Cisco Meeting Server

Cisco Meeting Server Release 2.7.1

リリース ノート

2020 年 2 月 20 日

目次

変更事項

バージョン	変更内容
2019 年 12 月 6 日	解決済みの問題が更新されました。（ドキュメントの省略）
2019 年 12 月 3 日	OVA ファイルのハッシュが追加されました。
2019 年 11 月 29 日	アップグレードの項に、Cisco Meeting Server 2000 の loadLimit 値の変更に関する注意点が追加されました。
2019 年 11 月 28 日	1 番目のメンテナンス リリース。 Yandex および Chromium ベースの Microsoft Edge ブラウザのベータ サポート、および会議に参加するためのオプションが新しく導入されました。 2.7.1 で解決済みの問題を参照してください。 ハッシュが更新されました
2019 年 9 月 19 日	解決済みの問題が更新されました（ドキュメントの省略）。
2019 年 8 月 28 日	解決済みの問題が更新されました（ドキュメントの省略）。
2019 年 8 月 13 日	Cisco Meeting Server ソフトウェアの新規リリース。

1 はじめに

これらのリリース ノートでは、Cisco Meeting Server ソフトウェアのリリース 2.7 の新機能、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、次でホストできます。

- 8 B200 ブレードと Meeting Server ソフトウェアをソウル アプリケーションとしてプレインストールした Cisco Meeting Server 2000、UCS 5108 シャーシ。
- Cisco Meeting Server 1000、VMware を使用して事前設定済みの Cisco UCS サーバおよび VM 導入としてインストールされた Cisco Meeting Server。
- Acano EX 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。

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、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 コマンド リファレンス ガイド』を参照してください。

注意：バージョン 2.7 にアップグレードすると、データベース クラスタの操作に影響する場合があります。バージョン 2.7 にアップグレードする前に、同じ認証局によって署名されたクライアント証明書とサーバ証明書が、クラスタ内のデータベース ノードを保持または接続している各 Meeting Server にアップロードされていることを確認します。詳細については、第 2.4 項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。

着信コールに関する注意：デフォルトでは、着信コールは許可されていません。
Cisco Meeting App ユーザへの着信コールを許可するには、API オブジェクト **`/user/profiles/<user profile id>`** のパラメータ **`canReceiveCalls=true`** を設定します。

1.1 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。

1.1.1 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。

注：Cisco Meeting Server ソフトウェアを実行している仮想プラットフォームが最新のパッチで更新されていることを確認するようにお勧めしますが、Cisco Meeting Server 1000 M5 のみを ESX 6.7 または ESXi 6.5 Update 2 にアップグレードする必要があります。詳細についてはこちらを参照してください。

1.1.2 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。

注：2019 年 8 月頃から、新しい Cisco Meeting Server 2000 でファブリック インターコネクト フェールオーバーがデフォルトで有効になる予定です。ただし、手動でデバイスを設定してフェールオーバーを有効にする必要がある場合は、こちらを参照してください。

1.1.3 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 1：コール キャパシティ

コールのタイプ	Cisco Meeting Server 2000	Cisco Meeting Server 1000
フル HD 通話（1080p30）	350	48
HD 通話（720p30）	700	96
SD 通話（448p30）	1000	192
音声通話	3000	3000

以下の表 2 では、単一またはクラスタの 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 バランシングとを比較しています。

表 2：ソフトウェア バージョン 2.6 以降の 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	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	48 96 192 3000	350 700 1000 3000
	サーバごとの会議あたりの HD 参加者数	96	450
	Web Bridge ごとの WebRTC 接続数	100	100
Call Bridge グループの Meeting Server	サポートされているコール タイプ	着信 SIP 発信 SIP Cisco Meeting アプリ	
	1080p30 720p30 SD 音声 負荷制限	48 96 192 3000 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	450
	Web Bridge ごとの WebRTC 接続数	100	100

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

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。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。

1.2 Cisco ミーティング アプリケーション WebRTC 重要事項

WebRTC アプリの機能がリリースされる時期、および WebRTC アプリに対して修正される時期の詳細については、『Cisco ミーティング アプリケーション WebRTC 重要な情報』ガイドを参照してください。WebRTC アプリに関連するすべての情報は、1 つのガイドにまとめられており、Meeting Server リリース ノートには含まれていません。

このガイドの構成は、次のとおりです。

- WebRTC アプリの新機能または変更された機能、およびこの機能/修正が利用可能な Meeting Server のバージョンを示す WebRTC アプリに関連する修正された問題と未解決の問題の詳細。
- WebRTC アプリに影響するブラウザの今後の変更、および推奨される回避策を含むアプリの影響を受けるバージョン。

WebRTC はまだ進化している技術であり、ブラウザ ベンダーによって頻繁に変更が実装されています。『Cisco ミーティング アプリケーション WebRTC 重要な情報』ガイドは、今後の変更をお知らせする必要がある場合に更新されます。

注：Cisco Meeting Server の Web アプリを使用している場合（つまり、Web Bridge 3 を導入している場合）は、『Cisco Meeting Server Web アプリ バージョン 2.9.0 重要事項』を参照してください。

1.3 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 2.7 のリリースで、シスコは、表 3 に記載されているソフトウェアのソフトウェア メンテナンス終了に関するタイムラインを発表します。

表 3：Cisco Meeting Server バージョンのソフトウェア メンテナンス終了に関するタイムライン

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 2.5.x	Cisco Meeting Server バージョン 2.7 の最初のリリースの 4 ヵ月後。

Cisco Meeting Server に関するシスコのソフトウェア 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 2.7 の新機能/変更点

Meeting Server ソフトウェアのバージョン 2.7 には、次のものが追加されています。

- バージョン 2.4 で最初に導入されたペイン配置機能の機能拡張
- Lync/Skype for Business クライアントと非 Lync クライアント（SIP エンドポイントおよび Cisco Meeting App ユーザ）の間で共有するコンテンツのパフォーマンス改善
- データベース クラスタ内のデータベース クライアントとデータベース サーバでの証明書の使用の強制
- Meeting Server の使用率を把握する目的で syslog に追加された使用率統計情報
- Web 管理インターフェイスの **[詳細トレース（Detailed tracing）]** ページに追加された ICE トレース。Meeting Server の Web 管理インターフェイスにログインします。**[ログ（Logs）]** > **[詳細トレース（Detailed tracing）]** に移動し、下にスクロールして ICE トレースを検索します。次に、適切な [有効（Enable）] ボタンを選択します。これらの新しい有用性機能は、問題の診断においてシスコのサポートを支援します。

