改訂：2024 年 3 月 29 日

Cisco Unified Communications Manager および IM and Presence Service の互換性マトリックス、リリース 15x

Cisco Unified Communications Manager と IM and Presence Service の互換性マトリックス

更新履歴

日付	リビジョン
2023 年 12 月 18 日	15 のバージョンサポートを追加。
2023 年 12 月 18 日	LDAP ディレクトリのサポート情報を更新。
2023 年 12 月 18 日	サポートブラウザのセクションを更新。
2023 年 12 月 18 日	「Microsoft Outlook とのカレンダー統合」セクションから、Windows Server 2012 での Active Directory 2012 のサポートを削除。
2023 年 12 月 18 日	Microsoft Lync Server 2013 が 2018 年 4 月 10 日に Microsoft のメインストリームサポート終了（EOS）を過ぎ、2023 年 4 月 11 日に EOS が延長されたため、IM and Presence Service の「Microsoft Lync Server を使用したリモートコール制御」のサポートを削除。

このマニュアルの目的

このドキュメントには、Cisco Unified Communications Manager（Unified Communications Manager）および Cisco Unified Communications Manager IM and Presence Service（IM and Presence Service）の 15x リリースの互換性情報が含まれています。これには、特に明記されていない限り、後続の SU リリースも含まれます。

COP ファイルでサポートされているアップグレードおよび移行パス

次の表に、Cisco Unified Communications Manager のリリース 15 と IM and Presence Service にアップグレードするためにサポートされているアップグレードパスを示します。次の表は、COP ファイルが必要なアップグレードパスを示しています。Cisco Unified OS 管理インターフェイスを使用してアップグレードを開始する前、または Cisco Prime Collaboration Deployment（PCD）ツールを使用してアップグレードまたは移行を開始する前に、各ノードに COP ファイルをインストールする必要があります。PCD を使用している場合は、アップグレードを開始する前に COP ファイルの一括インストールを実行できます。

（注） 特に指定がない限り、各リリースカテゴリにはそのカテゴリ内の SU リリースが含まれています。

Cisco Unified Communications Manager および IM and Presence Service の COP ファイルは、https://software.cisco.com/download/home/268439621 からダウンロードできます。アップグレードの宛先バージョンを選択した後、[**Unified Communications Manager ユーティリティ（Unified Communications Manager Utilities）**] を選択して、COP ファイルのリストを表示します。

（注） 必須ではありませんが、アップグレードの成功を最大化するためにアップグレード前にアップグレード準備の COP ファイルを実行することを強く推奨します。Cisco TAC では、有効なテクニカルサポートを提供するために、この COP ファイルを実行する必要がある場合があります。

（注） ソースが FIPS モードおよび/または PCD が FIPS モードの場合、COP ファイル `ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop` に関する情報については、https://www.cisco.com/web/software/286319173/139477/ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop-ReadMe.pdf を参照してください。このドキュメントでは、15 の移行先バージョンへの直接アップグレードまたは直接移行に必要な前提条件について詳しく説明します。

（注） ソースリリースからリリース 15 への直接標準アップグレードが利用可能な場合は、単一ノードまたはクラスタ全体のアップグレードを選択できます。

クラスタ全体をアップグレードし、期間、ダウンタイム、サービスへの影響、または管理者の介入が最小になるようにするには、Unified OS Admin アップグレードまたは CLI アップグレードを使用した Unified CM パブリッシャ経由のクラスタアップグレードの詳細を示す「クラスタ全体のアップグレードタスクフロー（直接標準）」の手順を使用します。ここでは、Unified CM パブリッシャのみをアップグレードし、クラスタ内の他のすべてのノードのアップグレードまたは再起動を調整します。

ソースをノードごとにアップグレードするか、ローカルの Unified OS Admin アップグレードまたは CLI アップグレードを使用して単一ノードのみを使用する場合は、「クラスタノードのアップグレード（直接更新）」セクションを参照してください。詳細については、『Cisco Unified Communications Manager および IM and Presence Service アップグレードおよび移行ガイド』を参照してください。

（注） 『アップグレードガイド』で説明されているように、アップグレード計画がノードシーケンシングルールに従っていることを確認する必要があります。IM and Presence Service ノードでバージョンを切り替える前に、まずパブリッシャノード、サブスクライバノードの順に Unified Communications Manager ノードを切り替える必要があります。

上記の手順に従わず、Unified Communications Manager Publisher ノードがバージョン 15 に切り替えられ、IM and Presence Service Publisher ノードのバージョンが 12.5.x または 14 および SU のバージョンのままであり、アップグレードされていない場合、[ソフトウェア アップグレード（Software Upgrades）] メニューの次のページは、IM and Presence Service ノードでは表示または機能しません。

- クラスタの再起動/バージョン切り替え
- クラスタソフトウェアの場所
- ソフトウェアのインストールおよびアップグレードクラスタ

（注） Unified Communications Manager および IM and Presence Service リリース 15 でサポートされている直接リフレッシュの更新のパスはありません。12.5.x より前のソースからリリース 15 へのアップグレードの更新はサポートされていません。

表 *1 : Cisco Unified Communications Manager* および *IM and Presence Service* のアップグレード パス

