Cisco Unified Communications Manager および IM and Presence Service リリース 12.5(1)SU4 のリリースノート

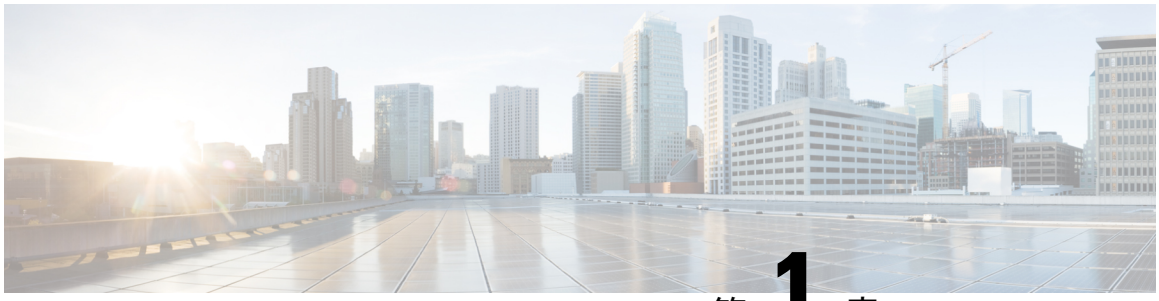
初版：2021 年 2 月 22 日

最終更新：2023 年 5 月 16 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

このリリースについて

リリース ノートについて

このリリースでは、Cisco Unified Communications Manager（Unified Communications Manager）および Cisco Unified Communications Manager IM and Presence Service（IM and Presence Service）の新機能、制限事項 および注意事項について説明します。このリリース ノートは、メンテナンス リリースごとに毎回更新されていますが、パッチまたはホットフィックス向けには更新されていません。

サポートされるバージョン

次のソフトウェアバージョンは、リリース 12.5(1)SU4 でサポートされています。

- Unified Communications Manager：12.5.1.14900-63
- IM and Presence Service：12.5.1.14900-4

Unified CM と IM and Presence Service 間のバージョンの互換性

バージョンの互換性は、IM and Presence Service の展開タイプによって異なります。次の表は、オプションおよびテレフォニーの導入と IM and Presence Service 展開との間でリリースの不一致がサポートされるかどうかの概要を示しています。リリースの不一致がサポートされる場合、リリースの異なる Unified Communications Manager テレフォニー展開と IM and Presence Service 展開を展開できます。

（注） Cisco.com リリース間で生成された再スピンまたはESは、以前のリリースの一部と見なされます。たとえば、ビルド番号が 12.5.1.18[0-2]xx の Unified Communications Manager ES は、12.5(1)SU7（12.5.1.17900-x）リリースの一部と見なされます。

リリース 12.5(1)SU7a の場合、ビルド番号が 12.5.1.181xx の Unified Communications Manager ES は、12.5(1)SU7a（12.5.1.18100-x）リリースの一部と見なされます。

表 *1 : Unified Communications Manager* と *IM and Presence Service* 間のバージョンの互換性

展開タイプ	リリースの不一致	説明
IM and Presence Service の標準展開	サポート対象外	Unified Communications Manager と IM and Presence Service は同じクラスタに存在し、同じリリースを実行する必要があります。つまり、リリースの不一致はサポートされません。
中央集中型IM and Presence Service の展開	サポート対象	IM and Presence Service の展開とテレフォニーの展開は異なるクラスタに存在し、異なるリリースを実行します。つまり、リリースの不一致はサポートされます。 （注） IM and Presence Service 中央クラスタには、データベースとユーザのプロビジョニングのためのスタンドアロン Unified CM Publisher ノードを含みます。この非テレフォニー ノードは、IM and Presence Service と同じリリースで実行される必要があります。 （注） リリース 11.5(1)SU4 以降では、IM and Presence Service の中央集中型の展開がサポートされています。

このリリースのドキュメント

このリリースで入手可能なマニュアルの完全なリストについては、『Cisco Unified Communications Manager および IM and Presence Service リリース 12.5(1) のドキュメンテーションガイド』を参照してください。

ドキュメンテーションの再構築 12.5(1)SU1 以降

以下は、12.5(1)SU1 の一部であったドキュメンテーションの再構築作業の概要です。今回リリースおよび以降のリリースでは、操作性を改善し、ドキュメンテーションセットを合理化するために、多くの Unified Communications Manager ドキュメントが再構築されました。この取り組みの一環として、新しいガイドが 1 つ追加され、3 つの既存のガイドが書き直され、5 つ

