既存の **/system/status** API に追加されました
- **dnsFailure**：既存の **/webBridges/<web bridge id>/status** API に追加されました
- **pmpAssigned**：既存の **/system/MPLicenseUsage に追加されました**

3.0 で導入された新しい API エラー理由：

- **dialInSecurityProfileDoesNotExist**
- **passcodeTooShort**
- **webBridgeProfileDoesNotExist**

3.0 で更新された API エラー理由：

- **recordingNotAllowedByLicensing**（従来の **recordingLimitReached**）
- **streamingNotAllowedByLicensing**（従来の **streamingLimitReached**）

3.0 で /system/alarms の計数として導入された新しいアラーム タイプ：

- **c2wConnectionFailure**

2.11.2 API の削除

バージョン 3.0 では、以下のコンポーネントまたは機能の削除によって API オブジェクトが削除されました。

- **/coSpaces/<coSpace id>/messages**
- **/recorders**
- **/streamers**
- **/system/configuration/xmpp**

バージョン 3.0 での API システム アラーム タイプの削除：

- **webBridgeXmppCertificatePushFailure**
- **xmppAuthenticationRegistrationFailure**
- **xmppRegistrationFailure**
- **recorderLowDiskSpace**
- **guestAccountConnectionFailure**
- **webBridgeBackgroundImageRetrievalFailure**
- **webBridgeBackgroundImagePushFailure**
- **webBridgeLoginLogoImageRetrievalFailure**
- **webBridgeLoginLogoImagePushFailure**
- **webBridgeArchivePushFailure**

3.0 で削除されたその他の API：

/userProfiles および /userProfiles/<user profile id> で削除されたパラメータ：

- **canCreateCoSpaces**
- **canCreateCalls**
- **canUseExternalDevices**
- **canMakePhoneCalls**
- **userToUserMessagingAllowed**
- **canReceiveCalls**
- **canSendEmailInvite**

/callProfiles で削除されたパラメータ

- **messageBoardEnabled**

/coSpaces/<coSpace id>/coSpaceUsers で削除されたパラメータ

- **canPostMessage**
- **canDeleteAllMessages**

/inboundDialPlanRules で削除されたパラメータ

- **resolveToUsers**

2.11.3 API の廃止

3.0 で廃止された応答パラメータ：

- **activated**（/system/status）
- **personalLicenseLimit**（/system/multipartyLicensing）
- **sharedLicenseLimit**（/system/multipartyLicensing）
- **capacityUnitLimit**（/system/multipartyLicensing）

2.11.4 API の変更/移動

従来は、**resolveCoSpaceUris** パラメータは API オブジェクト **/webBridges/<web bridge id>** に存在していました。バージョン 3.0 以降では、このパラメータは以下の API オブジェクトに存在します。

- **/webBridgeProfiles**
- **/webBridgeProfiles/<web bridge profile id>**
- **/webBridges/<web bridge id>/effectiveWebBridgeProfile**
- **/tenants/<tenant id>/effectiveWebBridgeProfile**
- **/system/profiles/effectiveWebBridgeProfile**

API オブジェクト **/webBridges/<web bridge id>** に存在していたその他のパラメータは、3.0 で移動されたか削除されました。

- **resourceArchive**：webBridgeProfiles に移動されました
- **idEntryMode**：廃止されました
- **allowWeblinkAccess**：**allowSecrets** として webBridgeProfiles に存在します
- showSignIn：userPortalEnabled として webBridgeProfiles に存在します
- **resolveCoSpaceCallIds**：webBridgeProfiles に移動しました
- **resolveLyncConferenceIds**：webBridgeProfiles に移動しました

2.11.5 新しい SIP ストリーマの使用

新しい SIP ストリーマを設定するために、次の操作で使用できる新しい API リクエスト パラメータ **sipStreamerUri** が追加されています。このパラメータは文字列の値を取ります。

- **/callProfiles** に対する POST 操作
- **/callProfiles/<call profile id>** に対する PUT 操作

パラメータ **sipStreamerUri** は、SIP ストリーマ ダイヤルアウト URI 文字列です。

SIP ストリーマ URI を確認するには、次の操作を実行します。

- **/callProfiles/<call profile id>** で GET を実行します。この応答は、最上位レベルの <callProfiles total="N"> タグとして構成され、その内部に複数の <callProfile> 要素が含まれる可能性があります。各 <callProfile> タグには、**sipStreamerUri** が含まれる可能性があります。

注：コールをストリーミング可能または録音可能にするには、階層の適切なレベルでコールプロファイルを設定し、**sipStreamerUri** の有効な値を使用する必要があります。コールプロファイル内の他のフィールドに従って、このパラメータをオーバーライドすることもできます。

2.11.6 ダイヤルイン セキュリティ プロファイルを使用した最小パスコード長の実装

dialInSecurityProfile のパラメータはすべて、使用は任意です。これらのパラメータがどのレベルでも指定されない場合、デフォルト設定は minPasscodeLength=0 と allowOutOfPolicy=true になります。dialInSecurityProfiles でのデフォルト設定は <unset> です。

2.11.6.1 ダイヤルイン セキュリティ プロファイルの作成、変更、および取得

新しい **/dialInSecurityProfiles** オブジェクトは、次のリクエスト パラメータを使用してダイヤルイン セキュリティ プロファイル を実装するために使用されます。

パラメータ	タイプ/値	説明/メモ
name	文字列	このダイヤルイン セキュリティ プロファイルに関連付けられた、人間が読める形式の名前
minPasscodeLength	数量	許容される最小パスコード長、0 ～ 200 の範囲（0 と 200 を含む） で指定可能
allowOutOfPolicy	true|false	ダイヤルイン セキュリティ プロファイルが適用される前に設定され、 新たに定義されたパスコード長を遵守しなくなった古いパスコードを、ユーザが使用してコールに参加することを許可するかどうか。作成（POST）操作でこのパラメータが指定されない場合、デフォルトは true になります。

この新しい API ノードは以下の操作をサポートします。

- 新しいダイヤルイン セキュリティ プロファイルを作成するための **/dialInSecurityProfiles** での POST 操作
- **/dialInSecurityProfiles/<dial in security profile id>** を使用した個別のプロファイルでの PUT 操作
- **/dialInSecurityProfiles** の計数は以下の URI パラメータを受け入れます。

URI パラメータ	タイプ/値	説明/メモ
offset		offset と limit は、名目上のリストの 1 ページ目以外のダイヤルイン セキュリティ プロファイルを取得する場合に指定できます。
limit		
usageFilter	unreferenced | referenced	グローバル設定または他のオブジェクトで参照されていないダイヤルイン セキュリティ プロファイルだけを取得する場合は、リクエストに 「usageFilter=unreferenced」を入力します。これは、プロファイルを削除する前のチェックとして有用です。少なくとも 1 ヵ所で参照されているダイヤルイン セキュリティ プロファイルだけを取得する場合は、 「usageFilter=referenced」を入力します。

この応答は、最上位レベルの <dialInSecurityProfiles total=" N" > タグとして構成され、その内部に複数の <dialInSecurityProfile> 要素が含まれる可能性があります。

各 <;dialInSecurityProfile> タグには、次の要素が含まれる場合があります。

応答要素	タイプ/値	説明/メモ
name	文字列	このダイヤルイン セキュリティ プロファイルに関連付けられた、人間が読める形式の名前
minPasscodeLength	数量	許容される最小パスワード長、0 ～ 200 の範囲（0 と 200 を含む）で指定可能
allowOutOfPolicy	true|false	ダイヤルイン セキュリティ プロファイルが適用される前に設定され、新たに定義されたパスコード長を遵守しなくなった古いパスコードを、ユーザが使用してコールに参加することを許可するかどうか。作成（POST）操作でこのパラメータが指定されない場合、デフォルトは true になります。

- **`/dialInSecurityProfiles/<dial in security profile id>`** を使用して個別のプロファイルで GET 操作を実行すると、以下の応答が返されます。

応答要素	タイプ/値	説明/メモ
name	文字列	このダイヤルイン セキュリティ プロファイルに関連付けられた、人間が読める形式の名前
minPasscodeLength	数量	許容される最小パスワード長、0 ～ 200 の範囲（0 と 200 を含む）で指定可能
allowOutOfPolicy	true|false	ダイヤルイン セキュリティ プロファイルが適用される前に設定され、新たに定義されたパスコード長を遵守しなくなった古いパスコードを、ユーザが使用してコールに参加することを許可するかどうか。作成（POST）操作でこのパラメータが指定されない場合、デフォルトは true になります。

