Cisco Meeting Server

Cisco Meeting Server リリース 3.1.2

リリース ノート

2021 年 3 月 15 日

目次

変更事項

バージョン	変更
2021 年 3 月 15 日	完全サポートの機能に関する情報を含む Cisco Meeting Server エッジセクションの短期的な資格情報を更新します。
2021 年 3 月 8 日	2 番目のメンテナンスリリース（3.1.2）。 ハッシュが更新されました 「解決済みの問題」を参照してください。
2021 年 1 月 20 日	[新機能（New Features）] セクションに「Vbrick API v2 のサポート」が追加されました。
2020 年 12 月 1 日	VM および CMS2K ハッシュが修正されました。
2020 年 11 月 30 日	バージョン 3.1 の最初のリリース

1 はじめに

これらのリリースノートでは、Cisco Meeting Server ソフトウェアの 3.1.2 における新機能、改善、および変更について説明します。

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

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

注：Cisco Meeting Management 3.1 には Meeting Server 3.1 が必要です。Meeting Management は、製品登録と、スマート ライセンスのサポートに関連するスマート アカウント（セットアップされている場合）とのやり取りを処理します。

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

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

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 シャーシ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ください。CiscoUCS Manager ファームウェア管理ガイドの指示に従ってください。プラットフォームが最新の状態に維持されていないと、Cisco Meeting Server のセキュリティが低下する場合があります。

1.1.3 コール キャパシティ

表 1 に、Cisco Meeting Server ソフトウェア バージョン 3.1.2 をホストしているプラットフォームのコール キャパシティの比較を示します。

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

コールのタイプ	Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5	Cisco Meeting Server 2000
フル HD コール 1080p60 ビデオ 720p30 コンテンツ	24	24	175
フル HD コール 1080p30 ビデオ 1080p30/4K7 コンテンツ	24	24	175
フル HD コール 1080p30 ビデオ 720p30 コンテンツ	48	48	350
HD コール 720p30 ビデオ 720p5 コンテンツ	96	96	700
SD コール 448p30 ビデオ 720p5 コンテンツ	192	192	1000
音声通話（G.711）	1700	2200	3000

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

表 2：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 2000
個々の Meeting Server またはクラスタの Meeting Server（注 1、2、3、4）	1080p30 720p30 SD 音声通話	48 96 192 1700	48 96 192 2200	350 700 1000 3000
	サーバごとの会議あたりの HD 参加者数	96	96	450
	Web アプリ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	350 700 1000 1000
Call Bridge グループ内の Meeting Server	サポートされるコール タイプ	着信 SIP 発信 SIP		
	1080p30 720p30 SD 音声通話の ロード制限	48 96 192 1700 96,000	48 96 192 2200 96,000	350 700 1000 3000 700,000
	サーバごとの会議あたりの HD 参加者数	96	96	450
	Web アプリ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	350 700 1000 1000

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

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

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

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

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

注 6：クラスタでサポートされるコール セットアップ レートは、SIP コールでは 1 秒あたり最大 40 コール、Cisco Meeting Server Web アプリケーションのコールでは 20 コールです。

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

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

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

Expressway（Large OVA または CE1200）は、Web アプリの規模が小～中の要件（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。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、SIP 容量まで拡張する必要なソリューションとして Cisco Meeting Server Web エッジをお勧めします（表 2 を参照 ）。

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 3 に示すように、Expressway により最大コール数の制限が適用されます。

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

表 3：Cisco Meeting Server Web アプリ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	大規模 OVA Expressway
Cisco Expressway ペア（X12.6 以降）	フル HD	150	150
	その他	200	200

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

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

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

スタンドアロンとクラスタのどちらの導入環境でも、内部と外部を組み合わせたコールの使用をサポートできます。内部参加者と外部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 2 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 3 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 Expressway のペアでは、音声のみの Web アプリケーション コールであれば混在で 1,000 までサポートしますが、外部参加者の数は、合計 1,000 のうち最大 200 に制限されます。

1.2 Cisco Meeting Server Web アプリケーション 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。

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

重要事項ガイドでは、以下のことを説明しています。

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

1.3 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 3.1 のリリースにあたり、シスコは、表 4 に示すソフトウェアのソフトウェア メンテナンス終了予定を発表しています。

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

Cisco Meeting Server ソフトウェアバージョン	ソフトウェアメンテナンス終了の通知期間
Cisco Meeting Server バージョン 2.9.x	Cisco Engineering が Cisco Meeting Server バージョン 2.9.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 3 月 1 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、ここをクリックしてください。

2 バージョン 3.1 の新機能と変更点

Meeting Server ソフトウェア バージョン 3.1 では、以下の新機能と変更が導入されています。

- 管理者は、ロビー/ウェルカム画面のテキストを使用して、SIP エンドポイントのウェルカム画面に会議のタイトルをオーバーレイテキストとして配置できます。
- 管理者がすべての参加者のビデオおよび/または音声のミュート/ミュート解除を有効化/無効化できるよう、新しいビデオの有効化/無効化および音声ミュート/ミュート解除モードを設定できます。
- coSpace プロビジョニング：管理者が LDAP 同期に基づいてユーザにスペースをプロビジョニングできる coSpace プロビジョニング機能が拡張されます。
- RTMPS ストリーミングサポート：内部の SIP ストリームアプリケーションの RTMP サポートを RTMPS に拡張し、これにより、ストリームトラフィックを暗号化できます。
- 有用性機能強化：
  - ICE トレースの改善。
  - パケットキャプチャが可能な限り有用であることを保証するために、サーバに負荷がかかっているときにパケットキャプチャサイズを増やすためのパケットキャプチャの改善。
  - パケットキャプチャが複数のインターフェイスで利用できるようになりました。
  - TURN サーバロギング の改善。
- Cisco Meeting Server Web アプリでは、3.1 で多くの新機能が導入されています。3.1 で導入された Web アプリケーションの機能の完全なリストについては、『Cisco Meeting Server 3.1 web app Important Information（Cisco Meeting Server 3.1 Web アプリケーション重要事項）』を参照してください。Meeting Server 側で設定が必要な Web アプリケーションの機能の一覧を以下に示します。
  - Cisco Meeting Server Web アプリのカスタム電子メール招待の変更
  - ユーザは、通話中に通話参加情報を表示できるようになりました
  - Web アプリのユーザインターフェイスのローカリゼーション
  - シングル サインオン
- Web 管理者ユーザインターフェイスの変更：外部アクセスの設定オプションが webBridgeProfiles API に移動しました。
- Web アプリの規模を拡大するために、エッジに Cisco Meeting Server を使用する新しいエッジソリューション。
- Cisco Meeting Server エッジ用の短期的な資格情報を使用したセキュリティ機能拡張。
- スケジュール済み LDAP 同期 API の追加と ldapSources のオブジェクト名ラベルの追加。

2.1 ビデオの有効化/無効化およびオーディオのミュート/ミュート解除モード

バージョン 3.1 では、ローカルとリモートのミュート間のリンクを分離する新しいビデオの有効化/無効化モードとオーディオのミュート/ミュート解除モードが導入され、管理者はすべての参加者のビデオを有効化/無効化したり、

オーディオをミュート/ミュート解除したりできるようになりました。

3.1 の管理者は、「リンクされた」ビデオの有効化と無効化、および音声のミュート/ミュート解除の動作を「リンク」と「分離」の間で選択できます。ここで、「リンク」は以前のリリースの動作です。つまり、ローカルビデオの有効化/無効化、デバイスのオーディオミュート/ミュート解除のステータス（ActiveControl 対応エンドポイント、Jabber クライアント 12.5 以降、Meeting Server Web アプリなど）は、サーバビデオの有効化/無効化、オーディオミュート/ミュート解除のステータスをミラーリングします。このモードは、たとえば、管理者が参加者をミュートする場合、参加者はデバイス上でローカルでミュートされ、自分のミュートをローカルで解除する必要があります（管理者はミュートを解除できません）。既存のミュート動作については、この FAQ で説明します。

新しい「個別」モードでは、ローカルビデオとサーバビデオの有効化/無効化と、オーディオミュート/ミュート解除モードのステータスが接続されません。この新しいミュートモードは、ローカルミュートが使用されない、管理者が参加者との対話なしで参加者をミュートおよびミュート解除できる機能が必要な使用例をサポートするために導入されました。

既存ユーザの場合、3.1 にアップグレードするとデフォルトの動作が「リンク」され、「個別」のビデオ有効/無効およびオーディオミュート/ミュート解除モードを使用するために再構成しない限り、ユーザエクスペリエンスは 3.1 以前と同じになります。

2.1.1　新しいオーディオミュートモードの動作

2.1.1.1　すべてのエンドポイント/クライアント（ローカル音声とサーバ音声のミュートは別）

- ユーザがローカルのミュート ボタンで自分をミュートした場合、ローカルではミュートされますが、Meeting Server/Meeting Management ではミュートされません。

エンドポイント/クライアント タイプ	以下がユーザに表示されます。	他の参加者	会議の管理	ユーザはローカルでミュートを解除できるか。
CE	ローカルのミュートインジケータ	参加者一覧にミュート状態が表示されない	ミュートされていることは表示されない	可
Jabber	（該当なし）ローカルミュートアイコンが淡色表示/無効	（該当なし）ミュートアイコンが淡色表示/無効	（該当なし）ミュートアイコンが淡色表示/無効	（非該当）
web app	ローカルのミュートインジケータ	他の Web アプリの参加者には、ミュートされていることを表示	ミュートされていることは表示されない	可

- 別のユーザがミュートを解除するか、実際のユーザが DTMF unmute コマンドを送信すると、サーバのミュートが削除され、動作は次のようになります。

以下がユーザに表示されます。	他の参加者	会議の管理	ユーザはローカルでミュートを解除できるか。
ビデオストリームからミュートアイコンが消える	ミュート解除されているものとして表示される	ミュート解除されているものとして表示される	ユーザはローカルのミュートボタンを押してミュートを解除することはできませんが、設定されている場合は DTMF を介してミュートを解除できる

2.1.2　新しいビデオの有効化/無効化モードの動作

2.1.2.1　Web アプリに適用る（ローカルビデオとサーバビデオの有効化/無効化は別）

- ユーザがローカルでビデオを無効にした場合：

以下がユーザに表示されます。	他の参加者	会議の管理	ユーザはビデオをローカルで有効にできるか。
ビデオが送信されないと言うメッセージ	通知されない	通知されない	ユーザはローカルでビデオを有効にしてビデオを再度送信できる

2.1.3　新しいビデオ有効化/無効化およびオーディオのミュート/ミュート解除モードをサポートする新しい API リクエストパラメータ

新しい**`muteBehavior`** API リクエストパラメータは、新しいミュート動作を実装するために 3.1 で導入されました。新しいタイプの**リンク**または**セパレートを使用してコールのミュートモードを設定するこのパラメータは、次の場合**に導入されます。

- **`/callProfiles`** に対する POST 操作
- **`/callProfiles/<call profile id>`** に対する PUT 操作
- **`/callProfiles/<call profile id>`** で GET を実行します。

2.2　スクリプト API v2 のサポート

Cisco Meeting Server 3.1.1 には Rev API v2 のサポートが含まれています。

次の表は、Cisco Meeting Server リリースでサポートされている、Cisco Meeting Server のバージョンに関する情報を提供します。

表 5：Cisco Meeting Server リリースでサポートされている Vbrick API バージョン

Vbrick API バージョン	Cisco Meeting Server リリース
Rev API v2 および Rev API v1	Cisco Meeting Server 3.1
Rev API v1	Cisco Meeting Server 3.0
Rev API v1	Cisco Meeting Server 2.9

注：Cisco Meeting Server のバージョン 2.9 および 3.0 は Rev API v1 のみをサポートし、2021 年 4 月 30 日までにはサポートを停止します。詳細については、https://portal.vbrick.com/rev-developersを参照してください 。Cisco Meeting Server バージョン 2.9 および 3.0 のユーザは、特に事前の通知なしに動作が停止する可能性があり、今後の Cisco Meeting server リリースを使用することはできません。

2.3 coSpace プロビジョニング

バージョン 3.1 では、管理者が LDAP 同期に基づいてユーザにスペースをプロビジョニングできる coSpace プロビジョニング機能が拡張されています。

これまでは、「ユーザインポート」の一部として ldapMapping オブジェクトに次のパラメータを指定することで、LDAP 同期の一部としてスペースをプロビジョニングすることができました（coSpaceUriMapping、coSpaceSecondlyMapping、coSpaceNameMapping、coSpaceCallIdMapping）。バージョン 3.1 では、この古い推奨されないプロビジョニング方法をサポートしています。ただし、新しく改良されたスペースのプロビジョニング方法を使用してユーザに対して複数のスペースをプロビジョニングする事が可能になり、廃止された古い方法ではなく、この方法でスペースをプロビジョニングすることを推奨します。

注：廃止された coSpace プロビジョニング方式は、今後ある時点で削除される可能性があります。

この機能により、バージョン 3.1 で次の新しい API オブジェクトが導入されました。

- **/ldapUserProvisionedCoSpaceMappings**
- **/ldapUserProvisionedCoSpaceMappings/<LDAP user provisioned coSpace mapping id>**
- **/ldapUserProvisionedCoSpaceSources**
- **serProvisionedCoSpaceSources/<LDAP user provisioned coSpace mapping id>**
- **/ldapUserProvisionedCoSpaceSources/<LDAP user provisioned coSpace source id>**
- **/users/<user id>/userProvisionedCoSpaces**
- **/users/<user id>/userProvisionedCoSpaces/<user provisioned coSpace id>**

userProvisionedCoSpace パラメータが /cospaces オブジェクトに導入されます。
この機能をサポートするすべての API の追加の詳細については、「API の追加の概要」を参照してください。