の既存のガイドが廃止されています。この全体的な労力により、Unified Communications Manager ドキュメンテーション スイートのサイズが4つのガイドで削減されます。

表 *2 : 12.5(1)SU1* 以降の再構成ドキュメント

再構成ドキュメント	説明
システム構成ガイド	12.5(1)SU1 では、『システム コンフィギュレーション ガイド』は、完全なインストール後のシステム セットアップを作成するために短縮され、簡素化されています。基本のセキュリティと SSO の設定は、高度な呼処理機能が『機能設定ガイド』に移動している間に基本的なセットアップに入力するために追加されています。この新しいガイドでは、高度なシスコ コール処理ソリューションを導入するための、Unified Communications Manager の前提条件を形成しています。
機能設定ガイド	このガイドは、次の高度な呼処理のトピックを『システム コンフィギュレーション ガイド』からこのガイドに移動するために拡張されました。 • Call Control Discovery（呼制御ディスカバリ） • 外部コール制御 • [コールキューイング（Call Queuing）] • コール スロットリング • 論理パーティション設定 • ロケーション認識 • フレキシブル DSCP マーキングおよびビデオ プロモーション • SIP の正規化および透過性 • [SDP透明性プロファイル（SDP Transparency Profile）] • モバイルおよびリモート アクセス さらに、次の新しいセクションが 12.5(1)SU1 とそれ以降に追加されています。 • ヘッドセット管理 • ビデオ エンドポイント管理

再構成ドキュメント	説明
アドミニストレーション ガイド	12.5(1)SU1 では、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』が、いずれも12.5(1)SU1 では廃止されている、『*IP* アドレス、ホスト名 およびドメインの変更』ドキュメント、『*Cisco Unified Reporting* アドミニストレーション ガイド』ドキュメント、および既存の『*Cisco Unified Serviceability* アドミニストレーション ガイド』ドキュメンテーションからの多数のセクションからの統合されたアドミニストレーション情報を含めるために拡張されています。 上記の更新に加えて、トラブルシューティング情報の概要がアドミニストレーション ガイドに挿入されました。
コール レポーティングおよび課金管理ガイド	この新しいドキュメントでは、コール レポーティングおよび課金管理のドキュメンテーションを簡素化し、現在ではいずれも廃止されている『*Cisco Unified CDR Analysis and Reporting* アドミニストレーション ガイド』および『コール詳細レコードアドミニストレーションガイド』ドキュメントからの既存の資料を統合しています。また、これまで Serviceability の資料とともに利用できた CDR Repository および課金サーバの情報を追加しました。この新しいガイドは、全体的な構造を簡略化し、より明確な設定プロセスを提供します。

表 *3 : 12.5(1)SU3* 以降の再構成ドキュメント

再構成ドキュメント	説明
セキュリティ ガイド	セキュリティガイドは、リリース 12.5(1)SU3 用に再構成されています。新しいガイドは合理化および強化されており、Unified Communications Manager および登録済みエンドポイントのセキュリティを簡単に設定および展開できるようになっています。この新しいガイドは、次の 3 つのセクションに分かれています。 • **基本セキュリティ**：Unified Communications Manager および登録済みエンドポイントで基本セキュリティを設定する方法に関する情報が含まれています。 • **ユーザーセキュリティ**：ID、認証、およびユーザーアクセスを管理する方法に関する情報が含まれています。 • **高度なセキュリティ機能**：FIPS モード、拡張セキュリティモード、V.150 などの高度なセキュリティ機能を展開する方法に関する情報が含まれています。 この本には、展開のセキュリティに関する決定を行うのに役立つ、セキュリティの強化やID管理などの主題に関する新しいトピックを含む拡張情報も含まれています。

再構成ドキュメント	説明
iPhone および iPad での Cisco Jabber のプッシュ通知の展開	このドキュメントでは、Cisco Unified Communications Manager と IM and Presence サービスを使用した iPhone および iPad での Cisco Jabber のプッシュ通知を設定する方法について説明します。このガイドは更新され、Android デバイスと iOS デバイスの両方で実行される Cisco Jabber および Cisco Webex クライアントのプッシュ通知サポートが含まれています。

インストール手順

システムのインストール方法の詳細については、『Cisco Unified Communications Manager および IM and Presence Service リリース 12.5(1) インストール ガイド』を参照してください。

