Cisco Meeting Server

Cisco Meeting Server リリース 2.9.1

リリース ノート

2020 年 7 月 6 日

目次

変更事項

バージョン	変更
2020 年 6 月 25 日	Web アプリケーションのチャットの廃止に関する注意事項が削除されました。
2020 年 6 月 16 日	Cisco Meeting Server Web アプリケーションのコール キャパシティの数値が追加されました。 Expressway ユーザに関する特記事項が更新されました。
2020 年 5 月 11 日	未解決の問題が更新されました。
2020 年 4 月 30 日	解決済みの問題が更新されました。
2020 年 4 月 29 日	初回メンテナンス リリース（2.9.1）。 ハッシュが更新されました 「解決済みの問題」を参照してください。
2020 年 4 月 8 日	バージョン 2.9 の初回リリース

1 概要

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 2.9 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。
- Acano X シリーズ ハードウェア。
- またはスペックベースの VM サーバ。

Acano X **シリーズに関する特記事項**：X シリーズのサポートは、Meeting Server ソフトウェアの将来のバージョンで削除される予定です。

Cisco Meetings Server ソフトウェアのことは、このリリースノート全体で Meeting Server と呼びます。

以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、バックアップを別のデバイスに安全に保存することをお勧めします。詳細については、『MMP Command Line Reference（MMP コマンド ライン リファレンス）』[英語] を参照してください。

証明書の検証に関する注意: バージョン 2.4 以降、Web Bridge では XMPP サーバの TLS 証明書が正しく検証されます。Meeting Server のアップグレード後に WebRTC アプリケーションユーザがログインできない場合は、アップロードされた XMPP 証明書が証明書ガイドラインのアドバイスに従っているか確認してください。具体的には、SAN フィールドで XMPP サーバのドメイン名が保持されます。バージョン 2.4 より前は、XMPP 証明書の検証に問題がありました。

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 Cisco 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 に投稿されます。また、その他の Cisco 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 2.9 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：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 は、単独の Meeting Server または Meeting Server クラスタのコール キャパシティと、コール ブリッジ グループ内でのロード バランシング コールを比較したものです。これらの数値は、WebRTC 用ミーティング アプリケーション を使用した Web Bridge 2 の導入環境に基づいています。

表 2：Meeting Server ソフトウェア バージョン 2.9 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 Bridge 2 あたりの WebRTC 接続数	100	100	100
Call Bridge グループ内の Meeting Server	サポートされているコール タイプ	インバウンド SIP アウトバウンド SIP Cisco ミーティング アプリケーション		
	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 Bridge 2 あたりの WebRTC 接続数	100	100	100

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：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）。

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。会議が複数の Call Bridge にまたがる場合は、分散リンクが自動的に作成され、サーバのコール数と容量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 の最新バージョン（6.0 Update 3、6.5 Update 2、および 6.7）での変更により、Cisco Meeting Server バージョン 2.8 以降で音声コールのスループットが低下しています（ビデオ キャパシティには影響ありません）。

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

このセクションでは、Web Bridge 3 および Web アプリケーションを使用した導入環境のコール キャパシティについて説明します。

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：内部コール

内部コールとは、メディア用のリバース プロキシまたは TURN サーバとして Cisco Expressway を経由することなく、クライアントが Call Bridge と Web Bridge 3 に到達できることを意味します。表 3 に、内部コールに関する Web アプリケーションのコール キャパシティを示します。

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

Cisco Meeting Server **プラットフォーム**	**コール タイプ**	Cisco Meeting Server 1000 M4/M5	Cisco Meeting Server 2000	Cisco Meeting Server 1000 **（24 ノード クラスタ）**	Cisco Meeting Server 2000 **（24 ノード クラスタ）**
個別の Meeting Server、クラスタ内の Meeting Server、または Call Bridge グループ内の Meeting Server	フル HD HD SD 音声通話	38 75 150 500	280 560 800 1000	912 1800 3600 12000	6720 13440 19200 24000

Web bridge 3 のキャパシティは、Call Bridge をクラスタリングし、各 Call Bridge に対して Web Bridge 3 インスタンスを追加することによって拡張できます。Web Bridge 3 のキャパシティを最大化するには、各 Call Bridge インスタンスと共存させる形で Web Bridge を導入します。Call Bridge と 1:1 ベースで Web Bridge 3 を導入し、内部コールを使用する場合、サポートされる Web アプリケーションの最大コール数は、単一インスタンスの値（表 3 を参照）にインスタンス数（最大 24 個の Call Bridge ノード）を乗算した値になります。

注：クラスタあたりの 24 個の Call Bridge ノードおよび 24 個の Web Bridge ノードという上限があります。8 ペア以上のノードで構成されるクラスタ設計は、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：Cisco Meeting Server Web アプリケーションのコールについては、クラスタのコール セットアップ レートが 1 秒あたり 20 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 アプリケーションコールのプロキシとして Expressway を使用する場合、表 4 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 4：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
	Other	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。

1.2.4.3 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 3 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 4 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 ミーティング アプリケーション WebRTC および Web アプリケーションに関する重要事項

アプリケーションに関する機能のリリース時期および問題の解決時期については、次に示す、該当する重要事項ガイドを参照してください。

- Cisco Meeting Server WebRTC アプリを使用している（すなわち Web Bridge 2 を導入している）場合は、『Cisco Meeting App WebRTC Important Information（Cisco ミーティング アプリケーション WebRTC 重要事項）』[英語] ガイド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（すなわち Web Bridge 3 を導入している）場合は、『Cisco Meeting Server web app Important Information（Cisco Meeting Server Web アプリ重要事項）』ガイド [英語] を参照してください。

アプリケーションに関連するすべての情報は、各アプリケーションの個別のドキュメントに含まれており、Meeting Server のリリース ノートには含まれていません。

重要事項ガイドでは、次のことを説明しています。

- アプリケーションの新機能または変更された機能、およびアプリ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を利用可能な Meeting Server のバージョンと共に示しています。
- 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アプリケーションのバージョンを、推奨される回避策と共に示しています。

WebRTC は発展途上の技術であり、ブラウザのベンダーによって頻繁に変更が実装されています。重要事項ガイドは、今後の変更について通知する必要がある場合に更新されます。

1.4　ソフトウェア メンテナンス終了

Cisco Meeting Server ソフトウェア バージョン 2.9 のリリースにあたり、シスコは、表 5 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 5：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 2.7.x	Cisco Meeting Server バージョン 2.9 の初回リリースの 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 2.5 の新機能および変更点

Meeting Server ソフトウェア バージョン 2.9 では、次の追加が行われています。

- Cisco Meeting Server Web アプリ（Web Bridge 3.0）* は新しい会議参加方法およびユーザ ポータルです。Web アプリは、最終的に Cisco ミーティング アプリケーション WebRTC を置き換えます。
- カスタム電子メール招待は、新しい Cisco Meeting Server Web アプリケーションで使用するものです。
- 追加のロック モードにより、会議のロックが可能になり、すべての参加者はロビーで待機状態となります。API を介して参加を許可されるか、ロック解除権限を持つユーザ（ホストとは限らない）によって会議がロック解除されるまで、会議に参加できません。（既存のロック モードでは特定の参加者にロックをバイパスさせることが可能でした）。
- 新しい API コマンドを使用して、参加者がロビーから会議に入室するのを許可する方法。
- サードパーティの SIP レコーダーの設定をサポート：録音が開始されると、Meeting Server のレコーダー コンポーネントを使用する代わりに SIP URI がコールされます。
- 参加者 2 人の会議でのパノラマ表示ビデオ レイアウト エクスペリエンスをサポート。この機能は、新しいパノラマ エンドポイントをサポートします。バージョン 2.9 では、ベータ サポートとなります。
- 4K コンテンツをサポートするあらゆるエンドポイントで 4k コンテンツをサポート。
- Chromium ブラウザのビデオ/コンテンツ品質が向上*。
- より強力な暗号化のサポートにより、セキュリティが向上。
- Meeting Server API を使用した、リモート システムのカメラの遠端カメラ制御（FECC）開始をサポート。
- Meeting Server Web インターフェイスで利用可能なシンプルな API ユーザ インターフェイス。
- オート ゲイン コントロール（AGC）を有効化する機能は、2.8 でベータ機能として導入され、現在は完全にサポートされています。
- API を使用した coSpace テンプレートの作成と適用をサポート。

注：アスタリスク（*）でマークされている機能は、バージョン 2.9 では Acano X シリーズでサポート**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。

注意：追加のロック モード機能により、デフォルトの動作が変更されます。バージョン 2.9 から、**`lockMode`** はデフォルトで **`all`** に設定されています。アップグレード後にデフォルトの動作を変更したくない場合は、クラスタのデフォルトを変更する必要があります。詳細については、セクション 2.3 を参照してください。

2.1 Cisco Meeting Server Web アプリケーション

Meeting Server バージョン 2.9 で、新しい Cisco Meeting Server Web アプリケーションが導入されました。これは、ユーザが会議（音声およびビデオ）に参加するための Cisco Meeting Server 用のブラウザベースのクライアントです。この機能を使用するには、新しい Web Bridge 3 を導入する必要があります。これに加えて、Meeting Server バージョン 2.9 では、元の Cisco ミーティング アプリケーション WebRTC（ここでは Web Bridge 2 とも呼ばれます）も引き続き提供しています。

このリリースでは、Cisco Meeting Server Web アプリケーションのすべての機能はまだ搭載されていません。いずれは、Cisco ミーティング アプリケーション WebRTC とほぼ同じ機能セットをサポートし、これを置き換えることを前提としています。

注：バージョン 2.9 の Web アプリケーションで現在サポートされていない機能および今後サポートされる予定の機能については、『Cisco Meeting Server web app Important Information（Cisco Meeting Server Web アプリ重要事項）』[英語] を参照してください。

注：Web アプリケーションをサポートする Web Bridge 3 コンポーネントは、Acano X シリーズでは実行できません。ただし、Acano X シリーズは、Call Bridge を実行して同じクラスタに含めることができます。Web Bridge 3 は、Cisco Meeting Server 1000 および 2000 プラットフォーム、仕様に基づくその他の VM で実行する必要があります。

注：Web アプリケーションには XMPP は必要ありません。XMPP コンポーネントは、将来のバージョンで削除される予定です。Cisco ミーティング アプリケーション WebRTC では、従来どおり XMPP が必要です。

注意：Expressway ユーザ向けの重要事項

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

Web Bridge 2 と WebRTC 用ミーティング アプリケーションのみを導入する場合は、X12.6 より前のバージョンの Expressway を引き続き使用できます。

2.1.1 Web Bridge 3 の設定に役立つ情報

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

- 「Call Bridge to Web Bridge」（C2W）プロトコルは、callbridge と webbridge3 の間のリンクです。
- callbridge に webbridge3 への接続を許可するために、（**`webbridge3 c2w listen`** を使用して）インターフェイス上でポートを開く必要があります（webbridge がそのポートをリッスンします）。この理由から、この webbridge について callbridge に情報を伝えるための API リクエストを実行するときに、このポートを指定したアドレスを使用する必要があります。この接続は、証明書を使用してセキュリティで保護する必要があります。
- 開いたポートを外部アクセスから保護することを推奨します。つまり、callbridge からのみポートに到達可能にする必要があります。
- callbridge は **`callbridge certs`** を使用して証明書セットを使用し、webbridge は **`webbridge3 c2w certs`** を使用して証明書セットを使用します。
- webbridge は、**`webbridge3 c2w trust`** によって設定された信頼ストアに含まれるいずれかの callbridge によって署名された、callbridge の証明書を信頼します。
- callbridge は、**`callbridge trust c2w`** によって設定された信頼ストアに含まれるいずれかの webbridge によって署名された証明書を持つ webbridge を信頼します。
- webbridge3 の https 証明書とポートは webbridge2 のものと同じであり、ユーザは https を使用して Web クライアントに到達できます。これらは、同じ導入環境で同時に使用できます。
- webbridge3 の c2w 証明書で拡張キーの使用が必要な場合は、「サーバ認証」にする必要があり、callbridge の証明書での拡張キーの使用を「クライアント認証」にする必要があります。ただし、これらの拡張はオプションであり、証明書に拡張キーがない場合は、Web Bridge 3 は、どのような使用方法も可能であるものと想定します。
- 公的機関が署名した証明書は必要ありません。MMP で作成した自己署名証明書を使用できます。
- SAN/CN は、callbridge API で Web Bridge 3 に登録するために使用する、c2w:// の URL で使用されている FQDN または IP アドレスと一致する必要があります。（これが一致しない場合、callbridge は TLS ネゴシエーションを失敗させ、webbridge が提示した証明書を拒否するため、webbridge との接続が失敗します）。
- 一般的な証明書の情報については、導入環境に応じた証明書のガイドラインを参照してください。

