導入シナリオ

オンプレミス展開

オンプレミス展開とは、社内ネットワークのすべてのサービスをセットアップ、管理、保守する展開です。

次のモードで Cisco Jabber を展開できます。

- **フル UC**：フル UC モードを展開するには、インスタント メッセージングとプレゼンス機能を有効にし、ボイスメールと会議機能をプロビジョニングし、音声とビデオ用のデバイスを使用してユーザをプロビジョニングします。
- **IM 専用**：IM 専用モードを展開するには、インスタント メッセージングとプレゼンス機能を有効にします。デバイスを使用してユーザをプロビジョニングしないでください。
- **電話機モード**：電話機モードでは、ユーザのプライマリ認証が Cisco Unified Communications Manager で行われます。電話機モードを展開するには、音声とビデオ機能用のデバイスを使用してユーザをプロビジョニングします。また、ボイス メールなどの追加サービスを持つ個人をプロビジョニングできます。

デフォルト製品モードは、ユーザのプライマリ認証が IM and Presence サーバで行われるモードです。

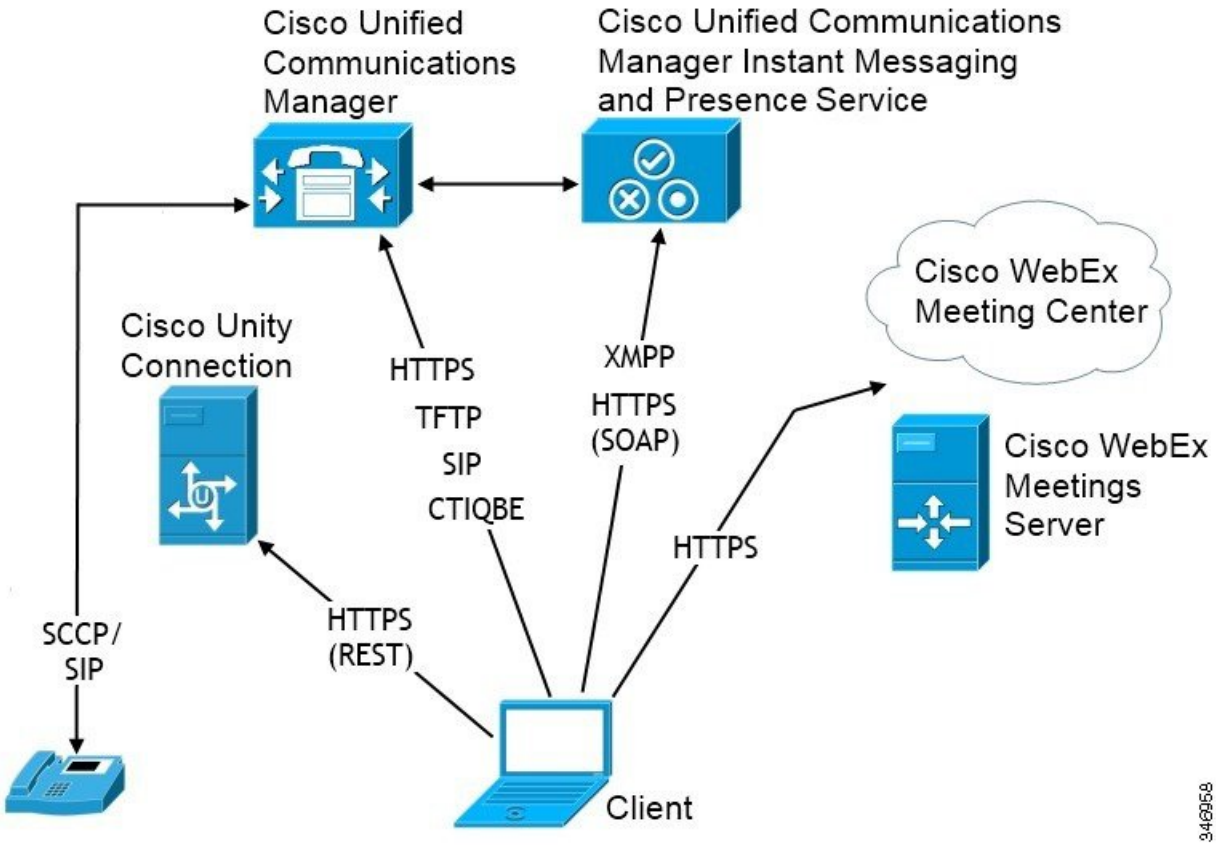
Cisco Unified Communications Manager IM and Presence Service によるオンプレミス展開

Cisco Unified Communications Manager IM and Presence サービスによるオンプレミス展開で使用可能なサービスは次のとおりです。

- **プレゼンス**：Cisco Unified Communications Manager IM and Presence Service を介して、アベイラビリティを公開したり、他のユーザのアベイラビリティを登録できます。
- **IM**：Cisco Unified Communications Manager IM and Presence Service 経由で IM を送受信します。
- **ファイル転送**：Cisco Unified Communications Manager IM and Presence Service 経由でファイルとスクリーンショットを送受信します。
- **音声コール**：卓上電話機を介して、またはコンピュータで Cisco Unified Communications Manager を介して音声コールを発信します。
- **ビデオ**：Cisco Unified Communications Manager 経由でビデオ コールを発信します。
- **ボイスメール**：Cisco Unity Connection 経由でボイス メッセージを送受信します。
- **会議**：次のいずれかと統合します。
  - Cisco WebEx Meeting Center：ホステッド会議機能を提供します。
  - Cisco WebEx Meeting Server：オンプレミス会議機能を提供します。

次の図は、Cisco Unified Communications Manager IM and Presence Service によるオンプレミス展開のアーキテクチャを示しています。

図 *1*：*Cisco Unified Communications Manager IM and Presence Service* によるオンプレミス展開



コンピュータ テレフォニー インテグレーション

Cisco Jabber for Windows および Cisco Jabber for Mac がサードパーティ製アプリケーションからの Cisco Jabber の CTI 従属をサポートします。