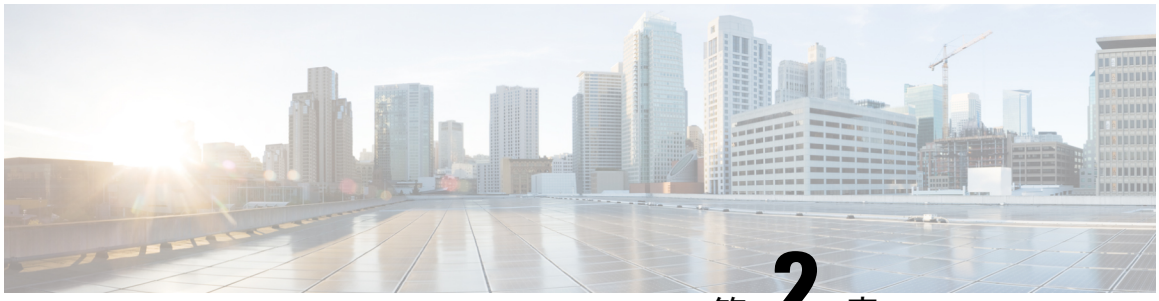
アップグレード手順

リリース 12.5(1) へのアップグレード方法については、『Cisco Unified Communications Manager および IM and Presence Service のアップグレードおよび移行ガイド リリース 12.5(1)』をご覧ください。

アップグレード中の Meltdown の脆弱性

このリリースの Unified Communications Manager、Cisco IM and Presence サービス、Cisco Emergency Responder および Cisco Prime Collaboration の導入には、Meltdown および Spectre のマイクロプロセッサの脆弱性に対処するためのソフトウェア パッチが含まれています。

リリース 12.5 (1) 以降にアップグレードする前に、シスコ コラボレーション サイジング ツールを使用して現在の展開をアップグレード済みの 12.5(1) SU4 展開と比較するように、チャネル パートナーまたはアカウントチームと連携させることをお勧めします。必要に応じて、VM リソースを変更して、アップグレードされた導入環境で最適なパフォーマンスが得られるようにします。



第 2 章

新機能および変更された機能

ヘッドセットとアクセサリのインベントリダウンロード

[ヘッドセット（Headsets）] メニューカテゴリは、Cisco Unified Communications Manager ユーザインターフェイスで **[ヘッドセットとアクセサリ（Headsets and Accessories）]** に名前が変更されました。

この機能を使用すると、管理者は Unified Communications Manager ユーザインターフェイスから展開内のヘッドセットとアクセサリの詳細レポートを CSV ファイルにダウンロードできます。

詳細については、Cisco Unified Communications Manager 機能設定ガイドの「ヘッドセットとアクセサリの管理」の章を参照してください。

Manager Assistant からの Oracle JRE の削除

Oracle Java Runtime Environment（JRE）は、Cisco Unified Communications Manager Assistant プラグインに含まれなくなりました。

Cisco Unified Communications Manager Assistant クライアントを新しいバージョンにアップグレードする前に、次の手順を実行します。

- マシンに現在インストールされている Cisco Unified Communications Manager Assistant クライアントをアンインストールします。
- 32 ビットまたは 64 ビットの Windows プラットフォームに JRE をインストールします。

詳細については、『Cisco Unified Communications Manager 機能設定ガイド』を参照してください。

認証ベースのプロキシによるスマートライセンス登録

この機能により、Unified Communications Manager のライセンスコンポーネントは、HTTP/HTTPS プロキシ経由の認証済み接続を使用して、クラウドベースの Cisco Smart Software Manager と通信できます。

Webex アプリケーションの SSO リダイレクト URI

SSO リダイレクト URI 機能により、外部ブラウザを使用して SSO を実行するソフトクライアント）Cisco Jabber/Cisco Webex アプリ）を、ブラウザが Cisco Jabber/Cisco Webex アプリバックエンド サービスにサインインできるように、SSO リダイレクト URI を使用してブラウザによってクロス起動できます。

Webex クライアントの埋め込みブラウザのサポート

この機能により、Cisco Jabber/Webex クライアント組み込みブラウザサポートのセキュリティが強化されます。

次の機能が拡張されています。

- RFC7636 により「認可コードの横取り攻撃」から保護します。
- Webex クライアントまたは Unified Communications Manager の使用中に SSO が有効になっている場合、改善された通話エクスペリエンスにより、二重ログインを回避できます。