2.11.6.2 最上位レベル（グローバル）ダイヤルイン セキュリティ プロファイルの設定

新しい API パラメータ **`dialInSecurityProfile`** を使用すると、指定したプロファイルを最上位レベル（グローバル）ダイヤルイン セキュリティ プロファイルに設定できます。
このパラメータは ID の値を取り、次の操作のために追加されています。

- /system/profiles に対する PUT 操作

この操作では、次のリクエスト パラメータを使用できます。

パラメータ	タイプ/値	説明/メモ
dialInSecurityProfile	ID	指定したプロファイルを最上位レベルのダイヤルイン セキュリティ プロファイルに設定します。「""」を指定することで設定を解除できます。

- /system/profiles で GET 操作を実行すると、次の応答が返されます。

応答値	タイプ/値	説明/メモ
dialInSecurityProfile	ID	存在する場合は、設定されている最上位レベルのダイヤルイン セキュリティ プロファイル。

2.11.6.3 テナントに対するダイヤルイン セキュリティ プロファイルの適用

新しい API パラメータ **`dialInSecurityProfile`** を使用すると、特定のダイヤルイン セキュリティ プロファイルをテナントに適用できます。このパラメータは ID の値を取り、次の操作のために追加されています。

- **`/tenants`** に対する POST 操作
- **`/tenants/<tenant id>`** に対する PUT 操作

  この操作では、次のリクエスト パラメータを使用できます。

パラメータ	タイプ/値	説明/メモ
dialInSecurityProfile	ID	指定した場合、指定したダイヤルイン セキュリティ プロファイルをこのテナントに関連付けます。「""」を指定することで設定を解除できます。

- /tenants/<tenant id> で GET 操作を実行すると、次の応答が返されます。

パラメータ	タイプ/値	説明/メモ
dialInSecurityProfile	ID	指定した場合は、このテナントに関連付けられている、指定されたダイヤルイン セキュリティ プロファイル。

2.11.6.4 coSpace に対するダイヤルイン セキュリティ プロファイルの適用

新しい API パラメータ **dialInSecurityProfile** を使用すると、ダイヤルイン セキュリティ プロファイルを coSpace に適用できます。このパラメータは ID の値を取り、次の操作のために追加されています。

- **/coSpaces** に対する POST 操作
- **/coSpaces/<cospace id>** に対する PUT 操作

この操作では、次のリクエスト パラメータを使用できます。

パラメータ	タイプ/値	説明/メモ
dialInSecurityProfile	ID	指定した場合は、指定したダイヤルイン セキュリティ プロファイルをこの coSpace に関連付けます。「""」を指定することで設定を解除できます。

- **/coSpaces/<cospace id>** で GET 操作を実行すると、次の応答が返されます。

パラメータ	タイプ/値	説明/メモ
dialInSecurityProfile	ID	指定した場合は、この coSpace に関連付けられている、指定されたダイヤルイン セキュリティ プロファイル。

2.11.6.5 アクセス方式に対するダイヤルイン セキュリティ プロファイルの適用

新しい API パラメータ **dialInSecurityProfile** を使用すると、ダイヤルイン セキュリティ プロファイルをアクセス方式に適用できます。このパラメータは ID の値を取り、次の操作のために追加されています。

- **/coSpaces/<cospace id>/accessMethods** に対する POST 操作
- **/coSpaces/<cospace id>/accessMethods/<access method id>** に対する PUT 操作

この操作では、次のリクエスト パラメータを使用できます。

パラメータ	タイプ/値	説明/メモ
dialInSecurityProfile	ID	指定した場合は、指定されたダイヤルイン セキュリティ プロファイルをこの coSpace アクセス方式に関連付けます。「""」を指定することで設定を解除できます。

- **/coSpaces/<cospace id>/accessMethods/<access method id>** で GET 操作を実行すると、次の応答が返されます。

パラメータ	タイプ/値	説明/メモ
dialInSecurityProfile	ID	指定した場合は、この coSpace アクセス方式に関連付けられている、指定されたダイヤルイン セキュリティ プロファイル。

2.11.6.6 coSpace テンプレートに対するダイヤルイン セキュリティ プロファイルの適用

新しい API パラメータ **dialInSecurityProfile** を使用すると、ダイヤルイン セキュリティ プロファイルを coSpace テンプレートに適用できます。このパラメータは ID の値を取り、次の操作のために追加されています。

/coSpaceTemplatesノード は、次の操作をサポートします。

- **/coSpaceTemplates** に対する POST 操作
- **/coSpaceTemplates/<coSpace template id>** に対する PUT 操作

パラメータ	タイプ/値	説明/メモ
dialInSecurityProfile	ID	指定した場合は、指定したダイヤルイン セキュリティ プロファイルをこの coSpaceTemplate に関連付けます。「""」を指定することで設定を解除できます。

- **/coSpaceTemplates** の計数

  この応答は、最上位レベルの <coSpaceTemplates total="N"> タグとして構成され、その内部に複数の <coSpaceTemplate> 要素が含まれる可能性があります。

各 <coSpaceTemplate>タグには、**dialInSecurityProfile** 要素が含まれます。この要素が指定されている場合、この coSpaceTemplate に関連付けられたダイヤルイン セキュリティ プロファイル が表示されます。

要素	タイプ/値	説明/メモ
dialInSecurityProfile	ID	指定した場合は、この coSpaceTemplate に関連付けられている ダイヤルイン セキュリティ プロファイルが表示されます。

- **/coSpaceTemplates/<coSpace template id>** で GET 操作を実行すると、次の応答が返されます。

応答値	タイプ/値	説明/メモ
dialInSecurityProfile	ID	指定した場合は、この coSpaceTemplate に関連付けられている、指定されたダイヤルイン セキュリティ プロファイル。

2.11.6.7 アクセス方式テンプレートに対するダイヤルイン セキュリティ プロファイルの適用

新しい API パラメータ **dialInSecurityProfile** を使用すると、ダイヤルイン セキュリティ プロファイルをアクセス方式テンプレートに適用できます。このパラメータは ID の値を取り、次の操作のために追加されています。

- **/coSpaceTemplates/<coSpace template id>/accessMethodTemplates** に対する POST 操作
- **/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates/<access method template id>** に対する PUT 操作

この操作では、次のリクエスト パラメータを使用できます。

パラメータ	タイプ/値	説明/メモ
dialInSecurityProfile	ID	指定した場合は、指定されたダイヤルイン セキュリティ プロファイル をこの coSpace アクセス方式テンプレートに関連付けます。「""」を指定することで設定を解除できます。

この応答は、最上位レベルの <accessMethodTemplates total="N"> タグとして構成され、その内部に複数の <accessMethodTemplate> 要素が含まれる可能性があります。

各 <accessMethodTemplate> タグには、次の要素が含まれる場合があります。

応答要素	タイプ/値	説明/メモ
dialInSecurityProfile	ID	指定した場合は、この coSpace アクセス方式テンプレートに関連付けられている、指定されたダイヤルイン セキュリティ プロファイル。

- **`/coSpaceTemplates/<coSpace template id>/accessMethodTemplates/<access method template id>`** で GET 操作を実行すると、次の応答が返されます。

応答値	タイプ/値	説明/メモ
dialInSecurityProfile	ID	指定した場合は、この coSpace アクセス方式テンプレートに関連付けられている、指定されたダイヤルイン セキュリティ プロファイル。

2.11.7 Web Bridge プロファイルの使用

バージョン 3.0 では、API 内の共通の場所に Web Bridge のオプションを設定できます。また、Web Bridge プロファイルを使用すると、Web Bridge ごとに適用するだけでなく、すべての Web Bridge または指定した Web Bridge のグループに対して、同じ設定を適用できるようになりました。

2.11.7.1 Web Bridge プロファイルの作成、変更、および取得

新しい **`/webBridgeProfiles`** オブジェクトは、以下のリクエスト パラメータを使用して Web Bridge プロファイルを実装するために使用されます。