2.3.1 ユーザに coSpace をプロビジョニングする方法

ldapUserProvisionedCoSpaceMapping を作成します。

1. Meeting Server Web 管理インターフェイスを使用する場合:
    a. Meeting Server Web 管理インターフェイスにログインし、[設定（Configuration）] > [API] を選択します。
    b. API オブジェクトのリストから、after/api/v1/ldapUserProvisionedCospaceMappings の後ろにある ► をタップします。
    c. [新規作成（Create new）] をクリックします。
    d. 必要な coSpace の URI に coSpaceUriMapping を定義します。
    e. オンプレミスの場合、HTTPのデフォルトは8090、HTTPSのデフォルトは8181です。必要に応じて、coSpaceNameMapping を設定します。たとえば、coSpaceNameMapping を「cn Personal coSpace」 に設定すると、各ユーザの coSpace に名前の後に「Personal coSpace」というラベルが付きます。
    f. coSpaceTemplate **フィールドに**移動し 、[選択（Choose）] をクリック します。
    g. 表示される「coSpaceTemplateオブジェクトセレクタウィンドウ」から、ユーザがプロビジョニングした coSpace マッピングに割り当てる coSpaceTemplate の**オブジェクト** ID の [**選択**（Select）] をクリックします。
    h. [作成（Create）] をクリックします。

ldapUserProvisionedCoSpaceSource を作成します。

2. API オブジェクトのリストから、/api/v1/ldapUserProvisionedCoSpaceSource の後ろにある ► をタップします。
    a. [新規作成（Create new）] をクリックします。
    b. ldapSource **フィールドに**移動し 、[**選択**（Choose）] をクリック します。

        結果の「ldapSource オブジェクトセレクタウィンドウ」から、使用する ldapSource の**オブジェクト** ID の [**選択**（Select）] をクリックします。（つまり、共空間をプロビジョニングするユーザのリストを提供するソースです。）
    c. ldapUserProvisionedCoSpaceMapping **フィールドに**移動し 、[**選択**（Choose）] をクリック します。

        結果の「ldapUserProvisionedCoSpaceMapping オブジェクトセレクタウィンドウ」から、ステップ 1 で作成した ldapUserProvisionedCoSpaceMapping の**オブジェクト** ID の [**選択**（Select）] をクリックします。
    d. オンプレミスの場合、HTTPのデフォルトは8090、HTTPSのデフォルトは8181です。必要に応じて 、**フィルタ**を設定します。これは、ソースの読み取り時に適用される追加の LDAP フィルタ文字列です。

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

e. [作成（Create）] をクリックします。

LDAP ソースと LDAP マッピングが作成され、LDAP 同期を実行する事が可能になりました。

3. API オブジェクトのリストから、/api/v1/ldapSyncs の後ろにある ▶ をタップします。
   a. [新規作成（Create new）] をクリックします。
   b. ldapSource **フィールドに**移動し 、[**選択**（Choose）] をクリック します。
   c. 結果の「ldapSource オブジェクトセレクタウィンドウ」から、同期する ldapSource の**オブジェクト** ID の [**選択**（Select）] をクリックします。
   d. [**作成**（Create）] をクリックして、LDAP 同期を実行します。
4. API オブジェクトのリストから、/api/v1/users の後にある「▶」をタップして、ユーザがプロビジョニングした coSpace のリストを表示します。

Web アプリのユーザは、Web アプリの UI から新しくプロビジョニングされた coSpace をアクティブ化できるようになります。詳細については、『Cisco Meeting Server Web アプリケーションの重要事項』を参照してください。

2.4 RTMPS ストリーミング

バージョン 3.1 は、内部 SIP ストリームアプリケーションの **RTMP** サポートを RTMPS に拡張します –TLS 接続を使用した基本的な RTMP です。これまでは、ストリームと RTMP サーバ間のすべてのトラフィックが暗号化されていませんでしたが、3.1 RTMPS がサポートされることで、このトラフィックを暗号化できます。

RTMPS と設定手順でサポートされる機能セットは、3.0 で導入および文書化されている RTMP の場合と同じです。

RTMPS サポートでは、**TLS** 証明書と信頼を設定できる新しい **MMP** コマンドが導入されています。さらに、**RTMPS** ストリームの設定に必要な **coSpaces API** の **`streamUrl`** パラメータに、**`rtmps://` のプレフィックスが付くストリーム `URL` のサポートが**導入されます。

2.4.1 新しい MMP コマンド

既存**の `tls`** MMP コマンドが拡張され、オプションで RTMPS の TLS 信頼 の設定が許可されます。この手順はオプションですが、推奨しています。TLS 信頼が設定されていない場合、RTMPS 接続は安全ではありません。**`help tls`** コマンド**の新しい出力 は次の情報です。**

```
cms> help tls
```

TLS 操作の使用法を構成します。

```
tls
tls (sip|ldap|dtls|webadmin|rtmps)
tls (sip|ldap|rtmps) trust <crt bundle>
tls (sip|ldap|rtmps) verify (enable|disable|ocsp) tls sip
ciphers <cipher string>
tls (sip|ldap|webadmin|rtmps) min-tls-version
<minimum version string>
tls min-dtls-version <minimum version string>
```

Trust and verify コマンドを使用して、信頼ストアを設定してから有効にできます。設定された **min-tls-version** もサポートされています。

2.4.2　RTMPS URL の設定

RTMP ストリーミングを構成するには、coSpaces API で **streamUrl** パラメータを設定してストリーム URL を設定する必要があります。これは 3.1 では同じですが、**rtmp**の代わりに **URL プレフィックス rtmp** を入力して RTMPS URL を示す事が可能です。たとえば、**rtmps://mystreamer.com/stream**

2.5　有用性に関する機能強化

2.5.1　ICE トレース

Web管理インターフェイスの [**ログ** > **詳細トレース**] の下に、ログメッセージを提供する ICE トレースボタンがあります。

3.1 は、メッセージ内容の完全な詳細を含め、メインフローを覆い隠していた不要で冗長なメッセージを削除することにより、ICE の詳細なトレースログメッセージの有用性を向上させます。

2.5.2　パケットキャプチャの改善

バージョン 3.1 では、パケットキャプチャが改善され、サーバの負荷が下がった場合のパケットキャプチャのサイズが大きく改善されています。ファイルキャプチャの最大サイズは、現在利用可能なファイルシステムスペースの 75% または 1 GB の小さい方に制限されていますが、この制限では、負荷がかけられているサーバで非常に長いキャプチャはできません。

バージョン 3.1 では、ファイルサイズの制限に到達せずに負荷がかけられているサーバで有用なパケットキャプチャを確実に実現できるよう、**pcap** MMP コマンドに次の 2 つの新しいオプションが導入 されています。

- **snaplen <length>** – このオプションでは、キャプチャされた各パケットが長い場合、最大バイト数に切り捨てされます。その結果、より多くのパケットが同じファイルサイズの制限に収まる可能性があります。これは、正確なパケットデータを抽出できないことを意味しますが、これが問題にならない場合があります。たとえば、
  - メディアが暗号化されているが、これによりパケットのカウントが可能な場合
  - 特定のトラフィックの有無を確認する必要がある場合

- **filter <filter-string>** – このオプションは、文字列内の条件に一致するパケットのみを選択します。これによりキャプチャが関心のあるパケットだけに減り、他のパケットのディスク容量を節約できます。この文字列の解析とパケットフィルタリングは、tcpdumpで使用されるものとまったく同じ基本ライブラリを使用して実行されるため、これはまったく同じ表現力とパフォーマンスを備えています。フィルタ式は、必要に応じて最大約 4080 文字長にすることができます。

この 2 つのオプションは、次のすべてとして **snaplen** コマンドを最初に使用して組み合わせることができます。

フィルタは、フィルタ式として扱われます。これら 2 つのオプションの使用例を次に示します。

```
pcap a snaplen 40 filter udp host 10.10.3.4 and portrange 40000-50000
```

このコマンドの例は、大きい番号のポート上の UDP トラフィックのみをキャプチャします。10.10.3.4 と各（おそらくメディア）パケットの最初の 40 文字だけを保持します。

2.5.2.1 複数のインターフェイスでのパケットキャプチャ

pcap MMP**コマンドは、インターフェイス名として任意の**受け入れるようになりました。これにより、有効なインターフェイスでキャプチャされます（有効になっていないインターフェイスはスキップされます）。以前のように単一のインターフェイス名を指定することもできます。

注：複数のインターフェイスからキャプチャする場合は、各インターフェイスが別の一時的なファイルにキャプチャされ、キャプチャが停止された時にファイルが統合されるなど、ディスク領域が追加される必要があります 。したがって、複数のインターフェイスでキャプチャするときに使用できるストレージは、単一のインターフェイスでキャプチャするときに使用できるストレージの半分です。

新しいオプションの any は次 のように使用されます。

```
pcap <interface>|any [snaplen <length>] [filter <filter-string>]
```

2.5.3 TURN サーバロギング の改善

3.1 以前の場合、TURN サーバは通常動作でいくつかの syslog エントリを生成しました。ロギングが 3.1 で拡張され、個々のメディアストリームの開始と終了を追跡し、TURN サーバの IP アドレスが失敗した接続メッセージに追加されます。

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

バージョン 3.1 では、Cisco Meeting Server Web アプリケーションにいくつかの新機能と変更が導入されています。

注：3.0 の Web アプリケーションのすべての新機能の詳細については、『Cisco Meeting Server 3.1 web app Important Information（Cisco Meeting Server 3.1 Web アプリケーション重要事項）』を参照してください。以下に示す新しい Web アプリ機能は、サーバ側の設定が必要な機能や、API の追加/変更が必要な機能です。

2.6.1 Cisco Meeting Server Web アプリのカスタム電子メール招待の変更

注：3.1 にアップグレードした場合は、以前のリリースから 3.1 への既存のカスタム電子メール 招待テンプレートの移行パスが存在せず、管理者がすべてのカスタム電子メール 招待テンプレートを再作成する必要 があります。

バージョン 3.1 では、カスタム電子メール招待テンプレートに対する次の変更が導入されています。

- カスタム電子メールの招待テンプレート言語が拡張され、複数の IVR 番号と Web ブリッジ アドレスがサポートされます。
- カスタム電子メール招待のテンプレートのコンテンツが新しいシンタックスを使用して作成されます。
- すべてのカスタム電子メール招待のテンプレートは、電子メールの本文からヘッダーを分離するため、「Subject:」の後に空の行で始まる必要があります。「Subject:」ヘッダーだけが現在ところはサポートされています。
- 電子メール招待のテンプレート用に追加された新しいデフォルト言語。

2.6.1.1 カスタム電子メール招待の言語拡張

3.1 では、テンプレート言語が拡張され、次のように複数の IVR 番号と Web ブリッジ アドレスがサポートされます。

Web ブリッジの場合:

```
#for webbridge in web_bridge_addresses
%webbridge.label% : %webbridge.address%
%webbridge.hyperlink%
#endfor
```

PSTN ダイヤルインの場合：

```
#for pstn in ivr_numbers
%pstn.label% :%pstn.number%
#endfor
```

2.6.1.2 新しいシンタックスで作成されたカスタム電子メール招待のコンテンツ

バージョン 3.1 では、カスタム電子メール招待を作成するための新しいシンタックスが導入されています。

注：3.1 にアップグレードした場合は、以前のリリースから 3.1 への既存のカスタム電子メール 招待テンプレートの移行パスが存在せず、管理者がすべてのカスタム電子メール 招待テンプレートを再作成する必要があります。

ヘッダー

すべてのカスタムメールテンプレートは、「Subject:」で始まり、その後に本文テキストと区別するための空の行が続く必要があります。件名ヘッダーは、ヘッダーで指定されたテキストを電子メールの件名として設定する電子メールリンクを生成するために使用されます。ヘッダーに新しい行の文字を含めることはできません。構文は次のとおりです。

```
Subject: <subject….> [空の行が続く]
```

形式

新しいカスタム電子メール招待のテンプレートシンタックスでは、変数、ループ、条件、含む、コールバック、およびコメント（必要に応じて組み合わせたもの）を使用できます。

条件コード、ループなどの記述を可能にしたエスケープシーケンス、つまり新しい行のエスケープシーケンス（3.1 以前と同じ）があります。# で始まる任意の新しい行には、テンプレートのステートメントが導入されます。例：

```
#if name
%name% #endif に設定されているため、名前変数を使用で
きます
```

「{%" and "%}」を使用してインラインステートメントを指定できます。例：

```
会議% if name %}: %name%{% endif %} に招待されています
```

また、「{# my comment #}」を使用してテンプレートにコメントを追加することもできます。したがって、これらのエスケープシーケンス間のテキストはレンダリングされません。例：

```
Hello, {# This section is just an intro #}
```

変数

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

%<var name>% will be substituted with the content of a variable.
The variables that are currently defined are detailed below:

表 6：招待テンプレートの変数

変数名、説明、および例

name
 	
これにより、cospace の名前に置き換えられます。コンテンツがあるかどうかを確認するには、コンテンツの長さ、または null でないかどうかを確認します。
例：
`#if name`
`cospace の名前は %name%`
`#endif です`
 	
`#if length(name)>0`
`cospace の名前は %name%`
`#endif です`

変数名、説明、および例
uri Web アプリ内の「join by uri」またはエンドポイントでダイヤルインするために使用できる cospace uri。長さによって、または null に設定した場合にチェックできます。 **#if uri** **uri：%uri% #endif** **#if length(uri) > 0 The uri is: %uri% #endif**
numeric_id これは、cospace. の callId です。通常、これは cospace の数値識別子です。長さによって、または null に設定した場合にチェックできます。 例： **#if numeric_id** **会議 ID は %numeric_id% #endif** **#if length(numeric_id) > 0** **会議 ID は %numeric_id% #endif**
パスコード cospace に割り当てられたパスコード。 長さによって、または null に設定した場合にチェックできます。 例： **#if passcode** **会議にはパスコード %passcode% #endif が必要です。** **#if length(passcode) > 0** **会議にはパスコード %passcode% #endif が必要です。**

