

Cisco Meeting Server およびウェブアプリ

リリース 3.12.2

リリースノート

2026 年 8 月 25 日

目次

変更内容	5
1 はじめに	6
1.1 Cisco Meeting Server	6
1.2 Cisco Meeting Server web app.....	6
1.2.1 ウェブアプリの使用	7
1.3 Smart Licensing.....	7
1.4 ソフトウェアメンテナンスの終了.....	8
1.5 非推奨通知.....	8
2 Cisco Meeting Server の新機能.....	9
2.1 coSpaces のパスコード要件と検証.....	9
2.1.1 API の変更	11
2.2 「callbridge wc3jwt expiry」 コマンドの再導入と更新.....	11
2.2.1 MMP の変更	12
2.3 Meeting Server と Cisco Unified Communications Manager/IMP Server 間の接続の耐障害性の向上	12
2.3.1 MMP の追加	12
2.4 セキュリティ改善 - ユーザデータの安全保存	13
2.4.1 MMP の追加と変更	14
2.5 ウェブアプリで参加者の名前を変更するための API 強化	15
2.5.1 API の追加	15
2.6 ウェブアプリのユーザ識別設定	15
2.6.1 API の追加	16
2.7 ウェブアプリでチャット履歴を保存するための API 強化	16
2.7.1 API の追加	16
2.8 参加者レベルで音声ゲインを適用するための API 強化.....	17
API の追加.....	17
2.9 音声プロンプトの改善	18
2.10 coSpace 生成時間の追跡.....	18
API の変更	18
2.11 ウェブアプリへのカスタマイズしたヘルプリンクの追加.....	19
2.12 API の追加と変更の概要.....	19

2.13	MMP の追加と変更の概要	20
2.14	イベント記録の変更概要	21
2.15	関連するユーザードキュメント	21
3	Cisco Meeting Server ウェブ アプリの新機能	23
3.1	ウェブアプリのセッションタイムアウトの Edge ブラウザ対応	23
3.2	Web App セッションのタイムアウト	23
3.3	参加者の名前の変更	24
3.4	刷新されたユーザインターフェース	26
3.5	チャット履歴を保存する	26
3.6	メンバー限定スペースのミーティング招待リンク	26
3.7	テスト済みブラウザのバージョン	27
	iOS 13 以降および macOS 10.15 以降を使用しているユーザ に関する重要事項	28
	MacOS 10.15 以降の Chrome 上での画面共有に関する重要事項	28
3.7.1	Safari ブラウザのアクセシビリティ設定に関する重要なメモ	28
3.7.2	Safari ブラウザで見られる音声および映像の問題に関する重要な注意点	28
3.7.3	Microsoft Edge のグループ ポリシー設定に関する重要なメモ	29
4	製品ドキュメント	30
5	Cisco Meeting Server ソフトウェアバージョン 3.12.2 のアップグレード、 ダウングレード、デプロイ	31
5.1	リリース 3.12.2 へのアップグレード	31
5.2	ダウングレード	34
5.3	Cisco Meeting Server の展開	35
5.3.1	注意すべき点	36
6	バグ検索ツール、解決済みおよび未解決の問題	37
6.1	Cisco Meeting Server で解決された問題	38
6.2	Cisco Meeting Server における未解決の問題	40
6.2.1	既知の制限	41
6.3	Cisco Meeting Server ウェブアプリで解決された問題	41
6.4	Cisco Meeting Server ウェブアプリの未解決の問題	41
付録 A:	Meeting Server プラットフォームのメンテナンス	43
	Cisco Meeting Server 1000/Small およびその他の仮想化プラットフォーム	43

A.1 Cisco Meeting Server 2000.....	43
通話容量.....	43
Cisco Meeting Server web app のコールキャパシティ	45
Cisco Meeting Server web app のコールキャパシティ - 外線通話.....	46
Cisco Meeting Server ウェブアプリの容量 - 混合 (内部 + 外部) 通話.....	47
付録 B: アプリ機能の比較	48
アクセシビリティ通知.....	53
アクセシビリティサポート機能	54
Cisco の法的情報.....	55
Cisco の商標または登録商標	56

変更内容

バージョン	変更内容 (Change)
2025 年 12 月 15 日	3.12.1 のメンテナンスリリース 「 3.12.1 の機能強化 」および「 解決済みの問題 」を参照してください。
2025 年 10 月 31 日	バージョン 3.12 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 ソフトウェアおよび Cisco Meeting Server ウェブアプリのバージョン 3.12.2 での変更点について説明します。

1.1 Cisco Meeting Server

Cisco Meeting Server ソフトウェアは、次の環境でホストできます。

- VM 導入としてインストールされた Cisco Meeting Server Small。
- VM 導入としてインストールされた Cisco Meeting Server 1000。
- Cisco Meeting Server 2000、8 台の B200 ブレードを搭載し、Meeting Server ソフトウェアが唯一のアプリケーションとしてプリインストールされた UCS 5108 シャーシ。
- または、仕様に基づく VM サーバー上。

これらのリリースノートの残りの部分では、Cisco Meeting Server ソフトウェアは Meeting Server と呼ばれています。

注: Cisco Meeting Management は、Smart Licensing サポートのための製品の登録とスマートアカウントとの対話を処理します。Meeting Server 3.12 では Meeting Management 3.12 が必要です。

- **アップグレード:** 推奨されるワークフローは、まず Meeting Management をアップグレードし、Smart Licensing を完了してから、Meeting Server をアップグレードすることです。

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、別のデバイスにバックアップを安全に保存することをお勧めします。詳細は MMP コマンドリファレンス文書をご覧ください。

1.2 Cisco Meeting Server web app

Cisco Meeting Server ウェブ アプリ (ウェブ アプリ) は、ユーザがミーティング (音声とビデオ) に参加し、画面上にあるものを共有できるようにする、Cisco Meeting Server 用のブラウザ ベースのクライアントです。

1.2.1 ウェブアプリの使用

Web App を使用すると、スペースで音声とビデオを使用してミーティングに参加できます。ミーティング中に画面またはプレゼンテーションを共有することもできます。

スペースにメンバーを追加または削除することができます。組織内外のユーザをミーティングに招待することもできます。

メモ: スペースは、ユーザのグループがミーティングのためにいつでも使用できる、永続的な仮想会議室です。詳細については、オンラインヘルプまたはウェブアプリのユーザガイドを参照してください。

ウェブアプリは、デスクトップ、モバイル、またはタブレットで、サポートされているブラウザから使用できます。詳細については、[ブラウザのリスト](#) を参照してください。

ウェブアプリの使用方法の詳細については、オンラインヘルプまたは『Cisco Meeting Server ウェブアプリのユーザーガイド』を参照してください。

目的に応じて次のオプションから選択できます。

- web app にサインイン - web app にサインインして、ミーティングに参加し、自分がメンバーであるすべてのスペースのリストを表示し、参加方法を表示して、招待状の詳細をコピーして誰かをミーティングに招待できます。適切な権限を持っている場合は、事前設定されたテンプレートを使用してスペースを作成したり、スペースを編集または削除したりできます。
- ミーティングに参加する - ミーティングに招待されている場合は、このオプションを使用します。招待状には、ミーティング ID、パスコード (オプション)、ビデオアドレス (URI) などの詳細を含める必要があります。
- ミーティングのスケジュール - ミーティングをスケジュールするには、ホームページで [ミーティングのスケジュール] をクリックします。名前を入力し、ミーティングに使用するスペースを選択します。ミーティングは 1 回だけスケジュールすることも、日単位、週単位、月単位で繰り返すこともできます。選択したスペースのすべてのメンバーを追加したり、選択した参加者を追加してミーティングのロールを設定することができます。

1.3 Smart Licensing

3.4 リリース以降、Smart LicensingはMeeting Serverに必須です。従来のライセンスのサポートは 3.4 以降のリリースで廃止されました。顧客はスマート ライセンシングに移行することをお勧めします。

Smart Licensing および 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。

1.4 ソフトウェアメンテナンスの終了

Cisco Meeting Server ソフトウェアバージョン 3.12.2 のリリースに伴い、Cisco は、表 1 にソフトウェアのソフトウェアメンテナンス終了までのスケジュールを発表しました。

表 1: Cisco Meeting Server の各バージョンのソフトウェアメンテナンス終了までのスケジュール

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 3.10	Cisco Engineering が Cisco Meeting Server バージョン 3.10.x 向けに最終的なソフトウェアメンテナンスリリースまたはバグ修正をリリースできる最終日は、2026 年 4 月です。

Cisco Meeting Server の Cisco 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。

1.5 非推奨通知

- Cisco は、Meeting Server における Skype for Business および TelePresence Interoperability Protocol のサポートを廃止するプロセスを開始しました。これらの機能のサポートは、今後のリリースで削除されます。サービスの中断を避けるため、サポートされる代替機能への移行を準備することをお勧めします。

2 Cisco Meeting Server の新機能

ドキュメントのこのセクションでは、以下の Meeting Server リリースで実装された次の新機能および変更点を一覧表示しています。

3.12.1 の新機能と強化:

- [coSpaces のパスコード要件と検証](#)
- [「callbridge wc3jwt expiry」コマンドの再導入と更新](#)

3.12 の新機能と変更点:

- [Meeting Server と Cisco Unified Communications Manager/IMP Server 間の接続の耐障害性の向上](#)
- [セキュリティの改善 - ユーザーデータの安全な保存](#)
- [ウェブアプリで参加者の名前を変更するための API 強化](#)
- [ウェブアプリユーザー識別の設定](#)
- [ウェブアプリでチャットメッセージを保存するための API 強化](#)
- [参加者レベルで音声ゲインを適用するための API 強化](#)
- [音声プロンプトの改善](#)
- [coSpace 生成時間の追跡](#)
- [ウェブアプリへのカスタマイズしたヘルプリンクの追加](#)

2.1 coSpaces のパスコード要件と検証

coSpaces のパスコードルールが更新され、パスコードの最小長が 8 桁に設定され、パスコードには数字のみを使用する必要があります。以前は、パスコードの最小長に関する要件はなく、パスコードには英数字の文字列を使用できました。

coSpace のパスコードの設定は任意です。管理者は、希望しない限り、パスコードを設定する必要はありません。ただし、パスコードを設定する場合は、8 ~ 63 桁で、数字のみを使用する必要があります。パスコードがこれらの条件を満たさない場合、エラーメッセージが表示されます。