パラメータ	タイプ/値	説明/メモ
name	文字列	この Web Bridge プロファイルに関連付けられている、人間が読める形式の名前。

パラメータ	タイプ/値	説明/メモ
resourceArchive	url	この Web Bridge プロファイルを使用する Web Bridge 用に Meeting Server が使用するカスタマイズ アーカイブ ファイルがある場合は、そのアドレス。
allowPasscodes	true | false	この Web Bridge プロファイルを使用する Web Bridge で、ユーザがパスコードと数値 ID/URI を組み合わせて coSpace（および coSpace アクセス方式）をルックアップすることを許可するかどうか。 作成（POST）操作でこのパラメータが指定されない場合、デフォルトは true になります。
allowSecrets	true | false	この Web Bridge プロファイルを使用する Web Bridge で、ユーザが数値 ID とシークレットを使用してミーティング参加リンクから coSpace（および coSpace アクセス方式）にアクセスすることを許可するかどうか。 作成（POST）操作でこのパラメータが指定されない場合、デフォルトは true になります。
userPortalEnabled	true | false	この Web Bridge プロファイルを使用する Web Bridge で、インデックス ページのサインイン タブを表示するかどうか。 作成（POST）操作でこのパラメータが指定されない場合、デフォルトは true になります。
allowUnauthenticatedGuests	true | false	この Web Bridge プロファイルを使用する Web Bridge でランディング画面からのゲスト アクセスを許可するのか、またはユーザーがユーザ ポータルにログイン済みである場合にのみゲスト アクセスを許可するのか。false の場合、ログインしているユーザに対してのみリンクが機能します。 作成（POST）操作でこのパラメータが指定されない場合、デフォルトは true になります。

パラメータ	タイプ/値	説明/メモ
resolveCoSpaceCallIds	true | false	この Web Bridge プロファイルを使用する Web Bridge で、coSpace ミーティングへのゲストの参加を許可する目的で coSpace と coSpace アクセス方式のコール ID を受け付けるかどうか。 作成（POST）操作でこのパラメータが指定されない場合、デフォルトは true になります。
resolveLyncConferenceIds	true | false	（現在表示されていますが、機能しません）。この Web Bridge プロファイルを使用する Web Bridge で、スケジュールされた Lync 会議 ID に解決される ID を受け付けるかどうか。 作成（POST）操作でこのパラメータが指定されない場合、デフォルトは false になります。
resolveCoSpaceUris	off | domainSuggestionDisabled | domainSuggestionEnabled	この Web Bridge で、coSpace ミーティングへのゲストの参加を許可する目的で coSpace および coSpace アクセス方式の SIP URI を受け付けるかどうか。 • off に設定されている場合は、URI を使用した参加は無効になります。 • domainSuggestionDisabled に設定されている場合、この Web Bridge プロファイルを使用する Web Bridge で URI を使用した参加が有効になりますが、URI のドメインの自動入力または検証は行われません。 • domainSuggestionEnabled に設定されている場合、この Web Bridge プロファイルを使用する Web Bridge で URI を使用した参加が有効になり、URI のドメインの自動入力または検証を使用できます。 作成（POST）操作でこのパラメータが指定されない場合、デフォルトは off になります。

この新しい API ノードは以下の操作をサポートします。

- 新しい Web Bridge プロファイルを作成するための、**/webBridgeProfiles** に対する POST 操作。
- **/webBridgeProfiles/<web bridge profile id>** を使用した、個別のプロファイルに対する PUT 操作
- **/webBridgeProfiles** の計数は以下の URI パラメータを受け入れます。

URI パラメータ	タイプ/値	説明/メモ
offset		名目上のリストの 1 ページ目以外の Web Bridge プロファイルを取得する場合は、offset と limit を指定できます。
limit		
usageFilter	unreferenced | referenced	グローバル設定または他のオブジェクトで参照されていない Web Bridge プロファイルだけを取得する場合は、リクエストに「usageFilter=unreferenced」を入力します。これは、プロファイルを削除する前のチェックとして有用です。少なくとも 1 ヵ所で参照されている Web Bridge プロファイルだけを取得する場合は、「usageFilter=referenced」と入力します。

この応答は、最上位レベルの <webBridgeProfiles total="N"> タグとして構成され、その内部に複数の <webBridgeProfile> 要素が含まれる可能性があります。

各 <;webBridgeProfile> タグには、次の要素が含まれる場合があります。

応答要素	タイプ/値	説明/メモ
name	文字列	この Web Bridge プロファイルに関連付けられている、人間が読める形式の名前

- **/webBridgeProfiles/<web bridge profile id>** で GET 操作を実行すると、次の応答が返されます。

応答値	タイプ/値	説明/メモ
name	文字列	この Web Bridge プロファイルに関連付けられている、人間が読める形式の名前。
resourceArchive	url	この Web Bridge プロファイルを使用する Web Bridge で、ユーザがパスコードと数値 ID/URI を組み合わせて coSpace（および coSpace アクセス方式）をルックアップすることを許可するかどうか。
allowPasscodes	true | false	この Web Bridge プロファイルを使用する Web Bridge で、ユーザがパスコードと数値 ID/URI を組み合わせて coSpace（および coSpace アクセス方式）をルックアップすることを許可するかどうか。
allowSecrets	true | false	この Web Bridge プロファイルを使用する Web Bridge で、ユーザが数値 ID とシークレットを使用してミーティング参加リンクから coSpace（および coSpace アクセス方式）にアクセスすることを許可するかどうか。
userPortalEnabled	true | false	この Web Bridge プロファイルを使用する Web Bridge で、インデックス ページのサインイン タブを表示するかどうか。
allowUnauthenticatedGuests	true | false	この Web Bridge プロファイルを使用する Web Bridge でランディング画面からのゲスト アクセスを許可するのか、またはユーザーがユーザ ポータルにログイン済みである場合にのみゲスト アクセスを許可するのか。false の場合、ログインしているユーザに対してのみリンクが機能します。
resolveCoSpaceCallIds	true | false	この Web Bridge プロファイルを使用する Web Bridge で、coSpace ミーティングへのゲストの参加を許可する目的で coSpace と coSpace アクセス方式のコール ID を受け付けるかどうか。

応答値	タイプ/値	説明/メモ
resolveLyncConferenceIds	true | false	（現在表示されていますが、機能しません）。この Web Bridge プロファイルを使用する Web Bridge で、スケジュールされた Lync 会議 ID に解決される ID を受け付けるかどうか。
resolveCoSpaceUris	off | domainSuggestionDisabled | domainSuggestionEnabled	この Web Bridge プロファイルを使用する Web Bridge で、coSpace ミーティングへのゲストの参加を許可する目的で coSpace と coSpace アクセス方式の SIP URI を受け付けるかどうか。 • off に設定されている場合は、URI を使用した参加は無効になります。 • domainSuggestionDisabled に設定されている場合、この Web Bridge プロファイルを使用する Web Bridge で URI を使用した参加が有効になりますが、URI のドメインの自動入力または検証は行われません。 • domainSuggestionEnabled に設定されている場合、この Web Bridge プロファイルを使用する Web Bridge で URI を使用した参加が有効になり、URI のドメインの自動入力または検証を使用できます。

2.11.7.2 Web Bridge プロファイルの作成と変更

新しい API パラメータ **`webBridgeProfile`** を使用すると、指定しれた Web Bridge プロファイルを Web Bridge に関連付けることができます。このパラメータは ID の値を取り、次の操作のために追加されています。

- **`/webBridges`** に対する POST 操作
- **`/webBridges/<web bridge id>`** に対する PUT 操作

この操作では、次のリクエスト パラメータを使用できます。

パラメータ	タイプ/値	説明/メモ
webBridgeProfile	ID	指定した場合、指定された Web Bridge プロファイルをこの Web Bridge に関連付けます。

- **/webBridges/<web bridge id>** で GET 操作を実行すると、次の応答が返されます。

応答値	タイプ/値	説明/メモ
webBridgeProfile	ID	指定した場合、この Web Bridge プロファイルに関連付けられている、指定された Web Bridge。

2.11.7.3 指定した Web Bridge で現在有効な Web Bridge プロファイルの確認

新しい API オブジェクト **/webBridges/<web bridge id>/effectiveWebBridgeProfile** を使用すると、指定された Web Bridge で現在有効な Web Bridge プロファイルおよび関連付けられた値を確認できます。次の操作がサポートされています。

- **/webBridges/<web bridge id>/effectiveWebBridgeProfile** で GET 操作を実行すると、次の応答が返されます。

応答値	タイプ/値	説明/メモ
resourceArchive	url	この Web Bridge 用に Meeting Server が使用するカスタマイズ アーカイブ ファイルがある場合は、そのアドレス。
allowPasscodes	true | false	この Web Bridge で、ユーザがパスコードと数値 ID/URI を組み合わせて coSpace（および coSpace アクセス方式）をルックアップすることを許可するかどうか。