送信元	送信先	メカニズム	前提条件	バージョン スイッチング * (送信元から宛先、またはその逆)
10.0	15	PCD 15 移行タスク（V2V）	15 への直接アップグレードはサポートされていません。移行先バージョンが 15 で、ソースバージョンが 10.0 の場合、移行には Cisco Prime Collaboration Deployment（PCD）を使用する必要があります。 移行先バージョンが 15 で、ソースバージョン 10.0 が FIPS モードの場合、Cisco Prime Collaboration Deployment (PCD) は非 FIPS モードである (または置かれる) 必要があります。	N/A
10.5	15	PCD 15 移行タスク（V2V）	アップグレード前チェック COP ファイルを実行します。 移行の前に、`ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512` COP ファイルをインストールする必要があります。 15 への直接アップグレードはサポートされていません。移行先バージョンが 15 で、ソースバージョンが 10.5 の場合、移行には Cisco Prime Collaboration Deployment（PCD）を使用する必要があります。 移行先バージョンが 15 で、ソースバージョン 10.5 が FIPS モードの場合は、次のいずれかを実行します。 • PCD は非 FIPS モードである（または置かれている）必要があります。 • PCD 移行タスクを使用する代わりに、データ インポートでフレッシュ インストールを使用します。	N/A
		データ インポートを使用したフレッシュ インストール（V2V）	• アップグレード前チェック COP ファイルを実行します。 • `ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512` • `ciscocm.DataExport_v1.0.cop.sgn`	サポート対象外

送信元	送信先	メカニズム	前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
11.0	15	PCD 15 移行タスク（V2V）	アップグレード前チェック COP ファイルを実行します。 移行の前に、ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 COP ファイルをインストールする必要があります。 移行先バージョンが 15 で、ソースバージョン 11.0 が FIPS モードの場合は、次のいずれかを実行します。 • PCD は非 FIPS モードである（または置かれている）必要があります。 • PCD 移行タスクを使用する代わりに、データインポートでフレッシュインストールを使用します。	サポート対象外
		データ インポートを使用したフレッシュ インストール（V2V）	• アップグレード前チェック COP ファイルを実行します。 • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.DataExport_v1.0.cop.sgn	サポート対象外

送信元	送信先	メカニズム	前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
11.5	15	PCD 15 移行タスク（V2V）	アップグレード前チェック COP ファイルを実行します。 移行の前に、ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 COP ファイルをインストールする必要があります。 移行先バージョンが 15 で、ソースバージョン 11.5 が FIPS モードの場合は、次のいずれかを実行します。 • PCD は非 FIPS モードである（または置かれている）必要があります。 • PCD 移行タスクを使用する代わりに、データインポートでフレッシュインストールを使用します。	サポート対象外
		データ インポートを使用したフレッシュ インストール（V2V）	• アップグレード前チェック COP ファイルを実行します。 • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.DataExport_v1.0.cop.sgn	サポート対象外

送信元	送信先	メカニズム	前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
12.0	15	PCD 15 移行タスク（V2V）	アップグレード前チェック COP ファイルを実行します。 移行の前に、ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 COP ファイルをインストールする必要があります。 ソースバージョンが Unified Communications Manager (12.0.1.10000-10) のリリース 12.0(1) の場合、次の COP ファイルをインストールする必要があります：ciscocm-slm-migration.k3.cop.sgn。これは、ソースバージョンがより高い場合（リリース 12.0(1)SU1 など）は必要ありません。	サポート対象外
		データ インポートを使用したフレッシュ インストール（V2V）	• アップグレード前チェック COP ファイルを実行します。 • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.DataExport_v1.0.cop.sgn	サポート対象外

送信元	送信先	メカニズム		前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
12.5	15	標準の直接アップグレード（シンプルアップグレード）	OS 管理者または CLI 経由	• アップグレード前チェック COP ファイルを実行します。	サポート対象
		直接標準アップグレード	PCD 15 アップグレードタスク経由		サポート対象

送信元	送信先	メカニズム		前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
				• アップグレード前チェック COP ファイルを実行します。 • Unified CM ソースが 12.5.1.14900-63 より古い場合は、次の COP ファイルをインストールします。 ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn • IM and Presence Service のソースが 12.5.1.14900-4 より古い場合は、次の COP ファイルをインストールします： ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn。 • 移行先バージョンが 15 で、ソースバージョン 12.5 が FIPS モードの場合は、次のいずれかを実行します。 • PCD は非 FIPS モードである（または置かれている）必要があります。 • PCD アップグレード タスクを使用する代わりに、データ インポートでフレッシュ インストールを使用します。 • Cisco Prime Collaboration Deployment を使用して IM and Presence Service クラスタをリリース 12.5.x からリリース 15 にアップグレードする場合は、アップグレードを開始する前に、リリース 12.5.x システムに次の COP ファイルをインストールします： ciscocm.imp15_upgrade_v1.0.k4.cop.sha512。 COP ファイルは、次の場合にのみ適用されることに注意してください。 • Unified Communications Manager の接続先バージョンはリリース 15 です。 • Unified Communications Manager の接続先バージョンがリリース 15 であり、IM and Presence Service の送信元を制限付きバージョンから無制限バージョンにアップグ	

