Cisco Meeting Server

Cisco Meeting Server リリース 3.4.2

リリースノート

2022 年 7 月 28 日

目次

変更事項

バージョン	変更
2022 年 7 月 21 日	メンテナンス リリース 3.4.2 「解決済みの問題」を参照してください。
2022 年 2 月 28 日	メンテナンス リリース 3.4.1 「解決済みの問題」を参照してください。
2021 年 12 月 17 日	解決された問題のセクションを更新しました。
2021 年 12 月 15 日	バージョン 3.4 の最初のリリース。

1 はじめに

このドキュメントでは、Cisco Meeting Server ソフトウェアのバージョン 3.4 における新機能、改善、および変更について説明します。

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。
- または仕様ベースの VM サーバ。

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

注： Cisco 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とのやり取りを処理します。Meeting Server 3.4 では、Meeting Management 3.4 が必要です。

- **アップグレード：**最初に Meeting Management をアップグレードし、スマート ライセンスを完了してから、Meeting Server をアップグレードするワークフローを推奨しています。
- **スマート ライセンス：**3.4 リリース以降、スマート ライセンスは Meeting Server に必須です。従来のライセンスのサポートは廃止されました。既存の従来のライセンスは、有効期限が切れるまで引き続きサポートされます。ライセンスの有効期限が切れたら、スマート ライセンスに移行する必要があります。

スマート ライセンスと Meeting Management のアップグレードの詳細については、Meeting Management リリース ノートを参照してください。

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 コマンドリファレンスガイド』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 Cisco Meeting Server Web アプリの重要事項

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。これらの詳細は、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、以下のことを説明しています。

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

1.2 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 3.4 3.5 のリリースでは、Cisco は、表 1 に記載されているソフトウェアのソフトウェアメンテナンス終了のタイムラインを発表しました。

表 1：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期間
Cisco Meeting Server バージョン 3.2.x	Cisco Engineering が Cisco Meeting Server バージョン 3.2.x の最終的なソフトウェア メンテナンス リリースやバグ修正をリリースする最終日は、2022 年 4 月 17 日です。
Cisco Meeting Server バージョン 3.3.x	Cisco Engineering が Cisco Meeting Server バージョン 3.3.x の最終的なソフトウェア メンテナンス リリースやバグ修正をリリースする最終日は、2022 年 8 月 22 日です。

Cisco Meeting Server に関する 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、こちらをクリックしてください。

2 バージョン 3.4 の新機能と変更点

Meeting Server ソフトウェアのバージョン 3.4 では、以下の新機能と変更が導入されています

- 議事録
- Call Bridge と Web 管理者間の証明書名を検証するためのセキュリティ強化
- ブラストダイヤルの着信拒否
- MMP コマンドによるログ バンドルの生成
- スケジューラの会議の招待状に共通の電子メール アドレスを構成する
- スケジューラ会議の招待状に表示名を含める
- 参加者をロビーに移動する
- クローズド キャプション
- 背景をぼかす（ベータ版機能）
- 遠端カメラ制御

2.1 議事録

バージョン 3.4 では、Web アプリの参加者が会議中にメモを表示および/またはメモを取り、他のすべての Web アプリの参加者に公開できるようにする**議事録**機能が導入されています。この機能は、コール レベルで有効になります。この機能の目的は次のとおりです。

- Web アプリの会議では、適切な権限を持つ参加者がメモを取り、公開でき、他の参加者は公開されたメモを表示できます。
- メモは会議中のみ閲覧できます。会議の開始後に参加する参加者は、最近公開されたメモがある場合はそれを表示できます。
- 会議には、公開されたメモを 1 つだけ含めることができます。その後のノートへの変更は、公開されたノートを編集して再公開することによって行う必要があります。 これにより、以前のメモが上書きされ、更新されたメモがすべての参加者に再度送信されます。
- 公開されていないメモは下書きとして保存され、会議中にいつでも編集および公開できます。
- メモを取っている参加者は、会議中にメモをダウンロードして自分のシステムに保存できます。

注：

- この機能は Web アプリでのみサポートされています。SIP エンド ポイントまたは Lync/Skype を介して参加する参加者は、メモを表示したり、メモを取ったりすることはできません。
- 特定の通話で複数の参加者にメモを取る許可を与えることができますが、複数の同時編集を避けるために、1 人の参加者にのみメモを取る許可を与えることをお勧めします。

2.1.1 API の追加

コールレベルでのメモの有効化/無効化を行う新しい API パラメータ notesAllowed が 3.4 で導入されました。設定可能な値は true または false です。このパラメーターは、次の API メソッドでサポートされています。

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

パラメータ	タイプ/値	説明/注意事項
notesAllowed	true| false	- true - コールでメモが許可されていることを示します。 - false - コールでメモが許可されていないことを示します。 このパラメータには、通話と通話プロファイルの階層に関する通常のルールが適用されます。階層のすべてのレベルで設定を解除すると、デフォルトで false になります。

さらに、管理者は、特定の通話でメモを取ることが可能な参加者を制御できます。これは、新しいパラメータ **noteContributionAllowed** によって有効になります。 参加者は、通話でメモ機能が有効になっていて、メモへの投稿が許可されている場合、メモを公開できます。新しいパラメータ **noteContributionAllowed** は、次の API メソッドに導入されています。

- **/callLegProfiles** に対する POST 操作
- **/callLegProfiles/<call leg profile id>** に対する GET 操作
- **/callLegProfiles/<call leg profile id>** に対する PUT 操作

- **/calls/<call ID>/callLegs** に対する POST 操作
- **/callLegs/<callLeg id>** に対する GET 操作
- **/callLegs/<callLeg id>** に対する PUT 操作
- **/calls/<call id>/participants** に対する POST 操作

注： **noteContributionAllowed** の設定が **true** の場合でも、コールレベルで **notesAllowed** の設定が **false**の場合でも（またはコールが **callProfile** 階層から継承した事による場合でも）メモは許可されません。