応答値	タイプ/値	説明/メモ
allowSecrets	true | false	この Web Bridge で、ユーザが数値 ID とシークレットを使用してミーティング参加リンクから coSpace（および coSpace アクセス方式）にアクセスすることを許可するかどうか。
userPortalEnabled	true | false	この Web Bridge で、インデックスページのサインイン タブを表示するかどうか。
allowUnauthenticatedGuests	true | false	この Web Bridge でランディング画面からのゲストアクセスを許可するのか、またはユーザがユーザポータルにログイン済みである場合にのみゲストアクセスを許可するのか。false の場合、ログインしているユーザに対してのみリンクが機能します。
resolveCoSpaceCallIds	true | false	この Web Bridge で、coSpace ミーティングへのゲストの参加を許可する目的で coSpace および coSpace アクセス方式のコール ID を受け付けるかどうか。
resolveLyncConferenceIds	true | false	（現在表示されていますが、機能しません）。この Web Bridge で、スケジュールされた Lync 会議 ID に解決される ID を受け付けるかどうか。
resolveCoSpaceUris	off | domainSuggestionDisabled | domainSuggestionEnabled	この Web Bridge で、coSpace ミーティングへのゲストの参加を許可する目的で coSpace および coSpace アクセス方式の SIP URI を受け付けるかどうか。 • off に設定されている場合は、URI を使用した参加は無効になります。 • domainSuggestionDisabled に設定されている場合、この Web Bridge で URI を使用した参加が有効になりますが、URI のドメインの自動入力または検証は行われません。 • domainSuggestionEnabled に設定されている場合、この Web Bridge で URI を使用した参加が有効になり、URI のドメインの自動入力または検証を使用できます。

2.11.7.4 テナントに対する Web Bridge プロファイルの適用

新しい API パラメータ webBridgeProfile を使用すると、特定の Web Bridge プロファイルをテナントに適用できます。このパラメータは ID の値を取り、次の操作のために追加されています。

- **`/tenants`** に対する POST 操作
- **`/tenants/<tenant id>`** に対する PUT 操作

  この操作では、次のリクエスト パラメータを使用できます。

パラメータ	タイプ/値	説明/メモ
webBridgeProfile	ID	指定した場合、指定された Web Bridge プロファイルをこのテナントに関連付けます。

- **`/tenants/<tenant id>`** で GET 操作を実行すると、次の応答が返されます。

パラメータ	タイプ/値	説明/メモ
webBridgeProfile	ID	指定した場合、このテナントに関連付けられている、指定された Web Bridge プロファイル。

2.11.7.5 指定したテナントで現在有効な Web Bridge プロファイルの確認

新しい API オブジェクト **`/tenants/<tenant id>/effectiveWebBridgeProfile`** を使用すると、指定されたテナントで現在有効な Web Bridge プロファイルおよび関連付けられた値を確認できます。次の操作がサポートされています。

- **`/tenants/<tenant id>/effectiveWebBridgeProfile`** で GET 操作を実行すると、次の応答が返されます。

応答値	タイプ/値	説明/メモ
resourceArchive	url	このテナントの Web Bridge で Meeting Server がデフォルトとして使用するカスタマイズ アーカイブ ファイルがある場合は、そのアドレス。
allowPasscodes	true | false	このテナントの Web Bridge で、ユーザがパスコードと数値 ID/URI を組み合わせて coSpace（および coSpace アクセス方式）をルックアップすることを許可するかどうか。
allowSecrets	true | false	このテナントの Web Bridge で、ユーザが数値 ID とシークレットを使用してミーティング参加リンクから coSpace（および coSpace アクセス方式）にアクセスすることを許可するかどうか。
userPortalEnabled	true | false	このテナントの Web Bridge で、インデックス ページのサインイン タブを表示するかどうか。
allowUnauthenticatedGuests	true | false	このテナントの Web Bridge でランディング画面からのゲスト アクセスを許可するのか、またはユーザがユーザ ポータルにログイン済みである場合にのみゲスト アクセスを許可するのか。false の場合、ログインしているユーザに対してのみリンクが機能します。
resolveCoSpaceCallIds	true | false	このテナントの Web Bridge で、coSpace ミーティングへのゲストの参加を許可する目的で coSpace および coSpace アクセス方式のコール ID を受け付けるかどうか。
resolveLyncConferenceIds	true | false	（現在表示されていますが、機能しません）。このテナントの Web Bridge で、スケジュールされた Lync 会議 ID に解決される ID を受け付けるかどうか。

応答値	タイプ/値	説明/メモ
resolveCoSpaceUris	off | domainSuggestionDisabled | domainSuggestionEnabled	このテナントの Web Bridge で、coSpace ミーティングへのゲストの参加を許可する目的で coSpace および coSpace アクセス方式の SIP URI を受け付けるかどうか。 • off に設定されている場合は、URI を使用した参加は無効になります。 • domainSuggestionDisabled に設定されている場合、このテナントの Web Bridge で URI を使用した参加が有効になりますが、URI のドメインの自動入力または検証は行われません。 • domainSuggestionEnabled に設定されている場合、このテナントの Web Bridge で URI を使用した参加が有効になり、URI のドメインの自動入力または検証を使用できます。

2.11.7.6 最上位レベル（グローバル）Web Brige プロファイルの設定

新しい API パラメータ **`webBridgeProfile`** を使用すると、最上位レベル（グローバル）の Web Bridge プロファイルを指定して設定することができます。このパラメータは ID の値を取り、次の操作のために追加されています。

- **`/system/profiles`** に対する PUT 操作

この操作では、次のリクエスト パラメータを使用できます。

パラメータ	タイプ/値	説明/メモ
webBridgeProfile	ID	指定したプロファイルを最上位レベルの Web Bridge プロファイルに設定します。

- **`/system/profiles`** で GET 操作を実行すると、次の応答が返されます。

応答値	タイプ/値	説明/メモ
webBridgeProfile	ID	存在する場合は、設定されている最上位レベルの Web Bridge プロファイル。

2.11.7.7 最上位レベル（グローバル）システム レベルで現在有効な Web Bridge プロファイルの確認

新しい API オブジェクト **`/system/profiles/effectiveWebBridgeProfile`** を使用すると、このシステムで現在有効な Web Bridge プロファイルおよび関連する値を確認できます。次の操作がサポートされています。

- **`/system/profiles/effectiveWebBridgeProfile`** で GET 操作を実行すると、次の応答が返されます。

応答値	タイプ/値	説明/メモ
resourceArchive	url	Meeting Server がこのシステム上の Web Bridge のデフォルトとして使用するカスタマイズ アーカイブ ファイルがある場合は、そのアドレス。
allowPasscodes	true | false	このシステム上の Web Bridge で、ユーザがパスコードと数値 ID/URI を組み合わせて coSpace（および coSpace アクセス方式）をルックアップすることを許可するかどうか。
allowSecrets	true | false	このシステム上の Web Bridge で、ユーザが数値 ID とシークレットを使用してミーティング参加リンクから coSpace（および coSpace アクセス方式）にアクセスすることを許可するかどうか。
userPortalEnabled	true | false	このシステム上の Web Bridge で、インデックス ページのサインイン タブを表示するかどうか。
allowUnauthenticatedGuests	true | false	このシステムの Web Bridge でランディング画面からのゲスト アクセスを許可するのか、またはユーザがユーザ ポータルにログイン済みである場合にのみゲスト アクセスを許可するのか。false の場合、ログインしているユーザに対してのみリンクが機能します。

応答値	タイプ/値	説明/メモ
resolveCoSpaceCallIds	true | false	このシステム上の Web Bridge で、coSpace ミーティングへのゲストの参加を許可する目的で coSpace および coSpace アクセス方式のコール ID を受け付けるかどうか。
resolveLyncConferenceIds	true | false	（現在表示されていますが、機能しません）。このシステム上の Web Bridge で、スケジュールされた Lync 会議 ID に解決される ID を受け付けるかどうか。
resolveCoSpaceUris	off | domainSuggestionDisabled | domainSuggestionEnabled	このシステム上の Web Bridge で、coSpace ミーティングへのゲストの参加を許可する目的で coSpace および coSpace アクセス方式の SIP URI を受け付けるかどうか。 • off に設定されている場合は、URI を使用した参加は無効になります。 • domainSuggestionDisabled に設定されている場合、このシステム上の Web Bridge で URI を使用した参加が有効になりますが、URI のドメインの自動入力または検証は行われません。 • domainSuggestionEnabled に設定されている場合、このシステム上の Web Bridge で URI を使用した参加が有効になり、URI のドメインの自動入力または検証を使用できます。