以前のバージョンで dial-in security profile のパスコードの最小長が 8 桁未満に設定されていた場合、または英数字が許可されていた場合は、バージョン 3.12.1 にアップグレードした後、パスコードの最小長を 8 ~ 63 桁の値に更新し、パスコードが数値のみで構成されるようにすることをお勧めします。

注意: Meeting Server 3.12.2 にアップグレードする際、すべての会議アクセス PIN は少なくとも 8 桁でなければなりません。Cisco TelePresence Management Suite でスケジュールされた会議で 8 桁未満の PIN を使用している場合、アップグレード後に Meeting Server で の起動に失敗します。

注意すべき点

- 更新されたパスコードルールは、パスコードが設定または変更された場合にのみ、coSpaces および dialInSecurityProfiles に適用されます。
- 既存の coSpaces と構成は、パスコードが変更されない限り影響を受けません。

以下の表は、パスコードが更新される際のさまざまなシナリオにおけるワークフローの概要を示しています。

シナリオ	ワークフロー
API の使用	
3.12 で作成 - coSpace ダイアルインプロファイルが有効で、パスコード長がたとえば 6 桁に設定されている API	アップグレード後 - 既存のスペース - パスコードが編集されるまで変更はありません。編集したパスコードが 8 桁未満の場合、または英数字の場合は、エラーメッセージが表示され、パスコードルールが適用されます。 既存のダイアルイン セキュリティ プロファイルを使用する新しいスペース - パスコードルールが適用されるため、パスコードは最低 8 桁である必要があります。
新しいダイアルイン セキュリティ プロファイルが有効な coSpace API	パスコードは 8 桁以上で、数字のみを使用する必要があります。
ダイアルインプロファイルが有効でない coSpace API	既存の coSpaces - パスコードが編集されるまで影響を受けません。パスコードを 8 桁未満に編集した場合、または英数字に編集した場合は、エラーメッセージが表示され、パスコードルールが適用されます。 新しい coSpaces - 最低 8 桁のパスコード/空のパスコードが必要です
CMM/webapp のようなポータルを使用する	
8 桁未満のパスコードが設定された旧テンプレートを使用して、Web App/CMM から作成された coSpace	テンプレートは古いダイアルインプロファイルを使用し、パスコードは指定された値に基づいて自動的に生成されます。したがって、パスコード規則は適用されません。
8 桁未満のパスコードが設定された新しいテンプレートを使用して、Web App/CMM から作成された coSpace	パスコードは 8 桁以上で、数字のみを使用する必要があります。
Cisco TelePresence Management Suite を介してスケジュールされた Meeting Server の会議	パスコードは 8 桁以上で、数字のみを使用する必要があります。アップグレード後は、8 桁未満の PIN が設定されている場合、Meeting Server で会議を開始できません。

パスコードルールは以下の API メソッドに適用されます:

- coSpaces の作成/変更
- アクセスメソッドの作成/変更
- dialInSecurityProfiles の作成/変更

2.1.1 API の変更

API メソッド	パラメータ	型/値	説明/メモ
/di-allSecurityProfiles の POST/PUT	minPasscodeLength	番号 (Number)	パスコードの最小許容桁数: 0 桁、または 8 桁から 63 桁まで (8 と 63を含む)。
/coSpaces/accessMethods の POST/PUT	パスコード	番号 (Number)	アクセス方法のセキュリティコード。パスコードの最小許容桁数: 0 桁、または 8 桁から 63 桁まで (8 と 63を含む)。
/coSpaces への POST/PUT	パスコード	番号 (Number)	coSpace のセキュリティコード。パスコードの最小許容桁数: 0 桁、または 8 桁から 63 桁まで (8 と 63を含む)。

上記のパスコードは web app にも適用され、すべてのアクセス方法で一貫したパスコード検証が保証されます。ユーザーが 8 ~ 63 桁の許容範囲外のパスコードを入力した場合、または英数字を含むパスコードを入力した場合、ウェブアプリに適切なエラーメッセージが表示されます。

2.2 「callbridge wc3jwt expiry」コマンドの再導入と更新

Meeting Server バージョン 3.12.1 では、以前削除された `callbridge wc3jwt expiry` コマンドが再導入されました。このコマンドを使用すると、管理者はタイムアウト値を時間単位 (1 ~ 24) で設定して、ウェブアプリのセッション有効期限を設定できます。未設定の場合、デフォルトの有効期限は 1 時間になりました (以前は 24 時間)。

警告: このコマンドは、管理者の指示の下で、慎重に使用する必要があります。

2.2.1 MMP の変更

コマンド/例	説明/メモ
<code>callbridge wc3jwt expiry</code> <有効期限 (時間)>	ウェブ アプリ セッションのタイムアウト時間を時間単位で設定します。1 ~ 24 までの整数を使用できます。未設定の場合、デフォルト値は 1 です。
	注: 変更を適用するには、コールブリッジを再起動してください。

注: 一部のブラウザは、デバイスの性能やタブスリープなどのブラウザ機能によって、長時間の非活動後にバックグラウンドタスクを一時停止または停止することがあります。セッションの有効期限が 1 時間を超えていると、5 分間の「セッション延長」ポップアップが必ずしも期待通りに表示されないことがあります。セッションは設定された有効期限で引き続き期限切れになりますが、ポップアップ通知はブラウザおよびシステムのリソース管理の影響を受けるため、ウェブアプリでは制御または変更できません。

2.3 Meeting Server と Cisco Unified Communications Manager/IMP Server 間の接続の耐障害性の向上

この Meeting Server のリリースでは、Jabber ユーザー向けに、Meeting Server と Cisco Unified Communications Manager (CUCM)/IMP Server 間の接続の耐障害性が向上しています。

Jabber ユーザーが Cisco Meeting Server ウェブアプリのミーティングにサインインすると、Meeting Server はアプリケーション ユーザー セッション キーを使用して、通話中のユーザーのプレゼンスステータスを動的に更新します。以前は、プレゼンス更新に対して無効な応答を受信すると、Meeting Server は Jabber ユーザーのプレゼンスステータスを更新できず、プレゼンス更新を再開するには手動で再起動する必要がありました。

サービスの中断を最小限に抑え、プレゼンス更新を継続的に行えるように、Meeting Server は 12 時間ごとにアプリケーションセッションキーを事前に検証するようになりました。さらに、管理者は新しい MMP コマンド `callbridge imps app_session_refresh_timer` を使用して、この検証間隔を設定できます。値は 1 ~ 24 時間の範囲で設定できます。

2.3.1 MMP の追加

コマンド	説明
<code>callbridge imps app_session_refresh_timer</code>	このコマンドにより、Meeting Server は CUCM 内のアプリケーション セッションを定期的に検証できるようになります。受け入れられる値の範囲は 1 時間から 24 時間です。設定されていない場合は、デフォルトで 12 時間になります。

さらに、このリリースでは、特に CUCM および IMP Server との統合において、Meeting Server の拡張性と応答性が大幅に向上しています。以前は、ユーザーがあるブラウザからミーティングにサインインした後、別のブラウザから別のミーティングに参加すると、IMPS サーバーに過剰な負荷がかかり、499 タイムアウトエラーが発生する可能性がありました。

これらの強化により、HTTP 499 エラーが減少し、プレゼンスのリセットによってユーザーの参加が遅延することがなくなるため、より安定した拡張性の高いミーティング環境を実現できます。

2.4 セキュリティ改善 - ユーザーデータの安全保存

バージョン 3.12 では、ミーティングサーバーのセキュリティ仕様にさらなる強化が加えられています。VM 導入 (仕様ベース / Meeting Server 1000/Small) では、セキュアストレージの強化が引き続き設定可能なオプションとして実装されており、MMP コマンド `secure_storage enable` を使用して有効にできます。

注: セキュアストレージを有効にした状態でバージョン 3.11 からアップグレードする場合は、設定が失われるリスクを回避するため、設定のバックアップを取得することを推奨します。

注意: 一度有効にすると、いかなるコマンドを使用してもセキュア ストレージを無効にすることはできません。この操作は 元に戻せません。 `<factory_reset full>` コマンドのみがセキュア ストレージ設定をリセットし、システム内の対応する変更がすべてリセットされます。そのため、バックアップ スナップショットを使用する構成設定のバックアップを取っておくことをお勧めします セキュア ストレージを有効にする前に、`<filename>` コマンドを実行してください。バックアップの取得方法の詳細については、[MMP コマンド リファレンス](#) ドキュメント を参照してください。

このリリースで導入されたセキュアストレージの改善には、以下の改善が含まれます。

秘密鍵を暗号化するためのパスフレーズの文字数制限

バージョン 3.12 では、`pki encrypt <key> <encrypted-key>` コマンドを使用して秘密キーを暗号化する際のパスフレーズに、14 文字以上の最小文字数が導入されています。パスフレーズには、英字、数字、特殊文字、記号、スペースを任意に組み合わせて使用できます。パスフレーズが 14 文字未満の場合はエラーメッセージが表示されます。

バックアップファイルの暗号化

セキュアストレージは、`backup snapshot <name>` コマンド。 `backup snapshot <name>` を使用する場合、ユーザーはパスワードを使用してバックアップファイルを暗号化するように求められるようになりました。 パスワードは 14 文字以上で、文字、数字、特殊文字、記号、スペースの任意の組み合わせを含めることができます。 これらのファイルは、ロールバック中に同じパスワードを使用して復号化できます。

注: セキュア ストレージを有効にすると、バックアップ ファイルはデフォルトで自動的に暗号化されるため、それ以上の暗号化は必要ありません。

さらに、ユーザが SFTP を使ってバックアップファイルをダウンロードする場合、セキュアストレージはバックアップファイルのダウンロードに対して暗号化を強制します。 新しい MMP コマンド、`backup encrypt` バックアップファイルをダウンロードする前に暗号化するため、`<name>` `<encrypted-name>` が追加されました。 暗号化しない場合、これらのファイルのダウンロード権限が拒否されます。

FIPS モードのサポート

このリリースでは、Secure Storage は FIPS が有効になっている場合に FIPS をサポートします。

FIPS が有効になっている場合、以前のリリース (3.11) で短いパスワードを使用して作成された秘密キー ファイルは、最小 14 文字のパスワードを使用して再生成する必要があります。

2.4.1 MMP の追加と変更

この実装の一部として、以下のコマンドが追加されています:

コマンド	説明
バックアップ暗号化 <code><名前></code> <code><暗号化された名前></code>	このコマンドは、SFTP を使用してバックアップファイルをダウンロードする際に、ファイルを暗号化します。 このコマンドを実行すると、ユーザーは 14 文字以上のパスワードを入力するように求められます。 パスワードには、英字、数字、特殊文字、記号、スペースを任意に組み合わせて使用できます。 既存のファイル名を再利用するのではなく、新しいファイル名を使用することをお勧めします。

下記のバックアップコマンドは、それに応じて追加の詳細を提供するように変更されます。

コマンド	説明
バックアップリスト	コマンドは、暗号化ステータスと、暗号化元のファイル名を含めるように変更されました。

2.5 ウェブアプリで参加者の名前を変更するための API 強化

バージョン 3.12 では、ミーティング中にウェブアプリの参加者が表示名を変更できるようにする新しい API が導入されます。新しい権限コントロールにより、権限を持つ参加者は、自分自身または他の参加者 (ロビーで待機している参加者を含む) の名前を変更できます。

2.5.1 API の追加

新しい API `renameParticipantAllowed` が導入され、以下の API メソッドで `callLegProfile` を介して管理されます。

`/callLegprofiles` への POST

`/callLegprofiles/<callLegprofileID>` に PUT します。

パラメータ	Value	説明
参加者の名前 変更許可	なし	参加者は表示名を変更できません。未設定の場合はデフォルト値 なし 。
	自己	参加者は自分の表示名を変更できます。
	participants	参加者は、自分自身や、ロビーにいる人を含む他の参加者の名前を変更できます。

ウェブアプリでこの機能の使用方法の詳細については、「[参加者の名前の変更](#)」を参照してください。

2.6 ウェブアプリのユーザ識別設定

Cisco Meeting Server ウェブアプリバージョン 3.11 では、**参加者リスト**に視覚的なインジケータが導入され、各参加者の参加方法を識別できるようになりました。たとえば、 (サインイン済みユーザーの場合)、 (サインインしていないユーザーの場合)、 (SIP ユーザーの場合) で示されます。

バージョン 3.12 では、Meeting Server に新しい API パラメータ `showParticipantIndicator` が導入され、この機能を設定できるようになりました。このパラメータにより、管理者はウェブアプリの参加者リストにおけるユーザー識別アイコンの可視性を制御できます。

2.6.1 API の追加

API パラメータ `showParticipantIndicator` が、グローバルレベルの `webBridgeProfiles` に導入されています。このパラメータにより、管理者はユーザー識別アイコンを表示または非表示にできます。

- `/webBridgeProfiles` への POST
- `/webBridgeProfiles/<web bridge profile id>` に対する PUT
- `/webBridgeProfiles/` に対する GET

パラメータ	タイプ/値	説明
<code>showParticipantIndicator</code>	True/False	参加者リストにユーザー識別アイコンを表示または非表示にします。 True - ユーザー ID アイコンを表示します。 False - ユーザー識別アイコンを非表示にします。

2.7 ウェブアプリでチャット履歴を保存するための API 強化

バージョン 3.12 以降、必要な権限を持つウェブアプリの参加者は、ウェブアプリのミーティング中にチャットメッセージをダウンロードして保存できます。管理者は新しい API、`allChatSave` を使って必要な権限を割り当てることができます。

2.7.1 API の追加

`allChatSave` パラメータは、次の `callLegs` および `callLegprofiles` API メソッドで導入されました。

- `/calls/<call ID>/callLegs` への POST
- `/callLegs/<callLegID>` に PUT します。
- `/callLegprofiles` への POST
- `/callLegprofiles/<callLegprofileID>` に PUT します。

パラメータ	タイプ/値	説明
<code>allChatSave</code>	真/偽	True - Web アプリの参加者は、チャットメッセージを .txt 形式でダウンロードして保存できます。 偽 - Web アプリの参加者はチャットメッセージをダウンロードして保存できません。

ウェブアプリでのこの機能の使用方法の詳細については、「[チャット履歴の保存](#)」を参照してください。

2.8 参加者レベルで音声ゲインを適用するための API 強化

Meeting Server は、進行中の会議中に特定の参加者に対して固定音声ゲインを適用することをサポートするようになりました。管理者は、非常に低いまたは高い音量レベルのエンドポイントの音声出力を制御できます。

新しい `audioGainDb` パラメータが、`callLegs` および `callLegProfile` API メソッド、ならびにサブスクライブ可能なイベントの `callRoaster` リソースに導入されています。このパラメータは、正の値と負の値を受け入れます。正の値は音量の増加、負の値は音量の減少を表します。

`audioGainDb` パラメータのゲインは `audioGainMode` パラメータとは独立して動作します。ただし、有効な音量は、`callLeg` プロファイルで `audioGainMode` パラメータが有効になっているかどうかによって異なります。AGC に設定されている場合、`audioGainDb` の固定ゲインが自動ゲインコントロールの後に適用されます。

API の追加

新しい `audioGainDb` パラメータが、次の `callLegs` および `callLegprofiles` API メソッドに導入されました。

- `/calls/<call ID>/callLegs` への POST
- `/callLegs/<callLegID>` に PUT します。
- `/callLegprofiles` への POST
- `/callLegprofiles/<callLegprofileID>` に PUT します。

パラメータ	タイプ/値	説明
<code>audioGainDb</code>	数値/整数	このパラメータは、特定の参加者のゲイン値をデシベル単位で設定します。値は 10 の倍数で入力する必要があります。たとえば、ゲイン値を 6 dB にするには、60 と入力します。+60 から -60 までの範囲内で、正の値（音量増加）と負の値（音量減少）を受け入れます。 注： <code>callLegProfile</code> を介して <code>audioGainDb</code> を変更しても、<code>callLeg</code> が確立された後に再度変更しない限り、その設定は適用されません。

イベントレコードの変更

`audioGainDb` パラメータが、サブスクライブ可能なイベントの `callRoster` リソースに追加されます。

パラメータ	タイプ/値	説明
<code>audioGainDb</code>	数値/整数	ゲイン値は特定の参加者に適用されます。

2.9 音声プロンプトの改善

Meeting Server は音声プロンプトをより適切に処理できるように強化され、ユーザーが IVR 経由で接続する場合や、PIN で保護されたスペースに参加する場合に、`coSpace` 参加プロンプトが 1 回だけ再生されるようになりました。

2.10 coSpace 生成時間の追跡

バージョン 3.12 以降、`coSpace` の GET 操作は作成時刻と所有者の詳細を取得し、`coSpace` がいつ、誰によって作成されたかの追跡に役立ちます。この情報は、WebAdmin の設定メニューオプションにある [スペース(Spaces)] ページにも表示されます。

注: バージョン 3.12 へのアップグレード前に作成された `coSpaces` の場合、`creationTime` にはアップグレード日が表示されます。ただし、`ownerJid` は含まれません。

API の変更

`coSpace` の GET 操作では、次の応答要素が返されます。

応答要素	タイプ/値	説明 / 注記
作成時間	文字列	スペースが作成された日時。選択したタイムゾーンに関係なく、協定世界時 (UTC) に基づいて yyyy-mm-dd hh:m-m:ss 形式で表示されます。
<code>ownerJid</code>	文字列	特定の Jid によって識別される <code>coSpace</code> の所有者。

2.11 ウェブアプリへのカスタマイズしたヘルプリンクの追加

バージョン 3.11 では、Meeting Server を設定して、ウェブアプリのデフォルトのヘルプリンクからカスタムページを表示するようにリダイレクトできる機能が導入されました。これはベータ機能として導入されました。この Meeting Server リリース以降、この機能は完全にサポートされるため、カスタマイズライセンスは必要ありません。

この機能は Web アプリでのみサポートされています。

ヘルプページを外部のカスタムヘルプページにリダイレクトするには、

`brand_external_help_link` を `text_strings_xx_XX.json` ファイル。ユーザーが  ヘルプアイコンをクリックすると、このファイルで提供されるカスタムヘルプリンクに移動します。ただし、外部ヘルプページへのリンクが追加されていない場合、ヘルプアイコンはデフォルトのオンラインヘルプページに移動します。

注: Meeting Server で設定されたカスタムヘルプページは、ウェブアプリ内のすべてのヘルプリンクを置き換えます。これには、サインイン ページ、会議中ページ、Cookie 通知ページが含まれます。したがって、カスタム ヘルプ リンクが Meeting Server に設定されている場合は、管理者は必要な情報がすべて含まれていることを確認する必要があります。無効な URL または複数の URL の場合、カスタム ヘルプ ページにエラー メッセージが表示されます。

2.12 API の追加と変更の概要

Meeting Server 3.12 の API 機能には、以下の新しい API パラメータが含まれます。

参加者の名前を変更するために、次の API パラメータ

`renameParticipantAllowed` が `callLegProfile` に導入されています。

- `/callLegprofiles` に POST する
- `/callLegprofiles/<callLegprofileID>` に PUT します

ユーザ識別アイコンを表示または非表示にするために、次の API パラメータが追加されました。

`showParticipantIndicator` が `webBridgeProfiles` にグローバルレベルで導入されました：

- `/webBridgeProfiles` への POST
- `/webBridgeProfiles/<web bridge profile id>` に対する PUT
- `/webBridgeProfiles/` に対する GET

Web アプリ会議中にチャット メッセージをダウンロードして保存するために、次の API パラメータが追加されました。

`allChatSave` パラメータは、次の `callLegs` および `callLegprofiles` API メソッドで導入されました。

- `/calls/<call ID>/callLegs` への POST
- `/callLegs/<callLegID>` に PUT します。
- `/callLegprofiles` への POST
- `/callLegprofiles/<callLegprofileID>` に PUT します。

進行中の会議中に特定の参加者に固定のオーディオ ゲインを適用するために、次の API パラメータが追加されました。

新しい `audioGainDb` パラメータが、次の `callLegs` および `callLegprofiles` API メソッドに導入されました。

- `/calls/<call ID>/callLegs` への POST
- `/callLegs/<callLegID>` に PUT します。
- `/callLegprofiles` への POST
- `/callLegprofiles/<callLegprofileID>` に PUT します。