パラメータ	タイプ/値	説明/注意事項
noteContributionAllowed	true| false	参加者がメモを公開できるかどうかを決定します。階層のすべてのレベルで設定を解除すると、デフォルトで false になります。

API の詳細についは、 『*Meeting Server 3.4 API リファレンス ガイド*』を参照してください。

2.2 Call Bridge と Web 管理者間の証明書名を検証するためのセキュリティ強化

クラスタ展開でピアと接続するときの Call Bridge は、Web 管理証明書を使用して検証されます。信頼できるチェーンを示さない Web 管理証明書は拒否されますが、証明書名は検証されません。

これらの既存の Call Bridge 検証に対するセキュリティの改善として、TLS 証明書名の検証がピア間で実装されます。この検証の一環として、**Call Bridge trust cluster** が有効になっている場合、クラスタリングで設定されたピアは、対応する Web 管理証明書の完全な FQDN と一致する必要があります。設定が一致しないと、Call Bridge が失敗します。

2.3 ブラストダイヤルの着信拒否

ブラスト ダイヤル機能で、参加者がスペースにダイヤルインすると、スペースのプリセットリストから他のすべての連絡先が同時にダイヤルアウトされます。以前のリリースでは、参加者が通話を拒否しても、Meeting Management は参加者への再ダイヤルを停止しませんでした。バージョン 3.4 以降、参加者は通話を拒否でき、会議の管理は参加者への再ダイヤルを停止します。新しいオーディオ プロンプトは、DTMF キー オプションを使用して参加者に通話を受け入れるか拒否するかを案内します。 参加者は、DMTF キー 1 を押して会議に参加するか、* を押して通話を拒否できます。その他の DMTF 入力は無視されます。

Meeting Management は、次の場合に再ダイヤルを停止します。

- 参加者は、[承認（Accept）] ボタンをクリックして着信通話を受け入れ、DTMF キー * を押します。
- 参加者は、SIP デバイスの [却下（Decline）] または [拒否（Reject）] ボタンをクリックして、通話を拒否します。
- 参加者は着信通話を受け入れ、[通話終了（End call）] をクリックして通話を終了します。

注：ユーザが PSTN デバイスの [却下（Decline）] または [通話終了（End call）] ボタンを使用して通話を拒否した場合、会議の管理は参加者へのリダイヤルを停止しない場合があります。* キーを使用して着信を拒否することをお勧めします。

2.3.1 CDR の変更

`callLegStart` および **`callLegUpdate`** CDR でサポートされる **`confirmStatus`** フィールドが、**`callLegEnd`** CDR に追加されました。

名前	タイプ	説明
confirmationStatus	required/notRequired/confirmed/rejected	- required：confirmation=true が設定されていて、ユーザが通話に参加するための DTMF 確認をまだ提供していないことを意味します。 - notRequired：は、confirmation=true が構成されていないことを意味します。 - confirmed：参加者が通話への参加を望んでいることを確認するために DTMF シーケンスが入力されたことを意味します。 - rejected：コールを拒否するために DTMF シーケンスが入力されたことを意味します。会議の管理は、参加者への再ダイヤルを停止します。

CDR の詳細については、『*Cisco Meeting Server 3.4 コール詳細レコードガイド*』を参照してください。

2.4 MMP コマンドを使用したログ バンドルの生成

Meeting Server ログ バンドルは、管理者が MMP 管理者ユーザ資格情報を使用して SFTP クライアントを MMP IP アドレスに接続してダウンロード プロセスを開始すると生成されます。バージョン 3.4 では、既存のプロセスに加えて、ダウンロードを開始する前にログ バンドルを生成するオプションが導入されています。

それぞれの Meeting Server で特定のファイル名でログ バンドルを生成するための新しい MMP コマンドが追加されました。 このコマンドが実行されるたびに、このコマンドを使用して以前に生成されたログ バンドルが最新のログ バンドルに置き換えられます。生成されたログ バンドルは、必要に応じてダウンロードできます。

Meeting Management を使用して、Call Bridge および Edge Server のログ バンドルを生成およびダウンロードすることもできます。詳細については、 *Meeting Management リリース ノート* を参照してください。

2.4.1 MMP の追加

Meeting Server のログ バンドルを生成するために、次の MMP コマンドが追加されています。

コマンド/例	説明/注意事項
generate_logbundle	Meeting Server は、**`SFTP get generatedlogbundle.tar.gz`** コマンドを使用してダウンロードできる特定のファイル名 **`generatedlogbundle.tar.gz`**を持つログ バンドル ファイルを生成します。

MMP コマンドの使用については、『*Meeting Server 3.4 MMP コマンド ライン リファレンス ガイド*』を参照してください。

2.5 Cisco Meeting Server スケジューラ

スケジューラ コンポーネントは、バージョン 3.3 のベータ機能として導入されました。これは、Web アプリ ユーザが会議をスケジュールし、スケジュールされた会議を変更し、電子メールで参加者に通知できるようにする新しいコンポーネントとして追加されました。バージョン 3.4 から、Scheduler は Meeting Server 1000 および仮想化展開上の Meeting Server で完全にサポートされます。 これは基本のマルチパーティ ライセンス（PMP Plus および SMP Plus）に含まれており、個別の機能ライセンスは必要ありません。

バージョン 3.4 では、スケジュール会議の招待状を共通の電子メール アドレスから送信することもできます。送信者を識別するために、電子メール アドレスの横に表示名として主催者の名前を含めることもできます。これらの機能の詳細については、「スケジューラの電子メール サーバーの構成」および「スケジューラの会議出席依頼に 表示名を含める」を参照してください。

注：スケジューラ コンポーネントは、Meeting Server 2000 ではサポートされていません。Meeting Server 2000 で実行される Call Bridge は展開でサポートされますが、スケジューラ コンポーネントは Meeting Server 1000 または VM 上の Meeting Server で実行する必要があります。