変数名、説明、および例
ivr_numbers これは、ラベルと番号を含むオブジェクトの配列です。 （これは、3.1 dial_pstn のカスタム電子メールのテンプレートで使用された変数に取って代用されます。） 空の配列にすることができ、内部変数であるラベルと数値にアクセスするにはループオーバーする必要があります。null を確認することはできず、長さだけで確認できます。 • label: Meeting Server API を使用して登録する際、この IVR 番号に割り当てられたラベル。 • number: ダイヤルインする IVR 番号。 例： **#if length(ivr_numbers) > 0** **次のダイヤルイン番号を使用することができます。：%ivr_numbers.0.number%** **%** **#endif** **#for ivr_number in ivr_numbers** **%loop.index1% - %ivr_number.label%: %ivr_number.number% #endfor**
web_bridge_addresses これは、ラベル、アドレス、ハイパーリンクを含むオブジェクトの配列です。 （ハイパーリンクと 3.1 webbridge_url のカスタム電子メールのテンプレートで使用される変数に取って代用されます。）空にすることはできますが、null を確認することはできず、長さだけで確認できます。 • label: Meeting Server API を介して登録する際、この Web ブリッジアドレスに割り当てられたラベル。 例：Web アプリのアドレス • address: この Web ブリッジ上の Web アプリにアクセスするために使用できる HTTPS アドレス。 例：https://join.mydomain.com/ • hyperlink: スペース内に callId が空でない（別名、会議 ID または number_id）と空ではないアドレスがある場合、パスコードを要求せずに特定の会議に直接参加するために使用できる固有のハイパーリンクが生成されます。 例： **#if length(web_bridge_addresses) > 0** **次の Web アプリアドレスを使用できます。%web_bridge_addresses.0.address% #endif** **#for wba in web_bridge_addresses** **ラベル: %wba.label%** **アドレス：%wba.address%** **Hyperlink: %wba.hyperlink%** **#endfor**

ループ（Loops）

ループは、「for」および「endfor」キーワードを使用して使用できます。例：

```
#for ivr_number in ivr_numbers
%loop.index1% - %ivr_number.label%: %ivr_number.number%
#endfor
```

ループ内の特殊変数は次のとおりです。

- loop.index (number): 0 から始まるループのイテレーション番号。
- loop.index1 (number): 1 から始まるループのイテレーション番号。
- loop.is_first (boolean): 繰り返しが最初の繰り返しである場合。
- loop.is_last (boolean): 繰り返しが最後の繰り返しである場合。
- loop.parent.*: ネストされたループでは、親ループ変数は loop.parent。loop.parent.<name of var> を使用して使用できます。例：loop.parent.is_first

web_bridge_address や ivr_number などのオブジェクトを反復処理することもできます。例：

```
#for ivr_number in ivr_numbers
{%- for key, value in ivr_number -%}
%key%: %value%
{%- endfor -%}
#endfor
```

条件（Conditions）

条件は、一般的な「if」および「else」ステートメントをサポートします。

例：パスコードの長さに応じて異なるものをコピー

```
{% if length(passcode) >= 3 %}…{% else if length(passcode) >= 10 %}…{% endif %}
```

特定のフィールドが web_bridge_address に設定されている場合にのみ何かをコピーします

```
{% if web_bridge_address.hyperlink %}…{% endif %}
```

論理的な操作

「and」、「or」および「not」を使用すると、複雑な条件を生成できます。例：

```
{% if numeric_id and passcode %}…{% endif %}
{% if not name %}…{% endif %}
```

機能

テンプレート構文内にいくつかの関数が実装されます。詳細は以下のとおりです。文字列の場合の上下の関数。例：

```
Join {% upper(name) %}
Join {% lower(name) %}
```

ループに便利な範囲関数。例：

```
{% for i in range(4) %} %loop.index1% {% endfor %}
```

```
{# It will show only the first two web_bridge_addresses #}
{% for i in range(2) %} %at(web_bridge_addresses, i).address% {% endfor %}
```

リストの最初と最後の要素を取得します。例：

```
The first ivr_number: % first(ivr_numbers).number %
The last ivr_number: % last(ivr_numbers).number %
```

リストの並べ替え。。例：

```
#for sort(ivr_numbers)
...
#endfor

{# Produces [1, 2, 3] #}
% sort([3,2,1]) %
```

数値を特定の精度にする概数。。例：

```
{# returns 1 #}
% round(1.4142135, 0) %
{# returns 1.4 #}
% round(1.4142135, 1) %
```

値が数値に対して偶数である、または割り当て可能な値か確認します。例：

```
{# returns true #}
% odd(1) %
{# returns true #}
% even(2) %
{# returns true #}
% divisibleBy(42, 7) %
```

リストの最大値と最小値。例：

```
{# returns 3 #}
% max([1,2,3]) %
{# returns 1 #}
% min([1,2,3]) %
```

文字列を数字に変換します。例：

```
# if int(ivr_number) >= 123123

#endif
```

変数が定義されていない場合は、デフォルト値を設定します。テンプレートをレンダリングしないと、テンプレートのレンダリングは失敗し、結果は表示されません。例：

```
{% if default(has_valid_ivr_number, false) %}... {% endif %}
```

オブジェクトにキーが存在するかどうかを確認します。例：

```
{# returns false #}
% exists("pstn_dial_in") %
{# returns true #}
% existsIn("a", myobj) %
{# returns false #}
```

```
% existsIn("c", myobj) %
```

キーが特定のタイプか確認します。例：

```
{# returns true #}
% isArray(ivr_numbers) %
{# returns true #}
% isString(ivr_numbers.0.number) %
{# returns false #}
% isString(int(ivr.numbers.0.number)) %
```

実装されている型の確認は、isArray、isBoolean、isFloat、isInteger、isNumber、isObject、isString、

空白制御

空白はデフォルトで削除されます。より読みやすいテンプレートスタイルをサポートするため、ステートメントと式の両方の空白を手動で削除することもできます。最初と最後に負記号 (-) を追加すると、そのブロックの前または後の空白が削除されます。例：

```
Cospace name: % name -%.
{# Produces: Cospace name: blah. #}
```

ステートメントまたは式の後ろを削除すると、新しい行も削除されます。

2.6.1.3　招待テンプレートの例

次の例を参考にして、数値に固有の値を使用してカスタマイズします。適切なファイル名の形式を使用して保存します。

注：本文テキストとは別に「Subject:」ヘッダーの後に空の行を続ける必要があります。

```
Subject: {% if name %}You are invited to join a meeting: %name%{% else %}You
are invited to join a meeting{% endif %}

#if numeric_id
Meeting ID: %numeric_id%
#if passcode
Meeting passcode: %passcode%
#endif
#endif

#for wba in sort(web_bridge_addresses)
#if wba.address or wba.hyperlink
#if loop.index == 0
```

コンピュータ、携帯電話、タブレット端末から参加 #endif

```
wba.label %} %wba.label%:{% endif %} {% if wba.hyperlink
%}%wba.hyperlink%{% else %}%wba.address%{% endif %}
#endif
#endfor
```

```
#for ivrn in sort(ivr_numbers)
#if ivrn.number
#if loop.index == 0
Join by phone
#endif
{% if ivrn.label %} %ivrn.label%:{% endif %} %ivrn.number%
#endif
#endfor

#if uri
```

ビデオ会議システムまたはアプリケーションダイヤル `%uri%` から参加

```
#endif
```

2.6.1.4　異なる言語の招待テンプレート

Meeting Server 上に Web アプリ用のデフォルト言語招待メールのテンプレートが 21 件追加されます。招待テンプレートには、次の形式が使用されます。

- invitation_template_xx_XX.txt

注：言語別の .txt ファイルには、言語バリアントに応じた適切な言語タグ（IANA Language Subtag Registry の定義に従う）を指定する必要があります。この言語タグでは、2 個の小文字が言語コードを表し、2 個の大文字が地域コードを表します。たとえば、invitation_template_fr_CA.txt、「fr」はフランス語、"CA" は地域（カナダ）です。

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

Web アプリのユーザは、アップロードされる言語テンプレートのみを選択できます –アップロードされていない場合、ドロップダウンリストには Web アプリのユーザに言語オプションは表示されません。

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

次の図は、デフォルトで使用可能ないくつかの異なる電子メール招待の言語の例を示しています。

図 1：電子メール招待オプション

詳細については、『カスタマイズのガイドライン』を参照してください。

2.6.2　コール参加情報の表示

この機能により、コールの進行中にスペース名、通話時間、コール参加情報を表示できます。この参加情報を使用して、ユーザは会議に参加する参加者を追加できます。

この機能では、次の新しい API タイプが導入されます。

- on request parameter **`scope`** for POST to **`/coSpaces/<coSpace id>/accessMethods`** and **`PUT to coSpaces/<coSpace id>/accessMethods/<access method id>.`**
  - **`member`**：この coSpace アクセス方式の詳細は、coSpace のメンバーに表示されます。
  - **`Directory`**：この coSpace アクセス方式の詳細は検索で確認できます [注：3.1 では検索は行っていないため、動作は**パブリックと同じです**]

さらに、パブリックとプライベートの既存の API タイプの定義は更新されます。

- **public**：この coSpace アクセス方式の詳細は、coSpace のメンバーおよび会議のすべての参加者に表示されます。
- **private**：この coSpace アクセス方式の詳細は、Web アプリ内のスペースの所有者にのみ表示されます。または Call Bridge API を使用して管理ユーザに表示されます。

2.6.3　Cisco Meeting Server Web アプリのローカライズされたユーザインターフェイス

バージョン 3.1 では、Web アプリのユーザインターフェイスのローカリゼーションが 21 言語で導入されています。デフォルトの Web アプリのユーザインターフェイス言語は、ブラウザのデフォルトに基づいて設定されます。Web アプリのユーザが別の言語を選択する場合、アプリにログインするか会議に参加する前に、その言語を選択できます。Web アプリのユーザが優先言語を選択する方法の詳細については、「Cisco Meeting Server 3.1 （以降）Web アプリの重要な情報」を参照してください。

この新しい機能をサポートするため、Cisco Meeting Server には、表 7 の説明に従って、「text_strings_xx_ XX.json」という新しい Web アプリ資産が追加されました。これらの言語はソフトウェアの一部であり、特定の言語ファイルをカスタマイズする場合に限り、特別な設定は不要です。特定の言語ファイルが存在しない場合、Meeting Server はデフォルトで text_strings.json ファイルを使用します。

表 7：Web アプリケーションのアセットの説明と仕様

ファイル名	説明	最大ファイル数：サイズ	推奨されるサイズ、形式、縦横比
text_ strings_ xx_ XX.json	特定の言語のテキスト文字列。たとえば、「text_strings_fr_CA.json」は、フランス語で Web アプリのユーザインターフェイスを提供します。 text_strings.json と同じものをサポートします。 この形式で定義されたテキスト文字列は、指定された言語の「text_strings.json」で指定されている文字列をオーバーライドします。 サポートされる文字列： • brand_title：メインのブランド名 • brand_subtitle：下に表示する 2 番目のテキスト • brand_title brand_tag_line：下に表示する 3 番目のテキスト • brand_subtitle brand_browser_tab_label：ブラウザのタブの名前	16 KB	推奨される長さ： • brand_title：最大 24 文字（1 行に表示）、または最大 48 文字（2 行に表示）。 • brand_subtitle：最大 24 文字（1 行に表示）、または最大 48 文字（2 行に表示）。 • brand_tag_line：最大 100 文字 • brand_browser_tab_label：最大 64 文字

2.7　Cisco Meeting Server Web アプリのシングルサインオン（SSO）

この機能により、Web アプリユーザは SSO プロバイダーを使用してログインし、ID を確認できます。

SSO は、Web アプリのユーザがログイン毎にパスワードを入力する必要が生じ、ID プロバイダーとのセッションを 1 つで行える状態になります（一元的な場所でユーザを認証し、それぞれのセッションを維持するエンティティ。OAuth、gmail など。）。

これにより、Web アプリユーザは同じ Web ブリッジ上の異なる SSO プロバイダーでログインできるようになります。

この SSO メカニズムでは、オープン標準であり、広く使用されている業界標準プロトコルである SAML（セキュリティ アサーション マークアップ言語）2.0 を使用します。

注: 現在 Meeting Server は、SAML 2.0 プロトコルで HTTP-POST バインドのみをサポートしています。つまり、メッセージは HTTP-POST の、3 つ以上のメッセージのみを受け入れ、HTTP-POST バインドが利用できないアイデンティティプロバイダーを拒否します。

注：SSO ログインを有効にした場合、LDAP ログインは使用できなくなります。

2.7.1　Meeting Server Web アプリで使用するための SSO の設定

SSO を使用するには、以下に詳細を示す、アイデンティティプロバイダーと Meeting Server（SAML 2.0 Exchange のサービスプロバイダーと見なされる）のいくつかの設定が必要です。

タスク 1：アイデンティティプロバイダーと Meeting Server ユーザのマッピング

Meeting Server がアイデンティティプロバイダーのユーザを自身のユーザに正しくマップされるようにするには、SSO で認証されるユーザごとに authenticationId を設定する必要があります。これは、標準の ldap 同期プロセスの一部として行なわれます。このフィールドの内容は、アイデンティティプロバイダーから渡されたカスタムパラメータに対して検証され、応答が成功します（タスク 2 を参照）。