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

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

2.1 バージョン 2.7.1 で導入された新機能

2.1.1 WebRTC アプリでの Yandex ブラウザのベータ サポート

バージョン 2.7.1 では、Windows 上で Yandex ブラウザを使用する WebRTC の Cisco Meeting App のベータ サポートが導入されています。これは、現在のバージョンではベータ版です。

2.1.2 WebRTC アプリでの Chromium ベースの Microsoft Edge ブラウザのベータ サポート

バージョン 2.7.1 では、Windows 上で Chromium ベースの Microsoft Edge ブラウザを使用する WebRTC の Cisco Meeting アプリのベータ サポートが追加されています。これは、現在のバージョンではベータ版です。

2.1.3 WebRTC アプリのマイクまたはカメラなしでのオプション参加

バージョン 2.7.1 では、いくつかの新しい通話参加オプションが導入されています。

会議に参加している間、**[参加オプション（Joining options）]** 画面から [カメラなし（no camera）] または [マイクなし（no microphone）] を選択できるようになりました。これは、カメラやマイクに障害があり、通話中の他の参加者を表示したり聞いたりできるが、他の参加者が自分を見たり聞いたりできない場合に役立ちます。

注：会議中にオプションを変更することは推奨されません。

ミーティング中にカメラまたはマイクを追加するには、次の手順を実行します。

1. **[戻る（Back）]** をクリックして、メイン画面に移動します。まだ会議に参加しています。
2. [] をクリックして **[設定（Settings）]** 画面を開きます。表示されたオプションから [カメラ（camera）] と [マイク（microphone）] を選択します。
3. **[会議に戻る（Return to meeting）]** をクリックして、[会議中（in-meeting）] の画面に戻り、選択した新しいオプションを使用して会議を続行します。

2.2 ペイン配置機能の改善

バージョン 2.4 で API ペイン配置機能が導入され、Meeting Server 上のスペースに入るエンドポイントの画面のペイン上に表示される参加者を制御できるようになりました。この機能は、バージョン 2.7 で拡張され、次の拡張機能が追加されています。

- **`panePlacementHighestImportance`** を、**`/coSpaces`** の他に **`/call`** 用にも設定できるようになりました。
- 重要度レベルが割り当てられた参加者を有効にして、ペイン レイアウト内に表示される自分のセルフ ペインを確認できるようにするセルフ ペイン モード。

さらに、バージョン 2.7 以降、Cisco Meeting Management では、アクティブ コールへのペイン配置とセルフビューの適用がサポートされています。詳細については、『Cisco Meeting Management 2.7 User Guide for Video Operators』を参照してください。Cisco Meeting Management では、スペース上のペインの配置はサポートされていません。

本項の情報は、『Cisco Meeting Server 2.7 Administrator Quick Reference Guide』の「Screen Layouts and Pane Placement」にも記載されています。

panePlacementHighestImportance2.2.1 の拡張機能

バージョン 2.7 では、**/calls** ノードで API メソッド POST を使用して新しいコールを作成する場合と、**/calls/<call id>** に PUT を使用してアクティブ コールを作成する場合に、API パラメータ **panePlacementHighestImportance** が適用されるようになりました。

/calls の **panePlacementHighestImportance** では、**/coSpaces** の **panePlacementHighestImportance** と同じ機能が提供されますが、次の優先順位が追加されます。

- **/calls** の **panePlacementHighestImportance** に設定された値を使用する
- **/call** の **panePlacementHighestImportance** が設定されていない場合は、/coSpace の **panePlacementHighestImportance** に設定された値を使用する（コールがスペースに対する場合）
- **panePlacementHighestImportance** が依然として設定されない場合は、ペインの配置を無効にする

panePlacementHighestImportance パラメータが画面レイアウトのペイン数より少ない値に設定されている場合、重要な参加者用として未使用になっている残りのペインは、重要度が割り当てられていない参加者によって取得され、引き続き動的に割り当てられます。

注：アクティブ コールで **panePlacementHighestImportance** を設定しても、そのコールにしか適用されず、コール間では保持されません。これは、コール間で保持される特定のスペースでの **panePlacementHighestImportance** パラメータの設定とは異なります。

注：ペインの配置が **/coSpace** レベルでアクティブ化されている場合、**/call** レベルでは非アクティブ化できません。

2.2.2 セルフ ペイン モード

セルフ ペイン モードは、バージョン 2.4 で導入されたペイン配置の拡張機能です。ペイン配置と同じ配置ロジックに従いますが、重要な参加者のエンドポイントに表示されるレイアウト内に重要な参加者のセルフ ペインを表示する機能が追加されています。セルフ ペイン モードは、Call Bridge クラスタ全体でサポートされています。

2.7 より前のバージョンでは、重要な参加者が自分自身をペイン上に表示することができず、無視される形でエンドポイントのペイン レイアウト内に表示されることはありませんでした。その結果、重要な参加者には他の参加者とは異なるレイアウトが表示されていました。バージョン 2.7 以降、コールまたはスペースに **panePlacementSelfPaneMode** パラメータを設定する管理者は、重要度レベルが割り当てられた参加者のレイアウトに「セルフ（自分自身の）」ペインを表示するか、空白のペインを表示するか、無視するかを選択できるようになりました。**panePlacementSelfPaneMode** パラメータをセルフまたは空白に設定し、**panePlacementHighestImportance** の値を設定して、選択した画面レイアウトのペイン数に一致するようにすると、コールまたはスペースに入るすべての SIP エンドポイントでペインの配置を固定できる効果があります。

セルフ ペイン モードを使用している場合は、各重要度レベルを 1 人の参加者のみに割り当てることをお勧めします。1 つの重要度レベルを複数の参加者に割り当てると、誤ったセルフ ペインが参加者に表示される可能性があります。

panePlacementHighestImportance パラメータがレイアウトのペイン数より少ない値に設定されている場合、重要な参加者用として未使用になっている残りのペインは、重要度が割り当てられていない参加者によって取得され、引き続き動的に割り当てられます。同様に、選択したレイアウトのペイン数が、重要度が割り当てられた参加者の数より少ない場合は、最も重要度の高いレベルが割り当てられている参加者のみがペインに表示され、セルフ ペインのみが表示されます。

通常、セルフ ペイン モードは画面レイアウトの設定と組み合わせて使用され、参加者による、**/dtmfProfiles** を使用した画面レイアウトの変更はできません。