コンピュータテレフォニーインテグレーション（CTI）を使用すれば、電話コールを発信、受信、および管理しながら、コンピュータ処理機能を利用することができます。CTI アプリケーションを使用すれば、発信者 ID から提供された情報に基づいてデータベースから顧客情報を取得したり、自動音声応答（IVR）システムが収集した情報を利用したりできます。

CTI の詳細については、該当するリリースの『*Cisco Unified Communications Manager System Guide*』の CTI の項を参照してください。また、Cisco Unified Communications Manager API を介して CTI 制御用のアプリケーションを作成する方法については、Cisco Developer Network 上の次のサイトを参照できます。

- Cisco TAPI： https://developer.cisco.com/site/jtapi/overview/

- Cisco JTAPI： https://developer.cisco.com/site/jtapi/overview/

電話機モードでのオンプレミス展開

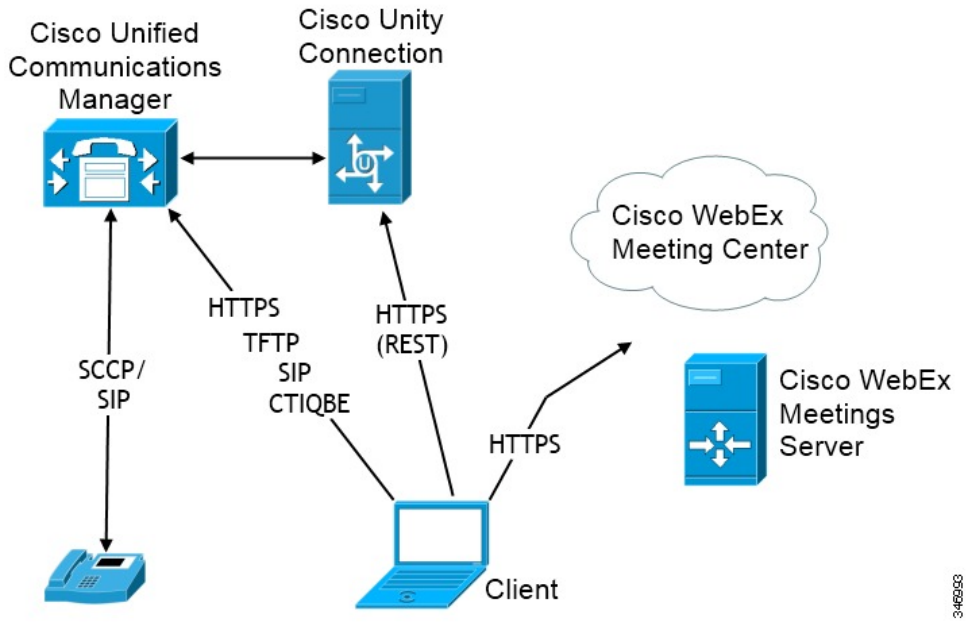
電話機モード展開で使用可能なサービスは次のとおりです。

- **連絡先**：モバイル クライアントのみに適用されます。Cisco Jabber は電話の連絡先アドレス帳から連絡先情報を更新します。
- **音声コール**：卓上電話機を介して、またはコンピュータで Cisco Unified Communications Manager を介して音声コールを発信します。
- **ビデオ**：Cisco Unified Communications Manager 経由でビデオ コールを発信します。
- **ボイスメール**：Cisco Unity Connection 経由でボイス メッセージを送受信します。
- **会議**：次のいずれかと統合します。
  - **Cisco WebEx Meeting Center**：ホステッド会議機能を提供します。
  - **Cisco WebEx Meeting Server**：オンプレミス会議機能を提供します。

（注） Cisco Jabber for Android と Cisco Jabber for iPhone and iPad は電話モードでの会議をサポートしません。

次の図は、電話モードでのオンプレミス展開のアーキテクチャを示しています。

図 *2*：電話機モードでのオンプレミス展開



ソフトフォン

ソフトフォン モードは TFTP サーバから設定ファイルをダウンロードし、SIP に登録済みのエンドポイントとして動作します。クライアントは CCMCIP または UDS サービスを使用して、Cisco Unified Communications Manager に登録するデバイス名を取得します。

デスクフォン

デスクフォン モードは、Cisco Unified Communications Manager との CTI 接続を作成して IP フォンを制御します。クライアントは CCMCIP を使用してユーザに関連付けられたデバイスについての情報を集め、クライアントが制御可能な IP フォンのリストを作成します。

デスクフォン モードの Cisco Jabber for Mac は、デスクフォン ビデオをサポートしません。

Extend and Connect

Cisco Unified Communications Manager の Extend and Connect 機能により、ユーザは、公衆電話交換網（PSTN）の電話や構内交換機（PBX）などのデバイスへの通話を制御できます。詳細については、お使いの Cisco Unified Communications Manager リリースの Extend and Connect 機能を参照してください。

Extend and Connect 機能は、Cisco Unified Communications Manager 9.1(1) 以降で使用することをお勧めします。

クラウドベース展開

クラウドベース展開は、Cisco WebEx がサービスをホストする展開の 1 つです。Cisco WebEx 管理ツールでクラウドベース展開を管理および監視します。