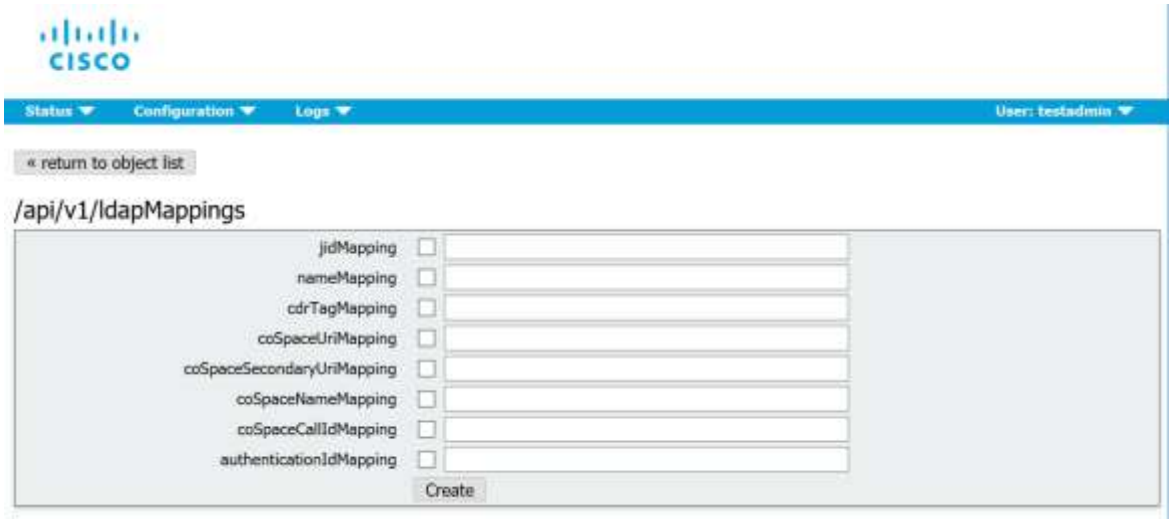
ユーザごとに一意の識別子を選択することを推奨しています（たとえば、$sAMAccountName$）。authenticationId の空の値は受け入れられません。

ldapSync の一部として authenticationId をセットアップするには、新しい ldapSync を作成するか、既存の ldapSync を変更します。

次に、ldapMapping を作成/変更し、authenticationIdMapping パラメータに適切な値（たとえば、$sAMAccountName$）を入力する必要があります。

Meeting Server Web 管理インターフェイスを使用する場合:

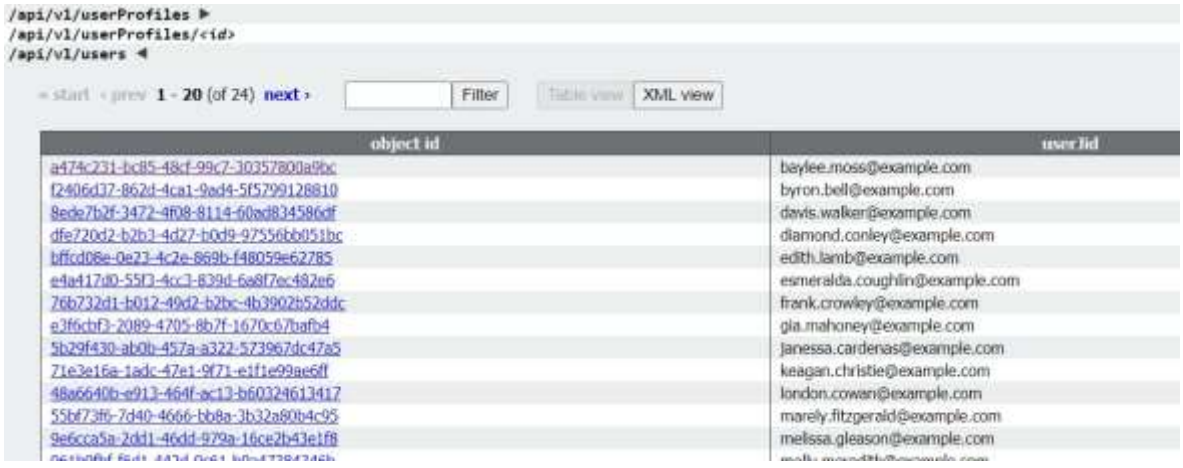
a. Meeting Server Web 管理インターフェイスにログインし、[**設定**（Configuration）] > [API] を選択します。
b. API オブジェクトのリストから、/api/v1/ldapMappings の後ろにある ► をタップします。
c. [**新規作成**（Create new）] をクリックするか、変更する既存の LDAP マッピングの ID を選択します。



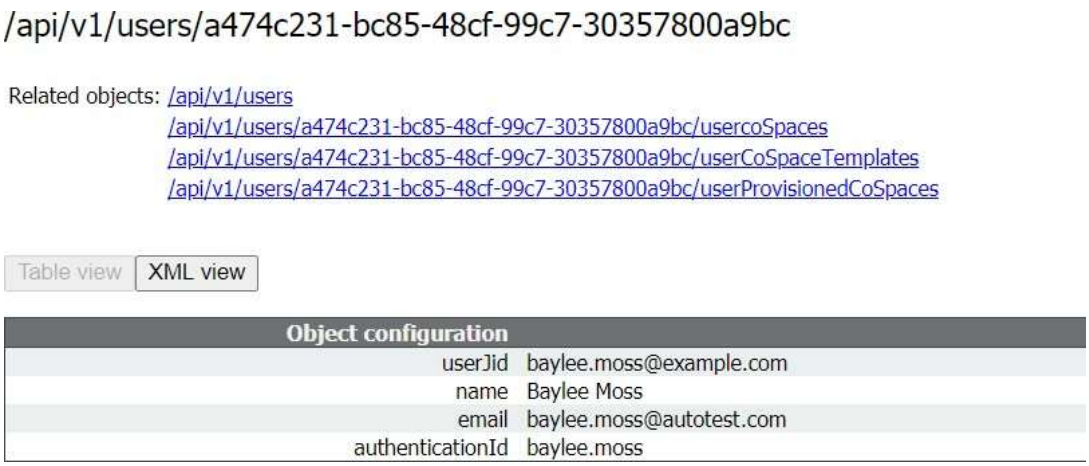
d. authenticationIdMapping パラメータに適切な値（$sAMAccountName$ など）を入力し、必要に応じて [**作成**（Create）] または [**変更**（Modify）] をクリックします。

e. ミーティングサーバで変更を有効にするには、ldapSync をトリガーする必要があります。API オブジェクトのリストから 、/api/v1/ldapSyncs **の後にある「▶」をタップし、必要に応じて**オブジェクト ID **または新規作成**を選択します。ldapSync が終了したら、Meeting Server ユーザの 1 人を調べて、このプロセスが成功したと確認できます。

f. まず、API オブジェクトのリストから、/api/v1/users の後にある「▶」をタップして、この例に示すユーザのリストを表示します。



g. authenticationId を設定する必要があるユーザを 1 人選択します（[フィルタ] フィールドを使用する必要がある場合があります）。この例に示すように、ユーザエントリには ldapSync から正しい値の authenticationId フィールドが含まれる必要があります。



タスク 2：アイデンティティプロバイダーの設定

1. すべてのアイデンティティプロバイダーは、サービスプロバイダーが登録されている（つまり、この場合の Meeting Server ）を表す、メタデータの xml ファイルをアップロードできます。一部のアイデンティティプロバイダーは、最も重要な情報を構成できるようにすることで、プロセスを簡素化します。メタデータ xml ファイルの例はここにあります。

   アイデンティティプロバイダーにアップロードされるメタデータの xml ファイルに含める値は次のとおりです。

   a. entityID：これは Web ブリッジの 3 アドレス（つまり、https://<domain>:port）です。このアドレスは、Web アプリユーザのブラウザから到達可能な有効な Web ブリッジ 3 アドレスである必要があります。

      注：導入環境に複数の Web ブリッジ 3 が導入されている場合は、負荷分散されたアドレスを使用する必要があります。

   b. 形式「https://<domain>:<port>/api/auth/sso/idpResponse」に従って entityId として定義された Web ブリッジアドレスの HTTP-POST AssertionConsumerService。

   c. オンプレミスの場合、HTTPのデフォルトは8090、HTTPSのデフォルトは8181です。アイデンティティプロバイダーが AuthnRequest 署名を検証する署名用の公開キー。

   d. オンプレミスの場合、HTTPのデフォルトは8090、HTTPSのデフォルトは8181です。アイデンティティプロバイダーが上記のアドレスを介して転送可能な Web ブリッジ 3 に送り返される情報を暗号化する暗号化用の公開キー。

注：Meeting Server では、メッセージに送信されたメッセージは、応答および/または電子メールレベルのアイデンティティプロバイダーによって署名されている必要があります。署名されていない通信は破棄されます。

2. アイデンティティプロバイダーから渡されたカスタムパラメータを正常な応答で設定する必要があります。各ユーザのコンテンツは、その Meeting Server ユーザの authenticationId として設定済みの値（たとえば、$sAMAccountName$）と一致する必要があります。通常、アイデンティティプロバイダーには、サービスプロバイダーエントリの作成の一部として特別なフォームまたはダイアログが表示されます。このパラメータは、任意の名前を選択できます。ただし、「uid」など、覚えやすいものを選択することをお勧めします（タスク 3 で名前が必要です）。

タスク 3：SSO アーカイブ zip ファイルの作成

1. Meeting Server を構成するには、その Meeting Server 上の Web Bridge 3 用に構成する SSO ごとに、sso_ <name>.zip という名前のアーカイブ zip ファイルを作成する必要があります。ファイル名は「sso_」で始まり、その後に意味のある名前を付ける必要があります。

   次のファイルを含む zip アーカイブファイルを作成します。

   a. idp_config.xml:これは、管理者が ID プロバイダーから受け取るファイルです。

   b. config.json：次が含まれます。

      - supportedDomains（文字列の配列）：Meeting Server ユーザがこのアイデンティティプロバイダーに対して認証を受け取るすべてのドメインの一覧です。つまり、タスク 1 の例を使用すると、supportedDomains には「example.com」の単一のエントリが含まれます。
      - authenticationIdMapping（文字列）：Meeting Server の authenticationIds に一致するタスク 2（「uid」など）の一部として設定されたアイデンティティプロバイダーの応答からパラメータの名前。SSO 用の Web アプリユーザには、authenticationIds がセットアップされている必要があります（タスク 1 を参照）。
      - ssoServicePro providererAddress（文字列）：アイデンティティプロバイダーが応答を送信するアドレス。これはタスク 2 の entityID で指定されている Web ブリッジ 3 と一致します。

   c. オプション。sso_sign.key：アイデンティティプロバイダー側で設定された公開署名キーの秘密キー。これは、Meeting Server からの発信 AuthnRequest に署名するために使用され、アイデンティティプロバイダー側の公開キーを使用して検証できます。

   d. オプション。 sso_encrypt.key：アイデンティティプロバイダー側で設定された公開暗号キーの秘密キー。これは、アイデンティティプロバイダー側の公開キーで暗号化された Meeting Server メッセージの復号化に使用されます。

   注：アイデンティティプロバイダーごとに異なる名前付き zip ファイルが必要です。

2. SSO ファイルを含むアーカイブ（zip）ファイルを作成します。

注：ファイルを圧縮する場合は、SSO ファイルを含むフォルダを圧縮して使用することはできません。これを行うと、フォルダの追加レイヤーが作成されます（zipファイル > フォルダー > SSOファイル）。代わりに、SSO ファイルを強調表示して右クリックして圧縮します（または、zip アプリケーションを開いてまとめて圧縮します）。これにより、フォルダの追加レイヤーを作成せずに、SSO ファイルを含む zip ファイルが作成されます（たとえば、zipファイル> SSOファイル）。

タスク 4：SSO アーカイブ zip のアップロード

SSO アーカイブ zip をアップロードし、ローカルの Web ブリッジ 3 でホストする必要があります。

注: 次の手順のコマンドは、コンソール/端末環境（コマンドプロンプトまたは端末）用であり、WinSCP などの SFTP クライアントには対応していません。

1. この zip アーカイブをローカルにホストする予定の Web Bridge 3 を有効化した Meeting Server ごとに、次の手順を実行します。
2. a. SFTP クライアントを MMP の IP アドレスに接続します。
   b. MMP の admin ユーザのログイン情報を使用してログインします。
   c. zip ファイル **sso_<name>.zip** をアップロードします。例：
   ```
   PUT sso_<name>.zip
   ```
   d. SSH クライアントを MMP の IP アドレスに接続します。
   e. MMP の admin ユーザのログイン情報を使用してログインします。
   f. Web Bridge 3 を再起動します。
   ```
   webbridge3 restart
   ```
3. 新しい SSO アーカイブファイルは、再起動後にピックアップされます。

注：Web アプリユーザがログインすると、Web アプリ アプリケーション上で、アイデンティティプロバイダーを持つユーザとは別のセッションが行われます。これは、同じユーザ名を入力した後に ID プロバイダ ではなく、Web アプリケーションからログアウトやサインアウトしても、Web アプリケーションに自動的に再許可されることを意味します。ただし、アイデンティティプロバイダーからサインアウトした場合、Web アプリアプリケーションからサインアウトされません。Web アプリアプリケーションからサインアウトする必要があります。このブラウザセッションに再度ログインできないようにするには、Web アプリケーションと ID プロバイダーの両方からサインアウトする必要があります。

2.7.2　例 1 config.json ファイル

次は config.json ファイルの例です。

```
{
    "authenticationIdMapping" : "<parameter_from_task_2>",
    "ssoServiceProviderAddress" : "https://<domain>:<port>",
    "supportedDomains" : ["<domain1>","<domain2>"]
}
```