API を使用して、**panePlacementSelfPaneMode** を次に設定します。

- 既存の特定のスペース。要求パラメータ **panePlacementSelfPaneMode** を **self**、**skip**、**blank** に設定するか未設定にして **/coSpaces/<coSpace id>** へ PUT メソッドを使用します。以下を参照してください。
- 新しいスペース。要求パラメータ **panePlacementSelfPaneMode** を選択した値に設定して /coSpaces へ POST メソッドを使用します。
- すでに存在しているアクティブ コール。要求パラメータ **panePlacementSelfPaneMode** を選択した値に設定して **/calls/<call id>** へ PUT メソッドを使用します。
- 作成中の新しいコール。要求パラメータ **panePlacementSelfPaneMode** を選択した値に設定して **/calls** へ POST メソッドを使用します。

panePlacementSelfPaneMode パラメータでは、次の値を使用できます。

self：重要度が設定された参加者は、ペイン レイアウトの特定のペインに自分自身が表示されます。

skip：2.7 以前のバージョンの動作と同じです。ビューアごとに、画面レイアウトでセルフ ペインがスキップされ、次の重要な参加者のペインが表示されます。

blank：重要な参加者を表示せずに、ペインを空白のままとします。これにより、重要な参加者は他のすべてのビューアと同じペインの配置で表示されます。

panePlacementSelfPaneMode パラメータの値が設定されていない場合、セルフ ペイン モードは次の優先順位に従います。

- **/calls** の **panePlacementSelfPaneMode** に設定された値を使用する
- **/call** の **panePlacementSelfPaneMode** が設定されていない場合は、/coSpace の **panePlacementHighestImportance** に設定された値を使用する（コールがスペースに対する場合）
- **/coSpace** の **panePlacementSelfPaneMode** も設定されていない場合は、上記で定義した**スキップ**の動作に戻る

デフォルトでは、**panePlacementSelfPaneMode** パラメータ値が未設定のままとなっています。

セルフ ペイン モードの設定セルフ ペイン モードを使用するには、次の手順を実行します。

1. コールまたはスペースに適した参加者の重要度レベルを設定します。
2. **panePlacementHighestImportanc** パラメータの値を設定します。注：**panePlacementHighestImportance** が設定されていない場合は、セルフ ペイン モードが有効になりません。
3. **/coSpaces**、**/coSpaces/<coSpace id>**、**/calls**、または **/calls/<call id>** で、必要に応じて **panePlacementSelfPaneMode** を **self**、**skip**、**blank** に設定するか、**<unset>** にします。

注：参加者に **panePlacementHighestImportance** に設定された値よりも大きい重要度レベルが割り当てられている場合、その参加者はセルフ ペインに表示されません。セルフ ペインは、重要度が **panePlacementHighestImportance** 以下に設定された参加者のエンドポイント レイアウトにのみ含まれます。ただし、重要度の値が **panePlacementHighestImportance** より大きい参加者であっても、引き続き他の参加者には表示されます。

注：参加者ラベルがオンになっている場合、その参加者ラベルがセルフ ペインに表示されます。

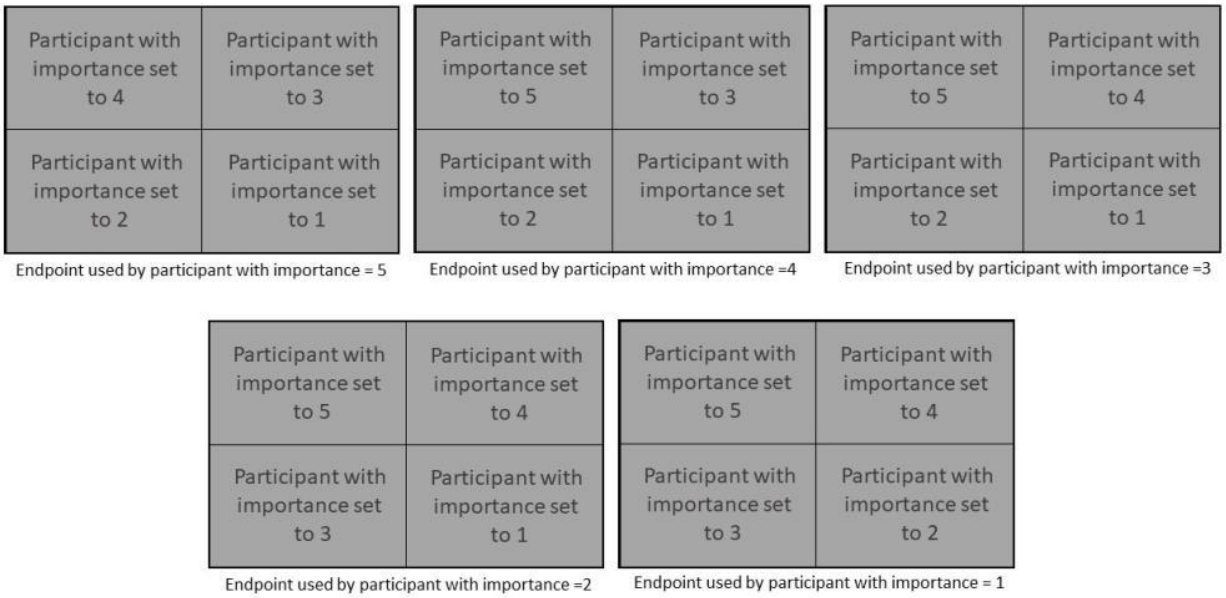
注：「セルフ ビュー」のないエンドポイントを使用している参加者は、自分のセルフ ペインを使用してそのペイン内で正しくフレーム化されるようにできますが、参加者がセルフビューをローカルに表示できるエンドポイントで、このようにセルフ ペインを使用することはお勧めしません。セルフ ペインのビデオ ストリームがトランスコードされ、遅延が増えるため、セルフ ペインの品質をローカルで表示されるセルフビューと同等に保つことができなくなります。

例

以下の図 1 および図 2 に、同じコールにダイヤルインしている 5 人の参加者が使用する、SIP エンドポイントのペイン レイアウトを示します。この例では、次のように想定しています。

