Cisco Jabber 12.8 計画ガイド

初版：2020 年 1 月 22 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/

目 次

はじめに：

新規および変更情報 xi

新規および変更情報 xi

第 1 章

要 件 1

サーバ要件 1

オペレーティング システム要件 2

Cisco Jabber for Windows のオペレーティング システム 2

Cisco Jabber for Mac のオペレーティング システム 3

Cisco Jabber for Android のオペレーティング システム 3

Cisco Jabber for iPhone and iPad のオペレーティング システム 4

ハードウェア要件 5

デスクトップ クライアントのハードウェア要件 5

CTI でサポートされるデバイス 5

iPhone および iPad 版 Cisco Jabber のハードウェア要件 6

Android 版 Cisco Jabber のハードウェア要件 7

ネットワーク要件 19

IPv6 の要件 19

Android で IPv6 をサポートするための要件 23

ポートおよびプロトコル 23

サポートされるコーデック 28

仮想環境の要件 29

音声およびビデオのパフォーマンス参照 30

メディア保証 30

高速レーン サポート 31

Cisco Jabber デスクトップ クライアントの音声ビット レート 31
Cisco Jabber モバイル クライアントの音声ビット レート 32
Cisco Jabber デスクトップ クライアントのビデオ ビット レート 32
Cisco Jabber for Android のビデオ ビット レート 33
Cisco Jabber for iPhone and iPad のビデオ ビット レート 33
プレゼンテーションのビデオ ビット レート 33
ネゴシエートされた最大ビット レート 34
帯域幅 35
Cisco Jabber デスクトップ クライアントの帯域幅パフォーマンス予測 35
Cisco Jabber for Android の帯域幅パフォーマンス予測 36
Cisco Jabber for iPhone and iPad の帯域幅パフォーマンス予測 37
ビデオ レート アダプテーション 38
帯域幅への H.264 プロファイルの影響 38
コール管理レコード 38

第 2 章 展開シナリオ 41
オンプレミス展開 41
Cisco Unified Communications Manager IM and Presence Service によるオンプレミス展開 42
コンピュータ テレフォニー インテグレーション 43
電話機モードでのオンプレミス展開 44
ソフトフォン 45
デスクフォン 45
Extend and Connect 45
電話モードの展開（連絡先を使用） 45
クラウドベース展開 46
クラウドベース導入での Cisco Webex Messenger サービス。 46
HyDeploymeCisco Webex Messenger Serviceを使ったハイブリッド クラウドベース展開 47
以下のものを使ってハイブリッド クラウドベース展開 Cisco Webex Platform サービス 48
Jabber チーム メッセージング モードにおける連絡先 49
仮想環境での展開 50
仮想環境とローミング プロファイル 51

VDI 向け Jabber ソフトフォンの展開 52
リモート アクセス 52
Expressway Mobile and Remote Access 52
Expressway for Mobile and Remote Access を使用した Jabber への初回サインイン 53
サポートされるサービス 54
Cisco AnyConnect の展開 62
シングル サインオンを使用した展開 63
シングル サインオンの要件 64
シングル サインオンとリモート アクセス 65

第 3 章 ユーザ管理 67
Jabber ID 67
IM アドレス スキーム 68
Jabber ID によるサービス ディスカバリ 69
SIP URI 69
LDAP ユーザ ID 69
フェデレーション用ユーザ ID の計画 70
ユーザの連絡先写真のプロキシ アドレス 70
認証および承認 70
Cisco Unified Communications Manager の LDAP 認証 70
Cisco Webex Messenger ログイン認証 70
シングル サインオン認証 70
Cisco Jabber for iPhone and iPad 向けの証明書ベースの認証 71
Cisco Jabber for Android の証明書ベースの認証 71
ボイスメール認証 72
OAuth 72
複数リソースのログイン 75

第 4 章 サービス ディスカバリ 77
クライアントがサービスに接続する方法 77
Cisco Webex Platform サービス ディスカバリ 78

Cisco Webex Messenger Service Discovery 78
シスコ クラスタ間検索サービス 78
Expressway for Mobile and Remote Access サービス ディスカバリ 78
推奨される接続方式 78
認証ソース 81
クライアントがサービスを検出する方法 81
方法 1：サービスの検索 83
クライアントによる利用可能なサービスの検出方法 83
クライアントが Cisco Webex Messenger Service向けの HTTP クエリを発行します。 85
クライアントからのネーム サーバのクエリー 86
クライアントの内部サービスへの接続 86
Expressway for Mobile and Remote Access を介したクライアントの接続 89
Cisco UDS SRV レコード 90
Collaboration Edge SRV レコード 92
DNS の設定 94
クライアントが DNS を使用する方法 94
ドメイン ネーム システムの設計 95
方法 2：カスタマイズ 98
サービス ディスカバリのカスタマイズ 98
Cisco Jabber for Windows のカスタム インストール 98
Cisco Jabber for Mac/iPhone and iPad/Android のカスタム インストール 99
方法 3：手動インストール 100
高可用性 100
インスタント メッセージおよびプレゼンスのハイ アベイラビリティ 100
フェールオーバー中のクライアントの動作 101
音声およびビデオのハイ アベイラビリティ 102
パーシステント チャットの高可用性 103
連絡先検索と連絡先の解決策の高可用性 103
ボイスメールの高可用性 103
設定のプライオリティ 103
[シスコ サポート フィールド（Cisco Support Field）] によるグループの設定 103

第 5 章 連絡先ソース 105

連絡先ソースとは 105

連絡先ソースサーバー 106

連絡先ソースが必要な理由 106

連絡先の送信元サーバを設定するタイミング 106

Cisco Directory Integration 向け連絡先ソースのオプション。 107

軽量ディレクトリ アクセス プロトコル 107

Cisco Directory IntegrationがLDAPと協力する方法 107

自動サービス検出: 推奨 108

LDAPサービスに対する手動設定 110

LDAP の考慮事項 110

Cisco Unified Communications Manager User Data Service 113

複数のクラスタでの連絡先の解決 114

UDS 拡張連絡先ソース 114

LDAP の前提条件 115

LDAP サービス アカウント 115

Jabber ID 属性マッピング 116

Jabber ID の検索 116

ローカル連絡先ソース 117

カスタム連絡先ソース 117

連絡先のキャッシュ 117

重複する連絡先の解決 117

ダイヤル プランのマッピング 118

Cisco Unified Communication Manager UDS for Mobile and Remote Access 118

クラウドの連絡先ソース 119

Cisco Webex 連絡先ソース 119

連絡先の写真の形式と寸法 119

連絡先の写真の形式 119

連絡先の写真の寸法 119

連絡先の写真の調整 120

第 6 章 セキュリティおよび証明書 123
暗号化（Encryption） 123
ファイル転送および画面キャプチャのコンプライアンスおよびポリシー管理 123
インスタント メッセージの暗号化 124
オンプレミス暗号化 124
クラウドベースの暗号化 125
暗号化アイコン 128
ローカルのチャット履歴 128
音声およびビデオの暗号化 129
セキュアメディア向け認証方法。 129
PIE ASLRサポート 129
連邦情報処理標準規格 129
コモン クライテリア 131
Secure LDAP 131
認証済み UDS 連絡先の検索 131
証明書 132
証明書の検証 132
オンプレミス サーバに必要な証明書 133
証明書署名要求の形式と要件 134
失効サーバ 134
証明書のサーバ識別情報 135
マルチサーバ SAN の証明書 136
クラウド展開の証明書検証 136
マルチテナントのホステッド コラボレーション ソリューション向けの SNI サポート。 136