モバイルおよびリモートアクセスデバイス登録のパフォーマンスカウンター

新しいパフォーマンスカウンターが Cisco Unified Real-Time Monitoring Tool に導入され、モバイルおよびリモートアクセスモードで Unified Communication Manager に登録された登録済み Cisco Webex アプリおよび Cisco Jabber デバイスを追跡します。これにより、管理者は、Unified CM に登録されているモバイルおよびリモートアクセスモードのデバイスの数を把握できます。トラブルシューティングの Perfmon データログを有効にすると、システムはこれらの新しいカウンターの統計を自動的に収集し、Perfmon ログに保存します。

新しいカウンターの詳細については、『Cisco Unified Real-Time Monitoring Tool Administration Guide』を参照してください。

UDS の機能拡張

UDS には、次の拡張機能が導入されています。

- 電子メールによる UDS 一括検索により、Cisco Jabber は、電子メール属性を使用してリクエストをバッチで送信し、UDS と Cisco Tomcat サービスによる CPU 使用率の上昇を防ぎます。
- UDS が拡張され、リモートクラスタ間でのユーザのホームクラスタの検出が改善されました。これは、Cisco Jabber のログインの失敗を回避し、データセンターの障害やシャットダウンが発生した場合に地理的な冗長性を確保するのに役立ちます。

証明書の同期とクラスタ間定期同期

IM and Presence サービスは、クラスタ間同期プロセスの一部として証明書の同期を実行します。この機能により、クラスタ間定期同期中に新しいサービスパラメータ Certificate Sync が導入され、管理者は **Cisco Unified Communications Manager IM and Presence Administration ユーザインターフェイスからクラスタ間定期同期**の一部として証明書同期を無効または有効にできます。

証明書同期機能は、次のオプションを導入します。

- **証明書同期の実行（Perform certificate sync）**：これは **[クラスタ間定期同期中の証明書同期（Certificate Sync during Inter-Cluster Periodic Sync）]** サービスパラメータのデフォルト値です。**[クラスタ間定期同期中の証明書の同期（Certificate Sync during Inter-Cluster Periodic Sync）]** サービスパラメータが **[証明書の同期を実行する（Perform certificate sync）]** に設定されていて、証明書がクラスタ間ピア間で同期されていない場合、データと証明書を同期するために強制手動同期操作が必要です。
- **証明書の同期を実行しない**：ICSA 同期中に証明書の同期を無効にするには、管理者が **[クラスタ間定期同期中の証明書の同期（Certificate Sync during Inter-Cluster Periodic Sync）]** サービスパラメータを **[証明書の同期を実行しない（Do not Perform Certificate Sync）]** に設定します。

（注） クラスタ間定期同期中に、証明書の同期に関連する展開でパフォーマンスの低下または高い CPU スパイクが発生した場合は、この機能を使用できます。

クラスタ間同期プロセスの一部として証明書の同期を無効または有効にする方法の詳細については、IM and Presence Service の設定および管理ガイドの「クラスタ間ピアの設定」の章を参照してください。

Expressway による IM and Presence ストリーム機能/サービスアドバタイズメントの改善

IM and Presence Service は、Cisco Expressway のモバイルおよびリモートアクセスを介して接続するクライアントへの XMPP ストリーム機能/サービスのアドバタイズメントをサポートします。

この新しい機能により、IM and Presence サービスのバージョンが混在する展開（たとえば、11.5(1)SU8 上の一部のクラスタと 12.5(1)SU3 上の一部のクラスタ）をCisco Expresswayと連携させ、割り当てられている IM and Presence サービスのホームクラスタに基づいて、Cisco Jabber クライアントが適切な機能を検出できるようになります。

このメカニズムを機能させるには、バージョン 11.5(1)SU9 または 12.5(1)SU4 以降を実行しているクラスタ間メッシュに、少なくとも 1 つの IM and Presence クラスタを搭載した Cisco Expressway が必要です。

現在の IM and Presence サービスのバージョンの組み合わせによっては、次の表に示す情報に従って、Expressway で FCM サービスフラグを使用してプッシュ通知機能を有効または無効にする必要があります。