2.7.3　例 2 シンプルなサービスプロバイダーのメタデータファイル。

これはシンプルなサービスプロバイダーのサンプルです。管理者は関連値を設定し、<domain> and <port> を変更する必要がある点に注意してください

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="https://<domain>:<port>" entityID="https://<domain>:<port>">
  <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</md:NameIDFormat>
    <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://<domain>:<port>/api/auth/sso/idpResponse" index="0"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

2.7.4　例 3 包括的なサービスプロバイダーのメタデータファイル。

これは、署名キーと暗号キー用の xml を含む、包括的なデータファイルの例です。

注：キーは、使用パラメータ（「encryption」または「signing」）に従って、対応する KeyDescriptor 要素の X509Cert いたサブ要素に配置する必要があります。キーのテキストコンテンツを「...」に置き換える必要があります（例：ds:X509CertificateMIID**<omitted_key_text>**+gb</ds:X509Certificate>）。

注：署名証明書を含めると、値 AuthnRequestsSigned は「true」に設定されます（例 2 のより単純なメタデータファイルでは「false」に設定されます）。

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="https://<domain>:<port>" entityID="https://<domain>:<port>">
  <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
         <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>...</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>...</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</md:NameIDFormat>
    <md:AssertionConsumerService
```

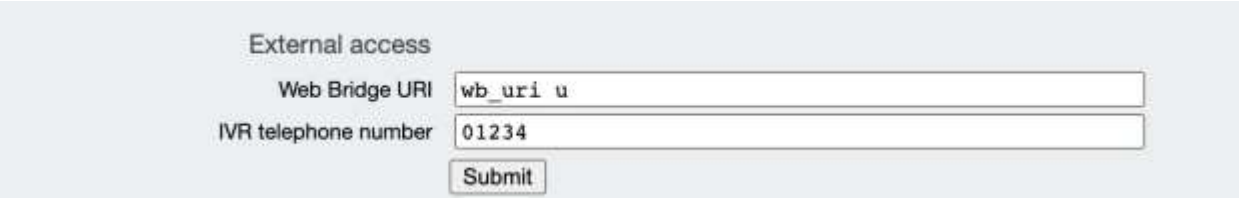
```
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://<domain>:<port>/api/auth/sso/idpResponse" index="0"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

2.8 Web 管理ユーザ インターフェイスの変更

バージョン 3.1 では、外部アクセス設定の Web 管理者ユーザインターフェイスが変更されます。

Web Bridge URI および IVR **電話番号**の設定を許可していた Web Admin ユーザインターフェイスの [構成 > 一般] ページの外部アクセスが削除されます。これらの構成フィールドは、Web ブリッジプロファイルに移動されました。

図 2：Web Admin **ユーザインターフェイスから削除された外部アクセス設定**



外部アクセスにあるフィールド は、 3.1 で次のように扱われます。

- Web Bridge URI：webBridgeProfiles API に移動
- IVR **の電話番号**：webBridgeProfiles API に移動

また、複数の IVR 番号と Web ブリッジアドレス（Web ブリッジプロファイルあたり最大 32 の IVR 番号と最大 32 の Web ブリッジアドレス）を指定できるようになりました。これらは、参加情報の表示、および電子メール招待の生成に使用されます。

注：ivrNumbers と webBridgeAddresses の構成には、システムレベルまたはテナントレベル（マルチテナンシーを使用している場合）で webBridgeProfile を使用することを強くお勧めします。

2.8.1　API の追加と変更

これらの新機能をサポートするため、バージョン 3.1 では、次の新しい API オブジェクトが導入されました。

- **/webBridgeProfiles/<web bridge profile id>/ivrNumbers**
- **/webBridgeProfiles/<web bridge profile id>/ivrNumbers/<ivr number id>**
- **/webBridgeProfiles/<web bridge profile id>/webBridgeAddresses**
- **/webBridgeProfiles/<web bridge profile id>/webBridgeAddresses/<web bridge address id>**

これらの各オブジェクトは、文字列形式 の**ラベル**および**番号**パラメータをサポートします。

次の新しい API エラーコードの理由は、バージョン 3.1 で導入され、これらの機能の変更に対応しています。

- **webBridgeAddressDoesNotExist**：有効な Webブリッジアドレスに対応していない ID を使用して、Webブリッジアドレスを変更、削除、または取得しようとしました。
- **ivrNumberDoesNotExist**：有効な IVR 番号に対応していない ID を使用して、IVR 番号の変更、削除、または取得を試みました。
- **maxNumberOfWebBridgeAddressesReached**：許可されるエントリの最大数がすでに定義されている Web ブリッジプロファイルに新しい Web ブリッジアドレスを追加しようとしました。別のものを追加できるようにするには、1 つを削除してください。
- **maxNumberOfIvrNumbersReached**：許可されているエントリの最大数がすでに定義されている Web ブリッジプロファイルに新しい IVR 番号を追加しようとしました。別のものを追加できるようにするには、1 つを削除してください。

次の応答値は、/accessQuery 応答で廃止になりました

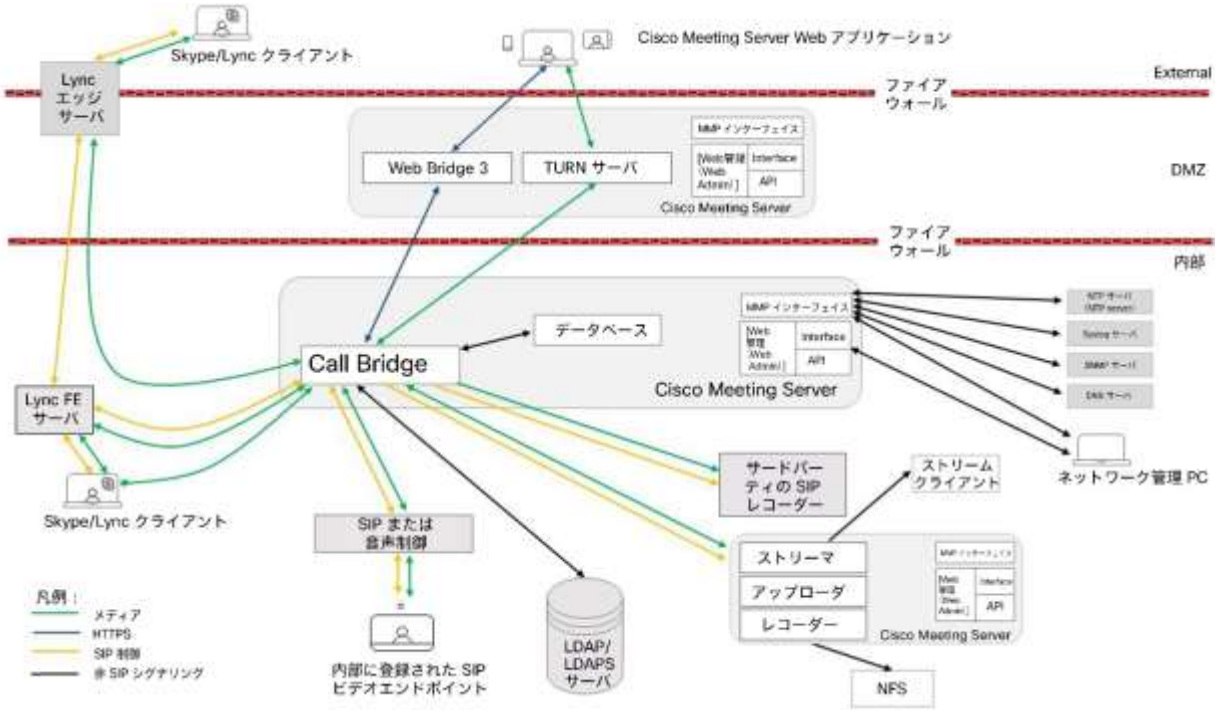
- **webAddress**
- **ivr**

2.9 Cisco Meeting Server の Web エッジソリューションの規模

Expressway（Large OVA または CE1200）は、Web アプリの規模が小～中の要件（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。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。

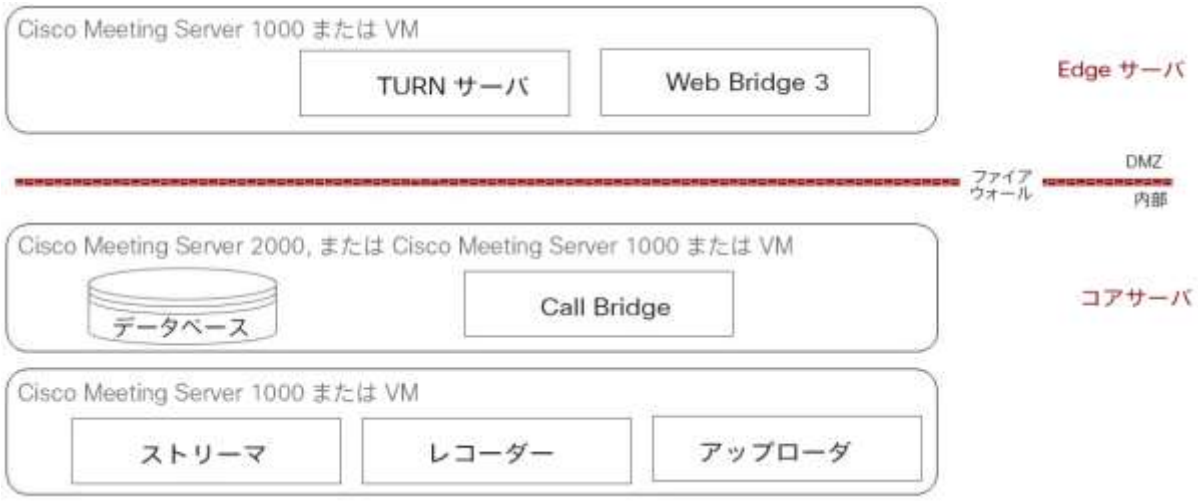
リモートワークの需要が高まり、Web アプリの規模を拡大する必要性が高まっているため、Cisco Meeting Server バージョン 3.1 が開発およびテストされ、この Web アプリの規模の拡大にエッジサポートを提供しています。図 3 は、Meeting Server Web エッジソリューションを導入して Web アプリの規模を拡大するために導入を最適化する方法の例を示しています。

図 3：分割サーバ展開で TURN サーバコンポーネントを使用する Meeting Server Web エッジ導入例



エッジサーバとして使用する場合、Meeting Server は、図 4 に示すように、既存の TURN サーバおよび Web アプリコンポーネント（コールブリッジコンポーネントではない）を使用します。

図 4：TURN サービスを提供する Cisco Meeting Server とサーバを分割する



注：これらすべてのコンポーネントを設定する必要があるだけでなく、導入環境に適したコンポーネントを設定する必要があります。

注：コアサーバとエッジサーバはどちらも、同じバージョンのソフトウェアを実行する必要があります。

Meeting Server Web エッジソリューションをサポートするために、新しい MMP コマンド **`turn high-capacity-mode (enable|disable)`** が導入され、TURN の拡張モードが有効になります。デフォルトでは有効になっています。

セクション 2.9.2 に説明があるように、2 つのサーバ仕様のいずれかを使用して Cisco Meeting Server Web エッジを実行することをお勧めします。推奨ハードウェアを備えたサーバ仕様を使用して達成できる通話容量を表 8 に示します。

表 8：推奨されるハードウェアを使用するサーバ仕様の通話容量

コールのタイプ	1 x 4 vCPU VM call capacity	1 x 16 vCPU VM call capacity
Full HD calls 1080p30 video	100	350
HD calls 720p30 video	175	700
SD calls 448p30 video	250	1000
音声通話（G.711）	850	3000

2.9.1　注意すべき重要なポイント：

- Web アプリが SIP スケールと一致する（クラスタごとに最大 24 のコールブリッジ）、複数のエッジサーバがサポートされます。ただし、コールブリッジグループ（各コールブリッジグループが最大 10 エッジサーバをサポート）は、コールブリッジグループごとに最大 10 台のエッジサーバを使用し、10 台を超えるエッジサーバが必要な導入では必要です。

  注：8 個以上のエッジサーバが必要な導入については、BU による確認が必要です。

- すべてのエッジサーバの容量を同じにすることをお勧めします。つまり、4 つの vCPU すべてまたは 16 の vCPU すべてを、両方を組み合わせて使用するのではなく、同じ容量にすることをお勧めします。
- コールブリッジ グループを設定することをお勧めします。これにより、各コールブリッジグループに TURN サーバの一意のグループを割り当てると、次の場合に便利です。
  - 負荷分散の支援
  - TURN サーバをコールブリッジで適切に地理的に配置し続ける
- エッジサーバのスケーリング：「コアコールブリッジ」と「エッジ VM」の比率は、many:1, 1:1, または 1:many のいずれかにすることをお勧めします。

- 1 つの vCPU から 1 つの物理 CPU をお勧めします。
- 同じ場所でのサポート：エッジ サーバを他の VM と同じ場所に常駐することができます。ただし、4 つの vCPUVM ごとに 1 Gbps の NIC 要件があり、16 の vCPU ごとに 10 Gbps の NIC 要件があります。VM ホストには、すべてのアプリケーションに十分な NIC 容量が必要です。

注：Meeting Server 1000 M4 ハードウェアは、1 Gbps NIC をサポートし、M5 は 10 個のネットワーク NIC をサポートします。