送信元	送信先	メカニズム	前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
			レードしようとしています。	
		PCD 15 移行タスク（V2V）	アップグレード前チェック COP ファイルを実行します。 移行の前に、ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 COP ファイルをインストールする必要があります。 移行先バージョンが 15 で、ソースバージョン 12.5 が FIPS モードの場合は、次のいずれかを実行します。 • PCD は非 FIPS モードである（または置かれている）必要があります。 • PCD 移行タスクを使用する代わりに、データインポートでフレッシュインストールを使用します。	サポート対象外
		データ インポートを使用したフレッシュ インストール（V2V）	• アップグレード前チェック COP ファイルを実行します。 • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.DataExport_v1.0.cop.sgn	サポート対象外

送信元	送信先	メカニズム		前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
14 および SU	15	標準の直接アップグレード（シンプルアップグレード）	OS 管理者または CLI 経由	アップグレード前チェック COP ファイルを実行します。	サポート対象

		直接標準アップグレード	PCD アップグレードタスク経由	アップグレード前チェック COP ファイルを実行します。
				• 移行先バージョンが 15 で、ソースバージョン 14 が FIPS モードの場合は、次のいずれかを実行します。
				  • PCD は非 FIPS モードである（または置かれている）必要があります。
				  • PCD アップグレード タスクを使用する代わりに、データ インポートでフレッシュ インストールを使用します。
				• Cisco Prime Collaboration Deployment を使用して IM and Presence Service クラスタをリリース 14 または SU からリリース 15 にアップグレードする場合は、アップグレードを開始する前に、リリース 14 または SU システムに次の COP ファイルをインストールする必要があります：`ciscocm.imp15_upgrade_v1.0.k4.cop.sha512`。COP ファイルは、次の場合にのみ適用されることに注意してください。
				  • Unified Communications Manager の接続先バージョンはリリース 15 で、IM and Presence Service の送信元ノードは 14 または 14SU1 バージョンです。
				  • Unified Communications Manager の接続先バージョンがリリース 15 であり、IM and Presence Service の送信元を制限付きバージョンから無制限バージョンにアップグレードしようとしています。
					サポート対象

送信元	送信先	メカニズム	前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
		PCD 15 移行タスク（V2V）	アップグレード前チェック COP ファイルを実行します。 移行の前に、ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 COP ファイルをインストールする必要があります。 接続先バージョンが 15 で、送信元バージョンが 14 または SU が FIPS モードの場合は、次のいずれかを実行します。 • PCD は非 FIPS モードである（または置かれている）必要があります。 • PCD 移行タスクを使用する代わりに、データインポートでフレッシュインストールを使用します。	サポート対象外
		データ インポートを使用したフレッシュ インストール（V2V）	• アップグレード前チェック COP ファイルを実行します。 • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.DataExport_v1.0.cop.sgn	サポート対象外

*バージョン切り替えとは、新しいバージョンを非アクティブバージョンとしてインストールし、必要に応じて新しいバージョンと古いバージョンを切り替えることができる機能です。この機能はほとんどの直接アップグレードでサポートされますが、移行ではサポートされません。

（注） PCD のアップグレードと移行：上記の表の PCD アップグレードタスクまたは PCD 移行タスクを使用してサポートされているすべてのパスでは、PCD リリース 15 を使用する必要があります。

サポートされるバージョン

次の表に、Unified Communications Manager と IM and Presence Service の以下のリリースでサポートされているソフトウェアの全バージョンを示します。

このリリースの対象	次のバージョンがサポートされています。
15	• Cisco Unified Communications Manager 15.0.1.10000-32 • IM and Presence Service 15.0.1.10000-10

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 15.0.1.13[0-2]xx の Unified Communications Manager ES は、15（15.0.1.10900-x）リリースの一部と見なされます。

表 *2 : 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。

Unified Communications Manager の互換性情報

シスコ コラボレーション システム アプリケーション

Cisco Unified Communications Manager および IM and Presence Service のこのリリースは、シスコ コラボレーション システム リリース 15 の一部であり、他のシスコ コラボレーション アプリケーションおよびバージョンと互換性があります。

リリース 15 を構成するシスコ コラボレーション アプリケーションおよびバージョンの完全なリストについては、https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/

CSR-Compatibility-Matrix-InteractiveHTML.html にある『*Cisco Collaboration Systems* リリース互換性マトリックス』を参照してください。

Android プッシュ通知の互換性に関する推奨事項

Android プッシュ通知機能は、次のソフトウェアバージョンからサポートされています。

- Unified Communications Manager 12.5(1)SU3
- IM and Presence Service 12.5(1)SU3
- Cisco Jabber 12.9.1
- Cisco Expressway X12.6.2

（注） この互換性情報は、Cisco Webex には適用されません。

表 *3 : Android* プッシュ通知サポートの推奨リリース要件

Unified Communications Manager および IM and Presence Service のバージョン	**Expressway のバージョン**	**Unified Communications モバイルおよびリモートアクセス**	**オンプレミス展開**
次の上のすべてのクラスタ： • 11.5(1)SU8 以前 • 12.5(1)SU2 以前	X12.6.2	Android プッシュ通知はサポートされていません	Android プッシュ通知はサポートされていません
次の上のすべてのクラスタ： • 12.5(1)SU3 以降	X12.6.2	メッセージング専用の Expressway で CLI **xConfiguration XCP Config FcmService: On** を使用して Android プッシュ通知を有効にする	Android プッシュ通知はサポートされています
バージョンが混在するクラスタ（11.5(1)SU8 以前、または 12.5(1)SU2 以前、および 12.5(1)SU3 以降）	X12.6.2	メッセージングの Android プッシュ通知はサポートされていません VOIP は、リリース 12.5(1)SU3 以降でサポートされています	Android プッシュ通知は、リリース 12.5(1)SU3 以降でサポートされています