2.11.7.8 Web Brige のステータスの取得

新しい **status** 応答値タイプ **dnsFailure** が導入され、次の操作で使用できます。

- **/webBridges/<web bridge id>/status** で GET 操作を実行すると、次の応答が返されます。

応答値	タイプ/値	説明/メモ
status	dnsFailure	dnsFailure：設定された Web Bridge の URI を解決できませんでした。

2.11.8 PMP ライセンスの割り当て履歴の表示

各ライセンス使用イベントに対して新しい応答パラメータ **pmpAssigned** が導入されました。

- **/system/MPLicenseUsage** で GET 操作を実行すると、次の応答が返されます。

応答値	タイプ/値	説明/メモ
pmpAssigned	数字	クラスタ内のユーザに割り当てられている個人ライセンスの数。

2.11.9 クラスタのライセンス情報の取得

3.0 以降では、既存 の **/system/licensing** API で GET 操作を実行すると、Meeting Server インスタンスごとにライセンス ファイルの内容（機能コンポーネント）だけが返されるようになりました。新しく導入された API オブジェクト **/clusterLicensing** を使用すると、Meeting Server クラスタのライセンス ステータスと有効期限（該当する場合）が返されます。

注：**/clusterLicensing** で返される有効期限フィールドは、最大でも 90 日後になります。

Meeting Server またはクラスタの現在のライセンス情報を取得するには、次の操作を実行します。

/clusterLicensing で GET メソッドを実行すると、次の応答が返されます。

応答要素	タイプ/値	説明/メモ
機能		ライセンスが有効である場合、<features> 要素には以下の要素が含まれます。

応答要素	タイプ/値	説明/メモ

名前	タイプ/値	説明
callBridge		

名前	タイプ/値	説明
status	noLicense | activated | expired	ライセンスのステータス： • noLicense：この機能に使用できるライセンスがありません • activated：機能のライセンスが付与されており、有効期限内です • expired：この機能のライセンスは有効期限を過ぎています
expiry	文字列	有効期限

名前	タイプ/値	説明
callBridgeNoEncryption		

名前	タイプ/値	説明
status	noLicense | activated | expired	ライセンスのステータス： • noLicense：この機能に使用できるライセンスがありません • activated：機能のライセンスが付与されており、有効期限内です • expired：この機能のライセンスは有効期限を過ぎています
expiry	文字列	有効期限

名前	タイプ/値	説明
customizations		

名前	タイプ/値	説明
status	noLicense | activated | expired	ライセンスのステータス： • noLicense：この機能に使用できるライセンスがありません • activated：機能のライセンスが付与されており、有効期限内です • expired：この機能のライセンスは有効期限を過ぎています
expiry	文字列	有効期限

名前	タイプ/値	説明
録音		

名前	タイプ/値	説明
status	noLicense | activated | expired	ライセンスのステータス： • noLicense：この機能に使用できるライセンスがありません • activated：機能のライセンスが付与されており、有効期限内です • expired：この機能のライセンスは有効期限を過ぎています
expiry	文字列	有効期限

2.12 CDR の変更の概要

バージョン 3.0 では、Meeting Server のコール詳細レコードに次の追加が導入されました。

- **recorderUrl** と **streamerUrl** は、それぞれ recordingStart レコードと streamingStart レコードから削除されました。これらは、新しい SIP レコーダーおよびストリーマ コンポーネントでは必要ありません。
- 新しいパラメータ **streamerUri**が streamingStart レコードに追加されました。これは文字列であり、ストリーマ デバイスの URI です。（従来は **path** と **streamerUrl** が常に提供されていましたが、これらは SIP ストリーマには送信されません。recordingEnd レコードには変更はありません）。

2.13 MMP の追加および変更の概要

バージョン 3.0 では、MMP に関する以下の変更がサポートされています。

2.13.1 Image Signing

バージョン 3.0 では、以下の MMP コマンドが導入されています。

表 9：バージョン 3.0 での Image Signing の MMP コマンドの変更と追加

コマンド	説明
upgrade [<name>]	既存の MMP コマンド：ただし、指定されたイメージを使用して Meeting Server をアップグレードする前に、署名と完全性のチェックが実行されるようになりました。それ以前にそのイメージに対して upgrade <name> verify コマンドが実行された場合でも、このチェックは実行されます。バージョン 3.0 で更新されました。
upgrade <name> verify	通常はアップグレード中に実行される完全性と署名のチェックをすべて実行しますが、続けてアップグレードを実行しません。このコマンドを使用は、イメージ タイプを表示する目的でも使用できます。バージョン 3.0 で追加されました。

コマンド	説明
信頼性	ソフトウェアの真偽に関するすべての情報を表示します。実行中のイメージがどのように検証されたか（キーのタイプと名前）、現在ロードされている公開キーとその詳細（タイプ、名前、ソース）。また、キーが信頼されているかどうかも表示します。特別なキーがインストールされているかどうか、その署名がマスター キーで検証済みであるかどうか（それ以外のキーは内部キーであり常に信頼されます）。バージョン 3.0 で追加されました。
authenticity key add <key-file>	特別なキーをインストールします。一度にインストールできる特別なキーは 1 つだけです。バージョン 3.0 で追加されました。
authenticity key none	現在インストールされている特別なキーを削除します。別のキーをインストールする前に既存のキーを削除する場合、またはキーをそれ以降使用しない場合に、このコマンドを使用する必要があります。バージョン 3.0 で追加されました。

2.13.2 SIP レコーダー

表 10：バージョン 3.0 でのレコーダーの MMP コマンドの変更、追加、削除

コマンド	説明
`recorder sip certs`	SIP 証明書を設定できます。バージョン 3.0 で追加されました。
recorder sip listen <interface> <tcp-port|none> <tls-port|none>	SIP レコーダーおよびストリーマ コンポーネントでは、https 接続をリッスンする必要はなくなりましたが、SIP 接続をリッスンする必要があります。この新しい MMP コマンドは、TCP と TLS の両方を設定するために導入されました。バージョン 3.0 で追加されました。
recorder sip trace <1m|10m|30m|24h|on|off>	すべての SIP メッセージのロギングを有効にします。すべての SIP メッセージがレコーダーに記録されます。デフォルトは「off」です。「on」を使用すると、永続的または固定された期間にわたって有効にすることができます。バージョン 3.0 で追加されました。

コマンド	説明
recorder limit <value|none>	拡張性を確保するためにレコーダーの制限を設定します。これは、コール制御によって別のデバイスにフェールオーバーできるようにする、コール拒否の上限です。バージョン 3.0 で追加されました。
recorder listen <a|b|c|d|lo|none [:<port>] allowed list> recorder listen a b	バージョン 3.0 で削除されました。 レコーダーがリッスンするインターフェイスとポートを設定します。recorder enable コマンドでリスニングを開始するには、サービスを有効にする必要があります。オプションの port 引数のデフォルトは 443 です。
recorder listen none	バージョン 3.0 で削除されました。 レコーダーのリスニングを停止します。
recorder certs <keyfile-name> <crt filename> [<crt-bundle>]	バージョン 3.0 で削除されました。 レコーダーのキー ファイルと .crt ファイル の名前を提供します。オプションで、CA によって提供された CA 証明書バンドルの名前を提供します。
recorder certs none	バージョン 3.0 で削除されました。 証明書の設定を削除します。
recorder trust <crt-bundle|crt-file>	バージョン 3.0 で削除されました。 どの Call Bridge インスタンスにレコーダーへの接続を許可するかを制御します。 信頼された Call Bridge がレコーダーと同じサーバで実行されている場合は、Call Bridge の公開証明書/証明書バンドルの名前を指定して recorder trust コマンドを発行するだけで十分です。Call Bridge が別のサーバで実行されている場合は、まず、レコーダーを有効にしたサーバに、Call Bridge の公開証明書/証明書バンドルを SFTP を使用してコピーする必要があります。
recorder trust none	バージョン 3.0 で削除されました。 すべての信頼設定をクリアします。

2.13.3 SIP ストリーマ

表 11：バージョン 3.0 でのストリーマの MMP コマンドの変更、追加、削除

コマンド	説明
streamer sip certs	SIP 証明書を設定できます。バージョン 3.0 で追加されました。
streamer sip listen <interface> <tcp-port|none> <tls-port|none>	SIP レコーダーおよびストリーマ コンポーネントでは、https 接続をリッスンする必要はなくなりましたが、SIP 接続をリッスンする必要があります。この新しい MMP コマンドは、TCP と TLS の両方を設定するために導入されました。バージョン 3.0 で追加されました。
streamer sip trace <1m|10m|30m|24h|on|off>	すべての SIP メッセージのロギングを有効にします。すべての SIP メッセージがストリーマに記録されます。デフォルトは「off」です。「on」を使用すると、永続的または固定された期間にわたって有効にすることができます。バージョン 3.0 で追加されました。
streamer limit <value|none>	拡張性を確保するためにストリーマの制限を設定します。これは、コール制御によって別のデバイスにフェールオーバーできるようにする、コール拒否の上限です。バージョン 3.0 で追加されました。
streamer sip resolution <audio|720p|1080p>	ストリーマで実行する最大解像度を設定します。デフォルトは 720p です。1080p を使用する場合は、ビデオの品質を最適化するために、送信 SIP コールの帯域幅を 3,500,000 ビット/秒に増やすことを推奨します。バージョン 3.0 で追加されました。
streamer listen <a|b|c|d|lo|none [:<port>] allowed list> recorder listen a b	バージョン 3.0 で削除されました。 ストリーマがリッスンするインターフェイスとポートを設定します。streamer enable コマンドでリスニングを開始するには、サービスを有効にする必要があります。オプションの port 引数のデフォルトは 443 です。
streamer certs none	バージョン 3.0 で削除されました。 証明書の設定を削除します。