`coSpace` に対する GET 操作は、その作成時刻と所有者の詳細を取得します。

`coSpace` の GET 操作では、次の応答要素が返されます。

2.13 MMP の追加と変更の概要

Cisco Meeting Server と Cisco Unified Communications Manager/IMP Server 間の接続を改善するために、次のコマンドが追加されました。値は 1 ~ 24 時間の間で設定できます。

コマンド	説明
<code>callbridge imps app_session_ refresh_timer</code>	このコマンドにより、Meeting Server は CUCM 内のアプリケーション セッションを定期的に検証できるようになります。受け入れられる値の範囲は 1 時間から 24 時間です。設定されていない場合は、デフォルトで 12 時間になります。

以下のコマンドは、**セキュア ストレージ** の機能強化の一部として追加されました。

注意: 一度有効にすると、いかなるコマンドを使用してもセキュア ストレージを無効にすることはできません。この操作は 元に戻せません。 `<factory_reset full>` コマンドのみがセキュア ストレージ設定をリセットし、システム内の対応する変更がすべてリセットされます。そのため、バックアップ スナップショットを使用する構成設定のバックアップを取っておくことをお勧めします セキュアストレージを有効にする前に、`<filename>` コマンドを実行してください。

FIPS が有効な場合に、最小 14 文字のパスフレーズを使用して、より短いパスフレーズで秘密キーファイルを再生成するための次のコマンドが追加されました。

コマンド	説明
バックアップ暗号化 <名前> <暗号化された名前>	このコマンドは、SFTP を使用してバックアップファイルをダウンロードする際に、ファイルを暗号化します。このコマンドは、ユーザに最低 14 文字のパスフレーズを入力するよう要求します。既存のファイル名を再利用するのではなく、新しいファイル名を使用することをお勧めします。

次のバックアップ コマンドは、それに応じて追加の詳細を提供するように変更されます。

コマンド	説明
バックアップリスト	コマンドは、暗号化ステータスと、暗号化元のファイル名を含めるように変更されました。

2.14 イベント記録の変更概要

audioGainDb パラメータが、サブスクライブ可能なイベントの callRoster リソースに追加されます。

パラメータ	タイプ/値	説明
audioGainDb	数値/整数	特定の参加者に適用されるゲイン値。

2.15 関連するユーザードキュメント

以下のサイトには、インストール、計画・展開、初期設定、製品の運用などに関する文書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 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 (導入計画と導入、証明書のガイドライン、簡易セットアップ、ロードバランシング 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 のリファレンスガイドおよび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 に関するよくある質問: <https://meeting-infohub.cisco.com/faq/category/25/cisco-meeting-server.html>
- Cisco Meeting Server 相互運用性データベース: <https://tp-tools-web01.cisco.com/interop/d459/s1790>

3 Cisco Meeting Server ウェブ アプリの新機能

このバージョンのウェブアプリソフトウェアでは、次の新機能と変更が導入されています:

3.12.1 での強化:

- [ウェブアプリのセッションタイムアウトの Edge ブラウザ対応](#)

3.12 の新機能と変更点:

- [Web App セッションのタイムアウト](#)
- [参加者の名前の変更](#)
- [刷新されたユーザーインターフェイス](#)
- [チャット履歴を保存する](#)
- [メンバー限定スペースのミーティング招待リンク](#)

3.1 ウェブアプリのセッションタイムアウトの Edge ブラウザ対応

バージョン 3.12 では、参加者が操作を行わない場合や別のタブに切り替えた場合に、ウェブアプリのセッションが 60 分で期限切れになる機能が導入されました。この機能は当初、Chrome、Firefox、Safari ブラウザのみでサポートされていました。バージョン 3.12.1 から、Edge ブラウザでもサポートされています。

3.2 Web App セッションのタイムアウト

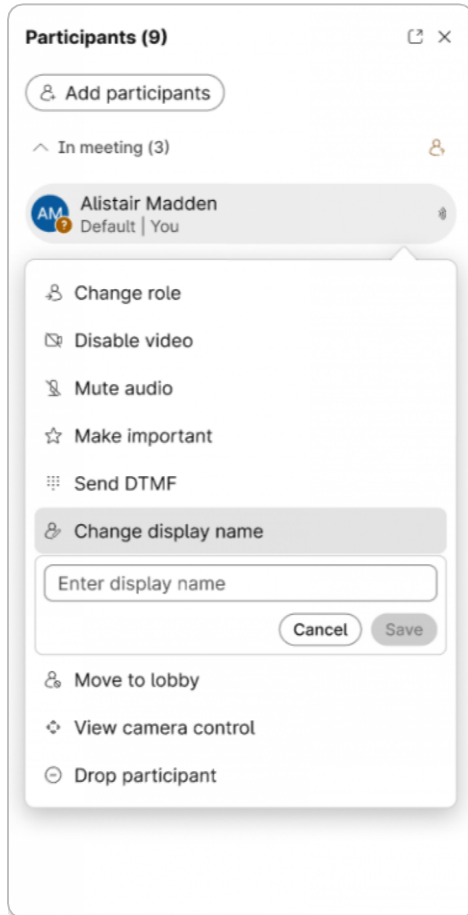
バージョン 3.12 以降、ウェブアプリのセッションは 60 分後に期限切れになるように設定されています。55 分経過時点で、参加者が操作を行っていない場合、または別のタブで操作している場合は、通知ポップアップが表示され、参加者はサインインしたままにするか、サインアウトするかを選択できます。ポップアップの表示後、セッションの期限が切れる前に参加者がウェブアプリのタブで操作を行うと、セッションが自動的に更新され、ポップアップが閉じられます。

注：

- ポップアップ通知は Windows または macOS のデスクトップブラウザにのみ表示されます。モバイル端末では表示されません。
 - この機能は、Chrome、Firefox、Safari ブラウザでのみサポートされています。
 - macOS では、Firefox のウィンドウが別のウィンドウで最大化されると、ポップアップ通知が別のタブに表示されることがあります。ただし、ポップアップが表示される Firefox ウィンドウに自動的にリダイレクトされることはありません。そのため、ユーザがそのウィンドウに積極的に関与していなければ、ポップアップ通知に気づかないままになる可能性があります。
 - 上記の動作は、フルスクリーンモード時のシステムの機能によって決まるものであり、ウェブアプリで制御または変更することはできません。
-

3.3 参加者の名前の変更

バージョン 3.12 以降、会議のホストや適切な権限を持つ参加者は、ロビーで待機する参加者を含め、会議中に自分の表示名や他の参加者の表示名を変更できるようになりました。新しいオプション、**[表示名を変更]** が、参加者リストウィンドウに追加されました。参加者は、表示名が変更されるたびに通知を受け取ります。



注：

- 表示名は最大 80 文字まで入力できます。
 - 変更された名前はビデオレイアウトラベルにも反映されます。
 - 参加者に名前の変更が通知されるのはミーティング中のみで、ロビーにいる間は通知されません。
 - ユーザーが大文字と小文字のみを変更して名前を変更した場合、表示名は更新されません。たとえば、「sally wood」を「Sally Wood」に、またはその逆。
 - 参加者が切断された場合、Web App が参加者を自動的に再接続しても、表示名は元の名前に戻ります。このような参加者は、再接続時に再度名前を変更する必要があります。
 - **表示名の変更** オプションは、必要な許可がなければ参加者には表示されません。Meeting Server で権限を付与する方法の詳細については、[ウェブアプリで参加者の名前を変更するための API の強化](#)を参照してください。
-

3.4 刷新されたユーザインターフェース

バージョン 3.12 以降、ウェブアプリでは、色、フォント、アイコンなどが更新され、視覚的な外観が強化された新しいユーザインターフェイスが導入されています。

3.5 チャット履歴を保存する

ウェブアプリでは、適切な権限を持つ参加者がミーティングのチャット履歴を .txt ファイルとしてエクスポートできるようになりました。エクスポート機能により、参加者はチャットコンテンツをローカルで保存・レビューできます。

ミーティング中、参加者は [チャット(Chat)] ウィンドウの [保存(Save)] ボタンをクリックできます。クリックすると、その時点までに参加者に表示されているすべてのチャットメッセージを含む .txt ファイルがダウンロードされます。ミーティング中はいつでも [保存(Save)] ボタンを使用できます。

エクスポートされるファイル名は以下の命名規則に従います:

<スペース名>-<チャット履歴>-<曜日 日付 時刻 タイムゾーン>.txt

エクスポートされたファイルには以下が含まれます。

- 送信者と受信者の名前
- 各メッセージのタイムスタンプ
- メッセージの内容

注:

- Meeting Server で **allChatSave** 権限が有効になっている参加者 (callLegProfile レベル) のみ、[保存(Save)] ボタンを表示してチャットをエクスポートできます。
 - 参加者はチャット履歴を複数回エクスポートできます。各エクスポートはエクスポート時に表示されるチャット内容を反映しています。
-

3.6 メンバー限定スペースのミーティング招待リンク

以前のバージョンのウェブアプリでは、サインイン済みのスペースメンバーは、メンバー限定スペースでスケジュールされたミーティングに、ミーティング招待リンクから直接参加することができませんでした。代わりに、ウェブアプリの該当スペース内の「会議に参加」ボタンをクリックする必要がありました。

バージョン 3.12 以降、リンクをクリックすると、サインイン済みのスペースメンバーはミーティングロビーページに直接移動します。すでにログインしている場合は追加のサインイン手順は不要です。ただし、非メンバーが招待リンクを使用してスペースのミーティン

グに参加しようとする、ウェブアプリにより、アクセスがメンバーのみに制限されていることを示す適切なメッセージが通知されます。

3.7 テスト済みブラウザのバージョン

表 2 は、特定のバージョンのウェブ アプリのリリース時にウェブ アプリに対してテストされたブラウザの一覧です。

常に最新バージョンのブラウザを使用することをお勧めします。

メモ: Google Chrome および Mozilla Firefox などの特定のブラウザは、自動的に最新バージョンに更新されることに注意してください。 次の表は、Cisco Meeting Server のバージョンの正式リリース時にテストされたブラウザのバージョンを示しています。 これは、これらのブラウザの以前のバージョンでこの特定のリリースをテストしていないことを意味します。

Cisco Meeting Server の各メジャー リリースの最新のメンテナンス リリースは、互換性を維持するために、すべてのブラウザの最新の公開バージョンに対してテストするよう努めています。問題が検出された場合は、できるだけ早く修正するよう努めます。