第 7 章 構成管理 139
高速サインイン 139

第 8 章 画面共有 143
画面共有 143

Cisco Webex 画面共有 143
BFCP の画面共有 144
IM 専用画面の共有 144
会議や共有へのエスカレーション 144

第 9 章 フェデレーション 145
ドメイン間フェデレーション 145
ドメイン内フェデレーション 146

第 章 Jabber がサポートされている言語 147

付録 A： サポートされる言語 149

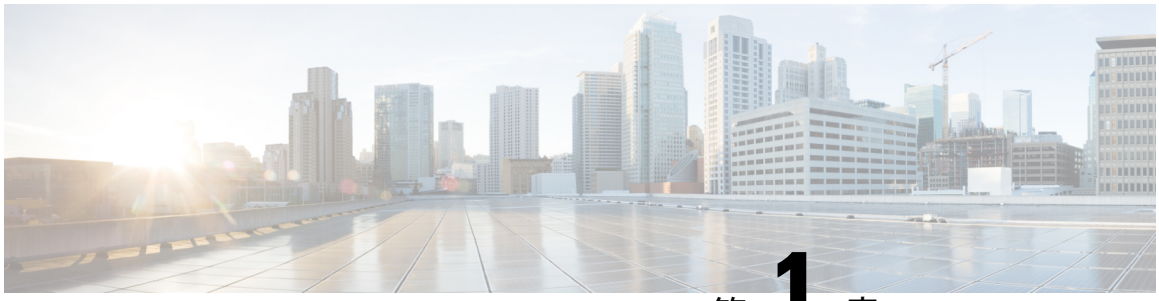
新規および変更情報

- 新規および変更情報 （xi ページ）

新規および変更情報

日付	ステータス	説明	場所（Location）
2020 年 1 月		ドキュメントの初公開	
	更新されました	要件の更新	要件
	新規	264 高プロファイルサポート上に追加された情報。	帯域幅への *H.264* プロファイルの影響
	更新されました	IM のみの画面共有に関する追加情報。	*BFCP* スクリーン共有*IM* のみスクリーン共有
	削除済み	サポートされているバージョンが EOL であるため、Survivable リモートサイトテレフォニーのサポートが削除されました。	サービス検出

新規および変更情報



第 1 章

要 件

- サーバ要件 （1 ページ）
- オペレーティング システム要件 （2 ページ）
- ハードウェア要件 （5 ページ）
- ネットワーク要件 （19 ページ）
- 仮想環境の要件 （29 ページ）
- 音声およびビデオのパフォーマンス参照 （30 ページ）

サーバ要件

次のソフトウェア要件は、このリリースのすべての Cisco Jabber クライアントに共通です。

サービス	ソフトウェア要件	サポートされるバージョン
IM と Presence	Cisco Unified Communications Manager IM and Presence Service	10.5 (2) 以降 (最小) 11.5 (1) SU2 以降 (推奨)
	Cisco Webex Messenger	
テレフォニー	Cisco Unified Communications Manager	10.5 (2) 以降 (最小) 11.5 (1) SU3 以降 (推奨)
連絡先の検索	LDAP ディレクトリ	Microsoft Active Directory 2008 R2 および Open LDAP 2.4 以降などの LDAP v3 準拠ディレクトリ
ボイスメール	Cisco Unity Connection	10.5 以降
マルチライン	Cisco Unified Contact Center Express	11.6

サービス	ソフトウェア要件	サポートされるバージョン
会議機能	Cisco Meeting Server	2.2 以降
	Cisco TelePresence Server	3.1 以降
	Cisco TelePresence MCU	4.3 以降
	Cisco ISR PVDM3	Cisco Unified Communications Manager 9.x 以降
	クラウド CMR	Cisco Webex Meetings Collaboration Meeting Room を伴うサーバ
	Cisco Webex Meetings サーバ	2.8 MR1 以降
	Cisco Webex Meetings 中央	WBS33 以降
リモート アクセス	Cisco Adaptive Security Appliance Cisco Jabber for Android にのみ適用。	8.4(1) 以降
	Cisco AnyConnect Secure Mobility Client Cisco Jabber for Android および Cisco Jabber for iPhone and iPad のクライアントのみ。	プラットフォームに依存
	Cisco Expressway C	X 8.10.1 以降
	Cisco Expressway E	X 8.10.1 以降。

Cisco Jabber では、起動時にドメイン ネーム システム（DNS）サーバを使用します。DNS サーバは Cisco Jabber の設定に必須です。

オペレーティング システム要件

Cisco Jabber for Windows のオペレーティング システム

次のオペレーティング システム上に Windows 版 Cisco Jabber をインストールできます。

- Microsoft Windows 10 （デスクトップ モード）
- Microsoft Windows 8.1 （デスクトップ モード）
- Microsoft Windows 8 （デスクトップ モード）

Windows 版 Cisco Jabber は、Microsoft .NET Framework または Java モジュールを必要としません。

Windows 10 のサービス オプション

Cisco Jabber for Windows は、Windows 10 の次のサービス オプションをサポートします。

- Current Branch（CB）
- Current Branch for Business（CBB）
- Long-Term Servicing Branch（LTSB）：このオプションでは、関連するサービスのアップデートが展開されていることを確認します。

Windows 10 のサービス オプションの詳細については、Microsoft の次のマニュアルを参照してください。https://technet.microsoft.com/en-us/library/mt598226(v=vs.85).aspx

（注） デフォルトで、Cisco Jabber は次のディレクトリに必要なファイルをインストールします。

- %temp%\Cisco Systems\Cisco Jabber-Bootstrap.properties ファイルおよび installation log
- %LOCALAPPDATA%\Cisco\Unified Communications-Logs およびテレメトリ一時データ
- %APPDATA%\Cisco\Unified Communications-Cached 設定およびアカウント クレデンシャル
- x86 Windows 用の %ProgramFiles%\Cisco Systems\Cisco Jabber-Installation ファイル
- x64 Windows 用の %ProgramFiles(x86)%\Cisco Systems\Cisco Jabber-Installation ファイル