- 2.5GHz 以上で実行されている Intel Xeon E5 2600 などのプロセッサ仕様を推奨します。

2.9.2 推奨される Meeting Server の Web エッジサーバの仕様

サーバの仕様 A

- サポートされている Cisco ハードウェアについて次の仕様の 1x Cisco Meeting Server： VM 4 GB RAM、4 vCPU、1Gbps ネットワークインターフェイス。
  - 次の使用をお勧めします。
    - Cisco Meeting Server 1000 あたり 1 x Meeting Server VM。
      または
    - Cisco Meeting Server 2000 あたり 4 x Meeting Server VM。

サーバの仕様 B

- サポートされている Cisco ハードウェアについて次の仕様の 1 Cisco Meeting Server： VM 8 GB RAM、4 vCPU、1Gbps ネットワークインターフェイス。
  - 次の使用をお勧めします。
    - 1 x Meeting Server VM は、最大 4 x Cisco Meeting Server 1000 または 1000 台まで使用できます。または、
    - 1 x Meeting Server VM は、1 x Cisco Meeting Server 2000 にサービスを提供できます。

2.9.3 Meeting Server Web エッジの展開

分割展開での Meeting Server の構成に関する包括的な情報は、ここの導入ガイドに記載されています。次の手順は、Meeting Server Web エッジを導入する方法の概要を示しています。

1. MMP を使用して Meeting Server エッジ上で TURN サーバを設定します。
2. MMP を使用して Meeting Server エッジに Web ブリッジ 3 を設定します。
3. Web Bridge 3 を CallBridge にリンクします（つまり、**構成と** API **の下の** Web 管理ユーザインターフェイスを介して callBridge パラメータ**を** /api/v1/turnServers **と** /api/v1/webBridges に**追加**し、Web Bridge 3 の証明書要件を確認します）。

4. 接続が正しく機能していることを確認します。これを行うには、Web アプリのアドレスからログインして手動でテストするか、Web 管理インターフェイスの [**ステータス**] と [**一般**] で**障害状態**と**最近のエラーと警告**を確認します。（Web Bridge 3/TURN 接続失敗メッセージは表示されないことに注意してください。）
5. ファイアウォールの設定を次のように追加します。
   a. TCP接続WebBridge 3 c2w 接続ポートを開く必要があります（API の「c2w://address:port」で指定されているように、つまり /api/v1/webBridges の url フィールドで指定されています）。
   b. コールブリッジから Meeting Server エッジの TCP 3478 上で接続を確立できる必要があります（つまり、TURN サーバコンポーネントと通信が可能）。
   c. Meeting Server エッジの TURN リレーポートは 50000～62000 であるため、コールブリッジと外部接続が UDP 上のポートに接続してメディアを送信できる必要があります。

2.10 Cisco Meeting Server エッジの短期的な資格情報

セキュリティを強化するため、3.1 では Cisco Meeting Server エッジ用の短期的な資格情報を導入しました。3.1 が最初にリリースされたとき、これは限られたソリューションテストのためにベータ機能でした。これでテストが完了し、機能が完全にサポートされます。したがって、「ベータ機能」の警告は削除されました。この機能はオプションであり、有効にすると、各資格情報セットは 24 時間有効になります。

デフォルトでは、Meeting Server TURN サーバコンポーネントは、引き続き長時間の資格情報を使用します。短期的なクレデンシャル機能を試す場合は、以下に詳細を示す新しい MMP コマンドと API パラメータを使用する必要があります。

注：TURN サーバコンポーネントは、UDP 用の標準ポート 3478 を常にサポートします。

2.10.1 MMP の追加

この機能では、次の新しい MMP コマンドが導入されます。

`turn short_term_credentials_mode (enable|disable)` ：TURN サーバを短期および長期のクレデンシャルモードに切り替えます。デフォルトは**無効**です。

`turn short_term_credentials <shared secret> <realm>` ：TURN サーバが短期的なクレデンシャルを使用するために必要な共有秘密とレルムを指定します。

2.10.2 API の変更

新しいパラメータ **`useShortTermCredentials`** と **`sharedSecret`** が **`/turnServers`** オブジェクト**に追加されます。**

- **use3rt Credentialials** ：true | false：この TURN サーバで短期的なクレデンシャルを使用する必要があるかどうか。作成（POST）操作でこのパラメータが指定されない場合、デフォルトは false になります。
- **sharedSecret** ：この TURN サーバで割り当てを行う際に使用する必要がある共有秘密（文字列）です（短期的なクレデンシャルモードが有効な場合）

2.10.2.1 パラメータの更新

/turnServers の既存の**ユーザ名**と**パスワード**のパラメータは、短期クレデンシャルモードが無効になっている場合にのみ適用されるようになりました。

2.10.3　Meeting Serverでの短期的な資格情報の実装

これらの手順は、すでにバージョン 3.1 にアップグレード済みであることを前提にしています。

注：タスク 1 とタスク 2 を逆にし、MMP ステップの前に API 構成を実行することもできますが、sharedSecret は両方の場所で同じである必要があります。

タスク 1：MMP を介した短期的なクレデンシャルの有効化と設定

1. MMP に SSH でログインします。
2. **turn short_term_credentials_mode enable** と入力して、短期クレデンシャルモードを有効にします。
3. **turn short_term_credentials <shared secret> <realm>** と入力して、必要な共有シークレットとレルムを設定します。例：**turn short_term_credentials mysharedsecret example.com**

タスク 2：API を介して短期的な資格情報を使用するための TURN サーバの設定

Meeting Server Web Admin インターフェイスを使用して TURN サーバの短期的な資格情報を設定するには、次の手順を実行します。

4. Meeting Server Web 管理インターフェイスにログインし、**[設定（Configuration）] > [API]** を選択します。
5. API オブジェクトのリストから、**/api/v1/turnServers** の後ろにある ► をタップします。
6. 既存の TURN サーバを構成または変更するには、**[新規作成]**または必要な既存の TURN サーバのオブジェクト ID を選択し、useShortTermCredentials **フィールドを true に設定します**。
7. **sharedSecret** フィールドに共有シークレット（タスク 1 のステップ 3 で設定）を入力します。
8. 新しい TURN サーバを構成する場合は **[作成]** をクリックし、既存のサーバを構成する場合は **[変更]** をクリックします。

2.11　スケジュールされた LDAP 同期 – API のタイムスタンプ追加

バージョン 3.1 では、ldapSync API オブジェクトに新しい 3 つのタイムスタンプが導入されています。これは、Meeting Server API と Meeting Management の両方で、管理者に関する追加情報を提供します。

3つのパラメーターは、GET の /ldapSyncs/<sync id> で使用できます。/ldapSync の GET の列挙リストに返されます。POST または PUT では、パラメータを設定できません。新しいパラメータは次のとおりです。

- **creationTime**：同期オブジェクトが作成された日時のタイムスタンプ。
- **startTime**：同期操作が開始された時刻のタイムスタンプ。
- **endTime**：同期操作が終了した日時のタイムスタンプ（成功または失敗）。

注：3 つのタイムスタンプのすべてについて、時刻は UTC です – RFC 3339 で指定されている形式/タイムゾーンです。例:「2014-02-11T12:10:47Z」など。

注：LDAP 同期は Web Admin ユーザインターフェイス から開始することもできますが、API で Web 管理者が開始した LDAP 同期を示します。したがって、Web 管理者が開始した LDAP 同期では、これらの新しいタイムスタンプの詳細にアクセスできます。

2.12　ldapSources API オブジェクト上の名前ラベル

バージョン 3.1 では、/ldapSources API オブジェクトに名前ラベルを設定できます。これは Meeting Server API の管理者に関する追加情報を提供し、Meeting Management のユーザエクスペリエンスも向上します。

Meeting Management には、テンプレートと一致するユーザインポートを管理者が選択する必要があるインターフェイスがあります。3.1 から、名前ラベルが設定されている場合は、ドロップダウンリストに表示される名前ラベルから、必要なユーザインポートを簡単に識別できます。

この名前ラベルの追加では 、/ldapSources オブジェクトに API パラメータ**名**が導入されます。ldapSources の名前は任意であり、デフォルトは空の文字列です。このパラメータは、次の操作をサポートします。

- **/ldapSources** への POST
- **/ldapSources/<ldap source id>** での PUT
- **/ldapSources** での GET の列挙
- **/ldapSources/<ldap source id>** での GET

2.13 API の追加および変更の概要

Meeting Server 3.1 の新しい API 機能には次のものが含まれます。

- coSpace プロビジョニングに対応する新しい API オブジェクトとパラメータ
- Web アプリのカスタム電子メール招待の変更に対応する新しい API オブジェクトとパラメータ（webBridgeProfiles）

2.13.1 API の追加

バージョン 3.1 では、次の新しい API オブジェクトが導入されました。

- **/ldapUserProvisionedCoSpaceMappings**
- **/ldapUserProvisionedCoSpaceMappings/<LDAP user provisioned coSpace mapping id>**
- **/ldapUserProvisionedCoSpaceSources**
- **serProvisionedCoSpaceSources/<LDAP user provisioned coSpace mapping id>**
- **/ldapUserProvisionedCoSpaceSources/<LDAP user provisioned coSpace source id>**
- **/users/<user id>/userProvisionedCoSpaces**
- **/users/<user id>/userProvisionedCoSpaces/<user provisioned coSpace id>**
- **/webBridgeProfiles/<web bridge profile id>/ivrNumbers**
- **/webBridgeProfiles/<web bridge profile id>/ivrNumbers/<ivr number id>**
- **/webBridgeProfiles/<web bridge profile id>/webBridgeAddresses**
- **/webBridgeProfiles/<web bridge profile id>/webBridgeAddresses/<web bridge address id>**

次のバージョン 3.1 で導入された新しい API エラーコードの理由。

- **ldapUserProvisionedCoSpaceMappingDoesNotExist**：有効な LDAP ユーザプロビジョニングされた coSpace マッピングに対応しない ID を使用して、LDAP ユーザプロビジョニングされた coSpace マッピングを変更または削除しようとしました。
- **userProvisionedCoSpaceDoesSpaceExist**：ユーザがプロビジョニングした coSpace を、そのユーザの有効なユーザ プロビジョニング coSpace に対応していない ID を使用して変更、削除、取得を試みました。
- **ldapUserProvisionedCoSpaceSourceDoesNotExist**：有効な LDAP ユーザプロビジョニングされた coSpace ソースに対応しない ID を使用して、LDAP ユーザプロビジョニングされた coSpace ソースを変更または削除しようとしました。
- **webBridgeAddressDoesNotExist**：有効な Webブリッジアドレスに対応していない ID を使用して、Webブリッジアドレスを変更、削除、または取得しようとしました。
- **ivrNumberDoesNotExist**：有効な IVR 番号に対応していない ID を使用して、IVR 番号の変更、削除、または取得を試みました。

- **maxNumberOfWebBridgeAddressesReached**：許可されるエントリの最大数がすでに定義されている Web ブリッジプロファイルに新しい Web ブリッジアドレスを追加しようとしました。別のものを追加できるようにするには、1 つを削除してください。
- **maxNumberOfIvrNumbersReached**：許可されているエントリの最大数がすでに定義されている Web ブリッジプロファイルに新しい IVR 番号を追加しようとしました。別のものを追加できるようにするには、1 つを削除してください。

サポートされている新しい API タイプ：

- on request parameter scope for POST to **/coSpaces/<coSpace id>/accessMethods** and PUT to **coSpaces/<coSpace id>/accessMethods/<access method id>.**
  - **member**：この coSpace アクセス方式の詳細は、coSpace のメンバーに表示されます。
  - **Directory**：この coSpace アクセス方式の詳細は検索で確認できます [注：3.1 では検索は行っていないため、動作は**パブリックと同じです**]

  また、パブリックおよび**プライベート用の既存の** API **タイプの定義は**更新されます。
  - **public**：この coSpace アクセス方式の詳細は、coSpace のメンバーおよび会議のすべての参加者に表示されます。
  - **private**：この coSpace アクセス方式の詳細は、Web アプリ内のスペースの所有者にのみ表示されます。または Call Bridge API を使用して管理ユーザに表示されます。

3.1 でサポートされている新しい API 要求パラメータ：

- **muteBehavior** parameter on POST to **/callProfiles**; PUT to **/callProfiles/<call profile id>**; GET on **/callProfiles/<call profile id>**
- **passthroughMode** H.264パススルー機能を許可するかどうかを制御するパラメータ。Introduced for POST on **/compatibilityProfiles**; PUT to **/compatibilityProfiles/<compatibility profile id>**, and GET on **/compatibilityProfiles/<compatibility profile id>** 値は次のとおりです。
  - **enabled**：可能な場合、ビデオのトランスコーディングを避けることを可能にします（設定されていない場合はデフォルト）
  - **無効化**：常にビデオをトランスコードする
- **userProvisionedCoSpace** パラメータが /cospaces オブジェクトに導入されます。
- **name** parameter introduced on POST to **/ldapSources**, PUT to **/ldapSources/<ldap source id>**, Enumerate of GET on **/ldapSources**, and GET on **/ldapSources/<ldap source id>**
- **creationTime**, **startTime**, **endTime** URI parameters are introduced on GET on**/ldapSyncs/<sync id>**
- **useShortTermCredentials** added on POST to **/turnServers** and PUT to **/turnServers/<turn server id>** objects, and GET on **/turnServers/<turn server id>**.

- **sharedSecret** are added on POST to **/turnServers** and PUT to **/turnServers/<turn server id>** objects.