以下の図では、Web Bridge 2 の一般的なセットアップの流れを、Web Bridge 3 と比較して示しています。

図 1：Web Bridge 2 のセットアップのフロー図

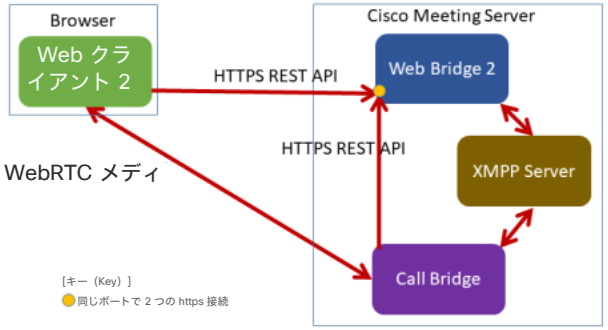
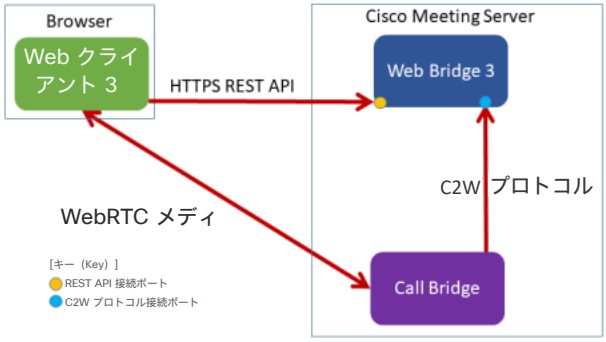


図 2：Web Bridge 3 のセットアップのフロー図



2.1.2　Web Bridge 3 を使用するための Meeting Server の設定

Meeting Server を 2.9 にアップグレードする場合、デフォルトでは、このリリースは既存の Web Bridge 2 の設定を使用します。ただし、Web Bridge 2 と並行して動作するように Web Bridge 3 を設定することもできます。Web Bridge 2 は XMPP を使用し、Web Bridge 3 は Call Bridge to Web Bridge（C2W）プロトコル接続を使用するため、並行しての動作が可能です。ただし、図 2 に示すように、それぞれ別のポートを使用するように設定する必要があります。

注：Web Bridge 3 用に XMPP サーバを設定する必要はありません。

Web Bridge 3 は、設定に関しては Web Bridge 2 と同様であり、SSH を介して MMP コマンドを使用してセットアップを実行します。主な違いは、Web Bridge 2 では 1 個の HTTPS ポートの設定が必要なのに対して、Web Bridge 3 では 1 個の HTTPS ポートと 1 個の C2W ポートの設定が必要な点です。

Web Bridge3 を使用するように Meeting Server を設定するには、次の手順を実行します。

1. MMP に SSH でログインします。
2. MMP で **webbridge3** コマンドを使用して、webbridge3 を設定します。
   webbridge3 の使用方法を表示するには、「**help webbridge3**」と入力します。

```
> help webbridge3
      Usage:
      webbridge3
      webbridge3 restart
      webbridge3 enable
      webbridge3 disable
      webbridge3 https listen <interface:port whitelist>
      webbridge3 https certs <key-file> <crt-fullchain-file>
      webbridge3 https certs none
      webbridge3 http-redirect (enable [port]|disable)
      webbridge3 c2w listen <interface:port whitelist>
      webbridge3 c2w certs <key-file> <crt-fullchain-file>
      webbridge3 c2w certs nonewebbridge3 c2w trust <crt-bundle>
      webbridge3 c2w trust none
      webbridge3 options <space-separated options>
      webbridge3 options nonewebbridge3 status
```

   詳細については、こちらの、2.9 MMP の追加機能の概要を参照してください。
3. （オプション）HTTP 接続用のポートをセットアップします。このポートは、Web アプリケーションが設定されているすべての Meeting Server インターフェイスに対して開かれます。着信 HTTP 接続は、着信したインターフェイスでの一致する HTTPS ポートに自動的にリダイレクトされます。**webbridge3 http-redirect enable [port]** でポートを指定しない場合、デフォルトのポートは 80 です。
4. HTTPS サービスがリッスンするポートを設定します。インターフェイスのポート 443 でリッスンするように設定するには、次のコマンドを実行します。

   webbridge3 https listen a:443
5. HTTPS 証明書を設定します。これらは Web ブラウザに対して提示される証明書であるため、認証局による署名が必要であり、ホスト名や目的などが一致している必要があります。（証明書ファイルは、エンド エンティティの証明書で始まりルート証明書で終わる完全な証明書チェーンです）。次のコマンドを入力します。

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

6. C2W 接続を設定します。このアドレスとポートは、Call Bridge からのみアクセス可能にすることを推奨します。次のコマンドを実行すると、インターフェイス a のポート 9999 に設定されます。

   webbridge3 c2w listen a:9999

   ここでは例としてポート 9999 を使用していますが、ネットワーク上の利用可能な任意のポートを使用できます。これは、443 とは異なり、固定ポートではありません。

7. C2W 接続の証明書を設定します。C2W 接続に使用する SSL サーバ証明書を設定する必要があります。（証明書の要件については、19 ページの「C2W 接続を使用するように Call Bridge を設定する」を参照してください。さらに詳細な情報については、この FAQ [英語] を参照してください）。

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

8. Web Bridge 3 C2W サーバは、Call Bridge がクライアント証明書を提示するものと想定しており、次のコマンドによって提供される信頼バンドルを使用して、Call Bridge を信頼するかどうかを検証します。

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

9. Web Bridge 3 を有効にします。

   webbridge3 enable

2.1.3 C2W 接続を使用するための Call Bridge の設定

C2W 証明書は、Call Bridge と Web Bridge 3 の間の接続に使用されます。Call Bridge が Web Bridge 3 との C2W 接続を確立するには、証明書を検証する C2W 信頼ストアを指定する必要があります。つまり、前述の手順 7 で設定した、Web Bridge 3 が提示する証明書です。

1. Call Bridge の使用方法を表示するには、MMP で次の **callbridge** コマンドを使用します。「**help callbridge**」と入力すると、次のように表示されます。

```
> help callbridge
Configure CMS callbridge
使用法：
callbridge listen <interface whitelist>
callbridge prefer <interface>
callbridge certs <key-file> <crt-file> [<cert-bundle>]
callbridge certs none
callbridge trust xmpp <bundle>
callbridge trust xmpp none
callbridge trust c2w <bundle>
callbridge trust c2w none
callbridge add edge <ip address>:<port>
callbridge del edge
callbridge trust edge <trusted edge certificate bundle>
callbridge trust cluster none
callbridge trust cluster <trusted cluster certificate bundle>
callbridge restart
```

2. Call Bridge の証明書を設定します。
   `callbridge certs cert.key cert.crt`
3. Web Bridge 3 が提示した SSL サーバ証明書の検証に使用する C2W 信頼ストアを設定します。（詳細については、この FAQ [英語] を参照してください）。
   `callbridge trust c2w c2w-callbrige-trust-store.crt`
4. Call Bridge を再起動します。
   `callbridge restart`
5. 次の図に示すように、Web Bridge 2 の場合と同様に、実行中の callbridge REST API に対して Web Bridge 3 の URL を登録します。つまり、「URL」「パラメータを指定して /api/v1/webbridges に対して POST を実行します。この URL プロトコルによって、webbridge2 と webbridge3 のどちらであるかを示します。このため、プロトコルが http:// または https:// の場合は webbridge2 として処理され、URL で c2w:// プロトコルを指定した場合は webbridge3 接続として処理されます。

   図 3：Call Bridge API に対する Web Bridge 3 の URL の登録

2.1.4 Web Bridge 3 によって提供される API メソッド

バージョン 2.9 では、Web Bridge 3 に特化した、情報を取得する新しい API メソッドが導入されました。これらの新しい API メソッドは、通常の Meeting Server API では見つからず、Web Bridge 3 によって提供される API でサポートされます。この API は、Web Bridge 3 と通信するためにブラウザで実行される Web アプリケーションによって使用されます。これらのメソッドは、管理者が診断目的で使用するために用意されています。

たとえば、Web Bridge 3 が **`join.meeting.space`** で実行されている場合、これらの API メソッドは **`https://join.meeting.space/api/bridge/info`** に配置されます。

新しいメソッドは次のとおりです。

- **`/api/bridge/info`** で GET を実行すると、この Web Bridge 3 の識別子が返されます。
- **`/api/v1/load`** で GET を実行すると、この Web Bridge 3 の識別子が返されます（従来の用途向け）。
- **`/api/bridge/callbridges`** で GET を実行すると、この Web Bridge 3 に対する現在の Call Bridge 接続に関する情報が返されます。

- **`/api/bridge/connections`** で GET を実行すると、この Web Bridge 3 によって提供されている現在の HTTP 接続に関する情報が返されます。*
- **`/api/bridge/websockets`** で GET を実行すると、この Web Bridge 3 によって提供されている現在の WebSocket に関する情報が返されます。*
- **`/api/configuration`** で GET を実行すると、カスタム電子メール招待およびその他の機密でない設定情報で利用可能な言語が返されます。

* 認証（Web アプリケーションのユーザがログインに使用するのと同じ認証）が必要です。

2.2 Cisco Meeting Server Web アプリケーションケーションのカスタム電子メール招待

Meeting Server バージョン 2.9 では、新しい Cisco Meeting Server Web アプリケーションと共に使用するカスタム電子メール招待が導入されます。

これにより、管理者はさまざまな電子メール招待テンプレートを作成してアップロードすることができます。これらのテンプレートを使用して、Web アプリケーションのユーザは次のことを実行できます。

- 電子メール招待の送信：他のユーザに将来の会議への参加を求める招待を、選択した言語で送信。
- 外部および社内の参加者など、さまざまな対象者に適した電子メール招待を送信。

注：Web アプリケーションのカスタム電子メール招待には、ローカルにホストされたブランディングを使用することを推奨します。ただし、より複雑な導入環境（マルチテナント環境など）で複数の言語を使用する場合は、リモートのブランディング Web サーバを使用する必要があります。詳細については、カスタマイズのガイドライン [英語] を参照してください。