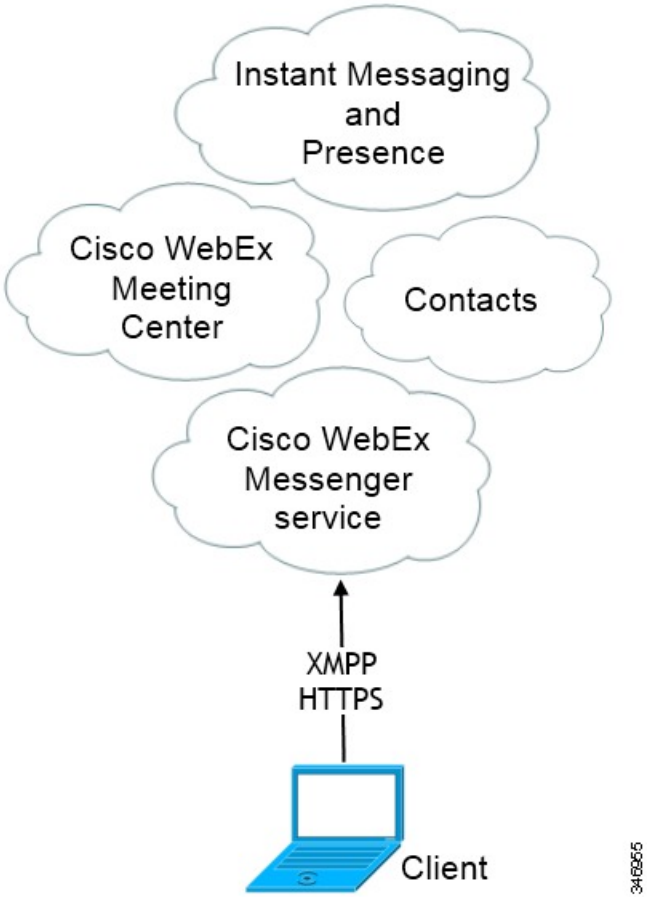
クラウドベース展開

クラウドベース展開で使用可能なサービスは次のとおりです。

- **連絡先ソース**：Cisco WebEx Messenger サービスは、連絡先を解決できるようにします。
- **プレゼンス**：Cisco WebEx Messenger サービスは、ユーザがアベイラビリティを公開したり、他のユーザのアベイラビリティを登録できるようにします。
- **インスタントメッセージ**：Cisco WebEx Messenger サービスは、ユーザがインスタント メッセージを送受信できるようにします。
- **会議**：Cisco WebEx Meeting Center はホステッド会議機能を提供します。

次の図は、クラウドベース展開のアーキテクチャを示しています。

図 *3*：クラウドベース展開



ハイブリッド クラウドベース展開

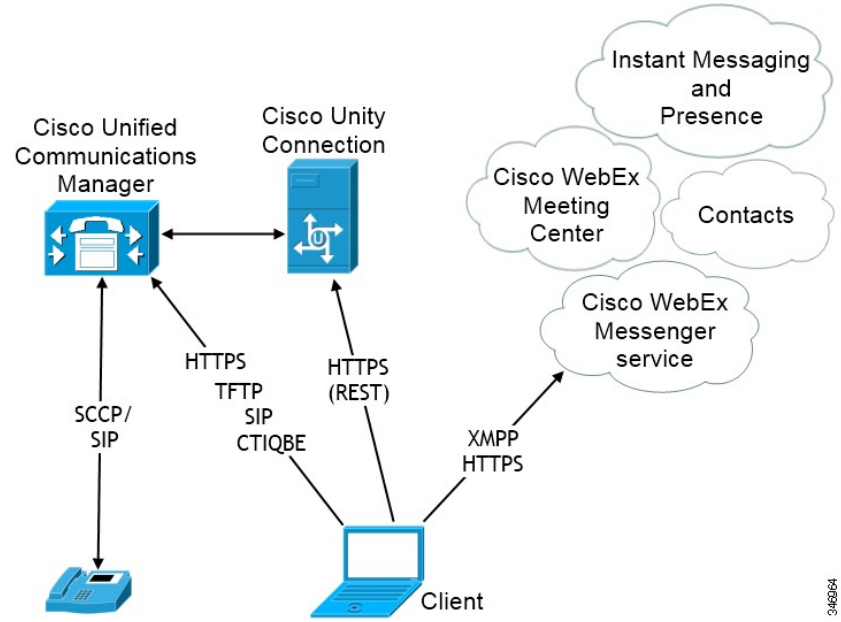
ハイブリッド クラウドベース展開で使用可能なサービスは次のとおりです。

- **連絡先ソース**：Cisco WebEx Messenger サービスは、連絡先を解決できるようにします。
- **プレゼンス**：Cisco WebEx Messenger サービスは、ユーザがアベイラビリティを公開したり、他のユーザのアベイラビリティを登録できるようにします。
- **インスタントメッセージ**：Cisco WebEx Messenger サービスは、ユーザがインスタント メッセージを送受信できるようにします。
- **音声**：卓上電話機を介して、またはコンピュータで Cisco Unified Communications Manager を介して音声コールを発信します。
- **ビデオ**：Cisco Unified Communications Manager 経由でビデオ コールを発信します。

- **会議**：Cisco WebEx Meeting Center はホステッド会議機能を提供します。
- **ボイスメール**：Cisco Unity Connection 経由でボイス メッセージを送受信します。

次の図は、ハイブリッド クラウドベース展開のアーキテクチャを示しています。

図 *4*：ハイブリッド クラウドベース展開



仮想環境での展開

仮想環境に Cisco Jabber for Windows を展開できます。

仮想環境でサポートされる機能は次のとおりです。

- 他の Cisco Jabber クライアントとのインスタント メッセージングおよびプレゼンス
- デスクフォン制御
- ボイスメール
- Microsoft Outlook 2007、2010、2013 とのプレゼンスの統合

仮想環境とローミング プロファイル

仮想環境では、ユーザが常に同じ仮想デスクトップにアクセスするわけではありません。一貫したユーザ エクスペリエンスを保証するために、クライアントが起動されるたびにこれらのファイルにアクセスできる必要があります。Cisco Jabber はユーザ データを次の場所に保存します。

- C:\Users*username*\AppData\Local\Cisco\Unified Communications\Jabber\CSF
  - **連絡先**：連絡先キャッシュ ファイル
  - **履歴**：コールとチャットの履歴
  - **写真キャッシュ**：ディレクトリの画像をローカルにキャッシュ
- C:\Users*username*\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF
  - **コンフィギュレーション**：ユーザ コンフィギュレーション ファイルを保持し、コンフィギュレーション ストア キャッシュを保存
  - **クレデンシャル**：暗号化されたユーザ名とパスワード ファイルを保存