2.5.1 概要

スケジューラは、単一および定期的なインスタンスでの会議をサポートします。会議テンプレートに異なるロール（ホストとゲストなど）がある場合、参加者をこれらのロールに割り当てることができます。Web アプリのユーザは、永続的なスペースまたは会議のために作成された一時的なスペースで会議をスケジュールできます。会議のスケジュール時に作成された一時スペースは、スケジュールされた会議の終了から 24 時間後に、会議の繰り返しを考慮して、スケジューラ コンポーネントによって削除されます。会議参加者またはスペース メンバーは、スケジュールされた会議の時間外であっても、スペースの存続期間中いつでもこのスペースにダイヤルインできます。Meeting Server は、スペースごとに複数の会議シリーズをサポートします。

会議がスケジュールまたはキャンセルされたとき、または参加者のリストが変更されたときに、電子メール通知が参加者に送信されます。 スケジュールされた会議が更新されると、更新された招待状は、スケジューラに含まれる招待者にのみ送信されます。電子メールの招待状は、共通の電子メール アドレスを使用して送信できます。共通の電子メール アドレスが構成されていない場合、SMTP サーバーによる認証では、MMP コマンド **`scheduler email username`** を使用して電子メール アドレスを構成する必要があります。MMP で構成されたこのアカウントには、Web アプリ ユーザの代わりに電子メールを送信できる適切な権限が必要です。

会議への招待メールは、次の内容で構成されます。

- Call Bridge への API 呼び出しを使用してスケジューラによって取得される会議参加情報。この情報は、電子メールの本文に記載されます。
- 電子メールに添付された業界標準の iCalendar（.ics）ファイルでの会議の詳細。ICS ファイルは、参加者が自分のカレンダーに保存できます。

招待テキストのカスタマイズの詳細については、『*Meeting Server 3.4 カスタマイズ ガイドライン*』を参照してください。

Web アプリのユーザは、スケジュールされた会議に 2 種類の参加者を招待できます。

- Web アプリの参加者：Web アプリのユーザが Web アプリにサインインすると、スケジュールされた会議が表示されます。Call Bridge LDAP 同期中にユーザの電子メール アドレスが正常にインポートされた場合、電子メールの招待状が送信されます。
- 参加者に電子メールを送信：たとえば、Web アカウントを持っていない人を招待するために、電子メール アドレスを指定できます。この場合、招待メールが送信されます。

スケジューラは、新しい時間の提案をサポートせず、招待の受諾または拒否を追跡しません。Web アプリからスケジューラを使用する方法の詳細については、『*Meeting Server 3.4 Web アプリ ユーザ ガイド*』を参照してください。

2.5.2 スケジューラの電子メール サーバーの構成

スケジューラ コンポーネントは、VM 展開上の Meeting Server 1000 および Meeting Server でサポートされます。仕様ベースの VM プラットフォーム上の Meeting Server では、スケジューラ コンポーネントを実行するために追加の 4 GB の RAM が必要です。 Meeting Server1000 には追加の RAM 要件はありません。

このリリースでは、スケジューラに IPv6 はサポートされていません。
スケジューラは、次のタイプの電子メール設定をサポートしています。

1. SMTP
2. 認証済みログインによる SMTP（認証ログイン）
3. SMTP と STARTTLS
4. 認証ログインと STARTTLS を使用した SMTP
5. SMTPS（SMTP トランザクション全体のエンドツーエンドの TLS 暗号化）
6. 認証ログインによる SMTPS

電子メール サーバーの構成と電子メール構成のタイプの詳細については、『*Meeting Server 3.4 インストール ガイド*』を参照してください。

2.5.3 スケジューラの導入

スケジューラは、Meeting Server MMP を使用して新しいコンポーネントとして導入されます。スケジューラが有効になっている場合は、ループバック インターフェイスを介して Call Bridge に API 要求を行います。 したがって、スケジューラは、Call Bridge もホストしている Meeting Server に展開する必要があります。リモート Call Bridge を使用するようにスケジューラを設定することはできません。

すべての Call Bridge と一緒にスケジューラを展開する必要はありません。1 つのスケジューラで 150,000 の会議をサポートします。レジリエンスを提供するために 2 つまたは 3 つのスケジューラを追加できますが、キャパシティは 150,000 のスケジュールされた会議のままです。 スケジュールされた会議のデータは Meeting Server データベースに保存され、クラスタ化されたデータベースとシングル ボックス データベースの両方の展開がサポートされています。スケジューラの導入の詳細については、『Meeting Server 3.4 導入ガイド』を参照してください。

2.5.3.1 API および MMP の追加

スケジューラ コンポーネントをサポートするために、新しい API ノードと MMP コマンドが導入されました。詳細については、『Meeting Server 3.4 API リファレンス ガイド』 および『 Meeting Server 3.4 MMP Command Line リファレンス ガイド』を参照してください。

2.5.4 スケジューラ 会議の招待状に共通の電子メール アドレスを構成する

バージョン 3.3 では、スケジューラを使用して会議をスケジュールすると、会議の招待状が主催者の電子メール アドレスから参加者に送信されました。これには、スケジューラがユーザに代わって電子メールを送信できる必要があります。この権限を有効にしたくない組織の場合、バージョン 3.4 から、共通の電子メール アドレスからすべての参加者に会議の招待状を送信できます。

Meeting Server で共通の電子メール アドレスを設定するための新しい MMP コマンドが追加されました。このコマンドは、共通の電子メール アドレスの構成に加えて、共通の電子メール アドレスの表示名を設定するオプションも提供します。関心のある名前は、電子メール ヘッダーの共通の電子メール アドレスの横に表示されるように構成できます。共通の電子メール アドレスと表示名の最大長は、それぞれ 320 文字と 78 文字です。