2.2.1 デフォルトの招待テンプレート

2.2.1.1 異なる言語の招待テンプレート

Meeting Server の Web アプリケーションでは、次の 2 つのデフォルト言語の招待電子メールが用意されています。

- invitation_template_es_ES.txt（スペイン語 - スペイン）

- invitation_template_en_US.txt（英語 - 米国）

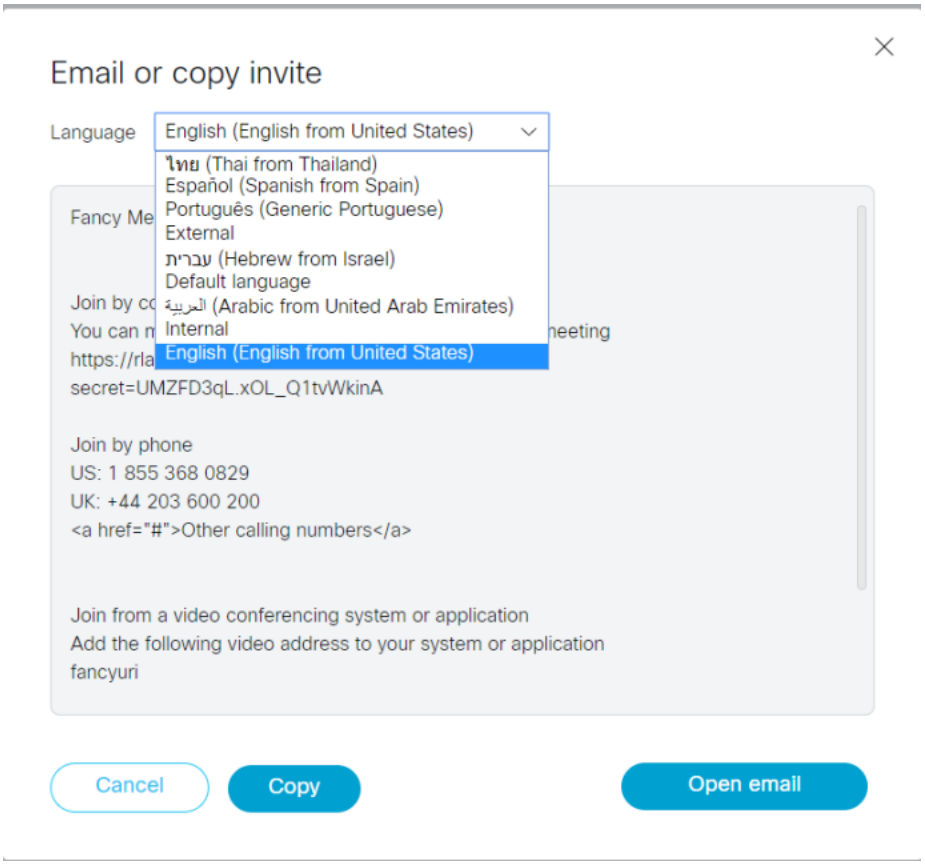
このデフォルトのテンプレートを上書きする場合は、言語タグを付けた独自のテンプレート ファイルを作成し、ローカルにホストされているブランディングにアップロードします。Meeting Server は、これらの言語タグを解釈し、Web アプリケーションに適切なテンプレート オプションを返します。

ユーザは、アップロードされている言語テンプレートのみを選択できます。アップロードされていない言語オプションは、ドロップダウン リストに表示されません。

注：テンプレート ファイルは、クラスタ内のすべての Meeting Server にアップロードする必要があります。

次の図に、この特定の Meeting Server で作成されアップロードされた、さまざまな電子メール招待の例を示します。

図 4：電子メール招待オプション



2.2.1.2　さまざまな対象者向けの招待テンプレート

ユーザは、社外および社内の参加者など、さまざまな対象者向けに異なる電子メール招待を生成できます。そのためには、invitation_template_Internal.txt のように、命名規則に従った招待テンプレート ファイルを作成する必要があります。このファイルは、図 4 に示すように、電子メール招待 オプションで [内部（Internal）] として表示されます。

電子メール招待オプションの使用の詳細については、『Cisco Meeting Server web app Important Information（Cisco Meeting Server Web アプリ重要事項）』[英語] を参照してください。

2.2.2　異なる言語バリアントでの招待テンプレート ファイルの作成

セクション 2.2.2.1 の情報を参照して、UTF-8 で invitation_template_xx_XX.txt ファイルを作成します。

2.2.2.1　使用できる条件文およびプレースホルダ

テンプレートには条件文とプレースホルダの両方を含めることができます。これにより、1 つのテンプレートを複数のスペースで使用でき、また、招待に一貫性を持たせることができます。

次の表に、現在定義されているプレースホルダ（それぞれの開始文字と終了文字は %）を示します。

表 6：招待テンプレートのプレースホルダ

プレースホルダ	タイプ
%name%	会議名
%uri%	会議のダイヤルイン URI
%numeric_id%	会議の数字識別子
%hyperlink%	Web Bridge 上の会議への直接ハイパーリンク
%passcode%	会議の数字 PIN

プレースホルダ	タイプ
%%	常に % に置き換えられます 注：テキストに含まれる % はすべて、プレースホルダの開始と解釈されます。テキストに「%」を 1 つ挿入するには、プレースホルダ %% を使用します。
%launch_link%	デスクトップまたは iOS Cisco ミーティング アプリケーションで会議を開始するための直接ハイパーリンク。 注：Microsoft Outlook を使用している場合は、リンクにプレフィックス「url:」を付加することで、Microsoft Outlook および電子メール クライアントでハイパーリンクとして認識できます。

以下の条件文がサポートされています。次の表を参照してください。必要に応じて入れ子にすることができます。

表 7：招待テンプレートの条件文

条件文	意味
#if 条件	この条件が true の場合は、ここから else 文または endif 文が出現するまでの行を処理します。この if 文の条件セクションは、いずれかのプレースホルダの形式をとります。たとえば、「#if name」となります。
#else	前の if 文の条件が false の場合は、ここから endif 文が出現するまでの行を処理します。
#endif	

2.2.2.2 招待テンプレートの例

- 招待テンプレートの .txt ファイルのサイズには、1 万バイトの制限 * があります。
- 招待テンプレートはすべて UTF-8 形式で指定する必要があります。
- 拡張 ASCII 文字はサポートされません。
- UTF-8 形式の招待テンプレート .txt ファイルには、（Windows で使用される）CRLF ではなく、UNIX の行末（LF）を含める必要があります。UNIX の行末を省略すると、ファイルが機能しません。
- 言語別の .txt ファイルには、言語バリアントに応じた適切な言語タグ（IANA Language Subtag Registry の定義に従う）を指定する必要があります。この言語タグでは、2 個の小文字が言語コードを表し、2 個の大文字が地域コードを表します。たとえば、invitation_template_en_GB.txt では、「en」は英語を表し、「GB」は地域（英国）を表します。
- ファイル名の「invitation_template」と「.txt」サフィックスの間の部分には、最大 32 文字の英数字と「_」（アンダースコア）を使用できます。つまり、次の正規表現で表される任意の文字を使用できます。^[a-zA-Z_]{1,32}$.

注：本書の発行時点では、Windows で Google Chrome から Web アプリケーションを使用しているときに、招待テンプレートのファイル サイズが 1,491 バイトを超える場合、**[電子メールを開く（Open email）]** オプションが失敗します。これは Google Chrome ブラウザに関する既知の問題です。この問題の詳細については、次のリンクを参照してください。
https://bugs.chromium.org/p/chromium/issues/detail?id=1034497 [英語]

この問題が発生した場合、**[電子メールを開く（Open email）]** が灰色表示になりますが、**[コピー（Copy）]** を選択することで、好みの電子メール クライアントに会議参加情報を貼り付けることができます。

次の例を参考にして、プレースホルダに固有の値を使用してカスタマイズします。言語バリアントに応じた **invitation_template_xx_XX.txt** ファイル名形式を使用して保存します。

```
#if name
%name% に招待されています
#else
Cisco スペースに招待されています #endif

#if hyperlink
   参加するにはリンクをクリックします：%hyperlink%
#else
#if numeric_id
   参加するにはリンクをクリックします：https://join.example.com     コール
ID: %numeric_id%
#endif
#endif

#if hyperlink
リンクをクリックすると、Web アプリケーションを使用して起動します：%launch_link%
#else
起動リンクを使用できません
#endif

#if uri
     またはコールインします：
    - ビデオ システム、Jabber、または Lync: %uri%

 #endif

 #if numeric_id
       電話アクセス：地域のアクセス番号をコールして、%numeric_id% を入力します
       通話料無料ダイヤル（米国）：(800)-555-1234
       通話料無料ダイヤル（英国）：(0800)-800-8000
#endif

#if passcode
   パスコード：%passcode%
#endif
```

注：**%launch_link%** プレースホルダは、**#if_hyperlink** 条件に含める必要があります。そうすることで、ハイパーリンクが有効な場合はテンプレートに含まれ、ハイパーリンクが無効な場合は含まれません。

ローカルにホストされているブランディング、またはリモートの Web サーバにホストされているブランディングに招待テンプレート .txt ファイルをアップロードする方法の詳細については、カスタマイズのガイドライン [英語] を参照してください。

注：Web アプリケーションのカスタム電子メール招待には、ローカルにホストされたブランディングを使用することを推奨します。ただし、より複雑な導入環境（マルチテナント環境など）で複数の言語を使用する場合は、リモートのブランディング Web サーバを使用する必要があります。詳細については、カスタマイズのガイドライン [英語] を参照してください。

2.3 会議の追加のロック モード

Meeting Server 2.9 から、会議をロックするための追加のロック モード機能が導入されました。

注意：この追加のロック モード機能により、デフォルトの動作が変更されます。バージョン 2.9 から、**lockMode** はデフォルトで **all** に設定されています。アップグレード後に、このデフォルト動作の変更が希望に沿わない場合は、**/system/profiles** にある callProfile の設定で、**lockMode** を **needsActivation** に設定することによって、クラスタのデフォルトを変更する必要があります。既存の動作と新しい動作について、さらに詳しく説明します。

既存の会議「ロック」機能は、「ゲストのロック」機能として動作するものであり、実際には会議そのものをロックするものではないため、特定のメンバーはロックをバイパス可能です。この機能は、**callLeg** オブジェクトの **needsActivation** パラメータを使用します。ゲストの場合は、このパラメータが **true** に設定され、ホストの場合は **false** に設定されます。これを設定するために、通常は、異なる **callLegProfiles** を持つ 2 つの異なる **accessMethods** が使用されます。ゲストは一方の **accessMethod** を使用して参加し、ホストはもう一方の **accessMethod** を使用して参加します。

会議が「ロック」されているときの既存の動作としては、ホストは会議に参加できますが、ホストがすでに参加している場合でもゲストはロビーで待機状態のままになります。会議が「ロック解除」されると、ホストが会議に参加中であるかどうかによって、ゲストは会議に参加するか、ロビーに留まるかになります。

2.9 の新機能では、会議そのものをロックできるため、すべての参加者をロビーで待機させることができます。この新機能では、callProfile オブジェクトに API パラメータ **lockMode** が導入されました。使用可能な値は、**all**、**needsActivation**、または **<unset>** です。このパラメータは、次の操作をサポートします。

- **/callProfiles** に対して POST を実行
- **/callProfiles/<callProfile id>** で PUT を実行
- **/callProfiles/<callProfile id>** で GET を実行

lockMode を **needsActivation** に設定すると、バージョン 2.9 より前の既存の動作が提供され、ゲストのみがロックされます。

lockMode を **all** に設定した状態で会議がロックされている場合、新規の参加者は、ゲスト、ホスト、coSpace メンバーなどいずれであっても、会議には参加できず、ロビーに入室することになります。バージョン 2.9 から、**lockMode** はデフォルトで **all** に設定されています。

会議がロック解除されると、ロビーにいる参加者および会議への参加を試みている新規参加者はすべて、アクティベーション設定に応じて、会議への参加を許可されます。この動作は、**lockMode** が **needsActivation** に設定されている場合の、ロック解除された会議と同じです。ホストは会議に参加できますが、ゲストは、ホストがすでに参加中である場合にのみ参加できます。ゲストのアクティベーション方法に関する既存の動作ルールが適用されます。最後のホストがコールから退出するときの既存の動作ルールも考慮されます（つまり、**deactivationMode** 設定に応じて決まります）。

注：コールのタイプが「forwarded」または「lync conferencing」である場合、ロック モードの動作（**all** と **needsActivation** の両方）は無効になります。

2.3.1 デフォルト設定

/callLegs のデフォルト設定では、**needsActivation** が **false** に設定されており、全員がホストということになります。このため、デフォルトを変更しない限り、**lockMode** を **all** に設定すると、会議をロックすると全員がロックされ、会議をロック解除すると全員が許可されるという意味になります。

同様に、**/callLegs** および関連する **/callLegProfiles** で **needsActivation** が **<unset>** に設定されていると、デフォルトの動作は **needsActivation=false** となり、ユーザはデフォルトでホストになります。（**<unset>** は、**/callLegProfiles** の階層に基づいて動作が継承されることを意味します）。

lockMode が **needsActivation** に設定されている場合に、すべての参加者について **needsActivation** が **false** に設定されているときは、会議では誰もロックされません。

異なる **accessMethods** を設定していない基本的な coSpace での使用には、この新しい **lockMode** を **all** に設定するのが適切です。

2.3.2　会議のロックとロック解除

機能の変更はありません。従来と同じように、DTMF、アクティブ コントロール（Cisco Jabber のみ）、または API を使用して、**locked** パラメータを **true** または **false** に設定して **/calls** または **/callProfiles** に適用することで、会議をロックまたはロック解除することができます。詳細については、『Cisco Meeting Server API Guide（Cisco Meeting Server API ガイド）』[英語] を参照してください。