Cisco Jabber for Mac のオペレーティング システム

Mac 版 Cisco Jabber は、次のオペレーティング システムへインストール可能です。

- macOS Catalina 10.15 以降
- macOS Mojave 10.14 以降
- macOS High Sierra 10.13 (またはそれ以降)
- macOS Sierra 10.12 (またはそれ以降)

Cisco Jabber for Android のオペレーティング システム

サポートされている最新のオペレーティングシステムバージョン情報については、Play Store を参照してください。

（注） Android 版 Cisco Jabber は、32 ビットアプリと 64 ビットアプリケーションとして使用できます。Android デバイスに 64 ビット OS が搭載されている場合は、64 ビット Jabber クライアントを実行することで、より高速で豊富な操作性が得られます。

32 ビット OS に 64 ビット アプリケーションをインストールすることはできません。ほとんどの 64 ビット プラットフォームで 32 ビット アプリケーションを使用すると、64 ビット アプリケーションにアップグレードするための通知が表示されます。

（注） Cisco Jabber が Android 6.0 Marshmallow OS 以降にインストールされており、アイドルが続いている場合：

- Cisco Jabber のネットワーク接続が無効になっています。
- ユーザは、コールまたはメッセージを受信しません。

[設定の変更（Change Settings）] をタップしてバッテリの最適化を無視し、コールおよびメッセージを受信するようにします。

Android 5. x サポート用の前回の Jabber リリース

Cisco Jabber 12.8 は、Android 5. x を実行しているデバイスをサポートする前回のリリースです。

次の Jabber リリースは Android 6. x にアップグレードできないすべてのデバイスのサポートを終了します。

Cisco Jabber for iPhone and iPad のオペレーティング システム

サポートされている最新のオペレーティングシステムバージョン情報については、App Store を参照してください。

重要 Cisco は、 iPhone および iPad 版 Cisco Jabber の現在の App Store バージョンのみサポートします。すべての Cisco Jabber for iPhone and iPad リリースで発生した障害は、現在のバージョンに対して評価されます。

ハードウェア要件

デスクトップ クライアントのハードウェア要件

要件	**Windows 版 Cisco Jabber**	**Mac 版 Cisco Jabber**
搭載されている RAM	Microsoft Windows 7 および Windows 8 上の 2 GB RAM	2 GB RAM
物理メモリの空き容量	128 MB	1 GB
ディスクの空き容量	256 MB	300 MB
CPU の速度およびタイプ	AMD モバイル Sempron プロセッサ 3600+（2 GHz） Intel Core 2 Duo プロセッサ T7400 @ 2 （16 GHz）	Intel Core 2 Duo もしくはそれ以降の次のいずれの Apple ハードウェアのプロセッサ • iMac Pro • MacBook Pro（Retina Display モデルを含む） • MacBook • MacBook Air • iMac • Mac Mini
I/O ポート	USB 2.0（USB カメラおよび音声デバイス用）	USB 2.0（USB カメラおよび音声デバイス用）

CTI でサポートされるデバイス

ユニファイド コミュニケーション マネージャで、コンピュータ テレフォニー インテグレーション (CTI) でサポートされているデバイスのリストを表示するには、次のようにします。

1. **シスコのユニファイド レポーティング**ページから、[**システム レポート (System Reports)**] メニューから [**ユニファイド CM 電話機能リスト (ユニファイ CM Phone Feature List)**] を選択します。
2. レポートを開いた後、**[機能]** ドロップダウンリストから**[CTI制御(CTI controlled)]**を選択します。

iPhone および iPad 版 Cisco Jabber のハードウェア要件

iOS 12.X、iOS 13.X および iPadOS以降の Cisco Jabber for iPhone and iPad でサポートされる Apple デバイスは次のとおりです。これらのバージョンにアップグレードされないデバイスはサポートされていません。

Apple デバイス	バージョン
iPad	第 5 世代、第 6 世代および第 7 世代
iPad Air	Air 1、Air 2 および Air 3
iPad Pro	9.7 および 10.5 インチ 12.9 インチ、第 1、第 2 および第 3 世代
iPad mini	Mini 2、 mini 3、mini 4 および mini 5
iPhone	5s, 6, 6 Plus, 6s, 6s Plus, 7, 7 Plus , 8, 8 Plus, X, Xs, Xs Max,11, 11 Pro, 11 Pro Max, XR および SE
iPod Touch	第 6 世代
Apple Watch	Apple Watch および Apple Watch 2、3、 4 で動作している WatchOS 5。

iPhone および iPadでは、次の Bluetooth ヘッドセットがサポートされます。

メーカー	モデル
Apple 社	AirPod
Cisco	561、562
Jabra	BIZTALK 2400、Easygo、Evolve65 UC ステレオ、EXTREME 2 および Motion[1]、PRO 9470、Cisco 用の Speak 450 、Speak 510、Stealth Supreme UC、Wave +
Jawbone	ICON（ Cisco Bluetooth ヘッドセット用）
Plantronics	Voyager Edge、Voyager Edge UC、Voyager Legend、Voyager Legend UC
Sony Eriksson	MW-600

[1] は、 Cisco Jabber コールの Bluetooth 制御に対応しています。この機能はファームウェアバージョン 3.72 でのみサポートされます。

Android 版 Cisco Jabber のハードウェア要件

Android デバイスの最小要件

Android オペレーティング システム	CPU	ディスプレー
5.0 以降	1.5 GHz デュアルコア 推奨: 1.2 GHz の quad core 以上	双方向ビデオ: 480p x 800p 以上。 IM のみ: 320p x 480p 以上。

Cisco Jabber for Android では、次に示す OS バージョンのデバイスで完全な UC モードがサポートされています。

表 *1* : サポートされる *Android* デバイス

デバイス	モデル	Android OS の最小バージョン	注
BlackBerry	Priv	5.1	Jabber を最近表示したアプリケーション リストから削除して、デバイスをしばらくアイドル状態にすると、Jabber は非アクティブになります。
Fujitsu	Arrows M357	6.0.1	

デバイス	モデル	Android OS の最小バージョン	注
Google	Nexus 4	5.1.1	
	Nexus 5	5.0	
	Nexus 5X	6.0	
	Nexus 6	5.0.2	
	Nexus 6P	6.0	Android OS バージョン 6.x または 7.0 を搭載した Google Nexus 6P デバイスを所有している場合、管理者は、Jabber 電話サービスをセキュア電話サービスとして設定する必要があります。設定しないと、デバイスが応答しない可能性があります。 Android OS のバージョンが 7.1 以降の場合は、アクションは不要です。
	Nexus 7	5.0	
	Nexus 9	5.0.2	
	Nexus 10	5.0	
	Pixel	7.0	
	ピクセル C	6.0	
	Pixel XL	7.0	
	ピクセル 2	8.0	Jabber 通話中に、ユーザが音声をモバイル デバイスからヘッドセットに切り替えると、一時的に音声に問題が生じる場合があります。
	Pixel 2 XL	8.0	Jabber 通話中に、ユーザが音声をモバイル デバイスからヘッドセットに切り替えると、一時的に音声に問題が生じる場合があります。
	ピクセル 3	8.0	電話機に接続されたヘッドセットを使用する場合、音声にいくつかの問題が発生することがあります。
	Pixel 3 XL	8.0	電話機に接続されたヘッドセットを使用する場合、音声にいくつかの問題が発生することがあります。