さらに、Meeting Server で設定されている共通の電子メール アドレスを削除するための新しい MMP コマンドが追加されました。

会議の招待状が共通の電子メール アドレスから送信された場合、受信者は主催者/ホストの詳細を知りません。そのため、主催者/ホスト名が招待メールのテキスト テンプレートに含まれています。電子メール招待テンプレートに新しい変数が追加され、電子メール招待に主催者の名前または電子メール アドレスが含まれます。

スケジューラが API リクエストを送信して電子メール テキストと会議への参加手順を取得すると、主催者の詳細がリクエストに含まれます。 これは、電子メール招待 API に新しいリクエスト パラメータを含めることによって実現されます。

2.5.4.1 API の追加

既存の API が変更され、新しいリクエスト パラメータ **`organizer`** が含まれるようになりました。これは、API に渡すことができるオプションのパラメーターであり、電子メールの招待テキストに主催者の詳細を含めます。

- **`/api/v1/coSpaces/<coSpace id>/accessMethods/<access method id>/emailInvitation`** に対する GET 操作
- **`/api/v1/coSpaces/<coSpace id>/emailInvitation`** に対する GET 操作

パラメータ	タイプ/値	説明/注意事項
organizer（オプション）	文字列	提供されている場合は、電子メールの招待テキストに主催者の詳細を含めます。オーガナイザーの詳細は、API に含まれている主催者/ホストの名前または電子メール アドレスである可能性があります。

API の詳細については、『*Meeting Server 3.4 API リファレンス ガイド*』を参照してください。

2.5.4.2 MMP の追加

Meeting Server で共通の電子メール アドレスを設定および削除するために、次のコマンドが追加されました。

コマンド/例	説明/注意事項
scheduler email common-address <address@mail.domain> "<Display name>"	Meeting Server での共通の電子メール アドレスと表示名を設定します。スケジューラは、共通の電子メール アドレスから参加者に会議の招待状を送信します。 共通の電子メール アドレスが空白の場合、スケジューラは主催者の電子メール アドレスから電子メールの招待状を送信します。
scheduler email common-address none	設定されている共通メールアドレスと表示名を削除します。

MMP コマンドの使用の詳細については、『*Meeting Server 3.4 MMP コマンド ライン リファレンス ガイド*』を参照してください。

2.5.4.3 電子メール招待テンプレート テキスト ファイルへの追加

電子メール招待テンプレートに新しい変数 **organizername** が追加されました。招待メールに主催者の名前を含めるには、invitation_template_xx_XX.txt ファイルに次の変数を追加する必要があります。

```
#if organizername
Organisator: %organizername%
#endif
```

詳細については、『*Meeting Server 3.4 カスタマイズ ガイドライン ドキュメント*』を参照してください。

2.5.5 スケジューラ会議の招待状に表示名を含める

バージョン 3.3 では、スケジュール担当者から会議出席依頼が送信された場合、電子メール ヘッダーの送信者の詳細には、主催者の電子メール アドレスのみが含まれていました。このバージョンから、送信者を識別するために、メールアドレスの横に主催者の名前を表示名として含めることができます。

Web アプリを使用して会議がスケジュールされると、Web アプリは、会議をスケジュールするユーザの名前を主催者の表示名としてスケジューラに送信します。スケジューラー API に新しいオプションのパラメータを含めることで、選択した名前を表示名として設定できます。表示する名前は 78 文字までです。

2.5.5.1 API の追加

電子メール ヘッダーに主催者/送信者の表示名を含めるために、新しい **organizerDisplayName** API パラメータが導入されました。このパラメーターは、次のメソッドでサポートされています。

- **/scheduler/meetings** に対する POST 操作。

パラメータ	タイプ/値	説明/注意事項
organizerDisplayName（オプション）	文字列	電子メールに表示される会議の主催者の名前。

API の詳細については、『*Meeting Server 3.4 API リファレンス ガイド*』を参照してください。

2.6 参加者をロビーに移動する

Meeting Server の以前のバージョンでは、ロックされた会議でロビーで待機している参加者を許可する API が提供されていました。バージョン 3.4 以降、Meeting Server は、ロックされた会議から参加者をロビーに戻すための API を提供します。

既存の API パラメータ **deactivated**を使用して、参加者をロビーに戻すことができます。さらに、参加者をロビーに移動できるかどうかを示す新しいパラメータ **canMoveToLobby**が追加されました。

この機能は、Meeting Management 3.4 でもサポートされています。『CMM リリースノート』を参照してください。

2.6.1 API の追加

既存の API パラメータ **deactivated** は、**true** と **false** の両方の値を取るように変更されます。こちらは、次のメソッドでサポートされています。

- **/participants/<participant id>** に対する PUT 操作
- **/calls/<call id>/participants** に対する POST 操作
- **/calls/<call id>/participants/*** に対する PUT 操作

パラメータ	タイプ/値	説明
非アクティブ化	true/false	- true - 参加者はロビーで待機するか、ロビーに移動できます。 - false - 参加者はロビーから会議に参加できます。

/participants/<participant id>に対する GET 操作 に新しい API パラメータ **canMoveToLobby** が追加されました。

応答要素	タイプ/値	説明/注意事項
canMoveToLobby	true/false	- true - 参加者をロビーに移動できます。 - false - 参加者をロビーに移動できません。

コール プロファイルで設定された **lockMode**パラメータの値によって、管理者が参加者をロビーに移動できるかどうかも決まります。

- **all**：会議がロックされているとき、会議がロックされた後に参加した場合、参加者はロビーで待機します。または、会議中はいつでも参加者をロビーに移動できます。 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、アクティベーションを必要としない新しい参加者は会議に参加できますが、会議中はロビーに移動できません。ただし、アクティベーションが必要な新しい参加者はロビーで待機し、会議中いつでもロビーに移動できます。coSpace のメンバーは、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。