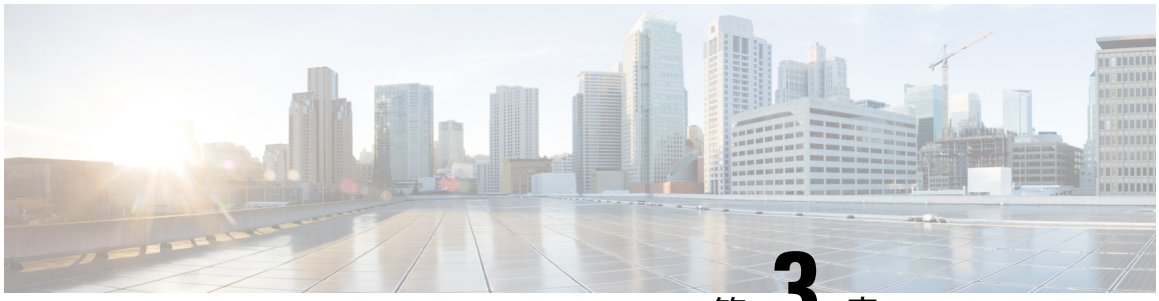
```
xConfiguration XCP Config FcmService: On/Off
```

（注） Apple Push Notification Service（APNS）は、FCM サービスフラグステータスの影響を受けません。

表 *4: Expressway CLI* の観点からのソリューションマトリックス：*Android* プッシュ通知（*FCM*）のコマンドの有効化/無効化

混合バージョンの IM and Presence クラスタ	Expressway X12.7の FCM フラグの予期されるステータス	Comment
任意の 11.5(1)SUと 12.5(1)SU2 以下	オフ	Android Push（FCM）はサポートされていません。
11.5(1)SU8（またはそれ以下）または 12.5(1)SU2（およびそれ以下）と 12.5(1)SU3	オフ	Android プッシュ（FCM）はサポートされていません
11.5(1)SU8（またはそれ以下）または 12.5(1)SU2（およびそれ以下）と 12.5(1)SU4（およびそれ以上）	オフ	12.5(1)SU4 以降のバージョンでサポートされる Android プッシュ（FCM）

混合バージョンの IM and Presence クラスタ	Expressway X12.7の FCM フラグの予期されるステータス	Comment
11.5(1)SU9（またはそれ以上）または 12.5(1)SU4（およびそれ以上）と 12.5(1)SU3	オン（On）	バージョン 12.5(1)SU3 以降でサポートされる Android プッシュ（FCM）
11.5(1)SU9 以降（12.5(1)SU4 以降）	フラグは不要です （Expressway 12.7 は新しい検出メカニズムに完全に依存しています）	12.5(1)SU4 以降のバージョンでサポートされる Androidプッシュ（FCM）



第 3 章

特記事項

新規インストールおよびアップグレード時のデフォルト CA 証明書

Unified Communications Manager リリース 12.5 (1) 以降をインストールすると、CAP_RTP_001 と CAP_RTP_002 証明書を除くすべてのデフォルト CA 証明書が存在します。これらの証明書を有効にするには、 **set cert default-ca list enable {all | common-name}**コマンドを使用します。

Unified Communications Manager リリース 12.5(1) 以降にアップグレードする場合は、アップグレード後に古いバージョンに存在していたデフォルトの証明書のみが表示されます。

無効なデフォルト 証明書 バックアップの失敗

ディザスタリカバリシステム (DRS) を使用してバックアップを実行する場合、 **set cert default-cal-list disable {all | common-name}**を使用してすべてまたは特定のデフォルト証明書が

無効になっている場合、バックアップに無効な証明書が含まれていません。新規にインストールされたサーバでバックアップを復元すると、それらの無効な証明書が再度表示されます。

ILS ネットワーキング キャパシティ

Intercluster Lookup Service（ILS）ネットワーク容量は、リリース 12.5(x) 以降で更新されています。ILS ネットワークを計画する際に念頭に置くべき推奨キャパシティは以下のとおりです。

- ILS ネットワーキングは最大 10 個のハブ クラスタをサポートしており、ハブあたりのスポーク クラスタ数は 20 個であるため、合計で最大 200 個のクラスタを使用できます。ハブとスポークの組み合わせによるトポロジは、各クラスタ内で多数の TCP 接続が作成されるのを回避するために使用します。
- ハブ クラスタとスポーク クラスタを最大数まで、またはそれを超えて使用すると、パフォーマンスに影響が出る可能性があります。1 つのハブに多数のスポーク クラスタを追加すると余分な接続が作成され、メモリまたは CPU の処理量が増加する可能性があります。1 つのハブ クラスタに接続するスポーク クラスタは 20 個以下にすることを推奨します。
- ILS ネットワーキングは、追加の CPU 処理をシステムに追加します。ハブアンドスポークトポロジを計画する場合は、ハブクラスタの CPU が負荷を処理するように設定されていることを確認します。CPU 使用率の高いシステムをスポーククラスタとして割り当てることをお勧めします。