コマンド	説明
streamer certs <keyfile-name> <crt filename> [<crt-bundle>]	バージョン 3.0 で削除されました。 ストリーマのキー ファイルと .crt ファイル の名前を提供します。オプションで、CA によって提供された CA 証明書バンドルの名前を提供します。
streamer trust <crt-bundle|crt-file>	バージョン 3.0 で削除されました。 どの Call Bridge インスタンスにストリーマへの接続を許可するかを制御します。 信頼された Call Bridge がストリーマと同じサーバで実行されている場合は、Call Bridge の公開証明書/証明書バンドルの名前を指定して streamer trust コマンドを発行するだけで十分です。Call Bridge が別のサーバで実行されている場合は、まず、ストリーマを有効にしたサーバに、Call Bridge の公開証明書/証明書バンドルを SFTP を使用してコピーする必要があります。
streamer trust none	バージョン 3.0 で削除されました。 すべての信頼設定をクリアします。

2.13.4 削除されたコンポーネントの MMP コマンド

3.0 で Meeting Server から削除された機能とコンポーネントに関連するすべての MMP コマンドは、以下のように削除されています。

- H.323 ゲートウェイのコマンド（**h323_gateway**）
- Web Bridge 2 のコマンド（**webbridge**）
- XMPP サーバのコマンド（**xmpp**）
- XMPP マルチドメインのコマンド（**xmpp multi_domain**）
- XMPP の復元力のコマンド（**xmpp cluster**）
- ロード バランサのコマンド（**loadbalancer**）
- トランクのコマンド（**trunk**）
- SIP エッジのコマンド（**sipedge** およびエッジ関連の **callbridge**）

- XMPP に依存していたレコーダーおよびストリーマのコマンド
- X シリーズ サーバに該当する MMP コマンド

3.0 で削除されたすべてのコマンドの詳細については、『MMP Command Reference（MMP コマンド リファレンス）』ガイドを参照してください。

2.13.5 MMP のその他の変更

MMP 応答のすべてのマスター/スレーブ参照は、プライマリ/レプリカに変更されました。

2.14 イベントの変更の概要

バージョン 3.0 に新しいイベントはありません。

3 Cisco Meeting Server ソフトウェア バージョン 3.0 のアップグレード、ダウングレード、および展開

このセクションでは、Cisco Meeting Server ソフトウェア バージョン 2.9 からアップグレードすることを前提としています。 それよりも前のバージョンからアップグレードする場合は、2.9.x リリース ノートの手順に従って 2.9 にアップグレードしてから、Cisco Meeting Server 3.0 リリース ノートに記載されている手順を実行することを推奨します。これは、Cisco Expressway が Meeting Server に接続されている場合に特に重要です。

注：シスコでは、2.9 よりも前のソフトウェア リリースからのアップグレードをテストしていません。

Cisco Meeting Server 1000、または以前に設定された VM 展開にインストールされている Cisco Meeting Server ソフトウェアのバージョンを確認するには、MMP コマンド **`version`** を使用します。

VM を初めて設定する場合は、『Cisco Meeting Server Installation Guide for Virtualized Deployments』の指示に従ってください。

注：Web Bridge 2 は 3.0 で削除されたため、3.0 にアップグレードする際は、Web Bridge 3 を使用するために Web Bridge を展開し直す必要があります。同様に、XMPP に依存する従来のレコーダーおよびストリーマは 3.0 で新しい内部 SIP レコーダーおよびストリーマ コンポーネントに置き換えられたため、アップグレード時にレコーダーとストリーマを展開し直す必要があります。

3.1 リリース 3.0 へのアップグレード

このセクションの手順は、クラスタ化されていない Meeting Server 展開に適用されます。クラスタ化されたデータベースを使用した展開については、クラスタ化されたサーバをアップグレードする前に、この FAQ の指示をお読みください。

注意：Meeting Server をアップグレードまたはダウングレードする前に、backup snapshot <filename> コマンドを使用して構成のバックアップを作成し、バックアップ ファイルを別のデバイスに安全に保存する必要があります。詳細については、『MMP Command Reference（MMP コマンド リファレンス）』ガイド [英語] を参照してください。アップグレード/ダウングレードプロセスが生成した自動バックアップファイルに依存**しないでください**。アップグレード/ダウングレードが失敗した場合にアクセスできない可能性があります。

ファームウェアのアップグレードは 2 段階のプロセスです。最初に、アップグレードされたファームウェアイメージをアップロードします。次に、アップグレードコマンドを発行します。これによりサーバが再起動します。再起動プロセスでは、サーバで実行されているすべてのアクティブ コールが中断します。したがって、ユーザに影響を与えることがないように、この段階は適切なタイミングで実行する必要があります。そうでない場合、ユーザに事前に警告する必要があります。

注：
Meeting Server 3.0 では、Cisco Meeting Management 3.0（またはそれ以降）を使用するための必須の要件が導入されています。Meeting Management は、製品登録と、スマートライセンスのサポートに関連するスマート アカウント（セットアップされている場合）とのやり取りを処理します。詳細については、セクション 2.2を参照してください。

Web Bridge 2 は 3.0 で削除されたため、Web Bridge 2 のユーザは、Web アプリケーションをサポートするため、Web Bridge 3 を使用できるように Web Bridge を展開し直す必要があります。Web Bridge 2 から Web Bridge 3 への自動アップグレードによる移行はありません。バージョン 2.9 の Web Bridge 3 をすでに展開している場合は、Web 管理または /web Bridges/<webbridge id> の設定から引き継がれないため、アップグレード後に設定を確認する必要があります。
また、XMPP に依存する従来のレコーダーとストリーマは、3.0 で新しい内部 SIP レコーダーおよびストリーマ コンポーネントに置き換えられました。3.0 にアップグレードする際に、レコーダーとストリーマを展開し直す必要があります。

セカンダリ サーバをインストールするには、次の手順に従います。

1. アップグレードするには、適切なアップグレード ファイルをシスコの Web サイトの [ソフトウェア ダウンロード] ページから取得します。

   Cisco_Meeting_Server_3_0_CMS2000.zip

   このファイルは、サーバにアップロードする前に単一の upgrade.img ファイルに解凍する必要があります。このファイルを使用して、Cisco Meeting Server 2000 サーバをアップグレードします。

   upgrade.img ファイルのハッシュ（SHA-256）：
   b9364f6a88a68b89c30d203725a22e6b97fdd00459d83e6ab1da1ea8cefb8be1

   Cisco_Meeting_Server_3_0_vm-upgrade.zip

   このファイルは、サーバにアップロードする前に単一の upgrade.img ファイルに解凍する必要があります。このファイルを使用して、Cisco Meeting Server 仮想マシンの展開をアップグレードします。

   upgrade.img ファイルのハッシュ（SHA-256）：
   585a804007f8bd9b199a59b96dcd9cd7e1c1c6174a39a8a364bab434cc906727

   Cisco_Meeting_Server_3_0.ova

   このファイルを使用して、VMware を介した新しい仮想マシンを展開します。

   vSphere 6 の場合、Cisco_Meeting_Server_3_0_vSphere-6_0.ova ファイルのハッシュ（SHA-512）：
   73daac9df9ea0039da339398b6a9173b66bb56ec76b68142d5e237be265edbfa26036c91896f829234f4dd16a9752e985c98fac71ff13cc95aff3ea781945348

   vSphere 6.5 以降の場合、Cisco_Meeting_Server_3_0_vSphere-6_5.ova ファイルのハッシュ（SHA-512）：83db84e31a4e30771dede8c10881259b0babb86aaba67473e7737a6d33ae9e02cd017b1190c14d9bcf672adb27dd2a4bcc2917b4b23ae42e64cf48bcd66035a6

2. OVA ファイルを検証するために、ダウンロードの説明にカーソルを合わせると表示されるポップアップ ボックスに、3.0.0 リリースのチェックサムが表示されます。さらに、上記の SHA-512 ハッシュ値を使用して、ダウンロードの整合性を確認することもできます。