API の詳細については、 『*Meeting Server 3.4 API リファレンス ガイド*』を参照してください。

2.7 クローズド キャプション

バージョン 3.4 以降、Meeting Server では、Web アプリの参加者が会議でクローズド キャプションを表示および公開できるようになりました。クローズド キャプションを使用すると、耳の不自由な参加者が会議に参加しやすくなります。会議中にリアルタイムで公開されるクローズド キャプションは、Meeting Server 管理者によってキャプション担当者として設定された参加者によって送信されます。

注：クローズド キャプションを公開する許可を会議の 1 人の参加者のみに与えることをお勧めします。

Web アプリ会議では、キャプション担当者がキャプションを入力して Enter キーを押すと、参加者の画面にキャプションが表示されます。参加者は、会議内のメニュー オプションとして使用できるクローズド キャプション ウィンドウで、Web アプリのクローズド キャプション履歴を表示することもできます。

クローズド キャプションはサーバーに保存されないため、会議中にのみ使用でき、会議が終了すると失われます。キャプション担当者は、Web アプリ画面の UI オプションを使用して、会議中にキャプションをローカル ドライブにダウンロードして保存できます。

注：この機能は Web アプリでのみサポートされています。SIP エンド ポイントまたは Lync/Skype を介して参加する参加者は、クローズド キャプションを表示できません。

2.7.1 API の追加

コール レベルでキャプションを有効または無効にするために、新しいパラメータ **captionsAllowed**が導入されました。こちらは、次のメソッドでサポートされています。

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

パラメータ	タイプ/値	説明
captionsAllowed	true/false	- true – コールでキャプションが許可されることを示します。 - false – コールでキャプションが許可されないことを示します。 このパラメータには、通話と通話プロファイルの階層に関する通常のルールが適用されます。階層のすべてのレベルで設定を解除すると、デフォルトで false になります。

さらに、参加者が会議でキャプションを送信できるようにするために、新しいパラメーター **captionContributionAllowed** が追加されました。こちらは、次のメソッドでサポートされています。

- **/callLegProfiles** に対する POST 操作
- **/callLegProfiles/<call leg profile id>** に対する GET 操作
- **/callLegProfiles/<call leg profile id>** に対する PUT 操作
- **/calls/<call id>/callLegs** に対する POST 操作
- **/callLegs/<callLeg id>** に対する GET 操作
- **/callLegs/<callLeg id>** に対する PUT 操作
- **/calls/<call id>/participants** に対する POST 操作

パラメータ	タイプ/値	説明
captionContributionAllowed	true/false	参加者が会議でキャプションを送信できるかどうかを決定します。 このパラメータには、callLeg および callLeg プロファイルの階層に関する通常のルールが適用されます。階層のすべてのレベルで設定を解除すると、デフォルトで false になります。 注：**captionsAllowed** がコール レベルで false に設定されている場合、**captionContributionAllowed** が true に設定されていても、参加者はクローズド キャプションを送信できません。

注：クローズド キャプションは常に Web アプリ画面の下部に表示されます。会議のためにクローズド キャプションとメッセージ テキストの両方を送信する場合は、**messagePosition** を top または middle として構成することをお勧めします。

新しい API **calls/<call id>/captions/** に対する POST 操作は、サードパーティの API ツールが会議でキャプションを送信できるようにするために導入されました。これらのキャプションを表示できるのは、Web アプリの参加者のみです。

パラメータ	タイプ/値	説明
captionsText	文字列	会議の画面にキャプションとして表示されるテキスト。

API の詳細については、『Meeting Server 3.4 API *リファレンス ガイド*』を参照してください。

2.8 背景をぼかす（ベータ サポート）

バージョン 3.4 では、Web アプリの参加者が会議の背景をぼかすことができます。背景をぼかすと、周囲がぼやけて見えるため、参加者の背後にある詳細が隠され、参加者が強調されます。参加者は、プレビュー ページではなく、会議に参加した後にのみ背景をぼかすことができます。Web アプリの会議カメラ設定の新しいオプション [**ぼかし**（Blur）] が含まれています。これはベータ版の機能であるため、このオプションはデフォルトで無効になっています。

注：Ciscoでは、ベータ機能が将来完全にサポートされる機能になることを保証しません。ベータ機能はフィードバックに基づいて変更される可能性があり、機能は将来変更または削除される可能性があります。

背景のぼかしは、Google Chrome および Mozilla Firefox ブラウザを搭載した Mac と Windows でのみサポートされています。この機能は、他のブラウザおよび Android または iOS デバイスではサポートされていません。

注：

- 背景のぼかしが有効になっている場合は、HD を無効にすることをお勧めします。背景をぼかした状態で HD が有効になっている場合、オーディオとビデオの同期の問題が発生する可能性があります。
- 背景のぼかしは、グラフィック プロセッシング ユニット（GPU）を備えたシステムで最適に機能します。
- 背景ぼかし機能を使用するには、次の最小システム構成が必要です。
  - Windows システムの場合：メモリ - 16 GB および CPU - 1.60 GHz
  - Mac システムの場合：メモリ - 16 GB および CPU - 2.30 GHz

2.8.1 API の追加

新しい API パラメータ **backgroundBlurAllowed**が導入され、コール レベルで背景のぼかしを有効または無効にします。こちらは、次のメソッドでサポートされています。

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

パラメータ	タイプ/値	説明
backgroundBlurAllowed	true | false	- true – 呼び出しで背景のぼかしが許可されていることを示します。 - false – 呼び出しで背景のぼかしが許可されていないことを示します。 このパラメータには、通話と通話プロファイルの階層に関する通常のルールが適用されます。階層のすべてのレベルで設定を解除すると、デフォルトで false になります。

API の詳細については、『*Meeting Server 3.4 API リファレンス ガイド*』を参照してください。

2.9 遠端カメラ制御

会議に正しい参加者をフレーミングするために、カメラを手動で制御する必要がある場合があります。バージョン 3.4 では、遠端カメラ制御（FECC）をサポートする他の参加者のカメラを制御する機能が導入されています。適切な権限を持つ参加者のみが、Web アプリで新しいオプション [**カメラ コントロールを表示**（View Camera Control）] を使用して、他の参加者のカメラを制御できます。 このオプションは、カメラが FECC をサポートしている参加者向けに含まれています。参加者は、一度に 1 人の参加者のカメラのみを制御できます。