デバイス	モデル	Android OS の最小バージョン	注
Honeywell Dolphin	CT50	5.0	
	CT40	7.1.1	
	CT60	7.1.1 および 8.1	Android OS 7.1.1 および 8.1 を含む CT60 のみがサポートされています。
HTC	10	6.0	
	A9	6.0	
	E9 PLUS	5.0.2	
	M7	5.0	
	M8	5.0	
	M9	5.0	
	One Max	5.0	
	X9	6.0	

デバイス	モデル	Android OS の最小バージョン	注
Huawei [2]	Honor 7	5.0	
	M2	5.0	
	Mate 7	5.0	
	Mate 8	6.0	
	Mate 9	6.0	
	Nova	7.0	
	Mate 10	8.0	
	Mate 10 Pro	8.0	
	P8	5.0	
	P9	6.0	
	P10	7.0	
	P10 Plus	7.0	
	P20	8.0	
	P20 Pro	8.0	
	Mate20	8.0	
	Mate20 Pro	8.0	
	P30	9.0	
	P30 Pro	9.0	
LG	G2	5.0	
	G3	5.0	
	G4	5.1	
	G5	6.0	
	G6	7.0	
	V10	5.0	
	V30	8.0	

デバイス	モデル	Android OS の最小バージョン	注
Motorola	MC40	5.0	Cisco Jabber は、MC40 デバイスの音声モードのみサポートします。Cisco Jabber は、MC40 デバイスからの Webex Meeting の起動をサポートしません。
	Moto G4	5.0	
	Moto G5	7.0	
	Moto G6	8.0	
	Moto X (第1世代)	5.0	
	Moto Z Droid	6.0	
Nokia	6.1	8.0	
OnePlus	1 つ	5.0	
	5	8.0	
	5T	8.0	
	6	9.0	
	6T	9.0	
パナソニック	Toughpad FZ-X1	5.0	Jabber 電話サービスをセキュア電話サービスとして設定するように管理者に連絡する必要があります。Jabber は、ringback トーンと 24 Khz の通話中トーンを再生します。

デバイス	モデル	Android OS の最小バージョン	注
Samsung	すべて（All）	5.0	• Android OS 5.x 以降を搭載した Samsung デバイスの場合、Jabber の auto-run オプションを有効化します。 Android OS 5.x の場合、auto-run オプションは **[設定（Settings）]** と **[デバイス マネージャ（Device Manager）]** の下にあります。 Android OS 6.x 以降の場合、auto-run オプションは **[アプリケーション スマート マネージャ（App Smart Manager）]** の下にあります。 • カナダ向けの Samsung Galaxy Tab Pro 8.4（モデル T320UEU1AOC1）では、Jabber の着信コール通知のポップアップ表示が遅れます。 • Samsung Xcover 3 では、Wi-Fi 接続を失った場合に、Jabber のネットワークへの再接続が遅れます。
Smartisan	M1L	6.0.1	
Sonim	XP8	7.1.1	

デバイス	モデル	Android OS の最小バージョン	注
Sony Xperia	M2	5.0	
	XZ	7.0	
	XZ1	8.0	
	XZ2	8.0	
	XZ3	9.0	
	Z1	5.0	
	Z2	5.0	
	Z2 tablet	5.0	
	Z3	5.0	Android OS 5.0.2 を搭載した Sony Xperia Z3（モデル SO-01G）の Jabber コールの音声品質は低いです。
	Z3 Tablet Compact	5.0	
	Z3+/Z4	5.0.2	Sony Z3 +/Z4 でビデオコールが不安定になっています。ビデオコールのビデオを無効にしてみてください。それ以外の場合は、音声コールのみを作成します。
	Z4 TAB	5.0	
	Z5 Premium と Z5	5.0.2	
	ZR/A	5.0	Android OS 6.0 の Sony デバイスは Jabber で Voice Mail を再生できないという制限があります。

デバイス	モデル	Android OS の最小バージョン	注
Xiaomi	4C	5.1	これらのデバイスでは、32 ビットのバージョンのみが実行されます。
	MAX	5.1	
	Mi 4	5.0	
	Mi 5	6.0	
	Mi 5s	7.0	
	Mi 6	7.0	
	Mi 8	8.0	
	Mi 9	9.0	
	Poco電話	8.0	
	Mi Note	5.0	これらのデバイスでは、32 ビットのバージョンのみが実行されます。
	Mi Note 2	7.0	
	Mi Pad 2	5.1	
	Mi MIX 2	8.0	
	Mi A1	8.0	
	Redmi 3	5.1	
	Redmi Note 3	5.1	
	Redmi Note 4X	6.0.1	
	Redmi Note 5	8.0	
	Redmi Note 6 Pro	8.1	

デバイス	モデル	Android OS の最小バージョン	注
Zebra	TC70	5.0	TC70 デバイスには、DHCP で構成されている Wi-Fi ネットワークへの接続の問題が発生することがあります。 TC70 では、[スリープ中も Wi-Fi をオンのままにする（Keep wifi on during sleep）] が [オフ（Off）] に設定されているため、Jabber を使用するためには、[常にオン（Always On）] に設定する必要があります。
	TC75X	6.0	
	TC51	6.0	

[2] EMUI 10 が変更されたため、デバイスがロックされていると、着信コール toasts が表示されない場合があります。Jabber では、**設定** > **通知**に移動して**バナー**を選択します。

Samsung Knox 向け Jabber のサポート

Android 版 Cisco Jabber は次のデバイスで Samsung Knox をサポートしています。

Knox バージョン	Samsung デバイス
2.6	Note 4 Note 5 Note Edge S5 S6 S6 Edge S6 Edge Plus S7 S7 Edge Note 10.1（2014 年版）
2.7.1	Galaxy Note5
3.1	Galaxy A5 (2017)
3.2	Galaxy On5 (2016)
3.3	Galaxy S10

Jabber は Samsung Dex をサポートしている

Android 版 Cisco Jabber は、Samsung S8、S8 Plus および Note 8 で Samsung Dex をサポートしています。

Cisco Jabber の以前の Android バージョンのサポート ポリシー

Android カーネルの問題により、一部の Android デバイスでは Cisco Jabber を Cisco Unified Communications Manager に登録できません。この問題を解決するには、次の手順を試してください。