表 2: ブラウザとバージョンでテストした Cisco Meeting Server ウェブ アプリ

ブラウザ	バージョン
Google Chrome(Windows および Android)	141.0.7390.107
Google Chrome(macOS)	141.0.7390.78
Mozilla Firefox (Windows)	144.0
Chromium ベースの Microsoft Edge (Windows)	141.0.3537.7
macOS 用 Apple Safari	26.0.1
iOS 版 Apple Safari	18.4

メモ: ウェブ アプリはレガシー Microsoft Edge ではサポートされていません。

メモ: ウェブアプリは、これらの対応ブラウザを実行する仮想マシンではサポートされていません。

iOS 13 以降および macOS 10.15 以降を使用しているユーザ に関する重要事項

iOS 13 以降および macOS 10.15 以降上の Safari でユーザがウェブアプリを使用できるようにするためには、次の場所に記載されている要件を遵守するように webbridge3 を適切に設定する必要があります: <https://support.apple.com/en-us/HT210176>。

これらの要件が満たされていない場合、ユーザは Safari でアプリケーションを開くことができません。

MacOS 10.15 以降の Chrome 上での画面共有に関する重要事項

MacOS バージョン 10.15 (Catalina) 以降では、Chrome 上で実行されているアプリケーションから画面またはアプリケーションを共有するには、アクセス許可を有効にする必要があります。手順は以下のとおりです。

1. Apple メニューから [システム環境設定(System Preferences)] を選択します。
2. [Security & Privacy (セキュリティとプライバシー)] をクリックします。
3. 上部の Privacy タブをクリックしてください。
4. 左側のカラムで下方向にスクロールし、[画面レコーディング(Screen Recording)] をクリックします。
5. Chrome が選択されていることを確認します。Chrome を再起動します。

3.7.1 Safari ブラウザのアクセシビリティ設定に関する重要なメモ

デフォルトでは、Safari ブラウザは「Tab」キーによる UI 要素のナビゲーションを許可せず、代わりに Option + Tab を使用します。これは Safari の基本設定で次のように設定できます。

Safari ブラウザのメニューから、[Safari] > [基本設定 (Preferences)] > [詳細設定 (Advanced)] > [アクセシビリティ (Accessibility)] > [タブを押してウェブページの各項目をハイライト表示 (Press Tab to highlight each item on a web page)] に移動して基本設定を変更します。

3.7.2 Safari ブラウザで見られる音声および映像の問題に関する重要な注意点

CSCwp32445 - MacBook システムの Safari バージョン 18.5 では、ユーザが画面共有セッション中に断続的な音声問題を体験します。他の参加者が別のブラウザを使用してコンテンツ音声付きで画面を共有すると、Safari ユーザーには最初は音声聞こえますが、その後、共有コンテンツの音声と参加者の音声の両方が聞こえなくなります。

回避策: ユーザーがミーティングに再参加すると、この問題は解決します。 場合によっては、数分後に自然に解消することもあります。

3.7.3 Microsoft Edge のグループ ポリシー設定に関する重要なメモ

WebRtcLocalhostIpHandling - [WebRTC によるローカル IP アドレスの公開を制限する (Restrict exposure of local IP address by WebRTC)] グループポリシーが Microsoft Edge ブラウザに適用されている場合、次のポリシーオプションのいずれか 1 つだけを使用してください。

- **AllowAllInterfaces** (デフォルト) または
- **AllowPublicAndPrivateInterfaces** (default_public_and_private_interfaces)

他のオプションは接続の問題を引き起こす可能性があります。

4 製品ドキュメント

ユーザーガイドやウェブアプリのビジュアル「How to」ガイドなどのエンドユーザー向けガイドは、次の場所にあります。

<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-user-guide-list.html>

5 Cisco Meeting Server ソフトウェアバージョン 3.12.2 のアップグレード、ダウングレード、デプロイ

このセクションでは、Cisco Meeting Server ソフトウェアバージョン 3.11 からのアップグレードを前提としています。以前のバージョンからアップグレードする場合は、まず 3.11 リリースノートの指示に従って 3.11 にアップグレードし、その後にこの Cisco Meeting Server 3.12 リリースノートの指示に従う必要があります。これは特に Cisco Expressway を Meeting Server に接続している場合に重要です。

注: Cisco は 3.11 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/Small、または以前に設定された VM 導入環境にインストールされている Cisco Meeting Server ソフトウェアのバージョンを確認するには、MMP コマンド `version` を使用します。

VM を初めて設定する場合は、『[仮想化展開のための Cisco Meeting Server インストールガイド](#)』の手順に従ってください。

5.1 リリース 3.12.2 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 の導入環境に適用されます。クラスタ化されたデータベースを使用する導入環境については、クラスタ化されたサーバーをアップグレードする前に、この [FAQ](#) を参照してください。

注意: Meeting Server のアップグレードやダウングレードを行う前に、まず `backup snapshot <filename> command` を使って設定バックアップを取り、バックアップファイルを別のデバイスに安全に保存してください。詳細については、[MMP コマンド リファレンス ドキュメント](#)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によって自動的に生成されるバックアップファイルには依存しないでください。アップグレード / ダウングレードに失敗した場合、アクセスできなくなる可能性があります。

注意: クラスタ化されたデータベースを展開している場合は、会議サーバーをアップグレードする前に `database cluster remove` コマンドを使ってすべてのノードをクラスターから削除してください。アップグレード後、適切な MMP コマンドを使ってノードをクラスタに再追加します。詳細な手順は [Cluster upgrade FAQ](#) 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 段階のプロセスで行います。まず、アップグレードするファームウェアイメージをアップロードし、次に upgrade コマンドを実行します。この操作によってサーバーが再起動します。再起動中は、サーバー上で実行中のすべてのアクティブな通話が中断されるため、この段階はユーザーに影響が出ない適切な時間に実施するか、事前にユーザーに警告してください。

注: セキュアストレージを有効にした状態でバージョン 3.11 からアップグレードする場合は、設定が失われるリスクを回避するため、設定のバックアップを取得することを推奨します。

サーバに最新のファームウェアをインストールするには、以下の手順に従ってください:

1. Cisco ウェブサイト [ソフトウェアダウンロード](#) ページから、適切なアップグレードファイルを入手します。

Cisco_Meeting_Server_3_12_2_CMS2000.zip

このファイルはサーバにアップロードする前に、1 つの upgrade.img ファイルに解凍する必要があります。このファイルを使って Cisco Meeting Server 2000 サーバをアップグレードしてください。

Hash (SHA-256) for upgrade.img

file:1f9178294766cfa6c5f30d8c08ee213027d79d2a7249eac21f16fd896e126a58

Cisco_Meeting_Server_3_12_2_vm-upgrade.zip

このファイルは、サーバーにアップロードする前に解凍して、1 つの upgrade.img ファイルにする必要があります。Cisco Meeting Server の仮想マシン導入環境をアップグレードするには、このファイルを使用します。

Hash (SHA-256) for upgrade.img

file:b240992ddd153a2e7ab41092714d0479ad22473a2b5f9f85057ad0d709bb8fd6

Cisco_Meeting_Server_3_12_2_vSphere-8_0.ova

このファイルを使って VMware 経由で新しい仮想マシンを展開します。

vSphere 8.0 以降用の場合、Cisco_Meeting_Server_3_12_vSphere-8_0.ova のハッシュ (SHA-512) は次のとおりです。

e89aaf982237d5ebf24df65e09275e593f7d4cd900355645a2e609e86d01a6b664257224f03ee8dff0f2938 e6d6e53e43aa2ec95e2e8507d76a172ce64857b41

2. OVA ファイルを検証するために、3.12.2 リリースのチェックサムは、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示されています。さらに、上記の SHA-512 ハッシュ値を使ってダウンロードの整合性を確認できます。

注: Meeting Server および Meeting Management のバージョン 3.12 は、ESXi 8.0 Update 3e をサポートします。

3. SFTP クライアントを使用して、その 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ているものです。Windows を使用している場合は、WinSCP ツールの使用をお勧めします。

注意: ファイル転送に WinSCP を使用している場合は、「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。間違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いことになります。

注:

- a) MMP インターフェースの IP アドレスは `iface a` MMP コマンドで見つけることができます。
 - 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/仮想サーバにコピーします。
5. アップグレードファイルの検証を行うには、`upgrade list` コマンドを発行してください。
 - a. MMP への SSH 接続を確立し、ログインします。
 - b. 利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、`upgrade list` コマンドを実行して出力します。

アップグレードリスト

- 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か確認してください。
6. アップグレードを適用するには、前の手順で使用した SSH 接続で MMP に接続し、`upgrade` コマンドを実行してアップグレードを開始します。
 - a. アップグレードコマンドを実行してアップグレードを開始してください。
`upgrade <image_name>.img` 例: `upgrade upgrade_spa.img`
 - b. サーバー/ 仮想化サーバーは自動的に再起動します。プロセスが完了するまで 10 分間待ちます。
7. MMP への SSH 接続を再確立し、次のコマンドを入力して、Meeting Server でアップグレードしたイメージが実行されていることを確認します。

バージョン

8. カスタマイズアーカイブファイルがあれば更新してください。
9. アップグレードは完了しました。

5.2 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後に予期しない問題が発生した場合は、Meeting Server ソフトウェアを以前のバージョン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 の **upgrade** コマンドで Meeting Server を必要なバージョンに「ダウングレード」します。

警告: 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設定のバックアップを取得し、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 ドキュメント](#) 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によって自動的に生成されるバックアップファイルには依存しないでください。アップグレード / ダウングレードに失敗した場合、アクセスできなくなる可能性があります。

注意: セキュアストレージを有効にしたバージョン 3.12.2 からダウングレードする場合、このプロセスは中止されます。続行するには、**<factory_reset full>** を実行してセキュアストレージの設定をクリアしてから、目的の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 / 仮想化サーバは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 Admin が使用可能になるまで 10 ~ 12 分間待ちます。
3. Web Admin にログインし、[**状況(Status)**] > [**全般(General)**] に移動して、[**システムステータス(System status)**] 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. サーバーで MMP コマンド **factory_reset app** を使用し、工場出荷時の状態へのリセット後に再起動するまで待ちます。
5. MMP コマンド **backup rollback <name>** コマンドを使って、古いバージョンの設定バックアップを復元してください。