IM and Presence ストリーム機能/サービスアドバタイズメント互換性の推奨事項

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。

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）
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）

Cisco エンドポイントのサポート

すべてのサポート終了および販売終了のお知らせは、https://www.cisco.com/c/en/us/products/eos-eol-listing.html にリストされています。

サポートされる Cisco エンドポイント

次の表に、このリリースの Cisco Unified Communications Manager でサポートされている Cisco エンドポイントを示します。販売終了（EOS）またはソフトウェアメンテナンス終了になったエンドポイントについては、EOS リンクをクリックしてサポートの詳細を表示してください。

（注） シスコは、エンドポイントが廃止されているかどうかにかかわらず、ソフトウェアメンテナンスの終了またはサポートの終了ステータスに達したエンドポイントのバグ修正またはセキュリティ拡張を発行しません。シスコは、Unified Communications Manager をサポート終了電話でテストしません。また、サポートが終了していない電話機で問題を再現できない限り、サポート終了の電話機に関連する Unified Communications Manager のバグは修正されません。

表 *5*：サポートされる *Cisco* エンドポイント

デバイスシリーズ（Device Series）	デバイス モデル
Cisco Unified SIP Phone 3900 シリーズ	Cisco Unified SIP Phone 3905
Cisco Unified IP Phone 6900 シリーズ	Cisco Unified IP Phone 6901
Cisco IP Phone 7800 シリーズ	Cisco IP 電話 7811 Cisco IP 電話 7821 Cisco IP Phone 7841 Cisco IP Phone 7861 Cisco IP Conference Phone 7832
Cisco Unified IP Phone 7900 Series	Cisco Unified IP Phone Expansion Module 7915 - EOS 通知 Cisco Unified IP Phone Expansion Module 7916 - EOS 通知 Cisco Unified IP Phone 7942-G - EOS 通知 Cisco Unified IP Phone 7945-G - EOS 通知 Cisco Unified IP Phone 7962-G - EOS 通知 Cisco Unified IP Phone 7965-G - EOS 通知 Cisco Unified IP Phone 7975-G - EOS 通知
Cisco IP Phone 8800 シリーズ	Cisco IP Phone 8811、8831、8841、8845、8851、8851NR、8861、8865、8865NR Cisco Wireless IP Phone 8821、8821-EX - EOL 通知 Cisco Unified IP Conference Phone 8831 - EOS 通知 Cisco IP 会議用電話 8832 Cisco Video Phone 8875 Cisco Video Phone 8875NR
Cisco Unified IP Phone 8900 シリーズ	Cisco Unified IP Phone 8945 - EOS 通知 Cisco Unified IP Phone 8961 - EOS 通知

デバイスシリーズ（**Device Series**）	デバイス モデル
Cisco Unified IP Phone 9900 シリーズ	Cisco Unified IP Phone 9951 - EOS 通知 Cisco Unified IP Phone 9971 - EOS 通知
Cisco Jabber	Cisco Jabber for Android iPhone および iPad 版 Cisco Jabber Mac 版 Cisco Jabber Windows 版 Cisco Jabber Cisco Jabber Softphone for VDI - Windows (旧 Cisco Virtualization Experience Media Edition for Windows) Cisco Jabber Guest Cisco Jabber ソフトウェア開発キット Cisco Jabber for Tablet
Cisco Headset Series	Cisco Headset 320 Cisco Headset 520 Cisco Headset 530 Cisco Headset 560 Cisco Headset 720 Cisco Headset 730
Cisco IP Communicator	Cisco IP Communicator - EOS 通知

デバイスシリーズ（**Device Series**）	デバイス モデル
Webex	Webex アプリ Webex Room Phone Webex Desk Cisco Desk Camera 4K Cisco Desk Camera 1080p Webex Desk Hub Webex Desk Pro Webex Desk Limited Edition Webex Share - EOS 通知 Board 55、55S、70、70S、85、85S Webex Room Panorama Webex Room 70 Panorama Cisco Webex Room 70 Panorama アップグレード Room 70 Room 70 G2 Room 55 Room 55 Dual Room Kit Pro Room Kit Plus Room Kit Room Kit Mini Webex Room USB
Webex Wireless Phone 800 Series	Webex Wireless Phone 840 Webex Wireless Phone 860
Webex Meetings	iPad および iPhone 用 Webex Meetings Webex Meetings for Android
Cisco アナログ テレフォニー アダプタ	Cisco ATA 190 Series アナログ電話アダプタ - EOS/EOL 通知 Cisco ATA 191 シリーズ アナログ電話アダプタ
Cisco DX シリーズ	Cisco Webex DX70 - EOS 通知 Cisco Webex DX80 - EOS 通知 Cisco DX650 - EOS 通知