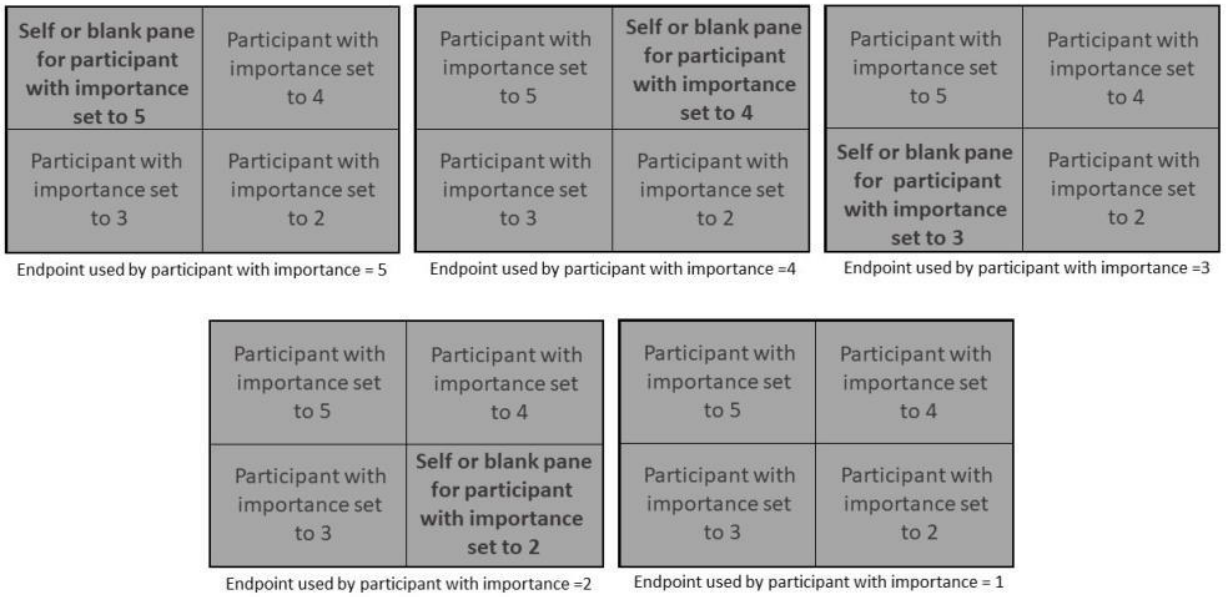
- 各エンドポイントは、固定された 2x2 レイアウトで **allEqualQuarters** 画面レイアウトを使用するように設定されています。
- 各参加者は、コールにダイヤルインするときに 5 ～ 1 の一意の重要度レベルが設定されています。
- コールの **panePlacementHighestImportance** は 5 です。
- **panePlacementSelfPaneMode** は **skip**、**self**、または **blank** のいずれかに設定されています。

図 1：skip（デフォルト モード）に設定された panePlacementSelfPaneMode



panePlacementSelfPaneMode を **skip** に設定すると、5 つのエンドポイントにそれぞれ異なるペイン レイアウトが表示されます。

図 2：`self` または `blank` に設定された `panePlacementSelfPaneMode`



`panePlacementSelfPaneMode` を **`self`** または **`blank`** に設定すると、5 つのエンドポイントに固定レイアウトが表示されます。重要度が 1 に設定されている参加者は、5 つのエンドポイントのいずれにも表示されず、他の重要度が設定されていない参加者がコールに参加した場合は、使用するエンドポイントで、重要度が 1 の参加者と同じペイン配置が表示されます。

2.3 Remote Desktop Protocol（RDP）の機能改善

バージョン 2.7 では、Microsoft Lync/Skype for Business/Office365 クライアントから Meeting Server に接続されたクライアントにコンテンツを共有する機能が強化されています。この機能強化では、Graphics Pipeline Extension をサポートする Skype クライアントが必要です。共有されるコンテンツによっては、初期コンテンツの共有が 4 倍速いか、フレーム レートが 4 倍向上する可能性があります。このパフォーマンスの向上によって、Graphics Pipeline Extension が Skype クライアントでサポートされている場合にフレームあたりの帯域幅が減少します。最新の Windows の Skype クライアントでは Graphics Pipeline Extension をサポートしていますが、Mac iOS の Skype クライアントではサポートされていません。

2.4 データベース クラスタに必要な証明書

バージョン 2.7 以降、データベース クラスタでは、クラスタ内のデータベースに保持または接続する各 Meeting Server に設定された CA と同じ CA によって署名されたクライアント証明書およびサーバ証明書が必要になります。証明書の使用を必須にすることで、クラスタ全体の機密性と認証の両方が確保されます。

すでに証明書が設定されている場合は、アップグレード時に引き続き使用できるようにする必要があります。証明書の要件に変更はありません。唯一の変更点は、2.7 以降証明書の設定が必須になったということです。

注：データベース クラスタに含まれない、ローカル モードで実行されるデータベースでは、証明書の設定は必要ありません。本項の「注意」に記載された内容は、ローカル モードには適用されません。

注意：クラスタを構成するデータベース ノードは、正規のノードのみがクラスタに接続できるように、信頼されたルート CA 証明書を使用して構成する必要があります。ノードは、信頼されたルート証明書で終わる証明書チェーンを提供する接続を信頼するようになります。したがって、各データベース クラスタは専用のルート証明書を使用する必要があります。ルート証明書や中間証明書を他の目的で使用することはできません。

注意：証明書を必要としない旧バージョンの Meeting Server ソフトウェアを使用して、証明書を使用せずにデータベース クラスタが構成されている場合、バージョン 2.7 にアップグレードするとデータベースが停止し、証明書が構成されデータベース クラスタが再作成されるまでアクセスできなくなります。

証明書は、無効になっているデータベース クラスタにのみ割り当てることができます。すでにデータベース クラスタを設定済みである場合は、クラスタ内のすべてのサーバで **`database cluster remove`** コマンドを実行し、ホスト サーバに証明書をアップロードおよび割り当てるコマンドを実行してからクラスタを再作成してください。証明書および証明書バンドルを作成、アップロードして、データベース クラスタに割り当てる方法については、『Certificate Guidelines』を参照してください。
この変更をサポートする方法

- **database cluster initialize**、**database cluster join**、および **database cluster connect** の各コマンドは、有効な証明書、キー、および CA 証明書がデータベース クライアントとサーバにアップロードされていないと実行されません。これを有効化するため、メッセージが送信されます。
- **database cluster status** コマンドは、構成済みの証明書がない場合に強調表示されます。

2.4.1 新規のエラー メッセージ

エラー：証明書を構成する必要があります（FAILURE: certificates must be configured）

データベース クラスタの作成、結合、または接続時に表示され、このデータベース サーバまたはクライアントで証明書が構成されていないことを示します。

2.4.2 更新された pki コマンドと新規の pki コマンド

データベース クラスタ証明書が 2.7 以降必須となりました。Meeting Server でデータベース クラスタのセットアップを簡単に行うには、次のようなデータベース クラスタの署名付き証明書を作成する更新/新規 pki コマンドがあります。

- **pki selfsigned <key/cert basename>[<attribute>:<value>]**
- **pki sign <csr/cert basename><CA key/cert basename>**