3. SFTP クライアントを使用して、IP アドレスを使用して MMP にログインします。ログイン資格情報は、MMP 管理者アカウントに設定された資格情報になります。Windows を使用している場合、WinSCP ツールの使用をお勧めします。

注：ファイル転送に WinSCP を使用している場合、[転送設定（Transfer Settings）] オプションが [テキスト（text）] ではなく [バイナリ（binary）] であることを確認してください。誤った設定を使用すると、転送されたファイルが元のファイルよりもわずかに小さくなり、アップグレードが正常に行われなくなります。

注：a）**`iface a`** MMP コマンドを使用して、MMP のインターフェイスの IP アドレスを見つけることができます。
b）SFTP サーバは、標準のポート 22 で実行されます。

4. ソフトウェアをサーバ/仮想化サーバにコピーします。
5. アップグレードファイルを検証するには、**`upgrade list`** コマンドを発行します。
   a. MMP への SSH 接続を確立し、ログインします。
   b. upgrade list コマンドを実行して、使用可能なアップグレードイメージとそのチェックサムを出力します。
      `upgrade list`
   c. このチェックサムが上記のチェックサムと一致していることを確認します。
6. アップグレードを適用するには、前の手順の MMP への SSH 接続を使用し、**`upgrade`** コマンドを実行してアップグレードを開始します。
   a. upgrade コマンドを実行して、アップグレードを開始します。
   b. **`upgrade`** サーバ/仮想化サーバは自動的に再起動します。処理が完了するまで 10 分かかります。
7. MMP への SSH 接続を再確立し、次を入力して、Meeting Server がアップグレードされたイメージを実行していることを確認します。
8. **`version`** 利用可能な場合は、カスタマイズ アーカイブ ファイルを更新します。
9. 拡張性または復元力のある導入環境を展開する場合は、『スケーラブルで復元力のあるサーバ導入ガイド』をお読みになり、残りの導入順序と構成プランを作成してください。

10. データベース クラスタを展開している場合は、アップグレード後に必ず **database cluster upgrade_ schema** コマンドを実行してください。データベース スキーマをアップグレードする手順については、『スケーラブルで復元力のあるサーバ導入ガイド』を参照してください。
11. アップグレードが完了しました。

3.2 ダウングレード

アップグレードプロセス中またはアップグレードプロセス後に予期しないことが発生した場合は、以前のバージョンの Meeting Server ソフトウェアに戻ることができます。通常のアップグレード手順を使用して、MMP **upgrade** コマンドを使用して、Meeting Server を必要なバージョンに「ダウングレード」します。

1. ソフトウェアをサーバ/仮想化サーバにコピーします。
2. ダウングレードを適用するには、MMP への SSH 接続を使用し、**upgrade<filename>** コマンドを実行してダウングレードを開始します。

   サーバ/仮想サーバが自動的に再起動します。プロセスが完了し、サーバのダウングレード後に Web 管理が使用可能になるまで 10 ～ 12 分かかります。
3. Web 管理画面にログインし、[ステータス（Status）] > [全般（General）]に移動して、[システムステータス（System status）]の下に新しいバージョンが表示されていることを確認します。
4. サーバで MMP コマンド **factory_reset app** を使用し、初期設定へのリセット後に再起動するのを待ちます。
5. MMP コマンド **backup rollback <name>** を使用して、古いバージョンの構成バックアップを復元します。

注：**backup rollback** コマンドは、既存の構成、license.dat ファイル、およびシステム上のすべての証明書と秘密キーを上書きし、Meeting Server を再起動します。したがって、注意して使用する必要があります。バックアップのロールバック プロセス中に上書きされるため、既存の cms.lic ファイルと証明書を事前にコピーしてください。.JSON ファイルは上書きされないため、上書きする必要はありません

Meeting Server が再起動して、バックアップ ファイルが適用されます。

クラスタ展開の場合、クラスタ内の各ノードに対して手順 1 ～ 5 を繰り返します。

6. XMPP クラスタの場合は、必要に応じて XMPP をクラスタ化し直す必要があります。
   a. 1 つのノードを XMPP プライマリとして選択し、このノードで XMPP を初期化します。
   b. XMPP プライマリが有効になったら、他の XMPP ノードをそれに結合します。
   c. 同じサーバから作成されたバックアップ ファイルを使用して復元すると、XMPP ライセンス ファイルと証明書が一致し、機能し続けます。
7. 最後に、次のことを確認してください。
   - 各 Call Bridge の Web 管理インターフェイスで coSpaces のリストを表示できる
   - ダイヤル プランが無傷である
   - XMPP サービスが接続されている（該当する場合）
   - Web 管理およびログ ファイルに障害状態が報告されていない
   - SIP および Cisco ミーティング アプリケーション（サポートされている場合は Web Bridge）を使用して接続できる

   これで、Meeting Server のダウングレード展開は完了です。

3.03.3 Cisco Meeting Server の展開

Meeting Server の展開方法の説明をシンプルにするため、3 つのモデルで展開を説明します。

- 単一統合型 Meeting Server：すべての Meeting Server コンポーネント（Call Bridge、Web Bridge 3、データベース、レコーダー、アップローダ、ストリーマ、TURN サーバ）が使用可能です。Call Bridge とデータベースは自動的に有効化されますが、それ以外のコンポーネントは展開の必要性に応じて個別に有効化することができます。有効化されたすべてのコンポーネントが単一のホスト サーバ上に存在します。

- 単一分散型 Meeting Server：このモデルでは、DMZ 内のネットワーク エッジに配置された Meeting Server 上で TURN サーバと Web Bridge 3 が有効化され、それ以外のコンポーネントは内部（コア）ネットワークに配置された別の Meeting Server 上で有効化されます。

- 3 つ目のモデルでは、展開環境の拡張性と復元力を高めるため、複数の Meeting Server をまとめてクラスタ化して展開します。

これらの 3 つのモデルすべてを網羅した導入ガイドは、こちらで参照できます。個々の導入ガイドには、別に証明書ガイドラインのドキュメントが付属しています。

注意点：

Cisco Meeting Server 2000 には、Call Bridge、Web Bridge 3、およびデータベース コンポーネントのみが含まれます。これは、単一のサーバとして、または複数のサーバのカスケードとして、内部ネットワークに展開するのに適しています。Cisco Meeting Server 2000 は DMZ ネットワークに展開しないでください。外部の Cisco Meeting Server Web アプリケーション ユーザ向けにファイアウォール トラバーサルのサポートが必要な場合は、代わりに次のいずれかも展開する必要があります。

- 内部ネットワークに Cisco Expressway-C、DMZ に Expressway-E、または
- TURN サーバを有効にして、DMZ に別個の Cisco Meeting Server 1000 または仕様ベースの VM サーバを展開します。

Cisco Meeting Server 1000 および仕様ベースの VM サーバは、Cisco Meeting Server 2000 よりもコール キャパシティは少なくなりますが、すべてのコンポーネント（Call Bridge、Web Bridge 3、データベース、レコーダー、アップローダ、ストリーマ、TURN サーバ）を各ホスト サーバ上で使用できます。Web Bridge、レコーダー、アップローダ、ストリーマ、および TURN サーバは、稼働させるためには有効化する必要があります。

4 バグ検索ツール、解決済みの問題と未解決の問題

シスコのバグ検索ツールを使用して、問題と利用可能な回避策の説明など、このミーティングアプリケーションの解決した問題または未解決の問題に関する情報を探すことができます。これらのリリース ノートに示されている ID によって、それぞれの問題の説明に直接移動できます。

1. Web ブラウザを使用して、バグ検索ツールに移動します。
2. cisco.com の登録ユーザ名とパスワードでログインします。

このマニュアルに記載された問題に関する情報を検索するには、次の手順を実行します。

1. [検索（Search）]フィールドにバグ ID を入力し、[検索（Search）]をクリックします。

ID がわからない場合に情報を検索するには、次の手順を実行します。

1. [検索（Search）]フィールドに製品名を入力し、[検索（Search）]をクリックします。

   または、

   [製品（Product）]フィールドで [シリーズ/モデル（Series/Model）]を選択し、「**Cisco Meeting Server**」と入力し始めます。次に、[リリース（Releases）]フィールドで [これらのリリースで修正済み（Fixed in these Releases）]を選択して、たとえば「**3.0.1**」とリリースを入力して検索します。
2. 表示されたバグのリストから、[変更日（Modified Date）]、[ステータス（Status）]、[重大度（Severity）]、[評価（Rating）] ドロップダウン リストを使用してリストをフィルタリングします。