（注） 非永続的 Virtual Deployment Infrastructure（VDI）モードで Cisco Jabber を使用している場合、Cisco Jabber クレデンシャル キャッシュはサポートされません。

必要に応じて、ファイルとフォルダを除外リストに追加することによって、それらを同期から除外できます。除外されたフォルダ内のサブフォルダを同期するには、そのサブフォルダを包含リストに追加します。

個人ユーザ設定を保持するには、次を実行する必要があります。

- 次のディレクトリを除外しないでください。
  - AppData\Local\Cisco
  - AppData\Local\JabberWerxCPP
  - AppData\Roaming\Cisco
  - AppData\Roaming\JabberWerxCPP
- 次の専用のプロファイル管理ソリューションを使用してください。
  - **Citrix Profile Management**：Citrix 環境向けのプロファイル ソリューションを提供します。仮想デスクトップのホストがランダムに割り当てられる展開では、Citrix Profile Management はインストールされているシステムとユーザ ストア間で各ユーザのプロファイル全体を同期させます。
  - **VMware View Persona Management**：ユーザ プロファイルを保存し、リモート プロファイル リポジトリと動的に同期させます。VMware View Persona Management は Windows ローミング プロファイルを必要としないので、VMware Horizon View ユーザ プロファイルの管理で Windows Active Directory をバイパスできます。Persona Management は、既存のローミング プロファイルの機能を強化します。

リモート アクセス

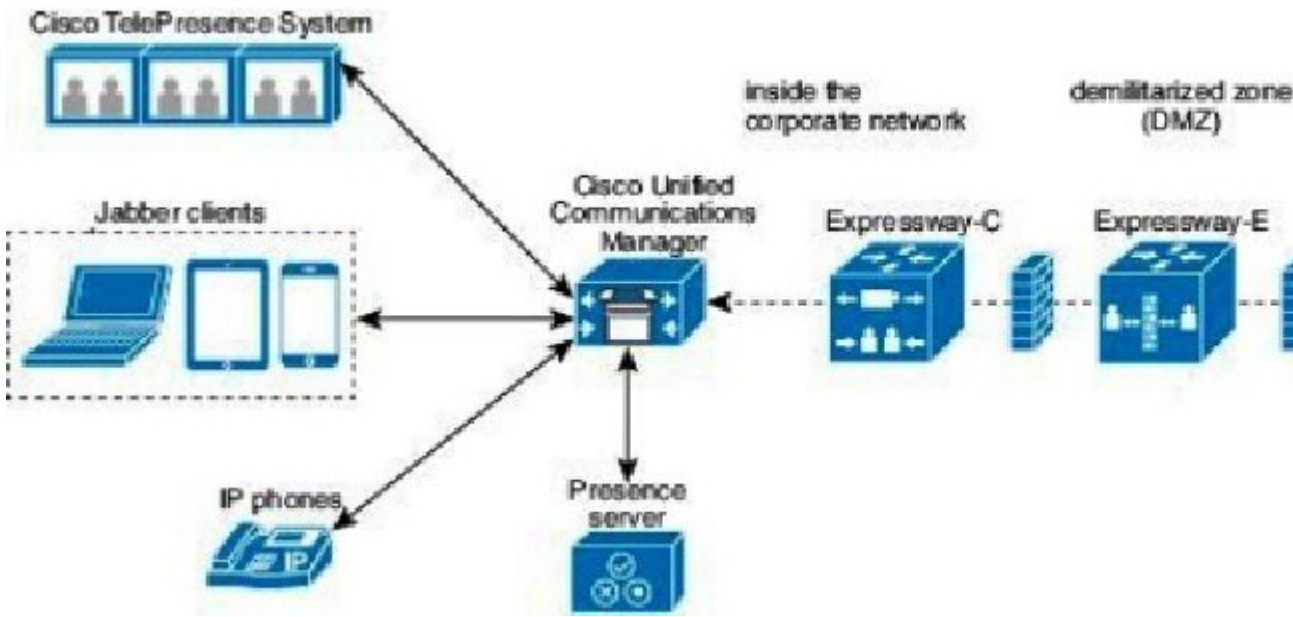
ユーザが企業ネットワークの外部の場所から作業にアクセスしなければならないことがあります。リモート アクセス用のいずれかのシスコ製品を使用して、ユーザが作業にアクセスできるようにします。

Expressway Mobile and Remote Access

Cisco Unified Communications Manager 用の Expressway for Mobile and Remote Access を使用すると、ユーザは仮想プライベートネットワーク（VPN）を使用しなくても、企業のファイアウォールの外側からコラボレーション ツールにアクセスできます。シスコのコラボレーション ゲートウェイを使用して、クライアントは公衆 Wi-Fi ネットワークやモバイル データ ネットワークなどのリモート ロケーションから社内ネットワークに安全に接続できます。

次の図は、Expressway for Mobile and Remote Access 環境のアーキテクチャを図に示したものです。

図 *5*：クライアントが、*Expressway for Mobile and Remote Access* に接続する方法



Expressway for Mobile and Remote Access を使用した Jabber への初回サインイン

モバイル クライアント向け Cisco Jabber に適用されます。

ユーザは最初に Expressway for Mobile and Remote Access を使用してクライアントにサインインすると、企業のファイアウォールの外からサービスに接続できます。ただし、次の場合は最初に社内ネットワーク内でサインインします。

- 音声サービス ドメインが他のサービス ドメインと異なる場合、ユーザは社内ネットワーク内から jabber-config.xml ファイルの適切な音声サービス ドメインを取得する必要があります。ただし、ハイブリッド展開の場合、管理者は jabber-config.xml ファイルの VoiceServicesDomain パラメータを設定できます。この場合、ユーザは社内ネットワーク内でサインインする必要はありません。
- Cisco Jabber が CAPF 登録プロセス（セキュア モードまたは混合モードのクラスタを使用する場合に必要）を完了する必要がある場合。