注: **backup rollback** コマンドは、既存の設定とシステム上のすべての証明書および秘密キーを上書きし、Meeting Server を再起動します。そのため、使用には注意が必要です。バックアップロールバックプロセス中に証明書が上書きされるため、事前に証明書をコピーしておいてください。json ファイルは上書きされず、再アップロードも必要ありません。

Meeting Server は、バックアップファイルを適用するために再起動します。

クラスタ化された導入環境の場合は、クラスタ内の各ノードで手順 1 ~ 5 を繰り返します。

6. 最後に、次の点を確認してください:

- 各 Call Bridge の Web Admin インターフェイスが coSpaces のリストを表示できること。
- ダイアル プランはそのまま、
- Web Admin とログファイルで障害が報告されないこと。
- SIP および Cisco Meeting Apps (サポートされている場合は Web Bridge も) を使用して接続できること。

Meeting Server の展開ダウングレードは完了しました。

5.3 Cisco Meeting Server の展開

Meeting Server の導入方法を簡単に説明するために、導入環境を 3 つのモデルに分けて説明します。

- 単一の統合 Meeting Server – Meeting Server のすべてのコンポーネント (Call Bridge、Web Bridge 3、Database、Recorder、Uploader、Streamer、TURN サーバー) を使用でき、Call Bridge と Database は自動的に有効になりますが、その他のコンポーネントは、展開の要件に応じて個別に有効化されます。有効になっているすべてのコンポーネントが、単一のホストサーバー上に配置されます。
- 単一の分割 Meeting Server – このモデルでは、ネットワークエッジの DMZ に配置された Meeting Server で TURN サーバー、Web Bridge 3、および MeetingApps が有効になり、その他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 で有効になります。
- 3 つ目のモデルでは、複数の Meeting Server をクラスタ化して導入し、導入環境の拡張性と耐障害性を高めます。

3 モデルすべてを網羅した展開ガイドは [こちら](#) で入手可能です。各導入ガイドには、個別の証明書ガイドラインドキュメントが付属しています。

5.3.1 注意すべき点

5.3.1.1 Cisco Meeting Server 2000

Cisco Meeting Server 2000 には Call Bridge、Web Bridge 3、データベースの各コンポーネントのみが搭載されています。内部ネットワークへの導入に適しており、単一サーバーまたは複数サーバーのカスケード構成として導入できます。Cisco Meeting Server 2000 は DMZ ネットワークに展開すべきではありません。一方、導入環境で外部の Cisco Meeting Server ウェブアプリユーザー向けにファイアウォールトラバーサルをサポートが必要な場合は、次のいずれかも導入する必要があります。

- 内部ネットワーク内の Cisco Expressway-C と DMZ 内の Expressway-E、または
- TURN サーバーを有効にした、DMZ に導入する別の Cisco Meeting Server 1000 または仕様ベースの VM サーバーを導入する。

5.3.1.2 Cisco Meeting Server Small/1000 および仕様に基づく VM サーバ

- Cisco Meeting Server 1000 および仕様に基づく VM サーバーは、Cisco Meeting Server 2000 よりも通話容量が低いですが、すべてのコンポーネント(Call Bridge、Web Bridge 3、Database、Recorder、Uploader、Streamer、TURN サーバー)は各ホストサーバーで利用可能です。Web Bridge 3、Recorder、Uploader、Streamer、TURN サーバーは、運用前に有効化が必要です。
- OVA を Vcenter にアップロードして展開するとき、発行者フィールドは「(信頼できる証明書)」を表示する必要があります。OVA のインポート時に、無効な証明書と信頼されていない証明書に関する警告が表示される場合は、次の記事を参照してください：
<https://kb.vmware.com/s/article/84240> OVA に署名するために使用される証明書に対応する中間証明書およびルート証明書を VECS ストアに追加する必要がある場合があります。中間証明書またはルート証明書を入手する場合、またはその他の問題については、[Cisco テクニカルサポート](#)に連絡してください。

6 バグ検索ツール、解決済みおよび未解決の問題

Cisco バグ検索ツールを使用して、問題の説明や利用可能な回避策など、Cisco Meeting Server とウェブアプリの未解決の問題と解決済みの問題に関する情報を検索できるようになりました。これらのリリース ノートにリストされている識別子から、各問題の説明に直接移動できます。

1. ウェブブラウザを使って、[Bug Search Tool](#) にアクセスしてください。
2. cisco.com 登録済みのユーザ名とパスワードでログインしてください。

このドキュメントで言及されている特定の問題に関する情報を検索するには:

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。

識別子を知らない場合に情報を探すには:

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** と入力を開始します。次に、**[リリース(Releases)]** フィールドで **[次のリリースで修正(Fixed in these Releases)]** を選択し、検索するリリース (例: 3.12.2) を入力します。

2. 表示されるバグのリストから、**[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で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。

6.1 Cisco Meeting Server で解決された問題

以前のバージョンで見られた問題で、3.12.2 で修正されています。

Cisco 識別子	概要
CSCws62493	Cisco Unified Communications Manager のクラスター間経由で Meeting Server のミーティングに転送された後、セッションが更新されると、ユーザーの音声が一方向になる問題が発生しました。
CSCwt00859	予期しないデータまたは不完全なデータによるプレゼンスまたはセッション関連の REST 要求の処理中に、競合状態が発生したため、管理プロセスで単発的なセグメンテーションフォールトが発生しました。
CSCwt00875	複数の Meeting Server 2000 サーバーで、短時間のうちにセグメンテーションフォールトによるクラッシュが繰り返し発生しました。クラッシュは、REST ベースのプレゼンスおよびセッションの更新処理中に発生し、Curl ライブラリ内で頻繁に報告されました。
CSCws27917	ユーザーが複数回接続および切断すると、標準画面レイアウトのロゴが SIP デバイスに表示されません。この問題は、接続を繰り返し試行した場合に、SIP エンドポイントでのみ発生します。

以前のバージョンで見られた問題で、3.12.1 で修正されています。

Cisco 識別子	概要
CSCwo73532	Cisco は、タイムスタンプ要求および応答に関連する CVE-1999-0524 で特定された脆弱性の影響を評価しました。Meeting Server 1000 および仮想環境への導入がこの脆弱性の影響を受けます。この問題に対処するため、Meeting Server ソフトウェアにファイアウォールの変更が実装され、問題が解決されています。
CSCwq92494	Meeting Server 2000 で次のエラーが発生してクラッシュします: 「server-!ServerMediaVideoComposition::configureContributors。」 100 人を超える参加者がいる進行中の会議で「参加者ごとのペイン配置」が適用され、「ペインのロール」機能が断続的に切り替えられると、Meeting Server 2000 の Media モジュールが断続的にクラッシュします。
CSCwr28875	Meeting Server 2000 がエラーでクラッシュします: 「server-!ServerMediaCall::writeVideoLayoutContributors」。100 人を超える参加者がいる進行中の会議で「参加者ごとのペイン配置」が適用され、「ペインのロール」機能が断続的に切り替えられると、Meeting Server 2000 の Media モジュールが断続的にクラッシュします。
CSCws26193	Meeting Server で次のエラーが発生してクラッシュします: 「mf_remote_media!dav1d_decoder_flush_frame_buffer [dav1d_interface.cpp.]」。複数の同時開催ミーティングと多数の参加者による高負荷状態のミーティング中に、コンテンツ品質の断続的な問題とメディアフレームワークの再起動が発生することがあります。この問題は、場所に関係なく、Meeting Server で AV1 ビデオコーデックを使用してコンテンツを共有するユーザーに影響します。
CSCwr77696	secure_storage enable コマンドの実行時に表示される警告メッセージが、次のように変更されました。 このコマンドは内部ファイルシステムの仮想 TPM 保護を可能にし、機密データのより強力な保護を実現します。警告: この操作は元に戻せません。進む前に必ず「バックアップ」を作成してください。システムはセキュアストレージの初期化のために再起動します。今すぐ再起動してもよろしいですか? (はい/いいえ)

以前のバージョンで発生していた問題のうち、3.12 で修正された問題。

Cisco 識別子	概要
CSCWq11063	Meeting Server 1000 は稀なケースで時折クラッシュし、以下のエラーが表示されます: 「server!ServerApp1Cmgr::getCallSummary(SfGuid const*, Server- CallOverallSummaryImplementation*)」。
CSCWr82907	LDAP 同期は、ユーザが 1 つの LDAP グループから削除され、その後別のグループに中間同期なしで再追加されると、「重複 cospace URI」エラーで失敗します。これにより、重複する URI によって新しいグループの同期プロセスがブロックされるため、他の LDAP ユーザーの同期が妨げられます。
CSCWr82906	Chrome で 4096x4097 解像度でコンテンツを共有すると、予期せぬコーデック交渉 (CN)が発生し、正しいエラーメッセージが表示されません。
CSCWp22989	Meeting Server 1000 が次のエラー理由で断続的にクラッシュします:「server- !ServerControlCmgrCall::updateConfiguration(ServerCallConfigurationImplementation const*)」(進行中のミーティングから参加者が切断された場合)。
CSCWp16290	まれな状況で、参加者がミーティングに参加すると Meeting Server がクラッシュします。
CSCWp67146	Meeting Server が短時間に連続して発信すると、アウトバウンド SIP 通話が均等に分散されません。
CSCWo68125	Meeting Server のメディアモジュールは、Firefox ブラウザから AV1 コーデックで 4K 以上の解像度でコンテンツを共有するとクラッシュします。
CSCWn13502	Meeting Server のミーティングで、参加者の表示名に含まれる数字のフォントが適切に表示されません。
CSCWk11099	Meeting Server の会議で、16 人を超える参加者がいて、表示名が長く、SIP URI (ディレクトリ URI) およびディレクトリ番号 (DN) が 64 バイトを超えている場合に、Active Control を有効にした SIP エンドポイントまたは Jabber クライアントが参加すると、そのエンドポイントで会議中の他の参加者が表示されないことがあります。 注: Cisco Meeting Server と Cisco Unified Communications Manager (CUCM) との統合の一環として、Jabber 通話用の SIP トランクを設定する際に、 [発信側および接続側情報形式(Calling and Connected Party Info Format)] を [接続された第三者の URI と DN を提供する(Deliver URI and DN in connected party)] に設定する場合は、結合された SIP URI (ディレクトリ URI)とディレクトリ番号 (DN) の合計を 64 バイト未満に抑えることを強く推奨します。これは Jabber が参加者リストを正確に表示し、通話体験を向上させるために重要です。
CSCVw10678	PIN で保護された CoSpace に参加する場合や、ユーザーが IVR 経由で参加する場合に、cospace_join.wav ファイル (「現在ミーティングに入っています」) が 2 回再生されます。