2.3.3　コールがロックまたはロック解除されたときのシグナリング

既存の API およびアクティブ コントロール イベントは従来から、コールがロックされるかロック解除されるときに信号を送出していました。これは、引き続き両方の **lockMode** 設定で動作します。

2.3.4　ロビーで待機中および会議に参加中の参加者を確認する方法

個別の **/callLeg/<call leg id>** API ノードの **status** セクションをチェックして、**deactivated** パラメータが表示されているかどうかを確認します。callLeg が非アクティブ化されていない場合は、このパラメータは **status** セクションには表示されず、参加者が会議に参加中であることを示します。**deactivated** パラメータは、**true** に設定されているときにのみ表示されます。これは、参加者がロビーで待機していることを示します。これは既存の動作です。

deactivated パラメータが **status** セクションに表示されていない場合は、関連する参加者は会議に参加中であり、パラメータが **true** に設定されている場合は、その参加者はロビーで待機しています。これは既存の動作です。

2.3.5　音声プロンプトの動作

新しいロック モードの動作をサポートするために、「この会議はロックされており、許可されるのを待っています（This meeting is locked, you are waiting to be allowed in）」という新しい音声プロンプトが導入されました。この新しい音声プロンプトのファイル名は locked_you_are_waiting.wav です。

この新しい音声プロンプトは、既存のプロンプトと同様にカスタマイズできます。詳細については、カスタマイズのガイドライン [英語] を参照してください。

非アクティブな参加者に対して流れる可能性があるプロンプトは次のとおりです。

1. 「Cisco Meeting へようこそ（Welcome to a Cisco Meeting）」
2. 「ホストが参加するのを待っています（Waiting for host to join）」/「この会議はロックされており、許可されるのを待っています（This meeting is now locked, you are waiting to be allowed in）」

参加者がアクティブ化されると、「会議に参加します（You are entering the meeting now）」という音声が流れ、会議に参加できます。

手順 2 で流れる可能性がある 2 つのプロンプトに関しては、参加者が非アクティブ状態であるときは、どちらかのプロンプトが流れる可能性があります。1 つ目は、参加者がゲスト（**needsActivation=true**）であり、ホストが会議に参加中ではない場合です。2 つ目は、参加者が非アクティブであるその他のすべての場合に流れます。

2.3.6　レコーダーおよびストリーマの動作の変更

会議がロックされているかどうか、および **callLegProfile** の **needsActivation** がどの値に設定されているかにかかわらず、レコーダーおよびストリーマは常に、ロビーをバイパスして会議に直接入室することができます。この動作は、どちらのロック モードでも同じです。

2.4　ロビーからの参加者の入室許可

参加者が会議に参加するときに、会議がロックされているか、ホストの参加を待っているために、一時的にロビーで待機状態になる可能性があります（27 ページの「会議の追加のロック モード」を参照してください。Meeting Server 2.9 から、新しい API コマンドを使用して、ロビーから会議への参加者の入室を許可する方法が導入されました。この機能では、すべての参加者を許可するか、個別の参加者を許可することができます。

/callLeg/<call leg id> API ノードでの GET 操作で使用する場合、既存の **deactivated** パラメータは **true** または **false** の値を取ることができます。値 **true** は、参加者がロビーにいることを意味し、**false** は、参加者が会議に参加中であることを意味します。

この新機能をサポートするために、API パラメータ **deactivated** の使用が PUT 操作と POST 操作にも拡張されました。詳細は以下のとおりです。これらの操作については、このパラメータが取ることのできる値は **false** のみです。

個別の参加者をアクティブ化して、ロビーから会議への入室を許可する場合、**deactivated** パラメータは以下の操作をサポートします。

- **/participants/<participant id>** に対して PUT を実行

すべての参加者をアクティブ化して、ロビーから会議への入室を許可する場合、**deactivated** パラメータは以下の操作をサポートします。

- **/calls/<call id>/participants/*** に対して POST を実行

どの API 操作が呼び出されるのかに応じて、現在ロビーにいる個別の参加者またはすべての参加者が、アクティブな参加者として会議に移されます。その後に参加する新規の参加者には、使用されている lockMode、コールのロック ステータス、および needsActivation の要求ステータスの組み合わせにより決定される動作が適用されます。会議への参加を許可されたゲスト（**needsActivation=true**）は、それ以降、最後のアクティベータがコールから退出するときの **deactivationMode** シナリオに従います。つまり、ロビーに戻されるか、切断されるか、コールに残ることを許可されます。

次の操作を使用して、API パラメータ **deactivated**（値 **false**）を指定した新規参加者を作成し、ロビーをバイパスして会議に直接入室させることもできます。

- **/calls/<call id>/participants** に対して POST を実行

参加者が移動した場合でも、同じ設定の組み合わせに従うことに注意してください。つまり、異なる扱いにはなりません。このため、移動した参加者がロビーをバイパスするためには、**deactivated=false** に設定する必要があります。

2.5 SIP レコーダーのサポート

Meeting Server 2.9 から外部のサードパーティ SIP レコーダーの設定が可能になり、録音開始時に、Meeting Server の内部レコーダー コンポーネントを使用する代わりに、管理者が設定した SIP URI がコールされます。

注：外部のサードパーティ SIP レコーダーのサポートについても、Meeting Server の録音ライセンスが必要です。

新しい SIP レコーダー機能は次のとおりです。

- ビデオとコンテンツの別々のストリームを受信するように BFCP をネゴシエートすることをレコーダーに許可します。これにより、録音のフォーマット方法について、より柔軟なオプションが提供されます。
- 標準 SIP コールの場合と同じ解像度をサポートします。
- 標準 SIP コールと同じ音声コーデックおよびビデオ コーデックをサポートします。
- 既存の Meeting Server 内部レコーダーの場合と同様に、SIP レコーダーから送信されたメディア コンテンツはすべて破棄されます。

注：SIP レコーダー機能では、TIP またはアクティブ コントロールはサポートされません。

2.5.1　SIP レコーダーの指定

SIP レコーダーを指定するために、**/callProfiles** オブジェクトに新しい API パラメータが導入されました。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。

- **sipRecorderUri**：これを設定した場合、録音が有効化されたときにダイヤルアウト先としてこの URI が使用されます。設定しない場合は、Meeting Server のレコーダー コンポーネント（**/recorders** で設定されている場合）が使用されます。

2.5.2　録音の開始および停止

Meeting Server のレコーダー コンポーネントでサポートされているのと同じ開始方法と停止方法を使用して、SIP レコーダーを開始できます。どのレコーダーが使用されるかは、API パラメータ **sipRecorderUri** を設定してあるかどうかによって決まります。現在サポートされている方法は次のとおりです。

- callProfile の **recordingMode** が **automatic** に設定されている場合、ユーザが参加すると録音が開始されます。ユーザが録音を開始または停止することはできません。
- **recordingMode** が **manual** に設定されている場合、ユーザは、dtmfProfile、アクティブ コントロール、ミーティング アプリケーション、またはコールに対して API の PUT または POST を使用して、録音を開始または停止できます。

2.5.3　録音ステータスの確認

Meeting Server のレコーダー コンポーネントでサポートされているのと同じ方法、たとえば、**callLegs/<call leg id>** に対する GET を使用して、SIP レコーダーのステータスを確認できます。この **status** 出力の **recording** の値が、その callLeg が録音中（**true**）であるかそうでないか（**false**）を示します。

2.6　パノラマ表示ビデオ レイアウト（ベータ サポート）

Meeting Server 2.9 から、参加者 2 人の会議でのパノラマ表示レイアウト エクスペリエンスのサポートが導入されました。この機能は、新しいパノラマ エンドポイントをサポートします。

- Cisco Webex Room Panorama
- Cisco Webex Room 70 Panorama
- Cisco Webex Room 70D Panorama アップグレード

会議の参加者がどちらもパノラマ エンドポイントである場合、Meeting Server は両者から 2 つのカメラ ストリームをリクエストできるため、両方の参加者は相手のルームを幅の広いパノラマ表示で見ることができます。

他のビデオ参加者が参加すると、Meeting Server はそのパノラマ エンドポイントから 1 つのカメラ ストリームのみをリクエストし、パノラマ表示レイアウトから既存のデュアル スクリーン レイアウトに移行します。パノラマ エンドポイントが 2 つある場合に、音声のみの参加者が会議に参加すると、パノラマ表示のエクスペリエンスが引き続き適用されます。

パノラマ表示レイアウトは、Meeting Server クラスタ全体で完全にサポートされます。パノラマ表示レイアウトでは、CE の既存の会議内制御（例：参加者リスト、ミュート、削除）がサポートされます。ローカル レイアウトやペイン配置の変更といったその他の機能は、パノラマ エンドポイントが既存のデュアル スクリーン レイアウトに移行した場合、つまりビデオ参加者が 3 人以上いる場合にのみサポートされます。

デュアル スクリーン エンドポイントは、パノラマ エンドポイントとの会議中に、パノラマ表示レイアウトを受信することができます。

パノラマ表示ビデオをサポートするために、次のように、既存の応答要素に新しい応答値が導入されました。

- **/callLegs/<callLeg ID>** で GET を実行：応答要素 **status** に要素 **multistreamVideo** が提供されます。この要素は次の 2 つの新しい値を返すことができます。
    - **numCameras** は、このコール レッグで現在アクティブな、マルチストリームのメインのビデオ カメラ ストリーム数を返します。
    - **numCamerasAvailable** は、このコール レッグで利用可能なものとして相手側がアドバタイズしているマルチストリームのメインのビデオ カメラ ストリーム数を返します。

2.6.1 Web インターフェイスの変更

2.9 から、デュアル カメラのサポートが導入されたのに伴い、明確化のために Web インターフェイスの「デュアル ビデオ」の表示が「デュアル スクリーン」に変更されました。

2.7　4K7fps コンテンツのサポート

バージョン 2.9 では、4K7fps を提供するシスコのエンドポイント上での 4K7fps コンテンツのサポートが導入されました。

注：サポートの対象は次のとおりです。

- メイン ビデオではなくコンテンツ ビデオのみ
- H.264 でのみサポート
- SIP コールでのみサポート

注：この機能は、バージョン 2.9 の Acano X シリーズではサポートされていません。

2.8　Chromium ブラウザのビデオおよびコンテンツの品質向上

バージョン 2.9 では、Chromium ブラウザのビデオおよびコンテンツの品質が向上しました。2.9 では、Chrome のソフトウェア デコーダを使用して 1080p のメイン ストリームとコンテンツ ストリームをデコードできるように、Chromium ブラウザの H.264 のデフォルト動作が変更されました。それによって会議の品質とユーザ エクスペリエンスが向上しました。

これにより、ほとんどのユーザにとって最適なエクスペリエンスが実現するものと考えています。従来、VP8 を強制的に使用していた場合は、この新しい H.264 の実装を試されることを推奨します。さらに、1080p をサポートするように、VP8 の実装も改善されています。

2.9 では、デフォルト動作でこの変更を実現するために、新しいパラメータ **`chromeWebRtcH264interopMode`** が導入されました。これは、**`compatibilityProfiles`** でグローバルに設定されるものであり、**`auto`**（新しいデフォルト動作）および **`none`**（従来の動作）の値を取ります。

注：この機能は、バージョン 2.9 の Acano X シリーズではサポートされていません。

2.9 より強力な暗号のサポート

バージョン 2.9 では、セキュリティ向上のために、SRTP メディア暗号化において、AES-128 および AES-256 バリアントによる GCM 暗号のサポートを導入しました。

SIP コールでは次の暗号がサポートされます（優先順位の順）：AEAD_AES_128_GCM、"AEAD_AES_256_GCM、AES_CM_128_HMAC_SHA1_80、AES_CM_128_HMAC_SHA1_32。

コールで使用される暗号は、トランクがどのように設定されているかに応じて、コール制御インフラストラクチャ（たとえば Cisco Unified CM）によって決定される可能性があります。つまり、特定の暗号、具体的には GCM（128 または 256 のバリアント）を強制的に使用するように設定できます。