API パラメータは 3.1 で更新されました。

- **/turnServers** の既存の**ユーザ名**と**パスワード**のパラメータは、短期クレデンシャルモードが無効になっている場合にのみ適用されるようになりました。

3.1 での API パラメータ廃止：

次のパラメータは、/ldapmappings オブジェクトで廃止されました。

- **coSpaceUriMapping**
- **coSpaceSecondaryUriMapping**
- **coSpaceNameMapping**
- **coSpaceCallIdMapping**

次のパラメータは 、**/system/status** 応答で廃止されました。

- **有効**

次のパラメータは 、**/system/multipartyLicensing** 応答で廃止 されました。

- **personalLicenseLimit**
- **sharedLicenseLimit**
- **capacityUnitLimit**

次の応答値は、**/accessQuery** 応答で廃止になりました。

- **webAddress**
- **ivr**

表示されたが、3.0 で機能しない **resolveLyncConferenceIds** パラメータは、次の API から削除されます。**/webBridgeProfiles/<webBridge profile id>** **/system/profiles/effectiveWebBridgeProfile**, **/tenant/<tenant id>/effectiveWebBridgeProfile**、, and **/webBridges/<web bridge id>/effectiveWebBridgeProfile.**

バージョン 3.1 で次の API エラーコードの理由が削除されます。

- **messageDoesNotExist**

2.13.2　LDAP ユーザがプロビジョニングした coSpace マッピングの作成、変更、および取得

この新しい API オブジェクトは以下の操作をサポートします。

- POST to **`/ldapUserProvisionedCoSpaceMappings`**
- PUT to **`/ldapUserProvisionedCospaceMappings/<LDAP user provisioned coSpace mapping id>`**

パラメータ	タイプ/値	説明/メモ
coSpaceUriMapping (*)	string	ldapMappings オブジェクトのマッピングと同様に、ユーザがプロビジョニングした coSpace の URI を生成するためのテンプレート。（バージョン 3.1 より）
coSpaceNameMapping	string	ldapMappings オブジェクトのマッピングと同様に、ユーザがプロビジョニングした coSpace の名前を生成するためのテンプレート。（バージョン 3.1 より）
coSpaceTemplate (*)	ID	ユーザがプロビジョニングした coSpace に使用する coSpace テンプレート。（バージョン 3.1 より）

- **`/ldapUserProvisionedCospaceMappings`** の計数は以下の URI パラメータを受け入れます。

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

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

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

応答要素	タイプ/値	説明/メモ
coSpaceUriMapping	string	ldapMappings オブジェクトのマッピングと同様に、ユーザがプロビジョニングした coSpace の URI を生成するためのテンプレート。（バージョン 3.1 より）
coSpaceNameMapping	string	ldapMappings オブジェクトのマッピングと同様に、ユーザがプロビジョニングした coSpace の名前を生成するためのテンプレート。（バージョン 3.1 より）
coSpaceTemplate	ID	ユーザがプロビジョニングした coSpace に使用する coSpace テンプレート。（バージョン 3.1 より）

- プロビジョニングされた個々の LDAP ユーザの coSpace マッピングでの GET は、

/ldapUserProvisionedCospaceMappings/<LDAP ユーザプロビジョニングされた coSpace マッピング id> は次の応答を示します。

応答要素	タイプ/値	説明/メモ
coSpaceUriMapping	string	ldapMappings オブジェクトのマッピングと同様に、ユーザがプロビジョニングした coSpace の URI を生成するためのテンプレート。（バージョン 3.1 より）
coSpaceNameMapping	string	ldapMappings オブジェクトのマッピングと同様に、ユーザがプロビジョニングした coSpace の名前を生成するためのテンプレート。（バージョン 3.1 より）
coSpaceTemplate	ID	ユーザがプロビジョニングした coSpace に使用する coSpace テンプレート。（バージョン 3.1 より）

2.13.3　LDAP ユーザがプロビジョニングした coSpace ソースの作成、変更、および取得

この新しい API オブジェクトは以下の操作をサポートします。

- POST to **/ldapUserProvisionedCoSpaceSources**
- PUT to **/ldapUserProvisionedCoSpaceSources/<LDAP user provisioned coSpace source id>**

パラメータ	タイプ/値	説明/メモ
ldapSource (*)	ID	ユーザの特定に使用される LDAP ソースの ID（バージョン 3.1 から）
ldapUserProvisionedCoSpace Mapping (*)	ID	マッピングを使用して、ユーザがプロビジョニングした coSpaces の名前と uri-hint を生成するために使用します（バージョン 3.1 から）
filter	string	送信元の読み取り時に適用される追加の LDAP フィルタ文字列（バージョン 3.1 から）

- **/ldapUserProvisionedCoSpaceSources** の計数は以下の URI パラメータを受け入れます。

URI パラメータ	タイプ/値	説明/メモ
offset		名目上のリストの 1 ページ目にある以外のエントリを取得するために、オフセットと制限を指定できます。（バージョン 3.1 から）
limit		

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

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

応答要素	タイプ/値	説明/メモ
ldapSource	ID	ユーザの特定に使用される LDAP ソースの ID（バージョン 3.1 から）
ldapUserProvisionedCoSpaceMapping	ID	マッピングを使用して、ユーザがプロビジョニングした coSpaces の名前と uri-hint を生成するために使用します（バージョン 3.1 から）
filter	string	送信元の読み取り時に適用される追加の LDAP フィルタ文字列（バージョン 3.1 から）

- **/ldapUserProvisionedCoSpaceSources/<LDAP user provisioned coSpace mapping id>** を使用して、個々の LDAP ユーザがプロビジョニングされた coSpace ソースで GET を 実行する。LDAP ユーザプロビジョニングされた coSpace マッピング ID は次の応答を示します。

応答要素	タイプ/値	説明/メモ
ldapSource	ID	ユーザの特定に使用される LDAP ソースの ID（バージョン 3.1 から）
ldapUserProvisionedCoSpaceMapping	ID	マッピングを使用して、ユーザがプロビジョニングした coSpaces の名前と uri-hint を生成するために使用します（バージョン 3.1 から）
filter	string	送信元の読み取り時に適用される追加の LDAP フィルタ文字列（バージョン 3.1 から）

2.13.4　ユーザがプロビジョニングした coSpace 情報の取得

バージョン 3.1 では、次の操作をサポートするためにこの API オブジェクトが導入されています。

- **/users/<user id>/userProvisionedCoSpaces** に対する GET の列挙
- **/users/<user id>/userProvisionedCoSpaces/<user provisioned coSpace id>** での GET

/users/<user id>/userProvisionedCoSpaces の列挙は次の URI パラメータを受け入れます。

URI パラメータ	タイプ/値	説明/メモ
offset		名目上のリストの 1 ページ目にある以外のユーザがプロビジョニングした coSpaces を取得するために、オフセットと制限を指定できます。（バージョン 3.1 より）
limit		

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

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

応答要素	タイプ/値	説明/メモ
coSpaceTemplate	ID	この coSpace がインスタンス化されるときに基づく coSpaceTemplate。（バージョン 3.1 より）
uriHint	string	この coSpace の uri の基礎（スペースをインスタンス化するときに他の uri とクラッシュした場合、このヒントに基づいて一意の uri が生成されます）。（バージョン 3.1 より）
name	string	この coSpace がインスタンス化される際に含まれる名前。（バージョン 3.1 より）
coSpace	ID	存在する場合、coSpace の ID は、この userProvisionedCoSpace にインスタンス化されました。（バージョン 3.1 より）

/users/<user id>/userProvisionedCoSpaces/<user provisioned coSpace id> を使用して、個々のユーザがプロビジョニングした coSpace を取得し、次の応答を返します。

応答要素	タイプ/値	説明/メモ
coSpaceTemplate	ID	この coSpace がインスタンス化されるときに基づく coSpaceTemplate。（バージョン 3.1 より）
uriHint	string	この coSpace の uri の基礎（スペースをインスタンス化するときに他の uri とクラッシュした場合、このヒントに基づいて一意の uri が生成されます）。（バージョン 3.1 より）
name	string	この coSpace がインスタンス化された時に持つ名前。（バージョン 3.1 より）
coSpace	ID	存在する場合、coSpace の ID は、この userProvisionedCoSpace にインスタンス化されました。（バージョン 3.1 より）

2.13.4.1　ユーザがプロビジョニングした coSpace からの新しい coSpace のインスタンス化

新しい API パラメータ userProvisionedCoSpace は、「ID」タイプで導入され、ユーザがプロビジョニングした coSpace から新しい coSpace をインスタンス化します。このパラメータが存在する場合、他のすべてのパラメータは無視されます。次の操作で導入されます。

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

2.13.5　webBridgeProfile の Web ブリッジアドレスの作成、変更、および取得

この新しい API オブジェクトは以下の操作をサポートします。

- **/webBridgeProfiles/<web bridge profile id>/webBridgeAddresses** に対する POST 操作
- **/webBridgeProfiles/<web bridge profile id>/webBridgeAddresses/<web bridge address id>** に対する PUT 操作

パラメータ	タイプ/値	説明/メモ
label	string	この **Web** ブリッジアドレスを説明するラベル名。例：**USA Web アプリ**（バージョン 3.1 から）
address	url	電子メール招待をレンダリングするときに使用するアドレス。例：**https://usa.mycompany.com/**（バージョン 3.1 から）

- **/webBridgeProfiles/<web bridge profile id>/webBridgeAddresses** の列挙は、次のURIパラメータを受け入れます。

URI パラメータ	タイプ/値	説明/メモ
offset		名目上のリストの 1 ページ目以外の Web Bridge アドレスを取得する場合は、offset と limit を指定できます。
limit		

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

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

応答要素	タイプ/値	説明/メモ
label	string	この **Web** ブリッジアドレスを説明するラベル名。例：**USA Web アプリ**（バージョン 3.1 から）

- **/webBridgeProfiles/<web bridge profile id>/webBridgeAddresses/<web bridge address id>** を使用して webBridgeProfiles の個々の Web ブリッジアドレスを取得し、次の応答を返します。

応答要素	タイプ/値	説明/メモ
label	string	この Web ブリッジアドレスを説明するラベル名。例：USA Web **アプリ**（バージョン 3.1 から）
address	url	電子メール招待をレンダリングするときに使用するアドレス。例：**https://usa.mycompany.com/**（バージョン 3.1 から）

2.13.6　webBridgeProfile の IVR 番号の作成、変更、および取得

この新しい API オブジェクトは以下の操作をサポートします。

- **/webBridgeProfiles/<web bridge profile id>/ivrNumbers** に対する POST 操作
- **/webBridgeProfiles/<web bridge profile id>/ivrNumbers/<ivr number id>** に対する PUT 操作

パラメータ	タイプ/値	説明/メモ
label	string	この IVR 番号を説明するラベル名。例：**米国のコールイン番号**（バージョン 3.1 から）
番号を入力します	string	電子メール招待をレンダリングするときに使用する IVR 番号。例：888-123123（バージョン 3.1 より）

- **/webBridgeProfiles/<web bridge profile id>/ivrNumbers** の列挙は、次のURIパラメータを受け入れます。

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

応答は、最上位レベルの <ivrNumbers total="N"> タグ（複数の可能性のあり）として構成されています。
その内部の <ivrNumber> 要素。

各 <ivrNumber> タグには、次の要素が含まれる場合があります。

応答要素	タイプ/値	説明/メモ
label	string	この IVR 番号を説明するラベル名。例：**米国のコールイン番号**（バージョン 3.1 から）

- **/webBridgeProfiles/<web bridge profile id>/ivrNumbers/<ivr number id>** を使用して webBridgeProfiles の個々の IVR 番号で GET を実行し、次の応答を返します。

応答要素	タイプ/値	説明/メモ
label	string	この IVR 番号を説明するラベル名。例：**米国のコールイン番号**（バージョン 3.1 から）
番号を入力します	string	電子メール招待のレンダリング時に使用される IVR 番号。例：888-123123（バージョン 3.1 より）

2.13.7 コールのミュート動作の設定

この機能では、次の操作でコールに対して muteBehor パラメータが導入されます。

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

パラメータ	タイプ/値	説明/メモ
muteBehavior	linked | separate	コールのミュート動作を定義します。 • Linked – このモードでは、Meeting Server でユーザの通話がミュートされている場合、エンドポイントまたは Web アプリのセッションでデバイスのローカルミュートが自動的に実行される場合があります。つまり、Meeting Server ミュートのエフェクトを別の API コマンドだけで元に戻す必要があります。ユーザ自身がデバイスのミュートを解除する必要があります。 • separate – このモードでは、Meeting Server とローカルデバイス上のユーザの通話のミュートステータスは互いに独立しています。つまり、他のユーザ/管理者は、すべての参加者をビデオ/音声でミュート/ミュート解除できます。 作成（POST）操作でこのパラメータが指定されない場合、デフォルトは linked になります。（バージョン 3.1 より）

- **/callProfiles/<call profile id>** で GET を実行します。
  応答は、最上位レベルの <callProfiles total="N"> タグ（複数の可能性のあり）として構成されています。
  その内部の <callProfile> 要素。

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

応答要素	タイプ/値	説明/メモ
muteBehavior	linked | separate	コールのミュート動作： • Linked – このモードでは、Meeting Server でユーザの通話がミュートされている場合、エンドポイントまたは Web アプリのセッションでデバイスのローカルミュートが自動的に実行される場合があります。つまり、Meeting Server ミュートのエフェクトを別の API コマンドだけで元に戻す必要があります。ユーザ自身がデバイスのミュートを解除する必要があります。 • separate – このモードでは、Meeting Server とローカルデバイス上のユーザの通話のミュートステータスは互いに独立しています。つまり、他のユーザ/管理者は、すべての参加者をビデオ/音声でミュート/ミュート解除できます。 作成（POST）操作でこのパラメータが指定されない場合、デフォルトは linked になります。（バージョン 3.1 より）

2.13.8 Cisco Meeting Server エッジの短期的な資格情報の構成

この機能により、これらの操作に次の 2 つの新しいパラメータ **useShortTermCredentials** と **sharedSecret** が導入されます。