6.2 Cisco Meeting Server における未解決の問題

以下は、このリリースの Cisco Meeting Server ソフトウェアにおける既知の問題です。詳細が必要な場合は、[Bug Search Tool](#) の検索欄に Cisco 識別子を入力してください。

Cisco 識別子	概要
CSCwq73418	サインイン済みのテナントユーザーが cospace のメンバーではない場合、非メンバーのアクセスが許可されていてもミーティングに参加できず、「ミーティングに参加できませんでした。(Meeting join failed.) スケジュールされたミーティングが見つかりません。(Unable to find the scheduled meeting.)」というエラーメッセージが表示されます。
CSCwr81825	ウェブアプリの参加者のみが参加しているミーティングでは、ローテーションペインの参加者が想定どおり 20 秒ごとに切り替わりません。代わりに、ペインの切り替えに最大 1 分かかる場合があります。
CSCwn81355	会議で「ビデオミュートオンエントリー」および「音声ミュートオンエントリー」を有効にすると、SIP 参加者は参加後にビデオや音声のミュートを解除できません。
CSCwn27875	<code>joinToneParticipantThreshold</code> および <code>leaveToneParticipantThreshold</code> パラメータに、設定されている最大値 100 を超える値を指定できます。
CSCwh41791	Meeting Server 2000 で断続的に webbridge にアクセスできませんでした。
CSCwd89530	パケットキャプチャを Ctrl+C で正常に停止せず、ターミナルを突然閉じると、CMS を再起動するまで、それ以降のパケットキャプチャを実行できません。
CSCwb77929	複数の Web Bridge を使用する導入環境では、ウェブアプリの参加者がミーティングノートを表示できるのは、ノートが最初に保存および公開された Web Bridge と同じ Web Bridge に接続している場合のみです。
CSCwa83782	TMS で接続タイプを [自動(Automatic)] にして会議を予約し、参加者の 1 人が管理対象外のデバイスから会議に参加しています。会議の開始時に CMS/TMS からその参加者に発信されますが、Meeting Server によってしばらくすると通話が切断されます。
CSCvz01886	参加者のロールにビデオ共有およびプレゼンテーションの権限がない状態で、ロールを変更してこれらの権限を付与した場合、その参加者がコンテンツを共有しても、他の参加者にプレゼンテーションが表示されません。
CSCvt74033	コンテンツの共有中に、Webex Room Panorama が 2 つのビデオストリームの送信から 1 つのビデオストリームの送信に切り替わるイベントが発生すると、Room Panorama からリモートエンドポイントが受信するビデオのフレームレートが大幅に低下する場合があります。
CSCvh23039	Uploader コンポーネントは、NFS に保存されたテナント録画では機能しません。

6.2.1 既知の制限

- バージョン 3.1 以降、Cisco Meeting Server は TURN の短期認証情報をサポートしています。この動作モードは、バージョン 3.1 以降の Meeting Server TURN サーバーのように、TURN サーバーが短期認証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 を使用する場合、短期認証情報はサポートされません。

6.3 Cisco Meeting Server ウェブアプリで解決された問題

以下の表は、3.12.1 で修正された以前のバージョンで見られた問題を示しています。

Cisco 識別子	概要
CSCws38615	ウェブアプリのホームページのタイトルの位置がずれており、通話情報セクションの電話番号が統一されていないフォントサイズで表示されます。

以下の表は、3.12 で修正された以前のバージョンで見られた問題を示しています。

Cisco 識別子	概要
CSCwo81653	ウェブアプリのミーティングで、チャットウィンドウの [To:] ドロップダウンリストの参加者名がメッセージセクションにはみ出して表示されます。

6.4 Cisco Meeting Server ウェブアプリの未解決の問題

Cisco 識別子	概要
CSCwp96170	「メールまたは招待コピー」画面では、「言語」ドロップダウン内の一部の言語名が正しく表示されていません。
CSCwi05238	参加者がログインするときに、ウェブ アプリに「ログインに失敗しました」というエラーメッセージが一時的に表示されます。
CSCwh48464	ウェブアプリの参加者がビデオに仮想背景を適用した後、ブラウザのタブを更新すると、Google Chrome および Mozilla Firefox ブラウザで仮想背景が黒く表示されます。
CSCwc76769	Google Chrome ブラウザで、参加者がビデオにブラーを適用してウェブ アプリのミーティングを退出しても、カメラはオンのままで、閉じません。
CSCwa17363	ウェブアプリでは、ミーティング管理からロビーに移動された参加者は、ロビーで待機している場合でも、ミーティングの参加者のリストを表示できます。
CSCvz01888	ミーティングの前にメンバーのロールがスペースで変更された場合、メンバーがミーティングに参加するとロールの変更通知が表示されます。

Cisco 識別子	概要
CSCvu98805	Firefox ブラウザの web app からミーティング中に、受信したプレゼンテーションを 2 番目のウィンドウで開くと、プレゼンタが共有を停止してから再開した場合、またはミーティングの別の参加者が同時にコンテンツの共有を開始した場合、コンテンツが応答しくなくなります。これは Firefox ブラウザでの問題です。詳細については、https://bugzilla.mozilla.org/show_bug.cgi?id=1652042 を参照してください。 回避策: 2 番目のウィンドウを最大化するか、またはプレゼンテーションウィンドウを一度閉じてから再度開きます。
CSCvt71069	ビデオレイアウトの「スピーカー大」が選択されている場合、ウィンドウのサイズは正しく変更されません。

付録 A: Meeting Server プラットフォームのメンテナンス

Cisco Meeting Server ソフトウェアが動作するプラットフォームは、最新のアップデートでメンテナンスされ、パッチが適用されていることが重要です。

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

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

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

A.1 Cisco Meeting Server 2000

Cisco Meeting Server 2000 は Cisco UCS 技術に基づいており、仮想化された展開としてではなく、物理的な展開として Cisco Meeting Server ソフトウェアを実行しています。

注意：プラットフォーム (UCS マネージャにより管理される UCS シャシーおよびモジュール) が最新のパッチで最新のものであることを確認します。『[Cisco UCS Manager Firmware Management ガイド](#)』の指示に従います。プラットフォームのメンテナンスを怠ると、Cisco Meeting Server のセキュリティが損なわれる可能性があります。

通話容量

次の表は、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間でのコールキャパシティの比較を示しています。

表 3 : Meeting Server プラットフォーム間のコールキャパシティ

通話のタイプ	Cisco Meeting Server 1000 M6	Cisco Meeting Server Small M7	Cisco Meeting Server 2000 M6
フル HD 通話 1080p60 ビデオ 720p30 コンテンツ	40	60	324
フル HD コール 1080p30 ビデオ 1080p30/4K7 コンテンツ	40	60	324
フル HD 通話 1080p30 ビデオ 720p30 コンテンツ	80	120	648
HD 通話 720p30 ビデオ 720p5 コンテンツ	160	240	1296
SD 通話 480p30 ビデオ 720p5 コンテンツ	320	480	1875
音声通話 (G.711)	3000	3000	3200

注 : Meeting Server Small M7 バリエントは、最大 94 個の vCPU と 128 GB の RAM をサポートします。

次の表では、単一またはクラスタ化された Meeting Server の通話容量と、Call Bridge グループ内で通話をロードバランシングする場合の通話容量を比較しています。

表 4: クラスタと Call Bridge グループのミーティング サーバーの通話キャパシティ

Cisco Meeting Server プラットフォーム		Cisco Meeting Server Small M7 (ノードあたり)	Cisco Meeting Server 2000 M6 (ノードあたり)
個別の会議サーバーまたは クラスタ内の Meeting Servers (注 1、2、3 および 4) と Call Bridge グループの Meeting Server	1080p30	120	648
	720p30	240	1296
	音声通話	3000	3200
	会議あたりサーバあたり HD 参加者数		
	web app の通話容量 (内線通話 & CMS での外部呼び出し Web Edge での外部通話):		
	フル HD	120	648
	HD	240	1296

Cisco Meeting Server プラットフォーム		Cisco Meeting Server Small M7 (ノードあたり)	Cisco Meeting Server 2000 M6 (ノードあたり)
	SD 音声通話	480 3000	1875 1875
Call Bridge グループの Meeting Server	サポートされているコール タイプ		
	読み込み制限	240,000	1,296,000

注意すべき点：

- クラスタあたり最大 24 個の Call Bridge ノード。8 個以上の Call Bridge ノードのクラスタ設計はシスコによる承認が必要です。詳細については Cisco Support にお問い合わせください。
- Call Bridge グループが設定されていないクラスタ化された Cisco Meeting Server 2000 は、最大通話数の整数倍（たとえば、700 HD 通話の整数倍）をサポートします。
- クラスタあたり最大 21,000 HD 同時通話（24 ノード x 875 HD 通話）は、SIP または web app の通話に適用されます。
- クラスタ内の Meeting Servers プラットフォームに応じて、クラスタあたり会議あたり最大 2600 人の参加者。
- 表 4 では、ビデオコールについては最大 2.5 Mbps-720p5 コンテンツ、音声コールについては G.711 のコールレートを想定しています。他のコーデックおよび高いコンテンツ解像度/フレームレートを使用すると、容量が減ります。会議が複数のコールブリッジをまたぐ場合、自動的に配信リンクが作成され、サーバーの通話数や容量にもカウントされます。読み込み制限値は H.264 のみに対するものです。
- クラスタでサポートされている通話セットアップレートは、SIP 通話で 1 秒あたり最大 40 通話、Cisco Meeting Server web app 通話で 1 秒あたり最大 20 通話です。
- Meeting Server Small M7 バリエーションは、最大 94 個の vCPU と 128 GB の RAM をサポートします。

Cisco Meeting Server web app のコールキャパシティ

この項では、外線および混合通話に Web Bridge 3 とウェブアプリを使用した導入のコールキャパシティについて詳しく説明します。（内線コールキャパシティについては、表 4 を参照してください。）

Cisco Meeting Server web app のコールキャパシティ - 外線通話

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

Cisco Meeting Server のウェブエッジソリューションの利用についての詳細は [Cisco Meeting Server Deployment Guides](#) をご覧ください。