デバイスシリーズ（Device Series）	デバイス モデル
Cisco TelePresence IX5000	Cisco TelePresence IX5000
Cisco TelePresence EX シリーズ	Cisco TelePresence System EX90 - EOS 通知
Cisco TelePresence MX シリーズ	Cisco TelePresence MX200 G2 - EOS 通知 Cisco TelePresence MX300 G2 - EOS 通知 Cisco TelePresence MX700D - EOS 通知 Cisco TelePresence MX800S - EOS 通知 Cisco TelePresence MX800D - EOS 通知
Cisco TelePresence SX シリーズ	Cisco TelePresence SX10 - EOS 通知 Cisco TelePresence SX20 - EOS 通知 Cisco TelePresence SX80 - EOS 通知

Ciscoエンドポイントごとに使用されるファームウェア バージョンのリストについては、http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/CSR-Compatibility-Matrix.html にある『*Cisco Collaboration Systems Release Compatibility Matrix*』を参照してください。

電話機をサポートするデバイスパックの互換性に関する詳細は、http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/matrix/CMDP_BK_CCBDA741_00_cucm-device-package-compatibility-matrix.html にある『*Cisco Unified Communications Manager Device Package Compatibility Matrix*』を参照してください。

サポート終了日

次の表は、サポート終了日は過ぎたがまだ廃止されていないCiscoエンドポイントを示しています。廃止されたエンドポイントとは異なり、これらのエンドポイントは引き続き最新リリースで展開できますが、積極的にサポートされておらず、テストもされておらず、動作しない可能性があります。

リンクをクリックして、各エンドポイントのサポートのお知らせを表示してください。

すべてのサポート終了およびサポート終了製品については、https://www.cisco.com/c/en_ca/products/eos-eol-listing.html を参照してください。

表 *6*: サポートを終了した *Cisco* エンドポイント

サポートを終了した Cisco エンドポイント
• Cisco Unified SIP Phone 3911、3951 • Cisco Unified IP Phone 6911、6921、6941、6945、6961、7906G、7911G、7931G、7940G、7941G、7960G、7961G、8941 • Cisco Unified IP Phone Expansion Module 7925G、7925G-EX、7926G • Cisco Unified IP Conference Station 7935、7936、7937G • Cisco TelePresence EX60 • Cisco TelePresence MX200-G1、MX200-G2、MX300-G1、MX300-G2 • Cisco TelePresence 500-32、500-37、1000 MXP、1100、1300-65、1300-47、3000 Series • Cisco ATA 190 シリーズ アナログ電話アダプタ

非推奨の電話のモデル

次の表に、このリリースの Unified Communications Managerで廃止されたすべての電話機モデルと、電話モデルが最初に廃止された Unified CM リリースを示します。たとえば、リリース 11.5 (1) で最初に廃止された電話機モデルは、すべてのリリース (12.x リリースを含む) では廃止されています。

これらの電話機モデルのいずれかを使用している場合、現在のリリースの Unified Communications Manager にアップグレードすると、その電話はアップグレード後に機能しなくなります。

表 *7*: このリリースで廃止された電話機モデル

このリリースで廃止された電話のモデル	最初に廃止になった Unified CM
廃止される追加のエンドポイントはありません	リリース 15
廃止される追加のエンドポイントはありません	リリース 14
• Cisco Unified Wireless IP Phone 7921 • Cisco Unified IP Phone 7970 • Cisco Unified IP Phone 7971	12.0 (1) 以降のリリース

このリリースで廃止された電話のモデル	最初に廃止になった **Unified CM**
• Cisco IP 電話 12 S • Cisco IP 電話 12 SP • Cisco IP 電話 12 SP+ • Cisco IP 電話 30 SP+ • Cisco IP 電話 30 VIP • Cisco Unified IP 電話 7902G • Cisco Unified IP 電話 7905G • Cisco Unified IP 電話 7910 • Cisco Unified IP 電話 7910G • Cisco Unified IP 電話 7910+SW • Cisco Unified IP 電話 7910G+SW • Cisco Unified IP 電話 7912G • Cisco Unified ワイヤレス IP 電話 7920 • Cisco Unified IP Conference Station 7935	11.5 (1) 以降のリリース

仮想化の要件

このリリースの Unified Communications Manager および IM and Presence Service は、仮想化展開のみをサポートします。ベアメタルサーバーへの展開はサポートされていません。詳細については、http://www.cisco.com/go/virtualized-collaboration を参照してください。

仮想化要件については、次の表を参照してください。

表 *8*: 仮想化の要件

以下の仮想化の要件	詳細については、以下を参照してください。
Unified Communications Manager	Unified Communications Manager の仮想化要件については、https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-communications-manager.html を参照してください。
IM and Presence Service	IM and Presence Service の仮想化要件については、https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html を参照してください。

以下の仮想化の要件	詳細については、以下を参照してください。
Cisco Business Edition の展開	Cisco Business Edition などのコラボレーション ソリューション展開における Unified Communications Manager の仮想化要件については、https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-infrastructure.html を参照してください。