既存の API パラメータ **controlRemoteCameraAllowed** および **cameraControlAvailable** Web アプリでこの機能をサポートするために使用されます。

API の詳細については、『*Meeting Server 3.4 API リファレンス ガイド*』を参照してください。

2.10 API の追加および変更の概要

Meeting Server 3.4 の API 機能には、次の新しい API パラメータと変更された API パラメータが含まれています。

会議メモ機能をサポートする新しい API パラメータ。

- **notesAllowed** は、以下で導入されます
  - **/callProfiles** に対する POST 操作
  - **/callProfiles/<call profile id>** に対する GET 操作
  - **/callProfiles/<call profile id>** に対する PUT 操作
  - **/calls** に対する POST 操作
  - **/calls/<call id>** に対する GET 操作
  - **/calls/<call id>** に対する PUT 操作

- **noteContributionAllowed は、以下で導入されます**
    - **/callLegProfiles** に対する POST 操作
    - **/callLegProfiles/<call leg profile id>** に対する GET 操作
    - **/callLegProfiles/<call leg profile id>** に対する PUT 操作
    - **/calls/<call id>/callLegs** に対する POST 操作
    - **/callLegs/<call leg id>** に対する GET 操作
    - **/callLegs/<call leg id>** に対する PUT 操作
    - **/calls/<call id>/participants** に対する POST 操作

共通の電子メール アドレスが使用されている場合に、スケジューラの会議の招待テキストに主催者の詳細を含めるための新しい API パラメータ

- **organizer**は以下で導入されます
    - **/coSpaces/<coSpace id>/accessMethods/<access method id>/emailInvitation** に対する GET 操作
    - **/coSpaces/<coSpace id>/emailInvitation** に対する GET 操作

スケジューラの会議の招待状で表示名をサポートする新しい API パラメータ

- **organizerDisplayName は、以下で導入されます**
    - **/scheduler/meetings** に対する POST 操作

参加者をロビーに移動できるかどうかを示す新しい API パラメータ。

- **canMoveToLobby は、以下で導入されます**
    - **/participants/<participant id>**に対する GET 操作

クローズド キャプション機能をサポートする新しい API パラメータ。

- **captionsAllowed**は、以下で導入されます
    - **/callProfiles** に対する POST 操作
    - **/callProfiles/<call profile id>** に対する GET 操作
    - **/callProfiles/<call profile id>** に対する PUT 操作
    - **/calls** に対する POST 操作
    - **/calls/<call id>** に対する GET 操作
    - **/calls/<call id>** に対する PUT 操作

- **captionContributionAllowed は、以下で導入されます**
    - **/callLegProfiles** に対する POST 操作
    - **/callLegProfiles/<call leg profile id>** に対する GET 操作
    - **/callLegProfiles/<call leg profile id>** に対する PUT 操作
    - **/calls/<call id>/callLegs** に対する POST 操作
    - **/callLegs/<call leg id>** に対する GET 操作
    - **/callLegs/<call leg id>** に対する PUT 操作
    - **/calls/<call id>/participants** に対する POST 操作

背景ぼかし機能をサポートする新しい API **パラメータ。**

- **backgroundBlurAllowed は、以下で導入されます**
    - **/callProfiles** に対する POST 操作
    - **/callProfiles/<call profile id>** に対する GET 操作
    - **/callProfiles/<call profile id>** に対する PUT 操作
    - **/calls** に対する POST 操作
    - **/calls/<call id>** に対する GET 操作
    - **/calls/<call id** に対する PUT 操作

API **オブジェクトとパラメーターの変更**

- **/cospace** オブジェクトの既存の API パラメータ **passcode**の最大制限は、63 桁を受け入れるように変更されました。
- **参加者をロビーに移動する**

  既存の API パラメータ **deactivated**は **true**と **false**の両方の値を取るように変更されます。こちらは、次のメソッドでサポートされています。
    - **/participants/<participant id>** に対する PUT 操作
    - **/calls/<call id>/participants** に対する POST 操作
    - **/calls/<call id>/participants/*** に対する PUT 操作

パラメータ	タイプ/値	説明
非アクティブ化	true/false	- true - 参加者はロビーで待機するか、ロビーに移動できます。 - false - 参加者はロビーから会議に参加できます。

- **遠端カメラ制御**

  既存の API パラメータ **`controlRemoteCameraAllowed`** および **`cameraControlAvailable`**は、Web アプリでこの機能をサポートするために使用されます。

新しい API **オブジェクト**

新しい API **`calls/<call id>/captions/`**に対する POST 操作は、サードパーティの API ツールが会議でキャプションを送信できるようにするために導入されました。

2.11 MMP の追加および変更の概要

バージョン 3.4 では、このセクションで説明する MMP の追加をサポートしています。

- **スケジューラ会議招待用の共通の電子メール アドレス**

  新しい MMP コマンド **`scheduler email common-address <address@mail.domain> "<Display name>`**および **`scheduler email common-address none`**が追加され、Meeting Server から共通の電子メール アドレスを構成および削除します。

- MMP **コマンドによるログ バンドルの生成**

  新しい MMP コマンド **`generate_logbundle`**が追加され、それぞれの Meeting Server で特定のファイル名 **`generatedlogbundle.tar.gz`** でログ バンドルが生成されます。

2.12 CDR 変更の概要

バージョン 3.4 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。

- **`callLegStart`** および **`callLegUpdate`** でサポートされる **`confirmationStatus`** フィールドCDR が **`callLegEnd`** CDR に追加されるようになりました。