（注） 上記の容量は、システムテストに基づく推奨事項にすぎません。Unified Communications Manager は、ILS ネットワーク内のクラスタの総数にも、ハブあたりのスポーククラスタ数にも制限を適用しません。上記のトポロジは、システムが過度にリソースを消費しないように、最適なパフォーマンスを保証するためにテストされています。

ILS の詳細については、Cisco Unified Communications Manager システム設定ガイド の「クラスタ間ルックアップサービスの設定」の章を参照してください。

Okta 経由の RTMT への SAML SSO ログインの Java 要件

Okta が id プロバイダーとして設定されている SAML SSO があり、SSO を使用して Cisco ユニファイド リアルタイム モニタリング ツールにログインする場合は、最小 Java バージョン8.221 を実行している必要があります。この要件は Cisco Unified Communications Manager および IM and Presence Service の 12.5(x) リリースに適用されます。

同じコールでサポートされていない複数のクロック レート

このリリースでは Cisco TelePresence エンドポイントと Cisco Jabber クライアントは、提供されたコーデックに一致するさまざまなクロックレートの複数の「電話イベント」 SDP 属性をサポートしていません。この機能は、VoLTE/IMS エンドポイントを完全にインターワーキングするために必要です。この更新のため、これらのエンドポイントタイプと VoLTE または IMS エンドポイント間の相互運用性の問題が、8 kHz の異なるクロックレートがネゴシエートされる通話中の再招待で発生する可能性があります。

これらのエンドポイント クラス間のコールの場合:

- 最初のコール セットアップは問題なく実行されます。
- 通話中の再招待では、INVITE が Unified Communications Manager によって開始された場合、問題は発生しません。
- エンドポイントによって開始された再招待では、8 kHz とは異なるクロックレートを使用すると、相互運用性の問題が発生する可能性があります。

新しい Cisco ゲートウェイのサポート

Unified Communications Manager の新しいリリースでは、次のシスコゲートウェイのサポートが導入されています。

- Cisco VG400 アナログ音声ゲートウェイ
- Cisco VG420 アナログ音声ゲートウェイ
- Cisco VG450 アナログ音声ゲートウェイ
- Cisco 4461 サービス統合型ルータ

次の表に、サポートが導入されたゲートウェイ モデルと、リリース カテゴリ別の最初のリリースを示します。各リリースカテゴリ（たとえば、11.5(x)、12.5(x)）内では、ゲートウェイモデルのサポートは、そのカテゴリの後のリリースとともに、指定されたリリースとともに追加されます。これらのリリースでは、Cisco Unified Communications Manager の [**ゲートウェイの設定（Gateway Configuration**）] ウィンドウでゲートウェイを選択できます。

表 *5:* リリース カテゴリ別の最初のリリースを使用する *Cisco* ゲートウェイ

ゲートウェイ モデル	11.5(x) リリース	12.5 （x） リリース	14(x) リリース
Cisco VG 202、202 XM、204、204 XM、310、320、350 アナログ音声ゲートウェイ	11.5(1) 以降	12.5(1) 以降	14 以降
Cisco VG400 アナログ音声ゲートウェイ	11.5（1）SU7 以降	12.5(1) 以降	14 以降
Cisco VG420 アナログ音声ゲートウェイ	サポート対象外	12.5(1)SU4 以降	14SU1 以降
Cisco VG450 アナログ音声ゲートウェイ	11.5（1）SU6 以降	12.5(1) 以降	14 以降
Cisco 4321、4331 4351、4431、4451 サービス統合型ルータ	11.5(1) 以降	12.5(1) 以降	14 以降
Cisco 4461 サービス統合型ルータ	11.5（1）SU6 以降	12.5(1) 以降	14 以降
Cisco Catalyst 8300 シリーズエッジプラットフォーム	—	12.5(1)SU4 以降	14 以降

Cisco アナログ電話アダプタ

Cisco アナログ電話アダプタは、アナログ電話機、またはファックスなどのアナログ デバイスをネットワークに接続します。これらのデバイスは、[**電話の設定**（**Phone Configuration**）] ウィンドウを使用して設定できます。次の表では、ATA シリーズのモデル サポートを取り上げています。