サポートされる LDAP ディレクトリ

次の LDAP ディレクトリがサポートされています。

- Windows Server 2016 の Microsoft Active Directory
- Windows Server 2019 の Microsoft Active Directory：15 以降のリリースでサポート
- Windows Server 2022 の Microsoft Active Directory： 15 以降のリリースでサポート
- Microsoft Lightweight Directory Services 2019 および 2022：15 以降のリリースでサポート
- Oracle Unified Directory 12cPS4
- OpenLDAP 長期サポート（LTS）リリース 2.5.16
- その他の LDAPv3 準拠ディレクトリ - Unified Communications Manager は、標準の LDAPv3 を使用してユーザのデータにアクセスします。DirSync で使用する LDAPv3 準拠のディレクトリ サーバーで supportedcontrol 属性が構成されていることを確認してください。（supportedcontrol 属性は、構成されている場合、`pagecontrolsupport` および `persistentcontrolsupport` サブ属性を返す場合があります。）

サポートされる Web ブラウザ

次の Web ブラウザがサポートされています。

- Windows 10 および 11（64 ビット）を搭載した Firefox、Chrome、および Microsoft Edge ブラウザ
- MacOS Ventura 13.4.1 上の Safari、Chrome、および Firefox

（注） サポートされているすべての Web ブラウザで最新バージョンを使用することをお勧めします。

SFTP サーバのサポート

内部テストでは、Cisco が提供し、Cisco TAC がサポートする Cisco Prime Collaboration Deployment（PCD）上で SFTP サーバを使用します。SFTP サーバ オプションの概要については、次の表を参照してください。

表 *9* : *SFTP* サーバのサポート

SFTP サーバ	サポートの説明
Cisco Prime Collaboration Deployment の SFTP サーバ	このサーバはシスコが提供およびテストした SFTP サーバのみであり、Cisco TAC がサポートします。 バージョンの互換性は、使用している Emergency Responder および Cisco Prime Collaboration Deployment のバージョンに依存します。バージョン（SFTP）または Emergency Responder をアップグレードする前に、『Cisco Prime Collaboration Deployment Administration Guide』を参照して、互換性のあるバージョンであることを確認してください。
テクノロジー パートナーの SFTP サーバ	これらのサーバはサードパーティが提供およびテストしたものです。バージョンの互換性は、サードパーティによるテストに依存します。テクノロジーパートナーの SFTP サーバまたは Unified Communications Manager をアップグレードする場合、テクノロジー パートナーのページで、互換性のあるバージョンを確認してください。 https://marketplace.cisco.com
他のサードパーティの SFTP サーバ	これらのサーバはサード パーティが提供するものであり、Cisco TAC はこれらのサーバを正式にサポートしていません。 バージョンの互換性は、SFTP バージョンと Emergency Responder バージョンの互換性を確立するためのベスト エフォートに基づきます。 （注） これらの製品がシスコでテストされていない場合、シスコはその機能を保証することができません。Cisco TAC は、これらの製品をサポートしていません。完全にテストされてサポートされる SFTP ソリューションとしては、Cisco Prime Collaboration Deployment またはテクノロジー パートナーの SFTP サーバを利用してください。

SAML SSO のサポート

シスコ コラボレーション インフラストラクチャは、SAML 2.0 への準拠を主張する他の IdP と互換性がある可能性もありますが、シスコ コラボレーション ソリューションでテストされているのは次の IdP だけです。

- Microsoft® Active Directory® Federation Services 2.0
- Microsoft Azure AD
- Okta
- OpenAM
- PingFederate®
- F5 BIG-IP

SAML SSO に関する追加情報は、『*Cisco Unified Communications* アプリケーション *SAML SSO* 導入ガイド』を参照してください。

API およびセキュア接続パッケージ

次の表に、このリリースでサポートされている API 開発パッケージとセキュア接続パッケージに関する情報を示します。

表 *10*：サポート パッケージ

パッケージ タイプ	詳細
API 開発	Cisco Unified Communications Manager と IM and Presence Service のリリース 15 は、アプリケーション開発用の OpenJDK バージョン 1.8.0.362 をサポートします。
TLS 接続	Transport Layer Security（TLS）接続の場合、このリリースは CiscoSSL 1.1.1t.7.2.500 をサポートします。
SSH クライアント	リリース 15 は、OpenSSH_8.8p1 に基づく CiscoSSH 1.10.32 をサポートします。

（注） システムにインストールされているパッケージの詳細については、`show packages active` CLI コマンドを実行してください。このコマンドとコマンド オプションの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

Unified Communications Manager でサポートされる暗号

Unified Communications Manager では、次の暗号がサポートされています。

表 *11 : TLS* 暗号のためのユニファイドコミュニケーションマネージャーの暗号サポート

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco CallManager	TCP/TLS	2443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384: AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256:AES128-SHA: ECDHE-RSA-AES256-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA128-SHA CAMELLIA256-SHA:
DRS	TCP/TLS	4040	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: DHE-RSA-CAMELLIA128-SHA: CAMELLIA128-SHA

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco Tomcat	TCP/TLS	8443 / 443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA: **（注）** リリース 14SU2 以降、次の暗号はサポートされていません。 DHE-RSA-CAMELLIA256-SHA: CAMELLIA256-SHA: DHE-RSA-CAMELLIA128-SHA: CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA:
Cisco CallManager	TCP/TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA: **（注）** リリース 14SU2 以降、次の暗号はサポートされていません。 ECDHE-ECDSA-AES256-SHA: CAMELLIA256-SHA: CAMELLIA128-SHA: ECDHE-ECDSA-DES-CBC3-SHA