Android のカーネルを 3.10 以降のバージョンにアップグレードします。

Cisco Unified Communications Manager の設定で、混合モードのセキュリティの使用、セキュア SIP コール シグナリングの有効化、ポート 5061 の使用を設定します。ご使用のリリースで Cisco CTL クライアントを利用して混合モードを設定する方法については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。セキュリティ ガイドは、Cisco Unified Communications Manager の『Maintain and Operate Guides』に記載されています。このソリューションは、次のサポート対象デバイスに適用できます。

デバイス モデル	オペレーティング システム
HTC M7	Android OS 5.0 以降
HTC M8	Android OS 5.0 以降
HTC M9	Android OS 5.0 以降
HTC One Max	Android OS 5.0 以降
Sony Xperia M2	Android OS 5.0 以降と 3.10.49 より前のカーネル バージョン Sony 製デバイスの Android OS が 5.0.2 以降であり、カーネル バージョンが 3.10.49 以降であれば、非セキュア モードをサポートできます。
Sony Xperia Z1	
Sony Xperia ZR/A	
Sony Xperia Z2	
Sony Xperia Z2 Tablet	
Sony Xperia Z3	
Sony Xperia Z3 Tablet Compact	
Xiaomi Mi4	Android OS 5.0 以降
Xiaomi Mi Note	Android OS 5.0 以降
Xiaomi Mi Pad	Android OS 5.0 以降
Sonim XP7	Android OS 5.0 以降
Honeywell Dolphin CT50	Android OS 5.0 以降

サポートされる Bluetooth デバイス

Bluetooth デバイス	依存関係
Cisco 561	
Cisco 562	
Plantronics Voyager Legend	
Plantronics Voyager Legend UC	
Plantronics Voyager Edge UC	
Plantronics Voyager Edge	
Plantronics PLT Focus	
Plantronics BackBeat 903+	Samsung Galaxy S4 を使用している場合は、これらのデバイス間の互換性に起因する問題が発生する可能性があります。
Jabra Motion	Jabra Motion Bluetooth ヘッドセットをファームウェア バージョン 3.72 以降にアップグレードします。 Jabra Motion Bluetooth ヘッドセット ファームウェア バージョン 3.72 以降は、 Cisco Jabber のコール制御をサポートします。
Jabra Wave+	
Jabra BIZ 2400	
Jabra Easygo	
Jabra PRO 9470	
Jabra Speak 510	
Jabra Supreme UC	
Jabra Stealth	
Jabra Evolve 65 UC Stereo	
Jawbone ICON（ Cisco Bluetooth ヘッドセット用）	Samsung Galaxy S4 を使用している場合は、これらのデバイス間の互換性に起因する問題が発生する可能性があります。

Bluetooth の制限：

- Samsung Galaxy SIII で Bluetooth デバイスを使用すると、呼出音と通話の音声にヒズミが生じる可能性があります。

- Jabber 通話中に Bluetooth ヘッドセットの接続を切り、再接続すると、音声が聞こえなくなります。Android 5.0 より前の OS を搭載した Android スマートフォンにこの制限が適用されます。
- Sony Z4/LG G4 のオペレーティングシステム Android 6.0 では、Jabber のコール開始後に Bluetooth ヘッドセットに切り替えたときに、音声ロスが発生する可能性があります。この問題の回避策としては、オーディオ出力を一旦スピーカーにし、その後 Bluetooth に切り替えることです。または Cisco Jabber 通話を発信する前に Bluetooth ヘッドセットに接続します。

サポートされる Android Wear

Cisco Jabber は、Android OS 5.0 以降および Google Play Service 8.3 以降が搭載されているすべての Android Wear デバイスで起動します。Cisco Jabber は、次の Android Wear デバイスでテストされています。

- Fossil Gen 3 SmartWatch
- Huawei watch
- LG G Watch R
- LG Watch Urbane
- Moto 360
- Moto 360（第 2 世代）
- Samsung Gear Live
- Sony SmartWatch 3

（注） Android 劣化デバイス用 Cisco Jabber インストーラーは、メインの Jabber APK ファイルから分離されています。ユーザは、Google Play ストアから Android 劣化インストーラーを取得します。これらは、モバイルデバイスと磨耗デバイスをペアリングしたときに使用されます。

サポートされている Chromebook モデル

Chromebook に Chrome OS v53 以降が搭載されている必要があります。Android 版 Cisco Jabber は、Google Play ストアからダウンロードすることができます。

- HP Chromebook 13 G1 ノートブック PC
- Google Chromebook Pixel
- Google Chromebook Pixelbook
- Samsung Chromebook Pro
- Asus C302

ネットワーク要件

社内の Wi-Fi ネットワークを介して Cisco Jabber を使用する場合は、次の作業を行うことを推奨します。

- エレベータ、階段、屋外廊下などのエリアを含め、カバレッジのギャップを可能な限り排除するように、Wi-Fi ネットワークを設計します。
- すべてのアクセス ポイントで、モバイル デバイスに同じ IP アドレスが割り当てられることを確認します。コール中に IP アドレスが変更されると、コールが切断されます。
- すべてのアクセス ポイントの Service Set Identifier（SSID）が同一であることを確認します。SSID が一致しない場合、ハンドオフに時間がかかる場合があります。
- すべてのアクセス ポイントで、SSID がブロードキャストされていることを確認します。アクセス ポイントで SSID がブロードキャストされていないと、モバイル デバイスはコールを中断して別の Wi-Fi ネットワークに参加することをユーザに求める場合があります。
- NAT (STUN) パケットに対するセッショントラバーサルユーティリティの通過を許可するように、エンタープライズファイアウォールを設定します。

サイト全体を調査し、音声品質に影響を与えるネットワークの問題を可能な限り解消してください。次のことをお勧めします。

- 重複しないチャネルの設定、アクセス ポイントのカバレッジ、および必要なデータ レートとトラフィック レートを確認します。
- 不正なアクセス ポイントは排除します。
- 考えられる干渉源の影響を特定して軽減します。

詳細については、次の資料を参照してください。

- 『Enterprise Mobility Design「 」Guide』の「*VoWLAN Design Recommendations*」の項。
- 『*Cisco Unified Wireless IP Phone 7925G Deployment Guide*』
- 『*Capacity Coverage & Deployment Considerations for IEEE 802.11g*』ホワイト ペーパー。
- ご使用のリリースの Cisco Unified Communications Manager の『*Solutions Reference Network Design (SRND)*』

IPv6 の要件

Cisco Jabber は IPv6 に完全に対応しており、この項に記載されている制限付きですが、ピュア IPv6 とハイブリッド ネットワークにおいて正常に機能します。シスコ コラボレーション ソリューションでは、現在、IPv6 を完全にはサポートしていません。たとえば Cisco VCS Expressway for Mobile and Remote Access にはピュア IPv6 ネットワークで制限があり、NAT64/DNS64 をモバイル キャリア ネットワークに展開する必要があります。Cisco Unified

Communications Manager と Cisco Unified Communications Manager IM and Presence は、現在ピュア IPv6 ネットワークで HTTPS をサポートしていません。