外部通話とは、クライアントが Cisco Meeting Server のウェブエッジや Cisco Expressway をリバースプロキシおよび TURN サーバーとして使用し、Web Bridge 3 および Call Bridge に接続することです。

Expressway を使用してウェブアプリの通話をプロキシする場合、Expressway は、下の表に示すように、最大通話数制限をかけます。

注： Web Bridge 3 および web app を導入する場合、Expressway バージョン X14.3 以降を使用する必要があります。以前の Expressway バージョンは Web Bridge 3 ではサポートされません。

表 5: Cisco Meeting Server ウェブアプリの通話容量 – 外部通話に Expressway を使用する場合

設定	コールタイプ	CE1200 プラットフォーム	大規模 OVA Expressway	中規模 OVA Expressway
Cisco Expressway あたり (X14.3 以降)	フル HD	150	150	50
	その他	200	200	50

Expressway 容量は、Expressway ペアをクラスタ化することで増やすことができます。Expressway ペアクラスタリングは最大 6 ノードまで可能で（4 はスケーリングに、2 は冗長性に使用されます）、合計コールキャパシティはシングルペアキャパシティの 4 倍になります。

注: Expressway クラスタの通話セットアップレートは、Cisco Meeting Server ウェブアプリの通話で 1 秒あたり 6 通話を超えてはなりません。

Cisco Meeting Server ウェブアプリの容量 – 混合 (内部 + 外部) 通話

スタンドアロン導入とクラスター導入の両方で、組み合わせた内部と外部の通話使用をサポートできます。 内部および外部の混合参加者をサポートする場合、ウェブアプリの合計容量は、内部通話については表 4 に従い、外部通話に Cisco Meeting Server Web Edge ソリューションを使用する場合も同様です。 ただし、エッジで Expressway を使用する場合、外部から接続できる参加者数は、合計参加者数の範囲内であっても、表 5 の制限を受けます。

例えば、単一の大規模 OVA Expressway ペアを持つ単一のスタンドアロン Meeting Server 2000 は、1000 の音声のみの Web App コールの混在をサポートしますが、外部の参加者の数は、合計 1000 のうちの最大 200 に制限されます。

メモ: 通話中に、通話を外部エンドポイントに移動したり、音声を通常の電話に移動したりすることはできません。

付録 B: アプリ機能の比較

表 6: Cisco Meeting Server ウェブ アプリの機能比較

機能	ウェブアプリ 3.12	ウェブアプリ 3.11	ウェブアプリ 3.10	ウェブアプリ 3.9
全般				
Cisco Meeting Server のバージョン	3.12	3.11	3.10	3.9
メンバーのアクセスを管理する	はい	はい	はい	はい
ユーザーレベルの権限（スペースの作成など）	はい	はい	はい	はい
ローカリゼーションのサポート	はい	はい	はい	はい
ブランディング	はい	はい	はい	はい
オンラインヘルプ	はい	はい	はい	はい
暗号化（Encryption）	はい	はい	はい	はい
シングルサインオン	はい	はい	はい	はい
オンラインヘルプでのカスタムページのサポート	はい	はい	不可	不可
刷新されたユーザインターフェース(色、フォント、アイコン)	はい	不可	不可	不可
ビデオ アドレス (URI) を使って参加する	はい	はい	はい	はい
通知				
参加者が参加/退出した際の音声通知	はい	はい	はい	不可
接続の復元性（不良ネットワークでの自動再接続）	はい	はい	はい	はい
Web App セッションのタイムアウト	はい	不可	不可	不可
ミーティングのスケジュール設定				
スケジュール済みミーティングの一覧を表示	はい	はい	はい	はい

機能	ウェブアプリ 3.12	ウェブアプリ 3.11	ウェブアプリ 3.10	ウェブアプリ 3.9
ミーティングのスケジュール設定	はい	はい	はい	はい
予定された会議を修正する	はい	はい	はい	はい
スケジュール済みミーティングを削除	はい	はい	はい	はい
スペース管理				
スペース メンバーの役割	はい	はい	はい	はい
メンバー限定スペースのミーティング招待リンク	はい	不可	不可	不可
メンバー以外のスペースへのアクセスを制限する	はい	はい	はい	不可
スペースの作成/編集	はい	はい	はい	はい
新しく提供された スペースを有効にする	はい	はい	はい	はい
スペース メンバーの追加/編集/削除	はい	はい	はい	はい
メンバーの追加機能のためのディレクトリ検索	はい	はい	はい	はい
スペースの情報を表示する	はい	はい	はい	はい
招待状を送信	はい	はい	はい	はい
音声と映像				
音声	OPUS	OPUS	OPUS	OPUS
ビデオ	H.264、VP8	H.264、VP8	H.264、VP8	H.264、VP8
マイク/カメラ設定コントロール	はい	はい	はい	はい
スピーカー構成のコントロール	はい	はい	はい	はい
バックグラウンドのぼかし	はい	はい	はい	はい
仮想背景	はい	はい	はい	はい
遠端カメラ制御	はい	はい	はい	はい
音声とビデオの自動優先順位付け	はい	はい	はい	はい

機能	ウェブアプリ 3.12	ウェブアプリ 3.11	ウェブアプリ 3.10	ウェブアプリ 3.9
画面共有				
コンテンツの拡大	はい	はい	はい	はい
コンテンツのズームをリセット	はい	はい	はい	はい
画面共有を表示	はい	はい	はい	はい
デスクトップ共有	はい	はい	はい	はい
アプリケーション共有	はい	はい	はい	はい
新しいウィンドウで画面共有を表示する	はい	はい	はい	はい
ビデオペインのサイズを変更する	はい	はい	はい	はい
コンテンツの音声を共有	はい	はい	はい	はい
テキスト用に最適化 (1080p での共有画面)	はい	はい	はい	はい
チャット				
チャット (ミーティングのすべての参加者にブロードキャスト)	はい、ミーティングのみ	はい、ミーティングのみ	はい、ミーティングのみ	はい、ミーティングのみ
チャット (プライベート)	はい、ミーティングのみ	はい、ミーティングのみ	はい、ミーティングのみ	はい、ミーティングのみ
チャット履歴をエクスポート	はい	不可	不可	不可
通話中				
画面上のメッセージ	はい	はい	はい	はい
全画面表示	はい	はい	はい	はい
レイアウト制御	はい	はい	はい	はい
名前ラベル	はい	はい	はい	はい
録音	はい	はい	はい	はい
ストリーミング	はい	はい	はい	はい
発言者のラベル (ベータサポート)	はい	はい	はい	はい
セルフ	はい	はい	はい	はい
セルフ ビューのピン留め	はい	はい	はい	はい
セルフ ビューをミラーリングする	はい	はい	はい	はい

機能	ウェブアプリ 3.12	ウェブアプリ 3.11	ウェブアプリ 3.10	ウェブアプリ 3.9
セルフビューを移動	はい	はい	はい	はい
HD/SD の選択	はい	はい	はい	はい
プレゼンテーションのプレビューをピン留めする	はい	はい	はい	はい
プレゼンテーションプレビューを移動	はい	はい	はい	はい
ミーティングメモ	はい	はい	はい	はい
クローズドキャプション	はい	はい	はい	はい
ファイルを共有する	はい	はい	はい	はい
ネットワーク状態インジケータとメディア統計	はい	はい	はい	はい
コンテンツの共有のメトリック	はい	はい	はい	はい
ロゴのサポート	はい	はい	はい	はい
アンケート	はい	はい	はい	はい
参加者				
参加者の名前の変更	はい	不可	不可	不可
参加者名の文字数制限増加	はい	はい	不可	不可
参加者リストでのユーザー識別	はい	はい	不可	不可
参加者リストで設定可能なユーザーインジケータ	はい	不可	不可	不可
参加者を移動	はい	はい	はい	はい
参加者を追加	はい (SIP のみ)	はい (SIP のみ)	はい (SIP のみ)	はい (SIP のみ)
参加者を削除する	はい	はい	はい	はい
ロックされたミーティングに参加者を許可する	はい	はい	はい	はい
参加者のロールを変更する	はい	はい	はい	はい
重要な参加者に指定	はい	はい	はい	はい
他の参加者の音声とビデオを個別にミュート/ミュート解除	はい	はい	はい	はい

機能	ウェブアプリ 3.12	ウェブアプリ 3.11	ウェブアプリ 3.10	ウェブアプリ 3.9
すべての参加者の音声とビデオをミュート/ミュート解除	はい	はい	はい	はい
ミーティング中に診断を送信する	はい	はい	はい	はい
招待を送信	はい	はい	はい	はい
通話情報を表示	はい	はい	はい	はい
通話中のマイク / カメラの操作	はい	はい	はい	はい
挙手	はい	はい	はい	はい
通話を移動				
このデバイスを画面共有と通話の管理のみに使用します (別のデバイスは音声とビデオに使用されます)	はい	はい	はい	はい

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 用の自主的製品アクセシビリティテンプレート(VPAT)はこちらで入手可能です:

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、

www.cisco.com/web/about/responsibility/accessibility/index.html で詳細情報を見つけることができます。

アクセシビリティサポート機能

キーボードナビゲーション

キーボードを使用して web app 内を移動することができます。

- Web アプリ内の領域間を移動するには、Tab を使用します。輪郭で囲まれた領域にフォーカスが合っていることがわかります。
Shift + Tab を使用すると、前にフォーカスしていた領域に移動できます。
- スペースバーまたは Enter キーを押して項目を選択します。
- 矢印キーを使用して、リストまたはドロップダウンリスト メニューをスクロールします。
- Esc を使用すると、開いている画面やメニューを閉じる、または解除できます。

スクリーンリーダーのサポート

JAWS スクリーンリーダーのバージョン 18 以降を使用できます。

スクリーンリーダーは、フォーカスされている領域/ボタン、通知、警告、画面に表示されるステータスメッセージなどの関連情報、および実行できるアクションを通知します。

たとえば、Web アプリ会議の **参加者の追加** 領域にフォーカスすると、スクリーンリーダーによって「参加者の追加」が読み上げられ、参加者の SIP アドレスを入力するように求められます。

Cisco の法的情報

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

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

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

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズ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システムズまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

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

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

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。

© 2026 Cisco Systems, Inc. All rights reserved.

Cisco の商標または登録商標

Cisco および Cisco ロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。Cisco の商標の一覧を表示するには、次の URL にアクセスしてください: www.cisco.com/go/trademarks。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1721R)