ユーザが Expressway for Mobile and Remote Access 環境でセキュアな電話機を使用している場合、最初のサインインはサポートされません。設定が暗号化された TFTP を含むセキュア プロファイルの場合、最初にオンプレミス内でサインインし、CAPF 登録を可能にする必要があります。Cisco Unified Communications Manager、Expressway for Mobile and Remote Access、および Cisco Jabber の各拡張機能を使用しないと、パブリック ネットワークで最初にサインインすることはできません。ただし、次の項目がサポートされます。

- 暗号化された TFTP（オンプレミスで最初にサインイン）。
- 暗号化されていない TFTP（Expressway for Mobile and Remote Access またはオンプレミスで最初にサインイン）。

サポートされるサービス

次の表に、クライアントが Expressway for Mobile and Remote Access を使用してリモートで Cisco Unified Communications Manager に接続した場合にサポートされるサービスと機能の概要を示します。

表 *1*：*Expressway for Mobile and Remote Access* でサポートされるサービスの概要

サービス	サポート対象	非サポート対象
ディレクトリ		
UDS ディレクトリ検索	X	
LDAP ディレクトリ検索		X
ディレクトリ写真解決	X * Cisco Expressway-C 上で HTTP ホワイト リストを使用	
ドメイン内フェデレーション	X *連絡先検索のサポートは連絡先 ID の形式に依存します。詳細については、以下の注記を参照してください。	

サービス	サポート対象	非サポート対象
ドメイン間フェデレーション	X	
インスタント メッセージおよびプレゼンス		
オンプレミス	X	
クラウド	X	
チャット	X	
グループ チャット	X	
ハイ アベイラビリティ：オンプレミス展開	X	
ファイル転送：オンプレミス展開	X Cisco Unified Communications Manager IM and Presence サービス 10.5(2) 以降を使用したファイル転送に使用可能な高度なオプション、後述の注意を参照してください。	
ファイル転送：クラウド展開	X	
ビデオ画面共有：BFCP	X（モバイル クライアント向け Cisco Jabber は BFCP 受信のみをサポートします）。	
IM 専用画面の共有		x
オーディオとビデオ		
音声コールとビデオ コール	X * Cisco Unified Communications Manager 9.1(2) 以降	
デスクフォン制御モード（CTI）（デスクトップ クライアントのみ）		X
Extend and connect（デスクトップ クライアントのみ）		X
リモートデスクトップ制御（デスクトップ クライアントのみ）		X

サービス	サポート対象	非サポート対象
サイレント モニタリングおよびコール録音		X
Dial via Office - リバース（モバイル クライアントのみ）	X	
セッションの永続性		X
アーリー メディア		X
セルフケアポータル アクセス		X
グレースフル登録	X * Cisco Jabber for Android に適用されます。 Jabber for Android は、Expressway for Mobile および Cisco Unified Communications Manager リリース 10.5.(2) 10000-1 のリモート アクセスに対するグレースフル登録をサポートします。	
共有回線	X 前提条件： • Cisco Expressway を X8.9.1 以降にアップグレード • Cisco Unified Communications Manager を 11.5 SU(2) 以降にアップグレード	
ボイスメール		
ビジュアル ボイスメール	X * Cisco Expressway-C 上で HTTP ホワイト リストを使用	
Cisco WebEx Meetings		
オンプレミス	X	
クラウド	X	

サービス	サポート対象	非サポート対象
Cisco WebEx 画面共有（デスクトップ クライアントのみ）	X	
インストール（デスクトップ クライアント）		
インストーラ更新	X * Cisco Expressway-C 上で HTTP ホワイト リストを使用	X Cisco Jabber for Mac ではサポートされない
カスタマイゼーション		
カスタム HTML タブ		X
Enhanced911 プロンプト	X * 企業ネットワークの外部で稼働するすべての Jabber クライアントで Web ページが正しく表示されるようにするには、スクリプトおよびリンク タグが E911NotificationURL パラメータでサポートされていないため、Web ページに静的な HTML ページを指定する必要があります。詳細については、『*Parameter Reference Guide for Cisco Jabber*』の最新版を参照してください。	
セキュリティ		
エンドツーエンド暗号化	X	
CAPF 登録		X
シングル サインオン	X	
Advanced Encryption Standard（AES）256 および TLS1.2	X * Cisco Jabber for Android に適用されます。 Advanced Encryption Standard は社内 Wi-Fi でのみサポートされます	
トラブルシューティング（デスクトップ クライアントのみ）		

サービス	サポート対象	非サポート対象
問題レポートの生成	X	
問題レポートのアップロード		X
ハイ アベイラビリティ（フェールオーバー）		
音声およびビデオ サービス		X
ボイスメール サービス		X
IM and Presence サービス	X	
構成管理		
高速サインイン	X	
認証および承認		
SSO Jabber ユーザ用の O-Auth サポート	X	

ディレクトリ

クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合は、次の制限付きでディレクトリ統合がサポートされます。

- LDAP を使用した連絡先解決：企業ファイアウォールの外側のクライアントは連絡先解決に LDAP を使用することができません。代わりに、連絡先解決に UDS を使用する必要があります。

  ユーザが企業ファイアウォールの内側にいる場合は、クライアントは連絡先解決に UDS と LDAP のいずれかを使用できます。企業ファイアウォールの内側に LDAP を展開する場合は、LDAP ディレクトリ サーバを Cisco Unified Communications Manager と同期させ、ユーザが企業ファイアウォールの外側にいるときにクライアントを UDS に接続できるようにすることをお勧めします。