表 *6: Cisco* アナログ電話アダプタ

ATA アダプタ	11.5(x) リリース	12.5 （x） リリース	14(x) リリース
Cisco ATA 190 アナログ電話アダプタ	11.5(1) 以降	12.5(1) 以降	14 以降
Cisco ATA 191 アナログ電話アダプタ	11.5(1)SU4 以降	12.5(1) 以降	14 以降

SDL リスニングポートの更新には、すべてのノードで CTIManager を再起動する必要がある

SDL リスニング ポートサービス パラメータの設定を編集する場合、サービスが実行されているすべてのクラスタ ノードで**Cisco CTIManager**サービスを再起動する必要があります。現在、ヘルプテキストにはサービスを再起動するように指示されていますが、サービスが実行されているすべてのノードでサービスを再起動する必要があるとは指示されていません。Cisco Unified CM の管理インターフェイスから、このサービスパラメータにアクセスするには、**システム** > **サービスパラメータ**に進み、**Cisco CTIManager**をサービスとして選択し、**[詳細(Advanced)]** をクリックして CTIManager サービスパラメータの完全なリストを表示します。

このアップデートは CSCvp56764 の一部です。

輸出規制対象のお客様向けのサテライトの導入を使用した輸出規制

Unified Communications Managerサテライトの導入（サテライト バージョン：7-202001）を使用して、輸出規制対象のお客様が Unified Communications Manager で輸出規制機能を有効にできるようサポートします。『Cisco Unified Communications Manager システム設定ガイド』の「スマートライセンシングの輸出コンプライアンス」の章で「スマート ソフトウェア ライセンシングの概要」のセクションを参照してください。サテライトの詳細については、https://software.cisco.com/download/home/286285506/type/286285517/os を参照してください。

IM and プレゼンス リリース 11.5(1) 以降からのデータベース スキーマのアップグレード

IM and Presence Service を使用して外部データベースとして導入された Microsoft SQL データベースがある場合は、次のいずれかのシナリオを選択してデータベーススキーマをアップグレードします。

表 *7: MSSQL* データベース スキーマのアップグレード シナリオ

シナリオ	手順
IM and Presence Service 11.5 (1)、11.5 (1) SU1、または 11.5 (1) SU2 リリースからのアップグレード	MSSQL データベースのアップグレード方法の詳細については、『IM and Presence Service データベース セットアップ ガイド』の「Microsoft SQL Server を使用したアップグレードに必要なデータベース移行」セクションを参照してください。 これにより、テキストから nvarchar (最大) の列タイプに必要な変更が行われます。
IM and Presence Service 11.5(1)SU3 以降からのアップグレード	IM and Presence Service サーバーに接続されている MSSQL データベースは、IM and Presence Service のアップグレード中に自動的にアップグレードされます。これにより、nvarchar (4000) から nvarchar (最大) までの列タイプに必要な変更が行われます。 （注） 列タイプが nvarchar (4000) の古いデータベースに接続するなど、何らかの理由でアップグレードを手動でトリガーする場合、次のアクションは列タイプを nvarchar (最大) に変更することによってデータベースをトリガーしてアップグレードします。 • Cisco xcp Config Manager を再起動した後、Cisco XCP Router サービスを再起動します。または • 外部データベースのスキーマ検証中：データベースをテキスト会議（TC）、メッセージアーカイバ（MA）、または非同期ファイル転送（AFT）サービスに割り当て、**[外部データベース設定（External Database Settings）]** ページをリロードします。（Cisco Unified CM IM and Presence 管理ユーザーインターフェイスから、**[メッセージング（Messaging）]** > **[外部サーバーの設定（External Server Setup）]** > **[外部データベース（External Databases）]** の順に選択し、データベースを見つけて選択して **[外部データベースの設定（External Database Settings）]** ページをロードします）。

応答しないリモート クラスタ ノード

問題

リモート クラスタのすべてのノードが一度にダウンします。

説明

上記の問題が発生した場合は、

- 2 つのクラスタはそれぞれ 4 つのノードを持っていて、両方のクラスタのすべてのノードが UDS に設定されています。
- クラスタ 2 は、クラスタ 1 ビューでパブリッシャ FQDN とともに定義されています。反対に、Jabber ユーザ はクラスタ 1 としてホーム クラスタを持ちますが、SRV はクラスタ 2 をポイントし、クラスタ 2 は クラスタ ビューでクラスタ 1 からのパブリッシャ の FQDN がコンフィギュレーションされ、到達可能になったときに最初に更新される [RemoteClusterServiceMapDynamic] テーブルのエントリをすべて保持します。
- クラスタ 2 の [RemoteClusterServiceMapDynamic] でクラスタ 1 の 3 つのノードすべてが停電により一度にダウンした場合、新しい Jabber のログインはホーム クラスタの検出に失敗します。
- ノードがダウンしていても、クラスタ 2 の `RemoteClusterServiceMapDynamic` は以前の IP を表示し続けます。
- クラスタ 2 では、[RemoteClusterServiceMapDynamic] からノードが順番に、または 1 つダウンした場合に、リスト内の次のノードのエントリが UDS アクティブによって更新されます。