/callLegs/<call leg id> オブジェクトに対する GET の応答に、新しいパラメータ **cipherSuite** が追加されました。このコール レッグのメディアのいずれかが暗号化されている場合、返される値は、使用中の SRTP 暗号化の暗号スイートを表し、次のいずれかになります。

- **AEAD_AES_128_GCM**：AES 暗号化、128 ビット、GCM
- **AEAD_AES_256_GCM**：AES 暗号化、256 ビット、GCM
- **AES_CM_128_HMAC_SHA1_80**：AES 暗号化、128 ビット、80 ビット SHA-1 認証タグ
- **AES_CM_128_HMAC_SHA1_32**：AES 暗号化、128 ビット、32 ビット SHA-1 認証タグ

2.10 API を使用した遠端カメラ制御の許可のサポート

バージョン 2.8 で導入された FECC サポートにより、Meeting Server の会議に参加している 1 つのエンドポイントが送信したカメラ制御コマンドが、別のエンドポイントに渡されます。送信先となるエンドポイントは、レイアウト上で制御システムの現在の「メインのペイン」になっているエンドポイントです。

バージョン 2.9 では、H.281 コマンドを使用してリモート システムのカメラの制御を可能にする API サポートが導入されました。制御しようとするシステムが、フォーカスされているレイアウトのメイン ペインになっている必要はありません。

リモート システムのカメラで FECC を許可するために、次の新しい API オブジェクトが導入されました。

- **/callLegs/<call leg id>/cameraControl** に対して PUT を実行

このオブジェクトは、新しいオプションのリクエスト パラメータをサポートしています。

- **pan**：**left** または **right**。リモート カメラを左または右にパンします。
- **tilt**：**up** または **down**。リモート カメラを上または下に傾けます。
- **zoom**：**in** または **out**。リモート カメラを拡大または縮小します。
- **focus**：**in** または **out**。リモート カメラにフォーカスを当てるか、フォーカスを外します。

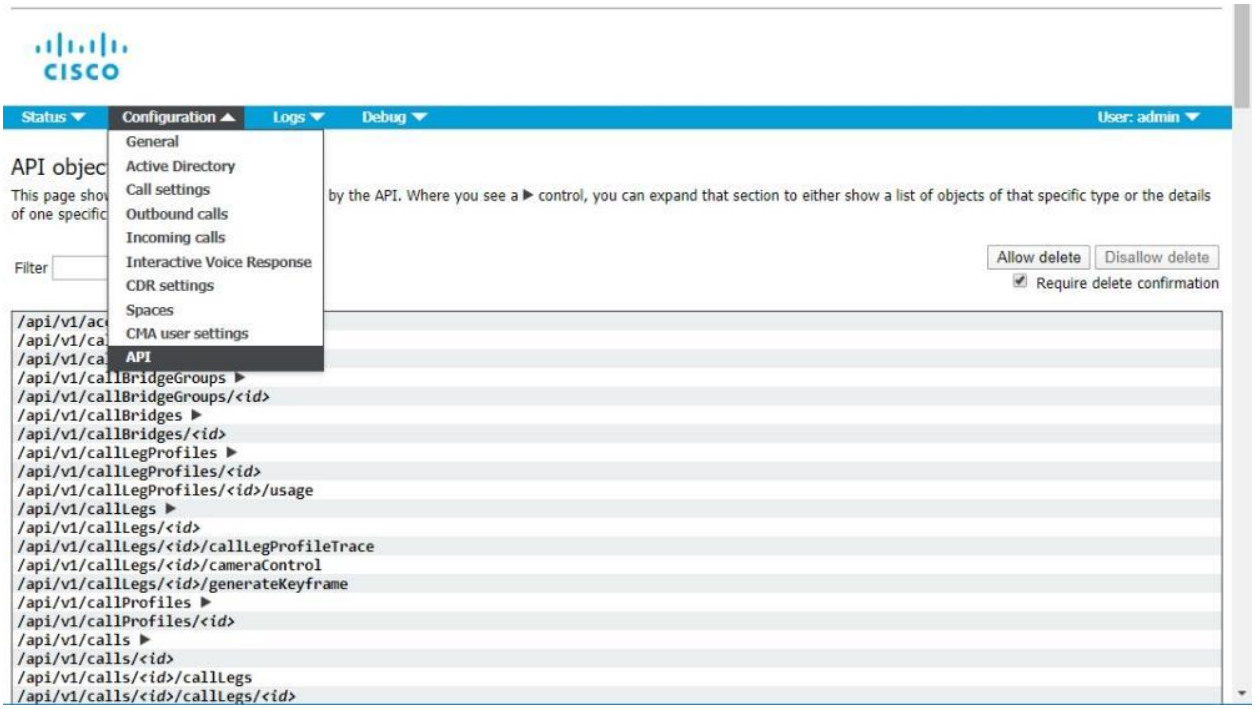
すべてのコール レッグで、カメラを制御する H.281 コマンドの受信がサポートされるわけではありません。FECC サポートをアドバタイズしたコール レッグのみに送信するには、それらのコール レッグのステータス応答の **cameraControlAvailable** 値を確認します。会議の途中でコール レッグのカメラ制御の可否を変更できることに注意してください。

2.11 Web インターフェイスでの API アクセス

バージョン 2.9 では、サードパーティ アプリケーションを必要とせずに API の使用方法をシンプルにするために、API 用のユーザ インターフェイスを導入しました。このインターフェイスには、Meeting Server Web インターフェイスの [**設定**（Configuration）] タブからアクセスできます（図 5 を参照）。

注：Web インターフェイスから API にアクセスするには、サードパーティ アプリケーションを使用する場合のように、MMP を使用して Meeting Server の初期設定および認証を実行する必要があります。詳細については、『MMP Command Reference Guide（MMP コマンド リファレンス ガイド）』[英語] を参照してください。

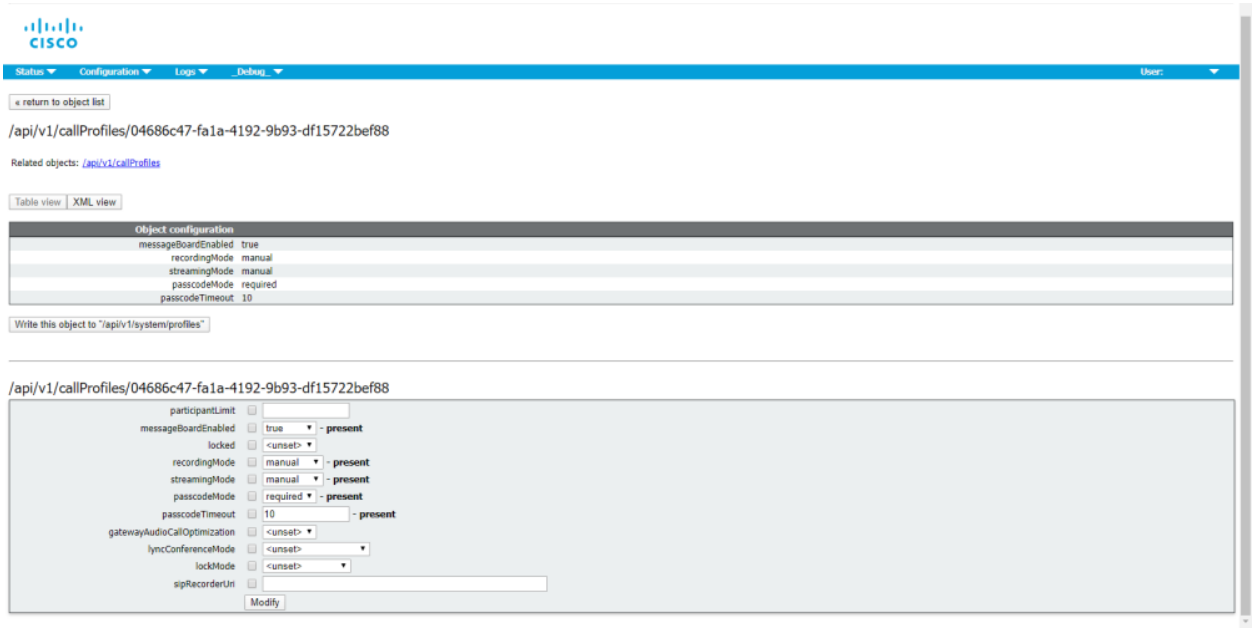
図 5：Meeting Server Web インターフェイスを介した API へのアクセス



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

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

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



2.12 オート ゲイン コントロール（AGC）を有効化する機能

注：この機能は、バージョン 2.8 でベータ機能として導入されましたが、バージョン 2.9 では完全にサポートされています。デフォルトでは、引き続き無効になっています。

サードパーティ クライアントによって設定されているさまざまなオーディオ レベルと、異なるヘッドセットのオーディオ レベルの差により、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。

2.8 以降、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 はデフォルトで無効になっており、新しいパラメータ **audioGainMode** に使用可能なオプション **agc** および **disabled** を使用してのみ有効にすることができます。この新しいパラメータは、次の API でサポートされています。

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

AGC が有効になっている場合、適用されるゲインは [ステータス（Status）] > [コール（Calls）] webadmin ページに表示されます。また、**rxAudio** セクションの下にある **/callLegs/<call leg id>** での GET 操作に応答して返される新規の API パラメータ、**gainApplied** もあります。

2.13 coSpace テンプレートの作成と適用

Meeting Server 2.9 から、coSpace テンプレートの作成と適用のサポートが導入されました。新しい API により、管理者は、定義済みの会議の特性を使用してテンプレートを作成できます。これらのテンプレートは、エンド ユーザによるスペースの作成をシンプルにするために Web アプリケーションで使用され、将来は、エンド ユーザにスペースを適用するために使用することが可能になります。エンド ユーザにテンプレートが割り当てられていない場合は、エンド ユーザが Web アプリケーションでスペースを作成することはできません。

従来は、ミーティング アプリケーションのクライアントまたはユーザは、権限を付与されている場合にスペースを作成できました。この権限は、そのユーザに割り当てられた userProfile の API パラメータ canCreateCoSpaces を使用して設定されていました。この設定は、新しい Web アプリケーションには適用されません。その代わりに、誰がスペースを作成できるかだけでなく、どのタイプのスペースを作成できるかについても、管理者がさらに詳細に制御できるようになりました。これは、coSpace テンプレートを作成し、Web アプリケーションのユーザがどのテンプレートを利用できるかを指定することで実現します。

注：この機能は、Meeting Server の API から設定できます。Cisco Meeting Management 2.9(RC1) 以降のバージョンでは、よりシンプルな Web ベースの方法でこの機能を設定できます。詳細については、Cisco Meeting Management 2.9 のリリース ノートを参照してください。

この機能により、バージョン 2.9 で次の新しい API オブジェクトが導入されました。

- **/coSpaceTemplates**
- **/coSpaceTemplates/<coSpace template id>**
- **/coSpaceTemplates/<coSpace template id>/accessMethodTemplates**
- **/coSpaceTemplates/<coSpace template id>/accessMethodTemplates/<access method template id>**
- **/ldapUserCoSpaceTemplateSources**
- **/ldapUserCoSpaceTemplateSources/<LDAP user coSpace template source id>**
- **/users/<user id>/userCoSpaceTemplates**
- **/users/<user id>/userCoSpaceTemplates/<user coSpace Template id>**

この機能をサポートするすべての API の追加の詳細については、「API の追加の概要」を参照してください。

2.13.1 テンプレートを作成してユーザに割り当てる方法

1. API を使用して coSpaceTemplates オブジェクトを作成します。
   - **`/coSpaceTemplates`** に対して POST を実行
   - 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
Name	文字列	この coSpace テンプレートに関連付けられる、人間が判読できる名前
description	文字列	このテンプレートを使用する理由についてユーザに説明するための、coSpace テンプレートの長い説明
callProfile	ID	これが指定されている場合は、指定されたコール プロファイルをこの coSpaceTemplate に関連付けます。
callLegProfile	ID	これが指定されている場合は、指定されたコール レッグ プロファイルをこの coSpaceTemplate に関連付けます。