3 Cisco Meeting Server ソフトウェアバージョン 3.4.2 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 3.3 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、3.3.x リリースノートの手順に従って 3.3 にアップグレードしてから、Cisco Meeting Server 3.4.x リリースノートに記載されている手順を実行してください。これは、Meeting Server に接続された Cisco Expressway がある場合に特に重要です。

注：Cisco は、3.3 以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 3.4.2 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。クラスター化されたデータベースを使用した導入については、クラスター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 コマンドリファレンス ガイド』を参照してください。アップグレード/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。

注：クラスター化されたデータベースをデプロイしている場合は、Meeting Server をアップグレードする前に、database cluster remove コマンドを使用してすべてのノードのクラスター化を解除します。ユーザは、ノードのクラスタ化を解除し、Meeting Server をアップグレードし、MMP コマンドを使用してノードをクラスタ化する必要があります。データベースのクラスタリングの手順については、『スケーラブルで復元力のあるサーバガイド』を参照してください。

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 の必須要件が導入されました。3.0 （以降）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。

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_4_2_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）：
   0aab334ee500c66ba42a0fc1b26714679625c7e686bcf2a277a6a835dade67a9

   Cisco_Meeting_Server_3_4_2_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）：
   012022eaf1d5f8a3efa510ca6398246b3ac5fe7b23fbf58efa5688ba42f86dba

   Cisco_Meeting_Server_3_4_2.ova

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

   vSphere6 での、Cisco_Meeting_Server_3_4_2_vSphere-6_0 のハッシュ（SHA-512）：
   712beef120a4f8690ef070ca0148c2af34717c06e06cbbf72a987540b3068a7bdc07f9dd20a392cf31d08653f5790b4662d68c77522f68f74687227e63da8532

   vSphere6.5 以降での、Cisco_Meeting_Server_3_4_2_vSphere-6_5 のハッシュ（SHA-512）：
   dd92b588a66b27fb390ebf489eb06cb8af00c0fddcb4d0ea087b3e1a5616690342518d324d2097cf8b91574edfcab579256aa4b3610ffee49863206c28cfb0f8

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、3.4.2 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 のインターフェースの IP アドレスを参照してください。

b) SFTP サーバーは、標準ポート 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。

      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、残りの展開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

アップグレード処理中またはアップグレード処理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 ソフトウェアに戻すことができます。通常のアップグレード手順を使用して、MMP **アップグレード** 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、工場出荷時設定からの再起動を待ちます。
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、cms.lic 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. a. 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。
   b. 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。
   c. 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。
   d. 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 会議アプリケーション（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。

3.3 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、Web Bridge 3 および MeetingApps 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 3、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、Cisco Meeting Server に関する解決済みの問題および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て [検索（Search）] をクリックするか、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「**3.2**」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 3.4.2 で修正済みの問題

Cisco **識別子**	**要約**
CSCwa68125	参加者がカスタム レイアウトを適用すると、固定ペインのビデオが画面全体に表示されません。
CSCwb39239	シスコは、openssl の CVE - CVE-2022-0778 によって特定された脆弱性の影響を評価しました。 この製品は脆弱性の影響を受けるため、openSSL バージョンは OpenSSL 1.1.1n にアップグレードされました。

Cisco 識別子	要約
CSCwb31492	シスコは、Apache-2.4.52 の CVE-2022-22719、CVE-2022-22720、CVE-2022-22721、CVE-2022-23943 で特定された脆弱性の影響を評価しました。脆弱性の詳細については、Apache HTTP サーバーの脆弱性を参照してください。 製品は脆弱性の影響を受けるため、Apache HTTP サーバーのバージョンは Apache-2.4.53 にアップグレードされます。
CSCwb43662	Spring Boot の Spring Framework バージョンが 5.2.20 にアップグレードされました。
CSCwc17966	コスペース URI の長さが 14 文字以上で、特殊文字で終わる場合、Meeting Server はクラッシュします。

以前のバージョンで発生し 3.4.1 で修正済みの問題

Cisco 識別子	要約
CSCwa59076	Meeting Server 3.4 にアップグレードした後、ユーザは、コントロール パネルから、または内蔵カメラなしでデスクトップを使用しているときに、マイクが有効でカメラが無効になっている Web アプリの会議に参加できません。
CSCvz75483	まれに、Meeting Server 2000 のバージョン 3.3.0.6 がクラッシュし、syslog ファイルに「sf_assert failed server/management/cmgr/server_management_cmgr.cpp:8849」というエラー メッセージが表示されます。
CSCwa58708	2021 年 9 月 16 日、Apache Software Foundation は、CVE ID で識別される Apache HTTP Server（httpd）2.4.48 以前のリリースに影響を与える 5 つの脆弱性を公開しました（CVE-2021-40438、CVE-2021-33193、CVE-2021-34798、CVE -2021-36160、CVE-2021-39275）脆弱性の詳細については、Apache HTTP サーバーの脆弱性を参照してください。 シスコは、この製品に対する脆弱性の影響を評価し、製品が次の影響を受けると結論付けました。 - CVE-2021-34798 - httpd コアでの NULL ポインタの逆参照 - CVE-2021-40438 - mod_proxy SSRF ただし、製品は、次の脆弱性の影響を受けません。 - CVE-2021-33193 - HTTP/2 メソッド インジェクションと mod_ プロキシを介したリクエスト分割 - CVE-2021-39275 - ap_escape_quotes バッファ オーバーフロー - CVE-2021-36160 - mod_proxy_uwsgi の範囲外の読み取り