問題は、[RemoteClusterServiceMapDynamic] からの 3 つのノードすべてが停電によりダウンした場合、4 番目のノードが [RemoteClusterServiceMapDynamic] に追加されていないことです。ただし、クラスタ 2 の応答可能なクラスタビューをクラスタ 1 のアクティブなサブスクライバーにポイントする場合、[RemoteClusterServiceMapDynamic] が自動的に更新されます。

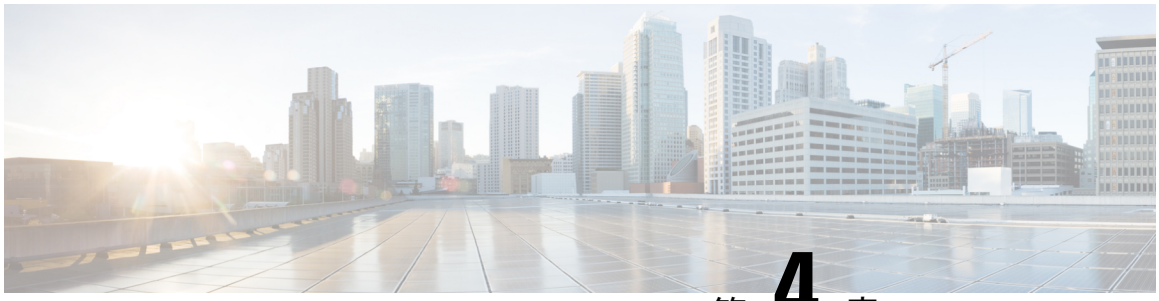
ソリューション

クラスタ ビューから非アクティブなリモート ノードを削除して、アクティブ ノードを追加します。

このアップデートは CSCvq5867 の一部です

Cisco Tomcat サービスの再起動

Security Assertion Markup Language シングルサインオン（SAML SSO）を有効または無効にした後、Cisco Tomcat サービスを再起動することをお勧めします。



第 4 章

不具合

バグ検索ツール

システムは、シビラティ（重大度）に従って既知の問題（バグ）を格付けします。これらのリリース ノートには、次のバグ レベルの説明があります。

- シビラティ（重大度）レベル 1 または 2 のすべてのバグ
- 重大度レベル 3 の重要なバグ
- お客様から報告されたすべてのバグ

任意のリリースの任意のシビラティ（重大度）のオープンな警告および解決済の警告は、お客様が必要に応じて障害情報を検索できるオンライン ツールである Cisco バグ検索ツールを使用して検索できます。

Cisco バグ検索ツールにアクセスするには、次のアイテムが必要です。

- インターネット接続
- Web ブラウザ
- Cisco.com のユーザ ID とパスワード

Cisco バグ検索ツールを使用するには、以下のステップに従います。

1. Cisco バグ検索ツールにアクセスします: https://tools.cisco.com/bugsearch/。
2. 自分の Cisco.com のユーザ ID とパスワードでログインします。
3. 特定の問題に関する情報を検索する場合は、**[Search for]** フィールドにバグ ID 番号を入力し、**[移動（Go）]** をクリックします。

ヒント　バグの検索、保存された検索の作成、バグ グループの作成などの方法については、[バグ検索] ページの **[ヘルプ (help)]** をクリックしてください。

12.5(1)SU4 に関する警告

次の表は、このリリースで開いている注意事項のリストです。https://bst.cloudapps.cisco.com/bugsearch/ のバグ検索ツールで障害を検索できます。

12.5(1)SU4 に関する警告

未解決の警告と解決済みの警告のリストについては、それぞれの Readme ファイルを参照してください。

- Cisco Unified Communications Manager リリース 12.5(1)SU4 の ReadMe ファイル
- Cisco Unified IM and Presence リリース 12.5(1)SU4 の ReadMe ファイル

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。