- ディレクトリ写真解決：クライアントが連絡先写真を確実にダウンロードできるようにするには、Cisco Expressway-C サーバのホワイト リストに、連絡先写真をホストするサーバを追加する必要があります。Cisco Expressway-C ホワイト リストにサーバを追加するには、[HTTP サーバ許可（HTTP server allow）] 設定を使用します。詳細については、関連する Cisco Expressway のマニュアルを参照してください。

- ドメイン内フェデレーション：ドメイン内フェデレーションを展開して、クライアントがファイアウォールの外側から Expressway for Mobile and Remote Access に接続した場合は、連絡先 ID に次の形式のいずれかが使用されている場合にのみ連絡先検索がサポートされます。

  - sAMAccountName@domain

- UserPrincipleName(UPN)@domain
- EmailAddress@domain
- employeeNumber@domain
- telephoneNumber@domain

- XMPP を使用するドメイン間フェデレーション：Expressway for Mobile and Remote Access は、XMPP ドメイン間フェデレーション自体を有効にするものではありません。Expressway for Mobile and Remote Access 経由で接続された Cisco Jabber クライアントでは、Cisco Unified Communications Manager IM and Presence で有効になっている XMPP ドメイン間フェデレーションを使用できます。

インスタント メッセージおよびプレゼンス

クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合は、次の制限付きでインスタント メッセージングとプレゼンスがサポートされます。

デスクトップおよびモバイル クライアントのファイル転送には次の制限があります。

- Cisco WebEx クラウド展開では、ファイル転送がサポートされます。
- Cisco Unified Communication IM and Presence サービス 10.5(2) 以降を使用したオンプレミス展開では、[マネージドファイル転送（Managed File Transfer）] オプションはサポートされますが、[ピアツーピア（Peer-to-Peer）] オプションはサポートされません。
- Cisco Unified Communications Manager IM and Presence サービス 10.0(1) 以前を使用したオンプレミス展開では、ファイル転送がサポートされません。

音声コールとビデオ コール

クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合は、次の制限付きで音声およびビデオ通話がサポートされます。

- Cisco Unified Communications Manager：Expressway for Mobile and Remote Access は、Cisco Unified Communications Manager バージョン 9.1.2 以降でビデオおよび音声通話をサポートします。
- デスクフォン制御モード（CTI）（デスクトップ クライアントのみ）：クライアントは、エクステンション モビリティを含むデスクフォン制御モード（CTI）をサポートしません。
- Extend and connect（デスクトップ クライアントのみ）：クライアントを以下の目的に使用することはできません。
  - オフィスの Cisco IP Phone でコールを発信および受信する。
  - 自宅電話、ホテルの電話、またはオフィスの Cisco IP Phone で、保留と復帰などの通話中制御を実行する。
- セッション永続性：クライアントが使用するネットワークが切り替わると、音声コールおよびビデオ コールが切断され、復帰できません。たとえば、ユーザがオフィス内で Cisco Jabber

コールを開始してから、建物を出て Wi-Fi 接続が切断されると、クライアントが Expressway for Mobile and Remote Access を使用するように切り替わるため、コールが切断されます。

- アーリー メディア：アーリー メディアを使用すれば、クライアントは、接続が確立される前にエンドポイント間でデータを交換できます。たとえば、ユーザが同じ組織に属さない通話者にコールを発信し、相手側がこれを拒否したまたはコールに応答しなかった場合、アーリー メディアによってユーザがビジー トーンを受け取るか、ボイスメールがユーザに送信されます。

  Expressway for Mobile and Remote Access を使用している場合は、電話の相手がコールを拒否するか、応答しないと、ビジー トーンが鳴りません。代わりに、ユーザは、コールが終了するまで約 1 分無音を受信します。

- セルフ ケア ポータル アクセス（デスクトップ クライアントのみ）：ユーザは、ファイアウォールの外側にいるときに Cisco Unified Communications Manager のセルフ ケア ポータルにアクセスできません。外部から Cisco Unified Communications Manager のユーザ ページにアクセスできません。

  Cisco Expressway-E は、ファイアウォールの内側のクライアントとユニファイド コミュニケーション サービス間のすべての通信をプロキシします。ただし、Cisco Expressway-E は Cisco Jabber アプリケーションではないブラウザからアクセスされるサービスをプロキシしません。

ボイスメール

ボイスメール サービスは、クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合にサポートされます。

（注） クライアントがボイスメール サービスに確実にアクセスできるようにするには、Cisco Expressway-C サーバのホワイト リストにボイスメール サーバを追加する必要があります。Cisco Expressway-C ホワイト リストにサーバを追加するには、[HTTPサーバ許可（HTTP server allow）] 設定を使用します。詳細については、関連する Cisco Expressway のマニュアルを参照してください。

インストール

Cisco Jabber for Mac：クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合は、インストーラ更新がサポートされません。

Cisco Jabber for Windows：クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合は、インストーラ更新がサポートされます。

（注） クライアントがインストーラ更新を確実にダウンロードできるようにするには、Cisco Expressway-C サーバのホワイト リストにインストーラ更新をホストするサーバを追加する必要があります。Cisco Expressway-C ホワイト リストにサーバを追加するには、[HTTPサーバ許可（HTTP server allow）] 設定を使用します。詳細については、関連する Cisco Expressway のマニュアルを参照してください。

セキュリティ

クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合は、次の制限付きでほとんどのセキュリティ機能がサポートされます。