注：これらの更新された pki コマンドおよび新規の pki コマンドは、証明書を作成する方法として新たに追加されました。引き続き、openssl などの他の方法を使用して証明書を作成することもできます。詳細については、『証明書のガイドライン』を参照してください。

2.4.3 pki コマンドを使用したデータベース クラスタ用証明書の作成

2.7 以降、新規/更新 pki コマンドを使用して、MMP からすべての証明書を直接生成できるようになりました。Meeting Server でローカル秘密キーおよび自己署名証明書を生成する手順は次のとおりです。

1. MMP にログインして次のコマンドを入力します。

   次に例を示します。

   pki selfsigned dbca CN:"My company CA"

   DBCA.key という名前のローカル秘密キーと、dbca.crt の共通名 **CN=My Company CA** を使用した自己署名証明書を作成します。

2. データベース サーバの秘密キーと証明書要求ファイルを作成します。データベース クラスタ内のすべてのサーバで同じ証明書を使用できます。この場合は、CN フィールドにいずれかのサーバの FQDN を指定し、SAN フィールドに他のサーバの FQDN を指定します。

   次に例を示します。

   ```
   pki csr dbserver CN:server01.db.example.com
   subjectAltName:server02.db.example.com
   ```

   で、dbserver.csr という名前の CSR ファイルと dbserver.key という名前の秘密キーを生成します。

3. データベース クライアントの秘密キーと証明書要求ファイルを作成します。データベース クライアントの CommonName（CN）は「postgres」である必要があります。

   次に例を示します。

   ```
   pki csr dbclusterclient CN:postgres
   ```

   dbclient.csr という名前の CSR ファイルと dbclient.key という名前の秘密キーを生成します。

4. dbserver.csr および dbclient.csr 証明書署名要求ファイルに署名し、これらに対応する dbserver.crt および dbclient.crt 証明書と内部 CA 証明書（バンドル）を取得します。

   次に例を示します。

   ```
   pki sign dbserver dbca
   pki sign dbclient dbca
   ```

5. データベース クラスタの証明書と秘密キーをインストールします。 最初に SFTP 経由でダウンロードしてから、同じデータベース クラスタに属する各 Meeting Server にアップロードします。

注意：これらの pki の指示はいつでも実行できます。ただし、生成された証明書（データベース クラスタの証明書）の構成では、データベース クラスタを無効化する必要があります。すでにデータベース クラスタを設定済みである場合は、クラスタ内のすべてのサーバで **database cluster remove** コマンドを実行、無効化し、生成した証明書を構成するコマンドを実行してからクラスタを再作成してください。

データベース クライアントの証明書では、CN を「postgres」に設定する必要があります。証明書が適切であることを確認するには、**pki inspect** コマンドを使用します。次に例を示します。

```
cms>pki inspect dbclient.crt Checking ssh public keys...not found Checking
user configured certificates and keys...found File contains a PEM encoded
certificate Certificate:
     Data:
         Version: 3 (0x2)
         Serial Number:
             58:00:00:00:1c:3b:92:8a:95:d2:21:89:58:00:00:00:00:00:1c
    Signature Algorithm: sha1WithRSAEncryption
         Issuer: DC=com, DC=support, CN=support-DC2-CA
        Validity
            Not Before: Sep 13 13:32:38 2015 GMT
            Not After : Sep 13 13:42:38 2017 GMT
        Subject: CN=postgres
```

データベース クライアント証明書の CN が postgres 以外に設定されていると、クラスタの構成時に「エラー：クライアント証明書の共通名が正しくありません（ERROR: Client certificate common name incorrect）」というエラー メッセージが表示されます。

注：**database cluster initialize**、**database cluster join**、および **database cluster connect** の各コマンドは、有効な証明書、キー、および CA 証明書がデータベース クライアントとサーバにアップロードされていないと実行されません。エラー メッセージ：「**エラー：証明書を構成する必要があります（FAILURE: certificates must be configured）**」が表示され、このデータベース サーバまたはクライアントに証明書が構成されていないことを示します。

2.4.4 データベース クラスタの証明書のアップロード

次に、証明書を Meeting Server にアップロードし、クラスタを構成する必要があります。

1. Call Bridge と同じ場所に配置されているかどうかに関係なく、すべてのデータベースのホスト サーバで次の手順を実行します。
    a. Call Bridge サーバに次の証明書とキーを SFTP で送信します。
        - dbserver.key
        - dbserver.crt
        - dbclient.key
        - dbclient.crt
        - 内部 CA で提供された証明書バンドルも送信します。この例では、ファイルは dbca.crt になります。

b. データベース クラスタの作成時に使用する証明書を指定します。次に例を示します。

```
cms>database cluster certs dbserver.key dbserver.crt dbclient.
key   dbclient.crt dbca.crt Certificates updated
cms> database cluster status
Status                    : Disabled
Interface                 : a Certificates
  Server Key              : dbserver.key
  Server Certificate      : dbserver.crt
  Client Key              : dbclient.key
  Client Certificate      : dbclient.crt
  CA Certificate          : dbca.crt
```

注：**database cluster status** コマンドは、構成済みの証明書がない場合に強調表示されます。

---

2. データベースと異なる場所に配置されたすべての Call Bridge に対して、次の手順を実行します。

   a. Call Bridge サーバに次の証明書とキーを SFTP で送信します。

      - dbclient.key
      - dbclient.crt
      - 内部 CA で提供された証明書バンドルも送信します。この例では、ファイルは dbca.crt になります。

   b. これらの証明書を使用するようにデータベース クラスタを設定します。

```
cms>database cluster certs dbclient.key dbclient.crt dbca.crt
Certificates updated cms> database cluster status
 Status : Disabled
 Interface: a Certificates
  Client Key : dbclient.key
  Client Certificate : dbclient.crt
  CA Certificate : dbca.crt
```

3. マスター データベースの選択とデータベース クラスタの作成の詳細については、ここで再度『Server Deployment Guide』を参照してください。

証明書の作成 と Meeting Server へのアップロードの詳細については、『Cisco Meeting Server 2.7, Certificate Guidelines for Scalable and Resilient Server Deployments』を参照してください。

2.5 使用率統計情報

バージョン 2.7 以降では、syslog メカニズムを使用して、Meeting Server から利用率指標を 5 分間隔で追跡できます。syslog メッセージとして、次の使用率統計情報が追加されています。

```
STATS: {"callsLegsPS":X, "callLegs":"<A>/<B>", "CMA":<A>/<B>",
"sip":{"std":"<A>/</B">, "peer":<A>/<B>} }
```