2. API を使用して、0、1、または複数のアクセス方式テンプレート オブジェクトを作成します。この accessMethodTemplate オブジェクトは、手順 1 で作成した coSpaceTemplate に固有のものです。
   - **`/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates`** に対して POST を実行
   - 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
Name	文字列	このアクセス方式テンプレートに関連付けられる、人間が判読できる名前
uriGenerator	文字列	このアクセス方式テンプレート用に URI 値を生成するために使用される式。使用可能な文字セットは、「a」から「z」、「A」から「Z」、「0」から「9」、「.」、「-」、「_」、および「$」です。空にしない場合は、文字「$」を少なくとも 1 個は含める必要があります。
callLegProfile	ID	これが指定されている場合は、指定されたコール レッグ プロファイルをこの accessMethodTemplate に関連付けます。
generateUniqueCallId	true または false	

この時点で、次の手順 3 で説明する API を使用するか、新しい /UserCoSpaceTemplateSources API を介して UserCoSpaceTemplateSource を作成し、既存の /ldapSources API および /ldapSyncs API を介して使用することで、ユーザにテンプレートを割り当てることができます。「LDAP を使用した userCoSpaceTemplates の適用」を参照してください。

3. API を使用して、coSpaceTemplate をユーザに割り当てます。
   - **`/users/<user id>/userCoSpaceTemplates`** に対して POST を実行

パラメータ	タイプ/値	説明/メモ
coSpaceTemplate	ID	coSpace をインスタンス化するためにユーザが使用を許可されている coSpace テンプレートの ID

2.13.2 LDAP を使用した userCoSpaceTemplates の適用

1. 通常のユーザ プロビジョニングの場合と同様に、次のように作成します。
   - ldapServer：/ldapServers ノードで POST を実行
   - ldapMapping：/ldapMappings ノードで POST を実行
   - ldapSource：/ldapSources ノードで POST を実行

   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. ldapSource については、ユーザのセットに対して適用する coSpaceTemplate ごとに 1 つずつ、0、1、または複数の ldapUserCospaceTemplateSources を作成します。
   - **`/ldapUserCoSpaceTemplateSources`** に対して POST を実行
   - 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。

リクエストパラメータ	タイプ/値	説明/メモ
coSpaceTemplate	ID	これらのユーザに適用される coSpace テンプレートの ID
ldapSource	ID	ユーザの検索に使用される LDAP ソースの ID
filter	文字列	ソースの読み取り時に適用される追加の LDAP フィルタ文字列

coSpaceTemplate が適用されるユーザのセットは、ldapSource によって生成されるセットで定義され、ldapUserCoSpaceTemplateSources の「filter」属性によってフィルタ処理されます。

ldapUserCoSpaceTemplateSources の coSpaceTemplate 属性および「filter」属性をそれぞれ設定します。

3. API から LDAP 同期を使用してユーザと userCoSpaceTemplates を適用します。
    - 通常の LDAP synchronization については、/ldapSyncs node で POST を実行します。

注：複数の ldapSources/<id> フィルタに同じユーザが表示される場合は、Meeting Server で使用する同期順序に基づいて、そのユーザに関連付けられた userProfile が変更される可能性があります。（userProfile には、そのユーザに PMP ライセンスを関連付ける hasLicense を含め、そのユーザに関連付けられた権限が格納されます）。これは、userProfile によって PMP Plus ライセンスが割り当てられている ldapSources/<id> フィルタの 1 つにユーザが含まれており、かつ、userProfile によってライセンスが割り当てられていない ldapSources/<id> フィルタにも含まれている場合、ユーザにライセンスが割り当てられているかどうかを制御できないことを意味します。

2.14 2.9 の API の追加および変更の概要

Meeting Server 2.9 の新しい API 機能には次のものが含まれます。

- Web アプリケーションをサポートするための新しい API 応答値
- 会議をロックするための新しい API パラメータ
- API パラメータの使用の拡張による、ロビーからの参加者の入室許可および参加者がロビーをバイパスして会議に参加することの許可
- サードパーティの SIP レコーダーを使用するための新しい API パラメータ
- パノラマ表示ビデオをサポートするための新しい API パラメータ
- リモート システムでの FECC を許可するための新しい API オブジェクトおよびパラメータ
- より強力な暗号をサポートするための新しい API オブジェクトおよびパラメータ
- WebRTC コール用に Chromium ブラウザで使用される H.264 パラメータを制御するための新しい API パラメータ
- coSpace テンプレートの作成と適用をサポートするための新しい API オブジェクトおよびパラメータ

バージョン 2.9 では、次の新しい API オブジェクトが導入されました。

- **/callLegs/<call leg id>/cameraControl**
- **/coSpaceTemplates**
- **/coSpaceTemplates/<coSpace template id>**
- **/coSpaceTemplates/<coSpace template id>/accessMethodTemplates**
- **/coSpaceTemplates/<coSpace template id>/accessMethodTemplates/<access method template id>**
- **/users/<user id>/userCoSpaceTemplates**
- **/users/<user id>/userCoSpaceTemplates/<user coSpace Template id>**
- **/ldapUserCoSpaceTemplateSources**

2.14.1 コール レッグでの Web アプリケーションケーション情報の取得

/callLegs/<call leg id> で GET を実行する際に、コール レッグのサブタイプが Web アプリケーションかどうかを確認するために、応答値 **subType** で **webApp** の新しい値を返すことができます。

2.14.2 追加のロック モードを使用した会議のロック

追加のロック モード機能を使用して会議をロックするために、次のように使用できる新しい API リクエスト パラメータ **lockMode** が追加されました。

- **/callProfiles** に対して POST を実行
- **/callProfiles/<call profile id>** に対して PUT を実行

これらのいずれの操作についても、**lockMode** を次のオプションのいずれかに設定できます。

- **all**：会議がロックされているときは、すべての新規参加者が会議への参加を許可されず、ロビーで待機状態になります。これには、アクティベーションを必要としない参加者も含まれます。
- **needsActivation**：会議がロックされているときに、アクティベーションを必要としない新規参加者は会議に入室します。ただし、アクティベーションを必要とする新規参加者はロビーに入ります。coSpace のメンバーである参加者は、すでに会議に参加中のアクティベータがいる場合には、アクティベーションが必要な場合であっても、ロックをバイパスして会議に入室します。

2.14.3 ロビーからの参加者の入室許可

/callLeg/<call leg id> API ノードでの GET 操作で使用する場合、既存の **deactivated** パラメータは **true** または **false** の値を取ることができます。値 **true** は、参加者がロビーにいることを意味し、**false** は、参加者が会議に参加中であることを意味します。

この新機能をサポートするために、API パラメータ **deactivated** の使用が PUT 操作と POST 操作にも拡張されました。詳細は以下のとおりです。これらの操作については、このパラメータが取ることのできる値は **false** のみです。

個別の参加者をアクティブ化して、ロビーから会議への入室を許可する場合、**deactivated** パラメータは以下の操作をサポートします。

- **/participants/<participant id>** に対して PUT を実行

すべての参加者をアクティブ化して、ロビーから会議への入室を許可する場合、**deactivated** パラメータは以下の操作をサポートします。

- **/calls/<call id>/participants/*** に対して POST を実行

2.14.4 ロビーをバイパスして会議に直接入室する参加者の作成

新規参加者を作成し、それらの参加者にロビーをバイパスして会議に直接入室させるために、次のように使用できる API パラメータ **deactivated** が追加されました。

- **/calls/<call id>/participants** に対して POST を実行し、API パラメータ **deactivated** を設定このパラメータが取ることができる値は **false** のみです。

指定された会議に新規参加者を作成するために、このパラメータは callLeg create 操作のとおりに設定されますが、結果として、リモートのクラスタ化された Call Bridge でコール レッグのインスタンス化が発生する（新しい参加者オブジェクトによって「所有」される）可能性があります。

2.14.5 サードパーティ SIP レコーダーを使用した録音

SIP レコーダーを使用して会議を録音するために、次のように使用できる新しいリクエスト パラメータ **sipRecorderUri** が追加されました。

- **/callProfiles** に対して POST を実行
- **/callProfiles/<call profile id>** に対して PUT を実行

sipRecorderUri パラメータは、SIP レコーダーのダイヤル アウト URI 文字列です。

SIP レコーダーの URI を確認するには、次の手順を実行します。

- **/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、**sipRecorderUri** が含まれる可能性があります。

2.14.6 API を使用した遠端カメラ制御（FECC）の許可

リモート システムのカメラで FECC を許可するために、次の新しい API オブジェクトが導入されました。

- **/callLegs/<call leg id>/cameraControl** に対して PUT を実行

このオブジェクトは、新しいオプションのリクエスト パラメータをサポートしています。

pan：**left** または **right**。リモート カメラを左または右にパンします。

tilt：**up** または **down**。リモート カメラを上または下に傾けます。

zoom：**in** または **out**。リモート カメラを拡大または縮小します。

focus：**in** または **out**。リモート カメラにフォーカスを当てるか、フォーカスを外します。

2.14.7 パノラマ表示ビデオの使用

パノラマ表示ビデオをサポートするために、次のように、既存の応答要素に新しい応答値が導入されました。

- **/callLegs/<callLeg ID>** で GET を実行：応答要素 **status** に要素 **multistreamVideo** が提供されます。この要素は次の 2 つの新しい値を返すことができます。
  - **numCameras** は、このコール レッグで現在アクティブな、マルチストリームのメインのビデオ カメラ ストリーム数を返します。
  - **numCamerasAvailable** は、このコール レッグで利用可能なものとして相手側がアドバタイズしているマルチストリームのメインのビデオ カメラ ストリーム数を返します。

2.14.8 コール レッグで使用される暗号スイートの決定

特定のコール レッグで使用される暗号スイートを確認するには、次の手順を実行します。

- **/callLegs/<call leg id>** での GET の実行による応答値は、新しいパラメータ **cipherSuite** をサポートします。このパラメータは、**status** の下で返されます。このコール レッグのメディアのいずれかが暗号化されている場合、返される値は、使用中の SRTP 暗号化の暗号スイートを表します。次のいずれかになります。
  - **AEAD_AES_256_GCM**：AES 暗号化、256 ビット、GCM
  - **AEAD_AES_128_GCM**：AES 暗号化、128 ビット、GCM
  - **AES_CM_128_HMAC_SHA1_80**：AES 暗号化、128 ビット、80 ビット SHA-1 認証タグ
  - **AES_CM_128_HMAC_SHA1_32**：AES 暗号化、128 ビット、32 ビット SHA-1 認証タグ

2.14.9 WebRTC コール用に Chromium ブラウザで使用される H.264 パラメータの制御

WebRTC コール用に Chromium ブラウザで使用される H.264 パラメータを制御するために、次のように使用できる新しいリクエスト パラメータ **chromeWebRtcH264interopMode** が追加されました。

- **/compatibilityProfiles** に対して POST を実行
- **/compatibilityProfiles/<compatibility profile id>** に対して PUT を実行

パラメータ **chromeWebRtcH264interopMode** は、**auto** または **none** になります。それぞれの意味は次のとおりです。

- **auto**：デフォルトの動作。Chrome のソフトウェア デコーダーを使用して 1080p のメイン ストリームおよびコンテンツ ストリームをデコードすることを許可します。
- **none**：従来の動作。

2.9 から、Chromium ブラウザはデフォルトでソフトウェア デコーダーを使用するようになったため、WebRTC セッションで CPU 使用率が上昇する可能性があります。これは PC に依存します。

注：このパラメータが変更された場合、すべての新規 WebRTC セッションに新しい設定が適用されます。一方で、アクティブな WebRTC セッションではページの更新が必要であり、コールに参加し直す必要があります。進行中の WebRTC コールは影響を受けません。

2.14.10 coSpace テンプレートの使用

2.14.10.1 coSpace テンプレートの作成、変更、取得、列挙、および削除

次のリクエスト パラメータを使用して coSpace テンプレートを実装するために、新しい API ノード **/coSpaceTemplates** が使用されます。

パラメータ	タイプ/値	説明/メモ
Name	文字列	この coSpace テンプレートに関連付けられる、人間が判読できる名前
description	文字列	このテンプレートを使用する理由についてユーザに説明するための、coSpace テンプレートの長い説明
callProfile	ID	これが指定されている場合は、指定されたコール プロファイルをこの coSpaceTemplate に関連付けます。
callLegProfile	ID	これが指定されている場合は、指定されたコール レッグ プロファイルをこの coSpaceTemplate に関連付けます。