- **/turnServers** に対する POST 操作
- **/turnServers/<turn server id>** に対する PUT 操作

パラメータ	タイプ/値	説明/メモ
useShortTermCredentials	true | false	この TURN サーバで短期的なクレデンシャルを使用する必要があるかどうか。 作成（POST）操作でこのパラメータが指定されない場合、デフォルトは false になります。（バージョン 3.1 より）
sharedSecret	string	この TURN サーバで alloc- ations を作成するときに使用する必要がある共有秘密（短期的なクレデンシャルモードが有効な場合）。（バージョン 3.1 より）

注：API GET 操作を使用して、/turnServers に対する短期的な TURN クレデンシャルにアクセスできない共有秘密でもできません。

- **`turnServers/<turn server id>`** を使用して個々の TURN サーバで GET を実行し、次の応答を返します。

応答要素	タイプ/値	説明/メモ
useShortTermCredentials	true | false	この TURN サーバで短期的なクレデンシャルを使用するかどうか。 （バージョン 3.1 より）

2.14 MMP の追加および変更の概要

バージョン 3.1 では、MMP に関する以下の変更がサポートされています。

2.14.1 RTMPS ストリーミング

RTMPS ストリーミングをサポートするため、**既存の `tls`** MMP コマンドが拡張され 、RTMPS に対する TLS 信頼の設定がオプションで許可されます。したがって、**`tls <service>` を備えた `MMP` コマンドラインで `tlsrtmps` を**サポートするようになります。

2.14.2 パケットキャプチャの改善

バージョン 3.1 では、以下の MMP コマンドオプションが導入されています。

表 9：バージョン 3.1 pcap MMP コマンドの追加

コマンド	説明
pcap (a|b|c|d|any) [snaplen <n>] [filter <pcap-filter-expression>]	**any は、**複数のインターフェイス、つまり有効なインターフェイスでのパケットキャプチャを許可します（有効になっていないインターフェイスはスキップされます）。 **注：**複数のインターフェイスからキャプチャする場合は、各インターフェイスが別の一時的なファイルにキャプチャされ、キャプチャが停止された時にファイルが統合されるなど、ディスク領域が追加される必要があります 。したがって、複数のインターフェイスでキャプチャするときに使用できるストレージは、単一のインターフェイスでキャプチャするときに使用できるストレージの半分です。 **snaplen は、**キャプチャされた各パケットがそれより長い場合、最大バイト数（n）に切り捨てられます。その結果、より多くのパケットが同じファイルサイズの制限に収まる可能性があります。 **filter は、**文字列内の条件に一致するパケットのみを選択します。これによりキャプチャが関心のあるパケットだけに減り、他のパケットのディスク容量を節約できます。この文字列の解析とパケットフィルタリングは、tcpdumpで使用されるものとまったく同じ基本ライブラリを使用して実行されるため、これはまったく同じ表現力とパフォーマンスを備えています。フィルタ式は、必要に応じて最大約 4080 文字長にすることができます。 バージョン 3.1 から追加された **snaplen** と**フィルタのオプション。**

注：Meeting Server ではパケットをキャプチャすることができますが 、Meeting Server が動作するパケットレートが高い場合、コールの処理における Meeting Server の通常の動作を妨害するのではなく、パケットキャプチャからパケットをドロップする場合があります。パケットキャプチャのパケット損失を回避するために、シスコでは Meeting Server ではなくネットワークスイッチでパケットをキャプチャすることををお勧めします。

2.14.3 Web アプリの規模を拡大する Cisco Meeting Server の Web エッジソリューション

バージョン 3.1 では、以下の MMP コマンドオプションが導入されています。

表 10：MMP コマンド追加の規模を拡大するバージョン 3.1 Meeting Serverweb エッジソリューション

コマンド	説明
高容量モードへの切り替え（有効化|可能）	TURN と Web アプリを実行している Meeting Server の Web アプリの規模の増加（デフォルト有効）のサポートが実装されています。これにより、Web エッジに Meeting Server を使用する場合のパケット処理量が増加します。シスコサポートから推奨されている場合にのみ無効にします。（バージョン 3.1 より）

2.14.4 Cisco Meeting Server エッジの短期的な資格情報

バージョン 3.1 では、以下の MMP コマンドオプションが導入されています。

表 11：Meeting Server エッジ MMP コマンド追加用のバージョン 3.1 の短期的なクレデンシャル

コマンド	説明
short_term_credentials_ モードをオンにする（有効化|無効化）	TURN サーバを短期クレデンシャルモードと長期クレデンシャルモード間で切り替えます。（バージョン 3.1 より）
short_term_credentials をオンにする <shared secret> <realm>	TURN サーバが短期的なクレデンシャルを使用するために必要な共有秘密とレルムを指定します。（バージョン 3.1 より）

2.15 CDR 変更の概要

バージョン 3.1 の CDR の変更はありません。

2.16 イベント変更の概要

バージョン 3.1 に新しいイベントはありません。

3 Cisco Meeting Server ソフトウェアバージョン 3.1 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 3.0 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、3.0.x リリース ノートの手順に従って 3.0 にアップグレードしてから、Cisco Meeting Server 3.1.x リリース ノートに記載されている手順を実行することを推奨します。これは、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、3.0 よりも前のソフトウェアリリースからのアップグレードをテストしていません。

Cisco Meeting Server 2000、Cisco Meeting Server 1000、または以前に設定された VM 展開にインストールされている Cisco Meeting Server ソフトウェアのバージョンを確認するには、MMP コマンド**バージョンを使用します**。

VM を初めて設定する場合は、『Cisco Meeting Server Installation Guide for Virtualized Deployments（Cisco Meeting Server 仮想化導入インストール ガイド）』の指示に従ってください。

3.1 リリース 3.1 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/**ダウングレードが失敗した場合にアクセスできない可能性があるため、アップグレード/ダウングレードプロセスによって生成された自動バックアップファイルに依存**しない**ようにしてください。**

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。

注意：
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_1_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）：
   a9b6d0e034f6b9f4cb85232e1aaf2d2b764cefd13e8c1674684b5f3dc23550aa

   Cisco_Meeting_Server_3_1_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）：
   a2adce1c0417d3e601c641e776f0d5d7ec434e1c7944221580d3334559e684

   Cisco_Meeting_Server_3_1_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 の場合、Cisco_Meeting_Server_3_1_2_vSphere-6_0.ova ファイルのハッシュ（SHA-512）：
   e434d0ddc022947516c97aa29567d1668f7c0693d8928539ed013480f65775865a1b3de4be224bb066858be39a03dbb5018d85eaa50310490f669b0e93b4b1dc

   vSphere6.5 以上の場合、Cisco_Meeting_Server_3_1_2_vSphere-6_5.ova ファイルのハッシュ（SHA-512）：
   bf30d59eacd168ab510c2ef214dda634210066c5f0cfbdb492d4e4ee5e8efbd06ed45cd1bf5ed888f880fc8ca584afd938192a352c893a67b0dc3cffe56f2c78

2. OVA ファイルを検証するために、ダウンロードの説明にカーソルを合わせると表示されるポップアップ ボックスに、2.9.1 リリースのチェックサムが表示されます。さらに、上記の SHA-512 ハッシュ値を使用して、ダウンロードの整合性を確認することもできます。
3. SFTP クライアントを使用して、IP アドレスを使用して MMP にログインします。ログイン資格情報は、MMP 管理者アカウントに設定された資格情報になります。Windows を使用している場合、WinSCP ツールの使用をお勧めします。

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

(注)
a) ifaceMMP 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、**アップグレードリスト**コマンドを発行します。
   a. MMP への SSH 接続を確立し、ログインします。
   b. upgrade list コマンドを実行して、使用可能なアップグレード イメージとそのチェックサムを出力します。

      upgrade list
   c. **このチェックサムが上記のチェックサムと一致していることを確認します。**
6. アップグレードを適用するには、前の手順の MMP への SSH 接続を使用し、**upgrade**コマンドを実行してアップグレードを開始します。
   a. upgrade コマンドを実行して、アップグレードを開始します。
      upgrade
   b. サーバ/仮想化サーバは自動的に再起動します。処理が完了するまで 10 分かかります。
7. MMP への SSH 接続を再確立し、次を入力して、Meeting Serverがアップグレードされたイメージを実行していることを確認します:
   version
8. 利用可能な場合は、カスタマイズアーカイブファイルを更新します。
9. 拡張性または復元力のある導入環境を展開する場合は、『スケーラブルで復元力のあるサーバ導入ガイド』をお読みになり、残りの導入順序と構成プランを作成してください。
10. データベースクラスタを展開している場合は、アップグレード後に必ず **database cluster upgrade_ schema** コマンドを実行してください。データベース スキーマをアップグレードする手順については、『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>`** 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: **バックアップロールアップ**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再アップロードされました。

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

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

3.3 Cisco Meeting Server 3.1 の展開

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

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

- 単一分散型 Meeting Server：このモデルでは、DMZ 内のネットワーク エッジに配置された Meeting Server 上で TURN サーバと Web Bridge 3 が有効化され、それ以外のコンポーネントは内部（コア）ネットワークに配置された別の Meeting Server 上で有効化されます。
- 3 つ目のモデルでは、展開環境の拡張性と復元力を高めるため、複数の Meeting Server をまとめてクラスタ化して展開します。

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

注意点：

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

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

Cisco Meeting Server 1000 および仕様ベースの VM サーバは、Cisco Meeting Server 2000 よりもコール キャパシティは少なくなりますが、すべてのコンポーネント（Call Bridge、Web Bridge 3、データベース、レコーダー、アップローダ、ストリーマ、TURN サーバ）を各ホスト サーバ上で使用できます。Web Bridge 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、
   [**製品**（Product）] フィールドで [**シリーズ/モデル**（Series/Model）] を選択してから「**`Cisco Meeting Server`**」と入力を開始し、さらに [**リリース**（Releases）] フィールドで [**このリリースで修正済み**（Fixed in these Releases）] を選択してから、検索するリリース（たとえば「**`3.1`**」）を入力します。
2. 表示されたバグのリストから、*[変更日（Modified Date）]*、*[ステータス（Status）]*、*[重大度（Severity）]*、*[評価（Rating）]* ドロップダウン リストを使用してリストをフィルタリングします。

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

4.1 解決済みの問題

注：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 3.1.2 で修正済みの問題

シスコの識別子	要約
CSCvx32832	**`toggleMuteSelfAudio`** を使用している場合、参加時に **`callLegProfile`** がミュート状態で参加者がミュート状態にされている場合、最初の DTMF コマンドが動作しない場合があります。
CSCvx04125	予期しないコールドロップが発生した場合は、自動再接続が失敗しています。ユーザには「**メディアに再接続できません**」エラーと会議に再参加するボタンが表示されます。
CSCvw98069	ある参加者がコンテンツを共有した後、しばらくの間、画面が厳しく点滅します。この点滅は、H264 ハイプロファイルでメディアが予期せず再起動した場合に発生します。

シスコの識別子	要約
CSCvx19320	アクティベーターがスペースを離れ、すべての非アクティブノードを切断すると、予期しない再起動が発生します。
CSCvx47165	ActiveControl は、SIP コールが置き換えられてから 15 分後に壊れます。

以前のバージョンで発生し 3.1.1 で修正済みの問題

シスコの識別子	要約
CSCvw18292	Cisco Meeting Server ではパケット損失が発生し、再起動後に回復します。

以前のバージョンで発生し 3.1 で修正済みの問題

シスコの識別子	要約
CSCvu38420	参加者がコンテンツを共有するために Macbook Chrome を使用する会議では、con-Tent のビデオで解像度が変更される場合があります。
CSCvv13875	Meeting Server 2.9.x のロックされた coSpace に needsActivation=False ダイヤルインしている音声のみのユーザには、連続ループで「この会議はロックされています。許可されるのを待っています」という音声プロンプトが聞こえます。
CSCvv32271	外部ユーザ（この場合は PSTN）が Meeting Server スペースに転送される場合、Meeting Server のディスプレイには、転送を行ったデバイスまたはエンドポイントが、スペースに転送されたデバイスまたはエンドポイントの番号と比べて不正確に示されます。
CSCvw61501	MMP 日付コマンドから返されたローカル時刻が間違っている可能性があります。この問題は、3.0 からリリースされたリリースにのみ影響します。
CSCvw03087	内部の RTMP キューが大きすぎると、ストリームはストリーミングコールレッグを破棄します。コールはフロー制御され、200 kbps に到達すると、ストリームにより却下されます。
CSCvv19087	Web 管理 UI のトレース詳細ページに [Web Bridge 接続のトレース（Web Bridge connection tracing）] オプションがまだ表示されていますが、現在は機能しません。これは Meeting Server から削除された Web Bridge 2 コンポーネント用に使用されていたものです。

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フィールドにCisco の識別子を入力してください。

シスコの識別子	要約
CSCvw61465	Web ブリッジ 3～C2W は、300 の DNS ルックアップ失敗後に接続の確立を試み停止します。
CSCvw61467	[JoinCall] ページで、このファイルの有効期限が切れた場合、SSO ログインを誤って実行すると、ポータルにユーザが移動します。
CSCvw61470	SSO ドメインは、大文字と小文字が区別されます（大文字と小文字を区別しません）。
CSCvw61548	TURN ログに現在のセッション数が正確に表示されない
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。
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。

シスコの識別子	要約
CSCve37087 ただし、CSCvd91302に関連	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。

4.2.1 既知の制限事項

Cisco Meeting Server は、バージョン 3.1 から TURN の短期的なクレデンシャル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 の Meeting Server TURN サーバなどの短期的なクレデンシャル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、短期的なクレデンシャルはサポートされません。

5 関連するユーザ マニュアル

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

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

6 アクセシビリティ通知

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

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

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

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および限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

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

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

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

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

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

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

Cisco の商標