引数の説明

"callsLegsPS" は、1 秒あたりの新規コール レッグの高水準値レートを提供します。これは、統計情報を返す Meeting Server で直近の 5 分間に確認された最大レートとなります。

<A> は、ロギング時にアクティブであった、コール レッグ タイプの数です。

<B> は、そのコール レッグ タイプの高水準レートを示します。

"callLegs" は、リストされたすべてのコール タイプの合計を示します。

"CMA" は、Wondows、Mac または iOS 用のネイティブの Cisco Meeting アプリと、WebRTC アプリを使用して作成された callLegs に対応します。

"sip" は "std" に分類され、SIP エンドポイントへの標準コールに使用されて、Nortel SIP ゲートウェイ コール レッグおよび Avaya コール レッグに追加されます。**また、"peer" は**別々の Call Bridges 間に配置された分散リンクを示し、分散会議でメディアを共有するために使用されます。

次に例を示します。

```
STATS: {"callsLegsPS":23, "callLegs":"139/262", "CMA":43/43",
"sip":{"std":"43/221, "peer":42/120} }
```

```
STATS: {"lync":{"AV":"A/B", "Tx":"A/B", "Rx":"A/B", "proxy":"A/B",
"conf":"A/B", "focus":"A/B", "IM":"A/B"}}
```

引数の説明

Lync には、Skype for Business と Office 365 が含まれています。

"AV" とは、音声/ビデオを意味します。

"Tx" および **"Rx"** は、着信/発信を共有するアプリケーションを表します。

"proxy" は LyncProxy コール レッグを表します。

"conf" は、会議サブスクリプション コール レッグを表します。

"IM" は、インスタント メッセージング（IM）コール レッグを意味します。

次に例を示します。

```
STATS: {"lync":{"AV":"2/7", "Tx":"1/3", "Rx":"0/1", "proxy":"1/4",
"conf":"2/14", "focus":"2/14", "IM":"2/13"}}
```

```
STATS: {"mediaLoad": 0}
```

"mediaLoad" は、統計情報の印刷時に Call Bridge にかかるメディア ロードのスナップショットです。これは、**/system/load** API ノードで GET を実行することで取得できる値と同じです。

次に例を示します。

```
STATS: {"mediaLoad": 0}
```

クラスタ化された展開では、各 Meeting Server の統計情報がほぼ同じ時間に syslog 処理される必要がありますが、必ずしも同期される必要はありません。各 Meeting Server で NTP が設定されていると想定した場合、クラスタ全体の syslog メッセージを組み合わせると、クラスタ使用率に関する十分に正確な情報を取得できます。

2.6 MMP の変更の概要

バージョン 2.7 では、次の MMP に関する変更がサポートされています。

コマンド	説明
database cluster status	コマンドが更新されました。2.7 以降、このコマンドは、構成済みの証明書がない場合に強調表示されます。 このデータベース インスタンスの観点から、クラスタリングの状態を表示します。
database cluster initialize	コマンドが更新されました。2.7 以降、このコマンドは、有効な証明書、鍵、および CA 証明書がデータベース クライアントおよびサーバにアップロードされない限り実行されません。このサーバの現在のデータベースの内容を唯一のデータベース インスタンス（マスター）として、新しいデータベース クラスタを作成します。
database cluster join <hostname/IP address>	コマンドが更新されました。2.7 以降、このコマンドは、有効な証明書、鍵、および CA 証明書がデータベース クライアントおよびサーバにアップロードされない限り実行されません。マスター データベースの内容をこのサーバにコピーし、そのサーバ上にあるデータベースの現在の内容を破棄して、新規のデータベース インスタンスをクラスタの一部として作成します。
pki selfsigned <key/cert basename>[<attribute>:<value>]	コマンドが更新されました。2.7 以降、属性/値を指定できるようになりました。
pki sign <csr/cert basename><CA key/cert basename>	新しいコマンド。2.7 以降、このコマンドは <csr/cert basename> で識別される CSR に署名し、<CA key/cert basename> で識別される CA 証明書とキーに署名されたベース名と同じベース名を持つ証明書を生成します。

2.6.1 新規のエラー メッセージ

エラー：証明書を構成する必要があります（FAILURE: certificates must be configured）

データベース クラスタの作成、結合、または接続時に表示され、このデータベース サーバまたはクライアントで証明書が構成されていないことを示します。

2.6.2 デフォルトの暗号ストリングの変更

ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!3DES:!aDH:!aECDH
、さらに **:!aDH:!aECDH:!SEED:!eNULL:!aNULL** が構成済みの暗号ストリングに自動で追加され、非常に弱い暗号は拒否されます

2.7 API の追加および変更の概要

Meeting Server 2.7 の新しい API 機能には次のものが含まれます。

- API パラメータ **panePlacementHighestImportance** を API の **/calls** オブジェクトに設定するためのサポート。
- API の **/coSpaces** オブジェクトおよび **/calls** オブジェクトでの新規 API パラメータ、**panePlacementSelfPaneMode**。これにより、「セルフ（自分自身の）」 ペインを SIP エンドポイントの画面レイアウトに挿入できるようになります。

2.7.1 **/calls** での **panePlacementHighestImportance** の設定

すべてのコールに対して、ペインの配置に最も重要性の高い値を設定するには、次の操作を行います。

- 要求パラメータ **panePlacementHighestImportance** を選択した値に設定して **/calls** へ POST メソッドを使用します。

特定のコールに対して、ペインの配置に最も重要性の高い値を設定するには、次の操作を行います。

- 要求パラメータ **panePlacementHighestImportance** を選択した値に設定して **/calls/<call id>** へ PUT メソッドを使用します。

コールの **panePlacementHighestImportance** 値を取得するには、**/calls/<call id>** で GET メソッドを使用します。

ペインの配置を削除するには、**panePlacementHighestImportance** パラメータを未設定のままにします（パラメータ値を空白のままにします）。

注：特定のコールで **panePlacementHighestImportance** を設定しても、そのコールにしか適用されず、コール間では保持されません。これは、コール間で保持される特定のスペースでの **panePlacementHighestImportance** パラメータの設定とは異なります。