この API ノード **/coSpaceTemplates** は、次の操作をサポートします。

- **/coSpaceTemplates** に対して POST を実行
- **/coSpaceTemplates/<coSpace template id>** に対して PUT を実行
- **/coSpaceTemplates/<coSpace template id>** で DELETE を実行
- **/coSpaceTemplates/<coSpace template id>** で GET を実行、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 coSpace テンプレートに関連付けられる、人間が判読できる名前
description	文字列	このテンプレートを使用する理由についてユーザに説明するための、coSpace テンプレートの長い説明
callProfile	ID	これが指定されている場合は、指定されたコール プロファイルをこの coSpaceTemplate に関連付けます。
callLegProfile	ID	これが指定されている場合は、指定されたコール レッグ プロファイルをこの coSpaceTemplate に関連付けます。
numAccessMethodTemplates	番号	この coSpace テンプレートに関連付けられているアクセス方式テンプレートの数

- **`/coSpaceTemplates`** で enumerate GET を実行、次の応答が返されます。

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 coSpace テンプレートを取得するために、オフセットと制限を指定できます。
limit		
filter	文字列	filter=<string> を指定すると、フィルタと一致する coSpace テンプレートのみが返されます。

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、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 coSpace テンプレートに関連付けられる、人間が判読できる名前
callProfile	ID	これが指定されている場合は、指定されたコールプロファイルをこの coSpaceTemplate に関連付けます。
callLegProfile	ID	これが指定されている場合は、指定されたコールレッグ プロファイルをこの coSpaceTemplate に関連付けます。
numAccessMethodTemplates	番号	この coSpace テンプレートに関連付けられているアクセス方式テンプレートの数

2.14.11 アクセス方式テンプレートの使用

2.14.11.1 coSpace テンプレートのアクセス方式テンプレートの作成、変更、取得、列挙、および削除

2.9 では、以下のリクエスト パラメータと共に新しい API ノード **`/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates`** が導入されました。

パラメータ	タイプ/値	説明/メモ
Name	文字列	このアクセス方式テンプレートに関連付けられる、人間が判読できる名前
uriGenerator	文字列	このアクセス方式テンプレート用に URI 値を生成するために使用される式。使用可能な文字セットは、「a」から「z」、「A」から「Z」、「0」から「9」、「.」、「-」、「_」、および「$」です。空にしない場合は、文字「$」を少なくとも 1 個は含める必要があります。
callLegProfile	ID	これが指定されている場合は、指定されたコール レッグ プロファイルをこの accessMethodTemplate に関連付けます。
generateUniqueCallId	true または false	このアクセス方式に固有の数値 ID を生成するかどうか。作成（POST）操作でこのパラメータが指定されていない場合は、この ID が coSpace のグローバルな ID より優先されます。デフォルトは false です。

新しい API ノード **`/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates`** は、次の操作をサポートします。

- **`/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates`** に対して POST を実行
- **`/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates/<access method template ID>`** に対して PUT を実行
- **`/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates/<access method template ID>`** で DELETE を実行
- **`/coSpaceTemplates/<coSpace template id>/accessMethodTemplates/<access method template id>`** で GET を実行。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	このアクセス方式テンプレートに関連付けられる、人間が判読できる名前
uriGenerator	文字列	このアクセス方式テンプレート用に URI 値を生成するために使用される式。使用可能な文字セットは、「a」から「z」、「A」から「Z」、「0」から「9」、「.」、「-」、「_」、および「$」です。空にしない場合は、文字「$」を少なくとも 1 個は含める必要があります。
callLegProfile	ID	これが指定されている場合は、指定されたコール レッグ プロファイルをこの accessMethodTemplate に関連付けます。
generateUniqueCallId	true または false	このアクセス方式に固有の数値 ID を生成するかどうか。作成（POST）操作でこのパラメータが指定されていない場合は、この ID が coSpace のグローバルな ID より優先されます。デフォルトは false です。

- **/coSpaceTemplates/<coSpace template ID>/accessMethodTemplates** で enumerate GET を実行。次の応答が返されます。

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 coSpace アクセス方式テンプレートを取得するために、オフセットと制限を指定できます。
limit		
filter	文字列	filter=<string> を指定すると、名前がフィルタと一致する coSpace アクセス方式テンプレートのみが返されます。
callLegProfileFilter	文字列	callLegProfileFilter=<string> を指定すると、指定されたコール レッグ プロファイルを使用する coSpace アクセス方式テンプレートのみが返されます。

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
Name	文字列	このアクセス方式テンプレートに関連付けられる、人間が判読できる名前
uriGenerator	文字列	このアクセス方式テンプレート用に URI 値を生成するために使用される式。使用可能な文字セットは、「a」から「z」、「A」から「Z」、「0」から「9」、「.」、「-」、「_」、および「$」です。空にしない場合は、文字「$」を少なくとも 1 個は含める必要があります。
callLegProfile	ID	これが指定されている場合は、指定されたコール レッグ プロファイルをこの accessMethodTemplate に関連付けます。
generateUniqueCallId	true または false	このアクセス方式に固有の数値 ID を生成するかどうか。作成（POST）操作でこのパラメータが指定されていない場合は、この ID が coSpace のグローバルな ID より優先されます。デフォルトは false です。

2.14.11.2　アクセス方式への名前ラベルの追加（オプション）

新しいオプションの API パラメータ **name** を使用すると、アクセス方式に名前ラベルを追加することができ、coSpace テンプレートとの関連付けで適切なものを選択しやすくなります。

アクセス方式に名前ラベルを追加するために、パラメータ **name** は文字列の値を取り、追加します。次のように使用できます。

- **/coSpaces/<coSpace id>/accessMethods** に対して POST を実行
- **/coSpaces/<coSpace id>/accessMethods/<access method id>** に対して PUT を実行

name パラメータは、**/coSpaces/<cospaceId>/accessMethods** での GET の応答で、アクセス方式ごとに返されます。

2.14.11.3 LDAP サーバへの名前ラベルの追加（オプション）

この API の追加により、ユーザ インターフェイスに表示される LDAP サーバが識別しやすくなります。LDAP サーバに名前ラベルを追加するために、新しいオプションの API リクエスト パラメータ **name** が追加され、文字列の値を取ります。次のように使用できます。

- **/ldapServers** に対して POST を実行
- **/ldapServers/<ldap server id>** に対して PUT を実行

name パラメータは、**/ldapServers** での GET の応答で、LDAP サーバごとに返されます。

2.14.11.4 ユーザへの coSpace テンプレートの適用

2.9 では、新しい API オブジェクト **/users/<user id>/userCoSpaceTemplates** が追加されました。このオブジェクトは、新しいリクエスト パラメータ **coSpaceTemplate** をサポートし、その値は、coSpace をインスタンス化するためにユーザが使用を許可された coSpace テンプレートの ID です。次の操作がサポートされます。

- **/users/<user id>/userCoSpaceTemplates** に対して POST を実行

パラメータ	タイプ/値	説明/メモ
coSpaceTemplate	ID	coSpace をインスタンス化するためにユーザが使用を許可されている coSpace テンプレートの ID

- **/users/<user ID>/userCoSpaceTemplates/<user coSpace template ID>** で DELETE を実行
- **/users/<user ID>/userCoSpaceTemplates/<user coSpace template ID>** で GET を実行すると、次の応答パラメータが返されます。

応答パラメータ	タイプ/値	説明/メモ
coSpaceTemplate	ID	coSpace をインスタンス化するためにユーザが使用を許可されている coSpace テンプレートの ID。
autoGenerated	true または false	この coSpace テンプレートが自動で追加されたのか、手動で追加されたのか true：このテンプレートは LDAP 同期操作の一部として自動的に追加されたため、同期操作のパラメータを変更する方法以外に、削除することはできません。 false：このテンプレートは API メソッドを使用して追加されました。API を使用して変更または削除することができます。

- **/users/<user ID>/userCoSpaceTemplates** で enumerate GET を実行。標準の URI パラメータである limit と offset をサポートします。その応答は、最上位レベルの <userCoSpaceTemplates total="N"> タグとして構成され、その下位に複数の <userCoSpaceTemplate> 要素が含まれる可能性があります。各 <userCoSpaceTemplate> タグには、リクエストと応答のパラメータ（coSpaceTemplate と autoGenerated）が含まれます。

URI パラメータ	タイプ/値	説明/メモ
offset		名目上のリストの 1 ページ目にある以外のアクセス方式を取得するために、オフセットと制限を指定できます。
limit		

2.14.11.5 LDAP を使用した userCoSpaceTemplates の適用

2.9 では、ユーザが LDAP 方式を使用してスペースを作成することを許可するために、新しい API オブジェクト **/ldapUserCoSpaceTemplateSources** が導入されました。これにより、テンプレートをソース オブジェクトに直接含めることができます。

この新しい API オブジェクト **/ldapUserCoSpaceTemplateSources** は、次の操作をサポートします。

- **/ldapUserCoSpaceTemplateSources** に対して POST を実行
- **/ldapUserCoSpaceTemplateSources** に対して PUT を実行

リクエストパラメータ	タイプ/値	説明/メモ
coSpaceTemplate	ID	これらのユーザに適用される coSpace テンプレートの ID
ldapSource	ID	ユーザの検索に使用される LDAP ソースの ID
filter	文字列	ソースの読み取り時に適用される追加の LDAP フィルタ文字列

- **/ldapUserCoSpaceTemplateSources/<LDAP user coSpace template source id>** で GET を実行、次の応答が返されます。

応答要素	タイプ/値	説明/メモ
coSpaceTemplate	ID	これらのユーザに適用される coSpace テンプレートの ID
ldapSource	ID	ユーザの検索に使用される LDAP ソースの ID
filter	文字列	ソースの読み取り時に適用される追加の LDAP フィルタ文字列

- **/ldapUserCoSpaceTemplateSources** で enumerate GET を実行、次の応答が返されます。

URI パラメータ	タイプ/値	説明/メモ
offset		名目上のリストの 1 ページ目にある以外のエントリを取得するために、オフセットと制限を指定できます。
limit		

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

各 <ldapUserCoSpaceTemplateSource&gt 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
coSpaceTemplate	ID	これらのユーザに適用される coSpace テンプレートの ID
ldapSource	ID	ユーザの検索に使用される LDAP ソースの ID

2.14.11.6 新しい API の障害理由

この機能について、2.9 で次の新しい API の障害理由が導入されました。

- **coSpaceAccessMethodTemplateDoesNotExist**：システム上の有効な coSpace アクセス方式テンプレートと対応していない ID を使用して、coSpace アクセス方式テンプレートを変更、削除、または取得しようとしました。
- **coSpaceTemplateDoesNotExist**：システム上の有効な coSpace テンプレートと対応していない ID を使用して、coSpace テンプレートを変更、削除、または取得しようとしました。
- **duplicateUserCoSpaceTemplate**：ユーザに対して同じ coSpace テンプレートを 2 回割り当てようとしました。
- **userCoSpaceTemplateDeletionProhibited**：自動生成された coSpace テンプレートの割り当てをユーザから解除しようとしました。これは許可されない操作です。

- **`userCoSpaceTemplateDoesNotExist`**：そのユーザに対する有効なユーザ coSpace テンプレートと対応していない ID を使用して、ユーザ coSpace テンプレートを変更、削除、または取得しようとしました。
- **`ldapUserCoSpaceTemplateSourceDoesNotExist`**：既存の LDAP ユーザ coSpace テンプレートのソース エントリに対応していない ID を使用して、削除または取得しようとしました。

2.15 CDR の変更の概要

バージョン 2.9 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。

- 新しい値 **`webApp`** が、callLegStart レコードの **`subType`** パラメータに追加されました。これは、コール レッグのサブタイプが Web アプリケーションであるかどうかを示します。
- 新しいパラメータ **`recorderUri`** が recordingStart レコードに追加されました。これは文字列であり、SIP レコーダーの場合は録音デバイスの URI です。（従来は、path と recorderUrl の両方を常に指定していましたが、これらは SIP レコーダーには送信されません。recordingEnd レコードには変更はありません）。