- 初期 CAPF 登録：Certificate Authority Proxy Function（CAPF）登録は、Cisco Jabber（または他のクライアント）に証明書を発行する Cisco Unified Communications Manager Publisher 上で動作するセキュリティ サービスです。正常に CAPF を登録するために、クライアントはファイアウォールの内側から接続するか VPN 接続を使用する必要があります。
- エンドツーエンド暗号化：ユーザが Expressway for Mobile and Remote Access 経由で接続し、コールに参加する場合：
  - Cisco Expressway-C と Cisco Unified Communications Manager に Expressway for Mobile and Remote Access を使用して登録されたデバイスとの間のコール パスで、メディアは常に暗号化されます。
  - Cisco Jabber または内部デバイスが暗号化セキュリティ モードに設定されていない場合は、メディアは Cisco Expressway-C と、Cisco Unified Communications Manager にローカルに登録されたデバイスの間のコール パス上で暗号化されません。
  - Cisco Jabber と内部デバイスの両方が暗号化セキュリティ モードに設定されている場合は、メディアが Expressway-C と、Cisco Unified Communnication Manager にローカルに登録されたデバイス間のコール パス上で暗号化されます。
  - Cisco Jabber クライアントが常に Expressway for Mobile and Remote Access を通じて接続されている場合は、エンドツーエンド暗号化を実現するための CAPF 登録は不要です。ただし、Cisco Jabber デバイスは引き続き暗号化セキュリティ モードで設定し、Cisco Unified Communications Manager が混合モードをサポートできるようにする必要があります。
- シングル サインオン（SSO）：オンプレミス展開で SSO を有効にすると、Expressway for Mobile and Remote Access 展開にも適用されます。SSO を無効にすると、オンプレミス展開と Expressway for Mobile and Remote Access 展開の両方で無効になります。

トラブルシューティング

Cisco Jabber for Windows のみ。問題レポート アップロード：デスクトップ クライアントが Expressway for Mobile and Remote Access を使用してサービスに接続した場合は、問題レポートが

HTTPS 経由で指定された内部サーバにアップロードされるため、問題レポートを送信できません。

この問題を回避するには、ユーザはレポートをローカルに保存し、別の方法でレポートを送信できます。

ハイ アベイラビリティ（フェールオーバー）

ハイアベイラビリティとは、クライアントがプライマリ サーバに接続できない場合に、サービスをほとんどまたは全く中断させることなく、セカンダリ サーバにフェールオーバーすることを意味します。Expressway for Mobile and Remote Access 上でサポートされるハイ アベイラビリティの場合は、特定のサービスをセカンダリ サーバ（Instant Messaging and Presence など）にフェールオーバーするサーバを意味します。

ハイ アベイラビリティについてサポートされない一部のサービスが Expressway for Mobile and Remote Access 上で使用できます。これは、ユーザが社内ネットワークの外部からクライアントに接続している場合に、Instant Messaging and Presence サーバがフェールオーバーしても、サービスが通常どおり提供されることを意味します。ただし、音声およびビデオ サーバまたはボイスメール サーバがフェールオーバーした場合は、関連するサーバがハイアベイラビリティをサポートしないため、それらのサービスは提供されません。

Cisco AnyConnect の展開

Cisco AnyConnect は、クライアントが Wi-Fi ネットワークやモバイル データ ネットワークなどのリモートの場所から社内ネットワークに安全に接続できるようにするサーバ/クライアント インフラストラクチャを意味します。

Cisco AnyConnect 環境は、次のコンポーネントで構成されます。

- Cisco 適応型セキュリティ アプライアンス：リモート アクセスを保護するためのサービスを提供します。
- Cisco AnyConnect セキュア モビリティ クライアント：ユーザのデバイスから Cisco 適応型セキュリティ アプライアンスへのセキュアな接続を確立します。

このセクションでは、Cisco AnyConnect セキュア モビリティ クライアントを使用して Cisco 適応型セキュリティ アプライアンス（ASA）を展開する場合に考慮すべき情報を提供します。Cisco AnyConnect は、Cisco Jabber for Android と Cisco Jabber for iPhone and iPad 用にサポートされている VPN です。サポートされていない VPN クライアントを使用している場合は、該当するサードパーティのマニュアルを使用して VPN クライアントがインストールされ、設定されていることを確認します。

Android OS 4.4.x を実行している Samsung デバイスの場合は、Samsung AnyConnect のバージョン 4.0.01128 以降を使用します。Android OS バージョン 5.0 以降の場合は、ソフトウェア バージョンが 4.0.01287 以降の Cisco AnyConnect を使用する必要があります。

Cisco AnyConnect は、Cisco 5500 シリーズ ASA へのセキュアな IPsec（IKEv2）または SSL VPN 接続をリモート ユーザに提供します。また、Cisco AnyConnect は、ASA からまたは社内ソフトウェア展開システムを使用してリモート ユーザに展開できます。ASA から展開する場合は、リモート

ユーザが、クライアントレス SSL VPN 接続を許可するように設定された ASA のブラウザで IP アドレスまたはDNS名を入力することによって、ASAへの初期SSL接続を確立します。その後で、ASAが、ブラウザウィンドウにログイン画面を表示し、ユーザがログインと認証を満たした場合に、コンピュータのオペレーティング システムにマッチするクライアントをダウンロードします。ダウンロード後、クライアントは自動的にインストールおよび設定され、ASA への IPsec（IKEv2）接続または SSL 接続が確立されます。

Cisco 適応型セキュリティ アプライアンスと Cisco AnyConnect セキュア モビリティ クライアントの要件については、「ソフトウェア要件」のトピックを参照してください。

関連トピック

Cisco ASA シリーズ ドキュメント一覧
Cisco AnyConnect Secure Mobility Client

シングル サインオンを使用した展開

Security Assertion Markup Language（SAML）シングル サインオン（SSO）を使用したサービスを有効にすることができます。SAML SSO は、オンプレミス、クラウド、ハイブリッド展開で使用できます。