この機能は、プロトコルを IPv4、IPv6、またはデュアル スタックへ設定する IP_Mode パラメータを使用して Jabber で設定されます。デフォルトの設定はデュアル スタックです。IP_Modeパラメータは Jabber クライアントの設定 (Cisco Jabber のパラメータリファレンスガイドの最新バージョンを参照)、Windows のブートストラップ、および Mac クライアントとモバイルクライアントの URL 設定に含めることができます。

サービスに接続するときに Jabber で使用されるネットワーク IP プロトコルは次の要因によって決定されます。

- Jabber クライアント設定の IP_Mode パラメータ。
- クライアントのオペレーティング システムの IP 機能。
- サーバのオペレーティング システムの IP 機能。
- IPv4 および IPv6 の DNS レコードの応答可能性。
- IPv4、IPv6、または両方のソフトフォン デバイス設定に対する Cisco Unified Communications Manager の SIP 設定。正常に接続するには、ソフトフォン デバイスの SIP 接続の設定を、Jabber の IP_Mode パラメータと同じにする必要があります。
- 基盤となる IP ネットワークの機能。

Cisco Unified Communications Manager では、IP 機能は一般的なサーバの設定とデバイス固有の設定によって決定されます。次の表は、さまざまな設定において考えられる Jabber 接続を示しています。ここでは、IPv4 と IPv6 の DNS レコードが両方とも設定されていることを前提にしています。

クライアント OS、サーバ OS、および Jabber IP_Mode パラメータが 2 つのスタックに設定されている場合、Jabber は RFC6555 に従ってサーバに接続するために IPv4 または IPv6 アドレスのいずれかを使用します。

クライアント OS	サーバ OS	Jabber IP_Mode パラメータ	Jabber 接続の結果
IPv4 のみ	IPv4 のみ	IPv4 のみ	IPv4 接続
		IPv6 のみ	接続失敗
		2 つのスタック	IPv4 接続
IPv4 のみ	IPv6 のみ	IPv4 のみ	接続失敗
		IPv6 のみ	接続失敗
		2 つのスタック	接続失敗

クライアント OS	サーバ OS	Jabber IP_Mode パラメータ	Jabber 接続の結果
IPv6 のみ	IPv4 のみ	IPv4 のみ	接続失敗
		IPv6 のみ	接続失敗
		2 つのスタック	接続失敗
IPv6 のみ	IPv6 のみ	IPv4 のみ	接続失敗
		IPv6 のみ	IPv6 接続
		2 つのスタック	IPv6 接続
IPv4 のみ	2 つのスタック	IPv4 のみ	IPv4 接続
		IPv6 のみ	接続失敗
		2 つのスタック	IPv4 接続
IPv6 のみ	2 つのスタック	IPv4 のみ	接続失敗
		IPv6 のみ	IPv6 接続
		2 つのスタック	IPv6 接続
2 つのスタック	IPv4 のみ	IPv4 のみ	IPv4 接続
		IPv6 のみ	接続失敗
		2 つのスタック	IPv4 接続
2 つのスタック	IPv6 のみ	IPv4 のみ	接続失敗
		IPv6 のみ	IPv6 接続
		2 つのスタック	IPv6 接続
2 つのスタック	2 つのスタック	IPv4 のみ	IPv4 接続
		IPv6 のみ	IPv6 接続
		2 つのスタック	IPv6 接続

IPv6 のみのモードで Jabber を使用する場合は、Cisco Webex Messengerサービス、Cisco VCS 08sway for Mobile および Remote Access Cisco Webex Platform サービスに接続するために、NAT64/DNS64 が必要です。

デスクトップのデバイス サポートは、IPv6-only のオンプレミス展開で利用可能です。Jabber モバイル デバイスは、すべて 2 つのスタックとして構成しなければなりません。

IPv6 の展開の詳細については、シスコ コラボレーション システム リリース 12.0 の IPv6 展開ガイドを参照してください。

制限事項

- HTTPS 接続
  - オンプレミス展開では、Cisco Jabber は Cisco Unified Communications Manager および Cisco Unified Communications Manager IM and Presence サービスに接続するために、IPv4 専用モードと 2 つのスタック モードをサポートしています。これらのサーバは現在、IPv6 HTTPS 接続をサポートしていません。

    Cisco Jabber は、IPv6 モードを使用しているボイスメール用の Cisco Unity Connection に対して HTTPS を使用して接続します。

- Cisco Webex Messenger 制限事項
  - Cisco Webex Messenger は IPv6 ではサポートされていません。

- テレフォニーの制限事項
  - Cisco Unified Communications Manager でユーザ デバイスを 2 つのスタックまたは IPv6 専用へアップグレードする場合、対応する Jabber クライアントは 11.6 以降にアップグレードする必要があります。
  - インストールに IPv4 エンドポイントと IPv6 エンドポイントが含まれている場合は、ハードウェア MTP を使用してこれらのデバイス間の音声とビデオにブリッジすることが推奨されます。これは Cisco IOS バージョン 15.5 のハードウェア MTP でサポートされます。たとえば、Cisco 3945 ルータは次の T-train ビルドを実行する必要があります。build: c3900e-universalk9-mz.SPA.155-2.T2.bin。
  - 現在、Jabber が含まれている Cisco エンドポイントで、IPv4 と IPv6 を同時にサポートするソリューション ロードマップはありません。Cisco Unified Communications Manager は、現在の機能（IPv4-Only と IPv6-Only）をサポートしています。IPv4-only エンドポイントと IPv6-only エンドポイント間、または IPv4-only ゲートウェイ、または IPv6-only ゲートウェイ間のコールをサポートするには、MTP が必要です。
  - Jabber 間のコールは IPv6 ではサポートされません。

- ファイル転送の制限事項
  - 高度なファイル転送：クライアントが 2 つのスタックに対して設定されており、Cisco Unified Communications Manager IM and Presence サービスで 2 つのスタックが有効になっている場合、Cisco Unified Communications Manager IM and Presence サービスの次のバージョンで、高度なファイル転送がサポートされます。
    - 10.5.2 SU2
    - 11.0.1 SU2
    - 11.5

- Person to Person ファイル転送：オンプレミス展開では、IPv4 クライアントと IPv6 クライアント間の person to person ファイル転送はサポートされません。IPv4 クライアントと IPv6 クライアントの両方が設定されているネットワークの場合は、高度なファイル転送を設定することが推奨されます。

- Mobile and Remote Access に関する制限事項
  - Cisco VCS Expressway for Mobile and Remote Access は IPv6 をサポートしません。
  - Cisco Unified Communications Manager が IPv6 SIP 接続に対して設定されている場合は、テレフォニー サービスを使用するために、Cisco VCS Expressway for Mobile and Remote Access を使用して Cisco Unified Communications Manager に接続することはできません。