2.16 MMP の追加の概要

Web Bridge2.16.1 3 サポート

バージョン 2.9 は、Web Bridge 3 を使用した新しい Web アプリケーションの実装について、これらの MMP の変更をサポートします。

コマンド	説明
webbridge3	Web Bridge 3 の現在の値のセットを表示します。
help webbridge3	webbridge3 のすべてのサブコマンドと共にヘルプを表示します。
webbridge3 restart	Web Bridge 3 を再起動します。
webbridge3 (enable|disable)	Web Bridge 3 を有効化または無効化します。
webbridge3 https listen <*interface*:port whitelist>	Web Bridge 3 がリッスンするインターフェイスとポートをセットアップします。コマンド **webbridge3 enable** を使用して、サービスを有効化し、リッスンを開始します。ポートのデフォルト値はなく、指定する必要があります。
webbridge3 https certs <key-file> <crt-fullchain-file>	Web Bridge 3 の HTTPS 証明書を設定します。これらは Web ブラウザに対して提示される証明書であるため、認証局（CA）による署名が必要であり、ホスト名や目的などが一致している必要があります。（証明書ファイルは、エンド エンティティの証明書で始まりルート証明書で終わる完全な証明書チェーンです）。
webbridge3 https certs none	HTTPS 証明書の設定を削除します。
webbridge3 http-redirect (enable [port]|disable)	（オプション）HTTP 接続のポートをセットアップすることで、HTTP リダイレクトを有効化または無効化します。このポートは、Web アプリケーションが設定されているすべての Meeting Server インターフェイスに対して開かれます。着信 HTTP 接続は、着信したインターフェイスでの一致する HTTPS ポートに自動的にリダイレクトされます。**webbridge3 http-redirect enable [port]** でポートを指定しない場合、デフォルトのポートは 80 です。

webbridge3 c2w listen <*interface*:port whitelist>	C2W 接続を設定します。Web Bridge 3 がリッスンするインターフェイスとポートをセットアップします。コマンド **webbridge3 enable** を使用して、サービスを有効化し、リッスンを開始する必要があります。このアドレスとポートは、Call Bridge からのみアクセス可能にすることを推奨します。
webbridge3 c2w certs <key-file> <crt-fullchain-file>	C2W 接続の証明書を設定：C2W 接続に使用する SSL サーバ証明書を設定する必要があります。C2W 証明書は、C2W プロトコルの接続ポートに接続する Call Bridge に対してのみ提示されます。ホスト名および目的などが一致する必要があります。（証明書ファイルは、エンド エンティティの証明書で始まりルート証明書で終わる完全な証明書チェーンです）。
webbridge3 c2w certs none	C2W 接続の証明書の設定を削除します。
webbridge3 c2w trust <crt-bundle>	Web Bridge 3 C2W サーバが Call Bridge クライアント証明書を検証し、それらのクライアントを信頼するかどうかを決定するための、信頼バンドルを設定します。
webbridge3 c2w trust none	C2W 接続の信頼バンドルの設定を削除します。
webbridge3 options <space-separated options>	指定された機能を切り替えます。複数の機能が有効になっている場合は、feature_names をスペースで区切ります。このコマンドは、Cisco サポートまたは Cisco EFT からの指示がある場合にのみ使用してください。これらの機能は、実稼働での使用には適していません。この機能は、再起動しても有効なままですが、アップグレード コマンドを使用すると自動的にクリアされます。（このコマンドは現在サポートされていません）。
webbridge3 options none	Webbridge オプション <feature_name>コマンドを使用して以前にスイッチされたすべての機能をオフにします。シスコ サポートから指示がある場合にのみ使用してください。（このコマンドは現在サポートされていません）。
webbridge3 status	Web Bridge 3 の現在の設定を表示します。

2.17 イベントの変更の概要

バージョン 2.9 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 2.9 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 2.8 からアップグレードすることを想定しています。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、Cisco Meeting Server 2.9 リリース ノートに記載されている手順に従う前に、2.8.x リリース ノートの手順に従って 2.8 にアップグレード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、2.8 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 2000、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**バージョン**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（Cisco Meeting Server 仮想化導入インストール ガイド）の指示に従ってください。

3.1　リリース 2.9 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、**バックアップ スナップショット <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。再起動プロセスは、サーバ上で実行されているすべてのアクティブコールを中断します。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。または、ユーザに事前に警告する必要があります。

セカンダリサーバをインストールするには、次の手順に。

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_2_9_1_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）：
   19cf569772909cfd1c4cb3e1a3bd0818f7c32cf74f491f6ab0d4a2dd5d21d646

   Cisco_Meeting_Server_2_9_1_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）：
   5550cde2f4002d6e2ca45d0f0acca457483a0b46dc3e45b17bc91ca5e127a88e

   Cisco_Meeting_Server_2_9_1_x-series.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、Acano X シリーズ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）：
   ce2444255217433fd6515857040bbdcc66078223ede33833a22acde0eb05f5cb

   Cisco_Meeting_Server_2_9_1.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。

   vSphere6 の場合、Cisco_Meeting_Server_2_9_vSphere-6_0.ova ファイルのハッシュ（SHA-512）：
   b0d548c48965b2f8e12b0289ea2ffdd5934291d649bff88a1bd053e82c10a8cbc963773adbc1949627bdcf8cadc8d62896e39f2cb67b8f63dedb8d9163aa6c22

   vSphere6.5 以降の場合、Cisco_Meeting_Server_2_9_vSphere-6_5.ova ファイルのハッシュ（SHA-512）：
   27c1ea70e1d955560b6e55268778027ccb5f8809395127acae3a4f5734b12ca6eee2cefb776290d99eb0544143310a173e91099f820d56b43d458bd4874966ad

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、2.9.1 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、転送設定オプションが「テキスト」ではなく「バイナリ」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 アドレスを確認できます。
b) SFTP サーバは、標準ポート 22 で動作します。

---

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。
      `upgrade`
   b. 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。
   version
8. 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、『拡張性と復元力の展開ガイド』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. コマンド **backup rollback <name>**コマンドを使用して、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 クラスタリングの場合、XMPP を再クラスタ化する必要があります:
    a. 1 つのノードを XMPP マスターとして選択し、このノードで XMPP を初期化します
    b. XMPP マスターが有効になったら、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 サービスは接続済みである
    - 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が完了しました。

3.3 Cisco Meeting Server 2.9 の展開

Meeting Server 展開方法の説明を単純化するために、3 つのモデルの観点から展開を説明します。単一の統合 Meeting Server、単一の分割 Meeting Server、および拡張性と復元力のための展開です。3 つの異なるモデルはすべて、実稼働ネットワークの異なる部分で使用できます。

3.3.1 単一ホストサーバを使用した展開

Meeting Server を単一のホストサーバとして展開する場合 (「組み合わせ」展開) 、次の順序でガイドを読んで従うことをお勧めします：

1. Cisco Meeting Server の適切なインストールガイド（Cisco Meeting Server 2000、Cisco Meeting Server 1000 仮想化導入、または Acano X シリーズ サーバのインストールガイド）。
2. 単一のホスト上のすべてのソリューションコンポーネントを有効にする、Meeting Server 単一統合型サーバ導入ガイド。このガイドでは、この展開の証明書の取得とインストールの詳細について、『単一統合型展開証明書ガイドライン』を参照します。に言及します。

注：Cisco Meeting Server 2000 には、Call Bridge、Web Bridge、XMPP サーバ、およびデータベースコンポーネントのみがあります。内部ネットワーク上の単一サーバとして展開できますが、展開に外部 Cisco ミーティング アプリケーションのクライアントのファイアウォール トラバーサルサポートが必要な場合は、TURN サーバと Load Balancer Edge コンポーネントを別の Cisco Meeting Server 1000 または仕様に導入する必要があります。ベースの VM サーバ-以下の「単一分割」展開を参照してください。

3.3.2 コア サーバとエッジ サーバでホストされる単一分割サーバを使用した展開

分割サーバモデルで Meeting Server を展開する場合、XMPP サーバをコアサーバに展開し、ロードバランサを Edge サーバに展開することをお勧めします。

次の順序でドキュメントを読み、それに従います。

1. Cisco Meeting Server の適切なインストールガイド
2. Meeting Server 単一分割サーバ導入ガイド。このガイドでは、この展開用の証明書の取得とインストールの詳細について、『単一分散型展開証明書ガイドライン』を参照しています。

3.3.3　拡張性と復元力を重視した展開

複数のホストサーバを使用して拡張性と復元力のために Meeting Server をインストールする場合、XMPP サーバを Core サーバに展開し、ロードバランサを Edge サーバに展開することをお勧めします。

次の順序でドキュメントを読み、それに従います。

1. Cisco Meeting Server の適切なインストールガイド
2. スケーラブルで復元力のあるサーバ導入ガイド。このガイドでは、この導入の証明書の取得とインストールの詳細については『スケーラブルで復元力のあるサーバ導入向けの証明書のガイドライン』を参照してください。

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。さらに、[**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「**2.9**」のように検索するリリースを入力します。
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: WebRTC アプリケーションに影響を与えた解決済みの問題の詳細については、Cisco Meeting App WebRTC 重要な情報ガイドを参照してください。

注：Web アプリケーションに影響を与えた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、2.9.1 で修正された問題

Cisco 識別子	要約
CSCvt91847	分散した会議でローカルとリモートの Call Bridge 間でロック ステータスが一貫していないことにより、Cisco Meeting Server の会議からすべての参加者が予期せず削除されます。
CSCvt92941	まれに、XML 解析エラーによって WebRTC の参加者が削除されます。
CSCvt91634	同じスペースにいるときに、SIP エンドポイントがプレゼンテーションまたはコンテンツを共有した後で、すべての WebRTC コールと Web アプリケーション コールが停止します。
CSCvt86179	Call Bridge で予期しない再起動が発生する場合があります。
CSCvt76282	まれに、予期しない再起動が発生し、アクティブなコールが停止することがあります。
CSCvt59193	多数の XMPP メッセージを処理しているときに、Meeting Server が予期せず再起動することがあります。

以前のバージョンで発生し、2.9 で修正された問題

Cisco 識別子	要約
	リストはありません。

4.2　未解決の問題

注：WebRTC 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 App WebRTC Important information（Cisco ミーティング アプリケーション WebRTC 重要事項）』ガイド [英語] を参照してください。

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 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。

Cisco 識別子	要約
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。
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。
CSCvt74035	Web Bridge 3 サービスを開始できないというメッセージが、警告レベルのメッセージであるべき場合に情報レベルのメッセージとして表示されます。
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。
CSCvt74047	Web Bridge 3 は、正常に接続された場合でも、API を介して誤った接続エラー ステータスをレポートする場合があります。
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。
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、ロックされた会議で参加者を明示的にアクティブ化してから、会議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「この会議はロック解除されました（this meeting is now unlocked）」が流れません。
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。

Cisco 識別子	要約
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。
CSCvh23028	Web Bridge がリッスンするインターフェイスを変更するか、DHCP リースの期限が切れると、Web Bridge が再起動します。WebRTC アプリケーションユーザーは、再度ログインする必要があります。
CSCvh22816	WebRTC app を使用したログインは、正しいクレデンシャルが指定されている場合でも失敗することがあります。これは、Web ブラウザから Web Bridge に特定の cookie 文字列が指定されている場合に発生します。これを回避するには、シークレット タブを開いて WebRTC app を使用するか、Web Bridge で使用されているドメインのすべての cookie をクリアします。たとえば、https://join.example.com の WebRTC app の場合は、すべての example.com cookie をクリアします。
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。

さらに、次の制限があります:

注意: 現在の Meeting Server ソフトウェアでサポートされている同時 XMPP クライアントの最大数は 500 です。この最大値は、クラスタ化された Meeting Server に同時に登録されたすべての異なるクライアント (Cisco ミーティング アプリケーション、WebRTC Sign in、WebRTC Guest clients) の合計数です。同時 XMPP 登録の数が 500 セッションを超える場合、サインインで予期しない問題が発生する可能性があります。または、現在登録されているすべてのユーザが再サインインする必要がある状況が発生する可能性があります。同時に、これによりすべてのユーザが次にサインインするときにサービス妨害が発生する可能性があります。

Cisco の法的情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ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（http://www.cisco.com/web/JP/about/office/index.html）をご覧ください。

Cisco の商標または登録商標