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco CTL Provider （注） Cisco CTL Provider は、リリース 14SU3 以降では使用できません。	TCP/TLS	2444	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:
Cisco Certificate Authority Proxy Function	TCP/TLS	3804	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA:
CTIManager	TCP/TLS	2749	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA
シスコ信頼検証サービス	TCP/TLS	2445	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco Intercluster Lookup Service	TCP/TLS	7501	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA: **（注）** リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA:
安全な設定ダウンロード (HAPROXY)	TCP/TLS	6971、6972	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA: **（注）** リリース 14SU2 以降、次の暗号はサポートされていません。 DHE-RSA-CAMELLIA256-SHA: CAMELLIA256-SHA: DHE-RSA-CAMELLIA128-SHA: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-DES-CBC3-SHA: CAMELLIA128-SHA:

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
認証済みUDS連絡先の検索	TCP/TLS	9443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 DHE-RSA-CAMELLIA256-SHA: CAMELLIA256-SHA: DHE-RSA-CAMELLIA128-SHA: CAMELLIA128-SHA: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-DES-CBC3-SHA:

SSH でサポートされる暗号

SSH では、次の暗号がサポートされています。

表 *12 : SSH* 暗号の暗号サポート

サービス	暗号/アルゴリズム

SSH サーバ	• 暗号
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	`aes128-gcm@openssh.com`
	`aes256-gcm@openssh.com`
	• MAC アルゴリズム：
	`hmac-sha2-256`
	`hmac-sha2-512`
	`hmac-sha1`
	• KEX アルゴリズム：
	`ecdh-sha2-nistp521`
	`ecdh-sha2-nistp384`
	`ecdh-sha2-nistp256`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group14-sha256`
	`diffie-hellman-group16-sha512`
	• 非 FIPS モードのホストキーアルゴリズム：
	`rsa-sha2-256`
	`rsa-sha2-512`
	`ssh-rsa`
	• FIPS モードのホストキーアルゴリズム：
	`rsa-sha2-256`
	`rsa-sha2-512`

サービス	暗号/アルゴリズム

SSH クライアント	• 暗号：
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	`aes128-gcm@openssh.com`
	`aes256-gcm@openssh.com`
	• MAC アルゴリズム：
	`hmac-sha2-256`
	`hmac-sha2-512`
	`hmac-sha1`
	• KEX アルゴリズム：
	`ecdh-sha2-nistp521`
	`ecdh-sha2-nistp384`
	`ecdh-sha2-nistp256`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group14-sha256`
	`diffie-hellman-group16-sha512`
	• 非 FIPS モードのホストキーアルゴリズム：
	`rsa-sha2-256`
	`rsa-sha2-512`
	`ssh-rsa`
	• FIPS モードのホストキーアルゴリズム：
	`rsa-sha2-256`
	`rsa-sha2-512`

サービス	暗号/アルゴリズム
DRS クライアント	• 暗号： aes256-ctr aes256-cbc aes128-ctr aes128-cbc aes192-ctr aes192-cbc • MAC アルゴリズム： hmac-md5 hmac-sha2-256 hmac-sha1 hmac-sha1-96 hmac-md5-96 • KEX アルゴリズム： ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group1-sha1 （注） Unified CM サーバーで暗号管理機能を設定している場合、Kex アルゴリズム diffie-hellman-group-exchange-sha256、diffie-hellman-group-exchange-sha1、および diffie-hellman-group1-sha1 は、リリース 12.5(1)SU4 からサポートされません。暗号が設定されていない場合、DRS クライアントはこれらのアルゴリズムを使用します。
SFTP クライアント	• 暗号： aes128-ctr aes192-ctr aes256-ctr • MAC アルゴリズム： hmac-sha2-256 hmac-sha2-512 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1
エンド ユーザ	hmac-sha512

サービス	暗号/アルゴリズム
DRS バックアップ/ RTMT SFTP	AES-128 - Encryption
アプリケーションユーザ	AES-256 - Encryption

IM and Presence Service の互換性情報

プラットフォームの互換性

IM and Presence Service は、Unified Communications Manager とプラットフォームを共有します。Unified Communications Manager の互換性に関するトピックの多くは、IM and Presence Service のサポート トピックを兼ねています。次の項目については、Unified Communications Manager の互換性の章を参照してください。

- 安全な接続
- 仮想化の要件
- 対応する Web ブラウザ

外部データベースのサポート

常設チャット、常設チャットの高可用性、メッセージアーカイバ、マネージドファイル転送など IM and Presence Service の多くの機能では、外部データベースを展開する必要があります。データベースのサポート情報については、『IM and Presence Service のデータベース セットアップ ガイド』を参照してください。