次の手順は、ユーザが Cisco Jabber クライアントを起動したあとの SAML SSO のサインイン フローを示しています。

1. ユーザが Cisco Jabber クライアントを起動します。Web フォームによるサインインをユーザに要求するようにアイデンティティ プロバイダー（IdP）を設定した場合は、クライアント内にそのフォームが表示されます。
2. Cisco Jabber クライアントが、Cisco WebEx Messenger サービス、Cisco Unified Communications Manager、Cisco Unity Connection などの接続先サービスに認証要求を送信します。
3. サービスが IdP に認証を要求するためにクライアントをリダイレクトします。
4. IdPがクレデンシャルを要求します。クレデンシャルは、次のいずれかの方法で指定できます。
   - ユーザ名とパスワードのフィールドがあるフォーム ベースの認証。
   - 統合 Windows 認証（IWA）用 Kerberos（Windows のみ）
   - スマート カード認証（Windows のみ）
   - HTTP 要求時にクライアントがユーザ名とパスワードを提示する、基本的な HTTP 認証方式。
5. IdP がブラウザまたはその他の認証方式に Cookie を提供します。IdP が SAML を使用して ID を認証すると、サービスはクライアントにトークンを提供できます。
6. クライアントが認証用のトークンを使用してサービスにログインします。

認証方式

認証メカニズムはユーザのサインオン方法に影響します。たとえば、Kerberos を使用する場合、クライアントはユーザにクレデンシャルを要求しません。ユーザがすでに認証を提示して、デスクトップへのアクセス権を取得しているからです。

ユーザ セッション

ユーザがセッションにサインインします。セッションからユーザに Cisco Jabber サービスを使用する事前定義の時間が提示されます。セッションの継続時間を制御するには、Cookie とトークンのタイムアウト パラメータを設定します。

IdP timeout パラメータを適切な時間に設定して、ユーザがログインを要求されないようにします。たとえば Jabber ユーザが外部 Wi-Fi へ切り替える場合にはローミング状態になり、そのユーザのラップトップは休止するか、ユーザがアクティブではないためにスリープ状態になります。IdP セッションがまだアクティブであれば、接続を再開した後にユーザがログインする必要はありません。

セッションの有効期限が切れて Jabber がサイレント更新できない場合、ユーザ入力が必要となるため、ユーザに再認証が要求されます。この現象は、認証 Cookie が有効でなくなった時点で発生する可能性があります。

Kerberos またはスマート カードが使用されている場合は、スマート カードから PIN が要求されなければ、再認証の操作をする必要はありません。ボイスメール、着信コール、インスタント メッセージングなどのサービスが中断するリスクはありません。

シングル サインオンの要件

SAML 2.0

Cisco Unified Communications Manager サービスを使用する Cisco Jabber クライアントに対してシングル サインオン（SSO）を有効にするには、SAML 2.0 を使用する必要があります。SAML 2.0 は SAML 1.1 と互換性がありません。SAML 2.0 標準を使用する IdP を選択する必要があります。サポートされているアイデンティティ プロバイダーは、SAML 2.0 への準拠がテスト済みなので、SSO の実装に使用できます。

サポートされるアイデンティティ プロバイダー

IdP は、Security Assertion Markup Language（SAML）に準拠している必要があります。クライアントは次のアイデンティティ プロバイダーをサポートします。

- Ping Federate 6.10.0.4
- Microsoft Active Directory Federation Services (ADFS) 2.0
- Open Access Manager (OpenAM) 10.1

（注） OpenAM で使用する Globally Persistent Cookie が設定されていることを確認します。

IdP を設定すると、その設定がクライアントへのサインイン方法に影響します。Cookie のタイプ（永続的またはセッション）や認証メカニズム（Kerberos または Web フォーム）などの一部のパラメータによって、ユーザの認証頻度が決定されます。

クッキー

ブラウザでの Cookie 共有を有効にするには、セッション Cookie ではなく、永続的な Cookie を使用する必要があります。永続的な Cookie は、ユーザに Internet Explorer を使用しているクライアントまたはその他のデスクトップ アプリケーションで 1 回クレデンシャルを入力するように要求します。セッション Cookie の場合は、ユーザがクライアントを起動するたびにクレデンシャルを入力する必要があります。IdP 上の設定として永続的な Cookie を設定します。Open Access Manager を IdP として使用している場合は、（Realm Specific Persistent Cookie ではなく）Globally Persistent Cookie を設定する必要があります。

ユーザが SSO クレデンシャルを使い Cisco Jabber for iPhone and iPad へのサインインに成功すると、クッキーはデフォルトで iOS のキーチェーンに保存されます。クッキーが iOS のキーチェーンにあれば、サインインの最中にクッキーの期限が切れない限り、ユーザは次回以降サインインのクレデンシャルを入力する必要がありません。クッキーは、以下の状況で iOS キーチェーンから自動的に削除されます。

- Cisco Jabber から手動でサインアウトしたとき
- Cisco Jabber がリセットされたとき
- iOS デバイスをリブートした後
- Cisco Jabber が手動でクローズされたとき

iOS システムがバックグラウンドで実行中の Cisco Jabber for iPhone and iPad を停止した場合は、Cisco Jabber はユーザがパスワード入力せずに自動的にサインインできるようにします。

必要なブラウザ

ブラウザとクライアント間で認証 Cookie（IdP から発行された）を共有するには、次のブラウザのいずれかをデフォルト ブラウザに指定する必要があります。

製品	必要なブラウザ
Cisco Jabber for Windows	Internet Explorer
Cisco Jabber for Mac	Safari
Cisco Jabber for iPhone and iPad	Safari
Cisco Jabber for Android	Chrome または Internet Explorer

（注） Cisco Jabber for Android で SSO を使用する場合、組み込みブラウザは外部ブラウザと Cookie を共有できません。

シングル サインオンとリモート アクセス

Expressway Mobile and Remote Access を使用して企業ファイアウォールの外側からクレデンシャルを入力するユーザの場合は、シングル サインオンに次の制限があります。

- シングル サインオン（SSO）は、Cisco Expressway 8.5 と Cisco Unified Communications Manager リリース 10.5.2 以降で使用できます。
- 使用するアイデンティティ プロバイダーは内部 URL と外部 URL を同じにする必要があります。URL が異なる場合は、ユーザが企業ファイアウォールの内側から外側にまたはその逆に移動するときに再度サインインするように要求されることがあります。