バグ検索ツールのヘルプページには、バグ検索ツールの使用に関する詳細情報があります。

4.1 解決済みの問題

注：Web アプリケーションに影響する解決済みの問題の詳細については、『Cisco Meeting Server web app Important information（Cisco Meeting Server Web アプリケーション重要事項』ガイド [英語] を参照してください。

以前のバージョンで発生し 3.0 で修正済みの問題

シスコの識別子	要約
CSCvu70860	コールで ICE とマルチストリームを同時に使用すると、Cisco Meeting Server が終了してコールが終了することがあります。
CSCvt92631	coSpace がパスワードで保護されている場合に、coSpace レベルで割り当てられた qualityMain/qualityPresentation によって、Meeting Server が reINVITE で誤った SDP を送信することがあります。
CSCvt23261	Meeting Server で SFTP を使用して証明書関連ファイルをダウンロードまたはアップロードすると、失敗することがあります。
CSCvu45771	Meeting Server の負荷が高くなると、エンド ユーザに対して音声プロンプトが再生されないことがあります（IVR/パスコード入力/唯一の参加者など）。
CSCvu30182	レコーダーが、Cisco Meeting Server Web アプリケーションの参加者リストに参加者としてリストされます。
CSCvu83901	「送信バッファーの上限に達しました（Send buffer limit reached）」という理由で、RTMP ストリームが 2.5 時間（約 2 GB サイズ）で終了します。
CSCvt29547	/secure パーティションが 100% になったことが報告されたときに、Meeting Server で次の処理が失敗することがあります。バックアップの作成/PCAP の開始/デバッグ ファイルの生成/ログ バンドルの収集。
CSCvm17422	TMS のアクティブでないスペースに参加者が IVR を使用してダイヤルインした場合、IVR はプロンプトを一切再生しません。
CSCvt74060	Web Bridge 3 は、コールへの参加時に次の警告を発行します。「sendRequest() エラー - WB3 Web ソケット接続が見つかりません（sendRequest() failure - cannot find WB3 websocket connection）」このログ メッセージには重大な影響はなく、無視してかまいません。[未確定]
CSCvt74047	Call Bridge との接続が正常に動作している場合でも、API /api/v1/webbridges/<webbridge id>/status が常に connectionFailure を返します。

シスコの識別子	要約
CSCvt74045	参加者の API ノードに対して deactivated=false を POST することによって、ロックされたミーティングで参加者を明示的にアクティブ化してから、ミーティングをロック解除する場合、その参加者には、想定されるプロンプト「このミーティングはロック解除されました（this meeting is now unlocked）」が流れません。
CSCvt74035	Web Bridge 3 が開始されていない場合に、[最近のエラーと警告（Recent errors and warnings）] または [障害状態（Fault conditions）] のいずれのセクションにも表示されません。
CSCvv19066	Meeting Server が相手先の最大 H.264 のビデオ ビット レート制限を誤って読み取り、その結果、リモート システムに対するビデオ レートが若干低下することがあります。

4.2 未解決の問題

注：Web アプリケーションに影響する未解決の問題については、『Cisco Meeting Server web app Important information（Cisco Meeting Server Web アプリケーション重要事項』ガイド [英語] を参照してください。

次に、Cisco Meeting Server ソフトウェアのこのリリースの既知の問題を示します。詳細が必要な場合は、バグ検索ツールの [検索（Search）] フィールドにシスコの識別子を入力してください。

シスコの識別子	要約
CSCvv19087	Web 管理 UI のトレース詳細ページに [Web Bridge 接続のトレース（Web Bridge connection tracing）] オプションがまだ表示されていますが、現在は機能しません。これは Meeting Server から削除された Web Bridge 2 コンポーネント用に使用されていたものです。
CSCvt11301	Web Bridge 2 または Webadmin が同じ https ポート番号をリッスンしている場合、異なるインターフェイスであっても、Web Bridge 3 を開始できません。
CSCvt74033	コンテンツの共有中に、イベントがトリガーとなって Webex Room Panorama が 2 つのビデオ ストリームの送信を 1 つに減らした場合、リモート エンドポイントが Room Panorama から受け取るビデオのフレーム レートが著しく低下する可能性があります。

シスコの識別子	要約
CSCvt52420	Meeting Server の system/load API で返される mediaProcessingLoad パラメータで、VP8 コーデックを使用したコールが正しく考慮されません。VP8 を使用する場合、API がレポートするよりも Meeting Server 上の実際のメディアの負荷が高くなる場合があります。
CSCvn65112	ローカルでホストされているブランドの場合、オーディオ プロンプト ファイルが省略されると、代わりにデフォルトの組み込みプロンプトが使用されます。すべての音声プロンプトを抑制するには、ファイルが全くないというよりも、ゼロバイトのファイルを使用します。
CSCvm56734	デュアルホーム会議では、出席者がビデオのミュートを解除した後、ビデオは再起動しません。
CSCvj49594	コールが Cisco Unified Communications Manager および Cisco Expressway を通過する場合、保留/再開後に ActiveControl は機能しません。
CSCvh23039	アップローダコンポーネントは、NFS に保持されているテナント録音では機能しません。
CSCvh23036	Meeting Server 2.4 のデフォルトの DTLS 設定である DTLS1.2 は、CE9.1.x を実行している Cisco エンドポイントではサポートされていません。ActiveControl は、MMP コマンド tls-min-dtls-version 1.0 を使用して DTLS が 1.1 に変更された場合に、Meeting Server とエンドポイントの間でのみ設定されます。
CSCvg62497	NFS が設定されているか、読み取り専用になっている場合、Uploader コンポーネントは同じビデオ録画を Vbrick に継続的にアップロードします。これは、アップローダーがアップロード完了としてファイルをマークできないためです。これを回避するには、NFS に読み取り/書き込みアクセス権があることを確認してください。
CSCve64225	OpenSSL CVE の問題を修正するには、Cisco Meeting Server 2000 用の Cisco UCS Manager を 3.1(3a) に更新する必要があります。
CSCve37087 ただし、 CSCvd91302 関連	Cisco Meeting Server 2000 のメディアブレードの 1 つが正しく起動しない場合があります。回避策：ファブリック インターコネクト モジュールを再起動します。

5 関連するユーザ マニュアル

以下のサイトに、インストール、計画と導入、初期設定、製品の操作などに関するドキュメントが掲載されています。

- リリース ノート（最新および以前のリリース）：
  https://www.cisco.com/c/ja_jp/support/conferencing/meeting-server/products-release-notes-list.html
- インストール ガイド（VM のインストール、Meeting Server 2000、インストール アシスタントの使用を含む）：https://www.cisco.com/c/ja_jp/support/conferencing/meeting-server/products-installation-guides-list.html
- 設定ガイド（展開計画と展開、証明書ガイドライン、簡素化されたセットアップ、ロード バランシングのホワイト ペーパー、管理者向けクイック リファレンス ガイドを含む）：https://www.cisco.com/c/ja_jp/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html
- プログラミング ガイド（API、DR、イベント、MMP リファレンス ガイド、カスタマイズ ガイドラインを含む）：
  https://www.cisco.com/c/ja_jp/support/conferencing/meeting-server/products-programming-reference-guides-list.html
- オープン ソース ライセンス情報：
  https://www.cisco.com/c/ja_jp/support/conferencing/meeting-server/products-licensing-information-listing.html
- Cisco Meeting Server の FAQ：
  https://meeting-infohub.cisco.com/faq/category/25/cisco-meeting-server.html [英語]
- Cisco Meeting Server の相互運用性データベース：
  https://tp-tools-web01.cisco.com/interop/d459/s1718 [英語]

6 アクセシビリティ通知

シスコは、利用しやすい製品およびテクノロジーの設計および提供に取り組んでいます。

Cisco Meeting Server に関する Voluntary Product Accessibility Template（VPAT）は次の場所で入手できます。

http://www.cisco.com/web/about/responsibility/accessibility/legal_regulatory/vpats.html#telepresence [英語]

アクセシビリティの詳細については、次を参照してください。

www.cisco.com/web/about/responsibility/accessibility/index.html [英語]

Cisco の法的情報

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

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

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

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

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

この文書の印刷されたハード コピーおよび複製されたソフト コピーは、すべて管理対象外と見なされます。最新版については、現在のオンライン バージョンを参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所と電話番号は、当社の Web サイト（www.cisco.com/go/offices）をご覧ください。

シスコの商標

Cisco および Cisco のロゴは、米国およびその他の国における Cisco およびその関連会社の商標を示します。シスコの商標の一覧については、www.cisco.com/go/trademarks をご覧ください。本書に記載されているサードパーティの商標は、それぞれの所有者の財産です。 「パートナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。（1721R）