Android で IPv6 をサポートするための要件

Android OS の要件

Android 5.0 以降

ネットワークの要件

- IPv4 専用モード（Android は IPv4 アドレスのみ承認）
- SLAAC でのデュアルスタック（Android は IPv4 および IPv6 アドレスを承認）
- NAT64 または DNS64（サーバは IPv4 アドレスを使用し、クライアントは IPv6 アドレスを使用）

制限事項

- DHCPv6 の制限事項
  - DHCPv6 は Android デバイスでサポートされません。

- Android OS の制限事項
  - Android OS は IPv6 専用ネットワークをサポートしません。この制限事項の詳細については、「Android developer link」を参照してください。

ポートおよびプロトコル

クライアントは、次の表に示すポートおよびプロトコルを使用します。クライアントとサーバ間にファイアウォールを展開する場合、次のポートおよびプロトコルを許可するようにファイアウォールを設定します。

	ポート	アプリケーション層プロトコル	トランスポート層プロトコル	説明
Configuration				
	6970	HTTP	[TCP]	TFTP サーバに接続し、クライアント設定ファイルをダウンロードします。
	6972	HTTPS	[TCP]	TFTP サーバに接続し、Cisco Unified Communications Manager リリース 11.0 以降用のクライアント コンフィギュレーション ファイルを安全にダウンロードします。
	53	DNS	UDP	ホスト名の解決。
	3804	CAPF	TCP	ローカルで有効な証明書（LSC）を IP フォンに発行する。このポートは、Cisco Unified Communications Manager Certificate Authority Proxy Function（CAPF）登録用のリスニング ポートです。
	8443	HTTPS		Cisco Unified Communications Manager と Cisco Unified Communications Manager IM and Presence Service へのトラフィック。
	8191	SOAP	TCP	Simple Object Access Protocol（SOAP）Web サービスを提供するためにローカル ポートに接続する。
Directory Integration：LDAP の連絡先を解決するため、次のポートのうちのいずれかが LDAP 設定を基に使用されています。				
	389	LDAP	TCP	LDAP TCP（UDP）は LDAP ディレクトリ サービスに接続する。
	3268	LDAP	TCP	連絡先を検索するためにグローバル カタログ サーバに接続する。
	636	LDAPS	TCP	LDAP ディレクトリ サービスにセキュアに LDAPS TCP 接続する。
	3269	LDAPS	TCP	グローバル カタログ サーバにセキュアに LDAPS TCP 接続する。
インスタント メッセージおよびプレゼンス				

	ポート	アプリケーション層プロトコル	トランスポート層プロトコル	説明
	443	XMPP	TCP	Webex メッセンジャー サービスへの XMPP トラフィック。クラウドベース導入のみで、クライアントはこのポートを介して XMPP トラフィックを送信します。ポート 443 がブロックされた場合、クライアントはポート 5222 にフォールバックします。
	5222	XMPP	TCP	インスタント メッセージングとプレゼンス用の Cisco Unified Communications Manager IM and Presence Service に接続します。
	37200	SOCKS5 バイトストリーム	TCP	ピアツーピアのファイル転送、オンプレミスでの展開では、クライアントはまた、画面キャプチャを送信するためにこのポートを使用します。
	7336	HTTPS	[TCP]	MFT ファイル転送（オンプレミスのみ）。
Communication Manager Signaling				
	2748	CTI	TCP	デスク フォンの制御に使用されるコンピュータ テレフォニー インターフェイス（CTI）。
	5060	SIP	TCP	Session Initiation Protocol（SIP）コール シグナリングを提供する。
	5061	SIP オーバー TLS	TCP	SIP over TCP がセキュアな SIP コール シグナリングを提供する。（セキュアな SIP がデバイスで有効な場合のみ使用）
	30000 ～ 39999	FECC	UDP	遠端カメラ制御（FECC）。
	5070 ～ 6070	BFCP	UDP	ビデオ画面共有機能の Binary Floor Control Protocol（BFCP）
音声またはビデオ メディアの変換（Voice or Video Media Exchange）				

	ポート	アプリケーション層プロトコル	トランスポート層プロトコル	説明
	16384 ～ 32766	RTP/SRTP	UDP	音声、ビデオ、BFCP ビデオ デスクトップ共有で使用される Cisco Unified Communications Manager メディアポートの範囲。
	33434 ～ 33598	RTP/SRTP	UDP	音声、ビデオで使用される Cisco ハイブリッド サービス (Jabber 間通話) メディアポートの範囲。
	49152 ～ 65535	RDP	TCP	IM 専用デスクトップ共有Cisco Jabber for Windows にのみ適用されます。
	8000	RTP/SRTP	TCP	Jabber Desk Phone Video Interfaceにより使われており、ユーザがクライアントを介してコンピュータ上のデスクフォンデバイスに転送されたビデオを受信できるようにします。
Unity Connection				
	7080	HTTP	[TCP]	Cisco Unity Connection でボイス メッセージ通知（新しいメッセージ、メッセージの更新、メッセージの削除）を受信するために使用されます。
	7443	HTTPS	[TCP]	Cisco Unity Connection でボイス メッセージ通知（新しいメッセージ、メッセージの更新、メッセージの削除）を安全に受信するために使用されます。
	443	HTTPS	[TCP]	ボイスメール用の Cisco Unity Connection に接続する。
Cisco Webex Meetings				
	80	HTTP	[TCP]	会議用の Cisco Webex Meetings センターに接続する。
	443	HTTPS	[TCP]	会議用の Cisco Webex Meetings センターに接続する。
	8443	HTTPS	[TCP]	Cisco Unified Communications Manager への Web アクセスで、次への接続が含まれます。 • 割り当てられたデバイス用の Cisco Unified Communications Manager IP Phone（CCMCIP）サーバ。 • 連絡先の解決のためのユーザ データ サービス（UDS）。

	ポート	アプリケーション層プロトコル	トランスポート層プロトコル	説明
アクセサリ マネージャ				
	8001		TCP	Cisco Jabber for Windows and Mac では、Sennheiser プラグインがこのポートをコール制御のローカルホスト トラフィックに使用します。

その他のサービスおよびプロトコルのポート

この項で示されているポートに加えて、展開におけるすべてのサービスとプロトコルに必要なポートを確認します。次のマニュアルで様々なサーバのポートとプロトコルの要件を参照してください。

- Cisco Unified Communications Manager、Cisco Unified Communications Manager IM and Presence Service については、『*TCP and UDP Port Usage Guide*』を参照してください。
- Cisco Unity Connection については、『*System Administration Guide*』を参照してください。
- Cisco Webex Meetings サーバーについては、*Adiminstration Guide*を参照してください。
- Cisco Meeting Serverについては、*Cisco Meeting Server Release 2.6 and 2.7: Single Combined Meeting Server Deployments*を参照してください。
- Cisco Webex サービスについては、*Administrator's Guide*を参照してください。
- Expressway for Mobile and Remote Access については、『*Cisco Expressway IP Port Usage for Firewall Traversal*』を参照してください。
- ファイル転送ポートの使用方法については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