2.7.2 **panePlacementSelfPaneMode** の設定

panePlacementSelfPaneMode パラメータでは、「skip」、「self」、「blank」、「""」の値を使用できます。以下を参照してください。このパラメータは、**panePlacementHighestImportance** も一緒に構成されている場合にのみ有効です。**panePlacementHighestImportance** は、**/coSpaces** または **/calls** オブジェクトで設定できます。

skip	これは、2.7 より前のバージョンのペイン配置と同じ効果があります。重要度レベルが「n」の参加者のペインは、その参加者のエンドポイントの画面レイアウトには表示されず、代わりに次の重要度レベルの参加者が表示されます。
self	重要度レベルが「n」の参加者のペインがエンドポイントの画面レイアウトに表示されるので、自分自身を確認できます。
blank	重要な参加者には、セルフ ペインではなく空白のペインが表示されます。これにより、重要な参加者には他のすべてのビューアーと同じペイン レイアウトが表示されます。
未設定、または ""	/call レベルの panePlacementHighestImportance 設定によって決定される優先順位に従うか、未設定のままとした場合は、上記で定義した skip 動作に戻ります。

すべてのコールとスペースに対してセルフ ペイン モードを設定するには、次の操作を行います。

- 要求パラメータ **panePlacementSelfPaneMode** を「skip」、「self」、「blank」、「""」の値に設定し（上記の表を参照）、/calls へ POST メソッドを使用します。
- 要求パラメータ **panePlacementSelfPaneMode** を選択した値に設定して **/coSpaces** へ POST メソッドを使用します。

特定のコールまたは特定のスペースに対してセルフ ペイン モードを設定するには、次の操作を行います。

- 要求パラメータ **panePlacementSelfPaneMode** を選択した値に設定して **/calls/<call id>** へ PUT メソッドを使用します。
- 要求パラメータ **panePlacementSelfPaneMode** を選択した値に設定して **/coSpaces/<coSpace id>** へ PUT メソッドを使用します。

コールまたはスペースの **panePlacementSelfPaneMode** 値を取得するには、**/calls/<call id>** または **/coSpaces/<coSpace id>** で GET メソッドを使用します。

2.8 CDR 変更の概要

バージョン 2.7 の新しい CDR レコードまたはパラメータはありません。

2.9 イベント変更の概要

バージョン 2.7 の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 2.7 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 2.6 からアップグレードしていること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、次の Cisco Meeting Server 2.7 リリース ノートに記載されている手順に従う前に、2.6.x リリース ノートの手順に従って 2.6 にアップグレードすることを推奨します。これは、会議サーバに接続された Cisco Expressway がある場合に特に重要です。

注：シスコでは、2.6 よりも前のソフトウェア リリースからのアップグレードをテストしていません。

Cisco Meeting Server 1000、または以前に設定された VM 展開にインストールされている Cisco Meeting Server ソフトウェアのバージョンを確認するには、MMP コマンド **`version`** を使用します。
VM を初めて設定する場合は、『Cisco Meeting Server Installation Guide for Virtualized Deployments』の指示に従ってください。

3.1 リリース 2.7 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導入については、クラスタ化されたサーバをアップグレードする前に、この FAQ の指示をお読みください。

注意：Meeting Server をアップグレードまたはダウングレードする前に、**`backup snapshot <filename>`** コマンドを使用して構成のバックアップを作成し、バックアップ ファイルを別のデバイスに安全に保存する必要があります。詳細については、『MMP 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。

注意：バージョン 2.7 にアップグレードすると、データベース クラスタの操作に影響する場合があります。バージョン 2.7 にアップグレードする前に、同じ認証局によって署名されたクライアント証明書とサーバ証明書が、クラスタ内のデータベース ノードを保持または接続している各 Meeting Server にアップロードされていることを確認します。詳細については、第 2.4 項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、upgrade 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。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。

注意: Meeting server 2000 を 2.5 (またはそれ以前) から 2.6 (またはそれ以降) にアップグレードする場合は、最大容量を確保するために、ロードバランスされた Meeting server 2000 展開の loadLimit の値を増やす必要があります。バージョン 2.6 のインストール時にすでに loadLimit 値を増やしていた場合は、これ以上増やす必要はありません。

アップグレードする Meeting Server 2000 ごとに、**`system/configuration/cluster`** API の **`Loadlimit`** フィールドを変更します。

- 50 万（2.5 以前に適しています）
- ～ 70 万（2.6 以降に適しています）

この変更は、2.6 リリース ノートで説明されている HD/fullHD の容量の増加でメリットを得るために必要です。この設定変更が実行されていない場合は、ロードバランシング導入の SD コールのキャパシティが低下します。

セカンダリ サーバをインストールするには、次の手順に従ってください:

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_7_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）：
   d51d3ef90854a7dd10aa9acb11975f8f5cf6de683c4ae4471ac0e77087912c2e

Cisco_Meeting_Server_2_7_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）：
dd0d49a729da16d31aa3658dc4d0193f3431216f4200082438057040e443413e

Cisco_Meeting_Server_2_7_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）：
3820cee312feb2b4e7eaa6419a0fecb575def8e84fecf51a1e5a48098c7d81a3

Cisco_Meeting_Server_2_7_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_7_vSphere-6_0.ova ファイルのハッシュ（SHA-512）：
939133faf0397ed5d56ebf5193674413dc9d1b9e37b6ba103daf8b6e7093f8226165b0705efde65a5d0a9ed6d764479ea89a79445134dc9b885c41e4e5fec06c

vSphere6.5 以上の場合、Cisco_Meeting_Server_2_7_vSphere-6_5.ova ファイルのハッシュ（SHA-512）：
2dd07380a3eca5bd5f56e7b96aa82599f678f907c3c92521413c932c3be0df0218d1c79843b4bb3fdc969dbe82e8d2b16e0fe112382aba3df8bbf0f42ff1f50c

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

注：a） **iface a** MMP コマンドを使用して、MMP のインターフェイスの IP アドレスを確認できます。
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。

      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。
7. MMP への SSH 接続を再確立し、次を入力して、Meeting Server がアップグレードされたイメージを実行していることを確認します。
8. **version** 利用可能な場合は、カスタマイズ アーカイブ ファイルを更新します。
9. 拡張または復元力のある展開を展開する場合は、拡張性と復元力の展開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。

3.3 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で、MMP の **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 管理者にログインし、**[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>** 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 サービスが接続済みである
- 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 Meeting app（サポートされている場合は Web Bridge）を使用して接続できます。

これで、Meeting Server のダウングレード展開が完了しました。

3.4 Cisco Meeting Serve 2.6 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。

3.4.1 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 向けのインストール ガイド (Cisco Meeting Server 2000、Cisco Meeting Server 1000 および仮想化された導入、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、単一の結合された Meeting Server 展開ガイド。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、『単一の組み合わせによるサーバ展開証明書ガイドライン』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 Meeting アプリ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。

3.4.2 コア サーバと Edge サーバでホストされる単一のスプリット 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、それに従ってください:

1. Cisco Meeting Server の適切なインストール ガイド
2. シングル スプリット Meeting Server 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、単一分割サーバ展開の証明書ガイドラインを参照しています。

3.4.3 拡張性と復元力の展開

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、それに従ってください。

1. Cisco Meeting Server の適切なインストール ガイド
2. 拡張性と復元力の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、『拡張性と復元力を重視した展開の証明書ガイドライン』を参照してください。

4 Bug Search Tool、解決済みの問題と未解決の問題

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には、Cisco Bug Search Tool を使用することができます。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、Bug Search Tool に移動します。
2. cisco.com に登録されているユーザ名とパスワードを使用してサインインします。

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`** を入力し始めます。その後 **[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 **`2.7.1`** のように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。

Bug Search Tool のヘルプ ページには、Bug Search Tool 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。

2.7.1 で修正された以前のバージョンで発生した問題

Cisco 識別子	まとめ
CSCvr86934	一部のシナリオで、ピア リンク コールの前に録音が開始されると、リモート Call Bridge からピア リンクを受信した後にその録音が断続的に停止することがあります。
CSCvs12175	AVMCU 会議への招待に対して [招待する（INVITE）] と応答するときに、連絡先ヘッダーに特定の Meeting Server の Call Bridge に対する FQDN が指定されていない場合、Skype For Business へのコールが失敗することがあります。
CSCvr80166	TMS でスケジュールされた会議で自動録音を開始できません。ここでは、TMS によってエンドポイントを別の Call bridge にダイヤルインし、同じ会議に参加します。
CSCvs03934	バージョン 2.7 以下を実行している Cisco Meeting Server で、予期しない Microsoft RDP の共有機能を受信すると、予期せず再起動を行うことがあります。
CSCvs08721	Skype 参加者のビデオが、話すときに SIP 側のコールに表示されません。
CSCvr58520	Call Bridge が Skype/Lync 環境への 「200 OK」応答で誤った連絡先ヘッダーを送信するコールに応答すると、デュアル ホーム コールおよびプレゼンテーション コールが失敗する場合があります。

Cisco 識別子	まとめ
CSCvr71743	participantLimit がテナント レベルで設定されている場合、ストリーミング セッションまたは録音セッションが参加者としてカウントされます。これにより、会議に参加できる実際の参加者の数が減少します。
CSCvq88442	クラスタ化された環境では、rxVideoMute=true を「/calls/<call id>/participants/*」に適用すると、すべてのピアノードのビデオがフリーズします。
CSCvq84608	参加者が会議に参加すると、スプラッシュ画面が左上のビデオ ウィンドウに瞬間的に表示されます（< 1 秒）。この現象は非常に短い時間で発生するため、新しく参加した参加者は気付かない場合があります。
CSCvq64378	Cisco Meeting Server で Call Bridge の動作可能時間が無許可でリセットされています。これは通常の操作には影響しません。
CSCvq81546	Meeting Server 2000 の複数のエンドポイントで重大なパケット損失とジッターが報告されました。
CSCvo80460	場合によっては、INVITE タイムアウトにより、遠端で SIP コールがドロップされることがあります。
CSCvo91844	劣化した音声が、多数の音声参加者が使用する、完全にロードされた Meeting Server で発生する場合があります。
CSCvq45298	WebRTC/Meeting アプリのポイント ツー ポイント コールで、各コールが個別の Call Bridge でホストされている場合、それらを接続するピア リンクが断続的に終了し、コールが切断されます。
CSCvq93115	Skype for Business のクライアントが、エンドポイントが Meeting Server を介してデフォルトでミュートになっている AVMCU 会議に参加するときに、最初にエンドポイントのミュートを解除することができません。2 番目のミュート解除から動作します。
CSCvk65529	まれに、Cisco Meeting Server が予期せず再起動し、次のメッセージが表示されることがあります。sf_assert failed server/media/startup/server_media_xccp_handler.cpp:767
CSCvr13451	ストリーマが切断され、パケット損失の状態で再接続されます。

Cisco Meeting Server 2.7 ソフトウェアで修正された、以前のバージョンの問題。

Cisco 識別子	まとめ
CSCvo41211	複数のクライアントと SIP エンドポイントで構成される Skype for Business ゲートウェイのコールで、Skype for Business クライアントがコンテンツを共有するときに、一部の SIP エンドポイントには表示されますが、表示されないエンドポイントがあります。
CSCvq19622	この問題は、FreeBSD および Linux Kernel に影響を与えている 6 月 17 日付けの Netflix によってリリースされた脆弱性に対して、この製品を評価して提供されています。 CVE ID: - CVE-2019-11477: SACK Panic - CVE-2019-11478: SACK の低速化または過剰なリソース使用 - CVE-2019-11479: 低 MMS 値による過剰なリソース使用 Cisco はこの製品を評価して、Linux Kernel のバージョンが脆弱性を含んでいるために脆弱性の影響を受けていると結論付けています。
CSCvp43740	3 つのスクリーン システムからの DTMF が、Meeting Server によって正しく認識されない場合があります。これらのシステムでは、CMS IVR をナビゲートしたり、会議のパスコードを入力したりできない場合があります。

4.2 未解決の問題

注：WebRTC アプリに影響を及ぼす未解決の問題については、『Cisco Meeting App WebRTC 重要な情報ガイド』を参照してください。

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	まとめ
CSCvp34817	Cisco Expressway の導入では、会議間で参加者を移動しても参加者の表示名は保持されません。これは、Web 管理インターフェイス、API、CDR レコードなどで返される表示名に影響します。さらに、参加者のコールレッグが Meeting Server 間で負荷分散されると、参加者の表示名は、参加者の表示名を決定するために CDR を使用するアプリケーション（Cisco Meeting Management など）に参加者の表示名が正しく表示されません。
CSCvn65112	ローカルでホストされているブランドの場合、音声プロンプト 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	まとめ
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。
CSCvm48344	レコーダが突然録画を停止すると、再生には適さない一時記録ファイルが作成されます。現在、.temp ファイルを .mp4 で再生するために変換できるツールはありません。
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 を実行しているシスコ 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 ユーザは、再度ログインする必要があります。
CSCvq62497	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 Meeting App、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。

シスコの法的情報

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、情報と推奨事項は、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。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムを適応したものです。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とソフトウェアは、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 アドレスと電話番号は、実際のアドレスと電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図とその他の図は、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。

このドキュメントのすべての印刷版と複製ソフトは管理対象外と見なされます。最新版については、現在のオンライン バージョンを参照してください。

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

シスコの商標

Cisco およびシスコ ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/go/trademarks をご覧ください。記載されている第三者機関の商標は、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シスコ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)