サポートされる LDAP ディレクトリ

次の LDAP ディレクトリがサポートされています。

- Windows Server 2016 の Microsoft Active Directory
- Windows Server 2019 の Microsoft Active Directory：15 以降のリリースでサポート
- Windows Server 2022 の Microsoft Active Directory： 15 以降のリリースでサポート
- Microsoft Lightweight Directory Services 2019 および 2022：15 以降のリリースでサポート
- Oracle Unified Directory 12cPS4
- OpenLDAP 長期サポート（LTS）リリース 2.5.16
- その他の LDAPv3 準拠ディレクトリ - Unified Communications Manager は、標準の LDAPv3 を使用してユーザのデータにアクセスします。DirSync で使用する LDAPv3 準拠のディレクトリ サーバーで supportedcontrol 属性が構成されていることを確認してください。（supportedcontrol 属性は、構成されている場合、`pagecontrolsupport` および `persistentcontrolsupport` サブ属性を返す場合があります。）

フェデレーションのサポート

SIP フェデレーション/SIP オープン フェデレーションのサポート

SIP オープン フェデレーションは、12.5(1)SU3 以降でサポートされます。

次の表に、サポートされている SIP 制御および SIP オープン フェデレーションの統合を示します。

Table 13: サポートされている ***SIP*** 制御およびオープン フェデレーション

サードパーティ製システム	単一エンタープライズ ネットワーク*（ドメイン内またはドメイン間フェデレーション）		B2B（企業間）（ドメイン間フェデレーション）
	ダイレクト フェデレーション	Expressway 経由	Expressway 経由
Skype for Business 2015（オンプレミス）	Y	サポート対象外	Y（トラフィック分類）
Office 365（クラウドでホストされている Skype for Business を使用）	N/A	N/A	Y（トラフィック分類）

* 単一エンタープライズ ネットワークは、サポート値がそれぞれ同じであるため、分割されたドメイン内フェデレーションまたはドメイン間フェデレーションにすることができます。B2B（企業間）フェデレーションは常にドメイン間フェデレーションです。

サポートされる XMPP フェデレーション

IM and Presence Service のこのリリースは、次のシステムとの XMPP フェデレーションをサポートしています。

- Cisco Webex Messenger
- IM and Presence Service リリース 10.x 以上
- その他の XMPP 準拠システム

クラスタ間ピアリングのサポート

IM and Presence Service のこのリリースは、次の IM and Presence Service リリースでクラスタ間ピアリングをサポートします。

（注） IM and Presence Service のバージョンが EOL/EOS になっている場合、クラスタ間ピアリングはサポートされません。

- リリース 11.5
- リリース 12.x
- リリース 14 および SU
- リリース 15

Microsoft Outlook カレンダー統合

IM and Presence Service は、オンプレミスの Exchange サーバーまたはホストされた Office 365 サーバーのいずれかとの Microsoft Outlook 予定表統合をサポートします。サポート情報については、以下の表を参照してください。

表 *14*：予定表統合のサポート情報

コンポーネント	互換性のあるバージョン
Windows Server	• Windows Server 2016 • Windows Server 2019 - 11.x リリースでは、IM and Presence Service の最小リリースは 11.5(1)SU7 です。12.x リリースでは、IM and Presence Service の最小リリースは 12.5(1)SU2 です。
Microsoft Exchange Server 2016	Microsoft Exchange 2016
Microsoft Exchange Server 2019	Microsoft Exchange 2019
Microsoft Office 365	ホストされた Office 365 サーバーの展開の詳細については、Microsoft のドキュメントを参照してください。 （注） 2020 年 10 月の時点で、Microsoft は、Exchange Online でサポートされている認証メカニズムを、OAuth ベースの認証のみを使用するように変更しています。この変更後、IM and Presence Service と Office 365 間で予定表統合を展開する場合は、IM and Presence Service をリリース 12.5(1)SU2 にアップグレードする必要があります。この変更は、オンプレミスの Exchange サーバーとの統合には影響しません。
Active Directory	• Windows Server 2016 を使用した Active Directory 2016 （注） Active Directory 内のユーザ名は、Unified Communications Manager に定義されたユーザ名と一致している必要があります。
サードパーティの証明書または証明書サーバー	証明書を作成するためには、これらのいずれかが必要。 （注） IM and Presence Service との Microsoft Exchange 統合は、RSA 1024 または 2048 ビットキーと SHA1 および SHA256 署名アルゴリズムを使用する証明書をサポートします。

IM and Presence Service でサポートされる暗号

次の暗号が IM and Presence Service でサポートされています。

表 *15 : Unified Communications Manager IM & Presence* 暗号サポートが *TLS* の暗号でサポートされています

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco SIP Proxy	TCP/TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA: **（注）** リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA:
Cisco SIP Proxy	TCP/TLS	5062	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA: **（注）** リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA:

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco SIP Proxy	TCP/TLS	8083	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA: **（注）** リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA:
Cisco Tomcat	TCP/TLS	8443、443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256:AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA: **（注）** リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA128-SHA: CAMELLIA256-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: DHE-RSA-CAMELLIA128-SHA: DHE-RSA-CAMELLIA256-SHA: ECDHE-ECDSA-AES256-SHA: EDH-RSA-DES-CBC3-SHA:

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco XCP XMPP Federation Connection Manager	TCP/TLS	5269	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: **（注）** リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA: ECDHE-RSA-AES256-SHA:
Cisco XCP Client Connection Manager	TCP/TLS	5222	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: **（注）** リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA128-SHA: CAMELLIA256-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA: ECDHE-RSA-AES256-SHA:

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。