以前のバージョンで発生し 3.4 で修正済みの問題

Cisco 識別子	要約
CSCvz91897	Syslog または監査ログ イベントは、認証なしで Meeting Server から設定済みのリモート ホストに送信できます。 新しいオプション syslog が tls MMP コマンドに追加され、証明書認証を通じてリモート ホストを検証します。
CSCvz28881	参加者が、Meeting Server で負荷分散が有効になっている分散型コール設定にある場合、API を使用して通話の録音を停止することはできません。
CSCvz21954	会議に参加する前に、参照メッセージを使用して通話を転送できます。
CSCvz34846	Meeting Server は、CallID API パラメータの英数字値を拒否するエラー チェックを実行しませんでした。
CSCvy95143	時折、SIP コールで、Meeting Server が同じコール ダイアログから同時に INVITE を送受信し、タイムアウトのためにコールを切断します。
CSCvx11659	Meeting Server で TLS SIP 検証が有効になっている場合、受信した証明書の有効性がチェックされず、無効または期限切れの証明書が許可されることがあります。
CSCwa52529	Meeting Server 2000v2（M5v2 ブレード サーバー）の loadLimit は 700000 を示していますが、Meeting Server 2000v2 の正しい loadLimit は 850000 です。

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 Cisco 識別子を入力してください。

Cisco 識別子	要約
CSCwa40239	スケジューラを使用して電子メール招待を送信する場合、参加者リストのすべての電子メール アドレスが有効である必要があります。スケジューラは、電子メール アドレスの 1 つが無効な場合でも、リストの参加者に電子メールを送信しない場合があります。
CSCvz01886	参加者のロールにビデオとプレゼンテーションを共有する権限がない場合、ロールが変更され、ビデオとプレゼンテーションを共有する権限がある場合、他の参加者がコンテンツを共有するときにプレゼンテーションは表示されません。
CSCvw61547	非常にまれなケースでは、Meeting Server TURN コンポーネントを介したコールの接続に失敗したり、メディア チャネルが不足している可能性があります。「RefreshTurnAllocationPending 状態での TURN 437 割り当ての不一致」と同様のエラーが、コールブリッジの syslog に表示されます。

Cisco 識別子	要約
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。
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 (関連：CSCvd91302)	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。

4.2.1 既知の制限事項

- Cisco Meeting Server は、バージョン 3.1 から TURN の短期のログイン情報をサポートしています。この操作モードは、TURN サーバがバージョン 3.1 以降の Meeting Server TURN サーバなどの短期のログイン情報もサポートしている場合にのみ使用できます。Expressway で Cisco Meeting Server を使用すると、短期のログイン情報はサポートされません。

5 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。

5.1 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

5.2 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。

5.3 コール キャパシティ

表 1 に、Cisco Meeting Server ソフトウェア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 2：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 1000 M5v2	Cisco Meeting Server 2000	Cisco Meeting Server 2000 M5v2
フル HD コール 1080p60 ビデオ 720p30 コンテンツ	24	24	30	175	218
フル HD 通話 （1080p30）ビデオ 1080p30/4K7 コンテンツ	24	24	30	175	218

コールのタイプ	Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5	Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 2000	Cisco Meeting Server 2000 M5v2
フル HD コール 1080p30 ビデオ 720p30 コンテンツ	48	48	60	350	437
HD コール 720p30 ビデオ 720p5 コンテンツ	96	96	120	700	875
SD コール 448p30 ビデオ 720p5 コンテンツ	192	192	240	1000	1250
音声通話（G.711）	1700	2200	2200	3000	3,000

表 3 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 3：クラスタおよびコールブリッジグループの Meeting Server 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 1000 M5v2	Cisco Meeting Server 2000	Cisco Meeting Server 2000 M5v2
個々の Meeting Server またはクラスタの Meeting Server（注 1、2、3、4） および Call Bridge グループ内の Meeting Server	1080p30 720p30 SD 音声通話	48 96 192 1700	48 96 192 2200	60 120 240 2200	350 700 1000 3000	437 875 1250 3000
	サーバごとの会議あたりの HD 参加者数	96	96	120	450	450
	Web アプリのコールキャパシティ（CMS Web エッジ上での内部コール & 外部コール）： フル HD HD SD 音声通話	48 96 192 500	48 96 192 500	60 120 240 500	350 700 1000 1000	437 875 1250 1250
Call Bridge グループ内の Meeting Server	サポートされるコール タイプ	着信 SIP 発信 SIP				
	負荷制限	96,000	96,000	120,000	700,000	875,000

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

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

注 3：SIP コールまたは Web アプリケーション コールにクラスタあたり最大 21,000 の HD 同時コール（24 ノード X 875 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 3 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：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。

5.4 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 3 を参照してください。）

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

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

Cisco Meeting Server Web エッジ ソリューションの使用の詳細については 、Cisco Meeting Server 3.1 リリース ノートを参照してください。

外部発信は、クライアントが Cisco Meeting Server の Web エッジ、または Cisco Expressway をリバースプロキシおよび TURN サーバとして使用して Web ブリッジ 3 とコールブリッジに到達する場合です。

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 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 アプリのコールキャパシティ – 外部コールに Expressway を使用

セットアップ	コール タイプ	CE1200 プラットフォーム (Platform)	大規模 OVA Expressway	中 OVA Expressway
Cisco Expressway（X12.6 以降）ペア	フル HD	150	150	50
	その他	200	200	50

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

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

5.6 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。内部参加者と外部の参加者が混在してサポートされている場合、Web アプリの合計キャパシティは、内部コールの場合と、外部コールに Cisco Meeting Server Web エッジソリューションを使用する場合は、表 3 に従います。ただし、エッジで Expressway を使用している場合でも、外部から接続できる合計内の参加者数は表 4 の制限に 制限されます。

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

6 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/en/us/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/en/us/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/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html
- プログラミング ガイド（API、CDR、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/en/us/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/en/us/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
- Cisco Meeting Server の相互運用性データベース： https://tp-tools- web01.cisco.com/interop/d459/s1790

7 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

アクセシビリティの詳細については、以下を参照してください。

www.cisco.com/web/about/responsibility/accessibility/index.html

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 ライセンスと限定保証は、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。

Cisco の商標または登録商標

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における登録商標または商標です。シスコの商標の一覧については、https://www.cisco.com/c/en/us/about/legal/trademarks.html 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）