サポートされるコーデック

タイプ（Type）	コーデック	コーデック タイプ	Android 版 Cisco Jabber	iPhone および iPad 版 Cisco Jabber	Mac 版 Cisco Jabber	Windows 版 Cisco Jabber
[音声（Audio）]	G.711	A-law	○ 通常モードをサポートします。		はい	はい
		μ-law/Mu-law	○ 通常モードをサポートします。		はい	はい
	G.722		はい		はい	はい
	G.722.1	24 kb/s および 32 kb/s	○ 通常モードをサポートします。		はい	はい
	G.729		G.729 でのビジュアルボイスメールはサポートされていませんが、ユーザは G.729 と [ボイスメールに発信（Call Voicemail）] 機能を使用してボイスメッセージにアクセスできます。		不可	不可
	G.729a		○ 狭帯域幅で使用するための最小要件です。 狭帯域幅モードをサポートするコーデックだけです。 通常モードをサポートします。		はい	はい
	Opus		はい		はい	はい

タイプ（Type）	コーデック	コーデック タイプ	Android 版 Cisco Jabber	iPhone および iPad 版 Cisco Jabber	Mac 版 Cisco Jabber	Windows 版 Cisco Jabber
[ビデオ（Video）]	H.264/AVC	ベースライン プロファイル	はい		はい	はい
		高プロファイル	不可		はい	はい
[ボイスメール（Voicemail）]	G.711	A-law	はい		はい	はい
		μ-law/Mu-law（デフォルト）	はい		はい	はい
	GSM 06.10		はい		はい	はい
	PCM リニア		はい		はい	はい

Android 版 Cisco JabberまたはiPhone および iPad 版 Cisco Jabberの使用中に音声品質に問題が発生した場合は、クライアント設定で狭帯域幅モードのオンとオフを切り替えることができます。

仮想環境の要件

ソフトウェア要件

仮想環境で Windows 版 Cisco Jabber を展開するには、次のサポートされるソフトウェア バージョンの中から選択します。

ソフトウェア	サポートされるバージョン
Citrix XenDesktop	7.9、7.8、7.6、7.5、7.1
Citrix XenApp	7.9 公開済みアプリケーションとデスクトップ 7.8 公開済みアプリケーションとデスクトップ 7.6 公開済みアプリケーションとデスクトップ 7.5 公開済みデスクトップ 6.5 公開済みデスクトップ
VMware Horizon View	7.0, 6.1, 6.0, 5.3

ソフトフォン要件

ソフトフォン コールに対して、 Jabber Softphone for VDIを使用します。

音声およびビデオのパフォーマンス参照

注目 次のデータは、ラボ環境でのテストに基づいています。このデータは、帯域幅の使用状況の点で予想できる内容を提供することを目的としています。このトピックの内容は、完全な内容を示したり、帯域幅の使用状況に影響を与える可能性があるすべてのメディア シナリオを反映したりするものではありません。

メディア保証

低いメディア品質が原因で会議が中断されないように、すべてのネットワーク タイプでリアルタイム メディアの品質を保証します。メディア保証により、最大 25% のパケット損失を軽減できます。

メディア保証は、Cisco Unified Communications Manager Release 10.x 以降のビデオおよび Cisco Unified Communications Manager Release 11.5 以降のビデオとオーディオでサポートされています。

Expressway for Mobile and Remote Access を展開する場合は、メディア保証に Cisco Expressway リリース 8.8.1 以降が必要です。

軽微なネットワーク条件から重度なものまで、Jabber は次の内容を可能にします。

- ストリームの帯域幅を一時的に制限します。
- ビデオを再同期します。
- 不要な輻輳によるバースト ロスを回避するようにパケットを調整します。
- 最初のメディア パケットから先行する SDP シグナリングを使用して、レジリエンス メカニズムを提供します。
- パケット損失を防止します。
- 稼働中のメディアの数が原因によるメディア輻輳ベースの損失を回避します。
- フレーム レート/ビット レートが低いストリームの保護を改善します。
- 認証済みおよび暗号化済み FEC をサポートします。

高速レーン サポート

高速レーン サポートにより、トラフィックが高くても、ビジネス クリティカルなアプリケーションはネットワーク上で優先されます。Jabberは音声とビデオのトラフィックの高速レーンをサポートしています。iOS 10 の場合、アクセス ポイント（AP）の高速レーン機能を使用すると、Cisco Unified Communications Manager で設定された DSCP 値は使用されなくなります。iOS 11 の場合、Jabber は Cisco Unified Communications Manager で設定された DSCP 値を使用して継続します。

Cisco Unified Communications Manager の DSCP 設定に関係なく、ワイヤレス AP が高速レーン機能をサポートする場合、Jabberは次のDSCPとユーザ指定の優先順位（UP）の値を自動的に設定します。

- 音声コールまたはビデオ コールの音声部分では、DSCP は 0x2e に、UP は 6 に設定されます。
- ビデオ コールのビデオ部分では、DSCP は 0x22 に、UP は 5 に設定されます。
- AP が高速レーンをサポートしない、または使用しない場合、DSCP 値は Cisco Unified Communications Manager によって指定された値に自動的に設定されます。

前提条件：

- AireOS 8.3 以降を実行する WLC
- AP1600/2600 シリーズ アクセス ポイント、AP1700/2700 シリーズ アクセス ポイント、AP3500 シリーズ アクセス ポイント、AP3600 シリーズ アクセス ポイント + 11ac モジュール、WSM、Hyperlocation モジュール、3602P、AP3700 Hyperlocation + WSM、3702P、OEAP600 シリーズ OfficeExtend アクセス ポイント、AP700 シリーズ アクセス ポイント、AP700W シリーズ アクセス ポイント、AP1530 シリーズ アクセス ポイント、AP1550 シリーズアクセス ポイント、AP1570 シリーズアクセス ポイント、およびAP1040/1140/1260 シリーズ アクセス ポイント
- ios 11またはそれ以降で実行されている ios デバイス。

Cisco Jabber デスクトップ クライアントの音声ビット レート

次の音声ビット レートが Cisco Jabber for Windows と Cisco Jabber for Mac に適用されます。

コーデック	RTP（kbit/秒）	実際のビット レート（kbit/秒）	注記（Notes）
G.722.1	24/32	54/62	高品質な圧縮
G.711	64	80	標準的な非圧縮
G.729a	8	38	低品質な圧縮

Cisco Jabber モバイル クライアントの音声ビット レート

次の音声ビット レートが、Cisco Jabber for iPad and iPhone と Cisco Jabber for Android に適用されます。

コーデック	コーデック ビット レート（kbit/秒）	利用ネットワーク帯域幅（kbit/秒）
g.711	64	80
g.722.1	32	48
g.722.1	24	40
g.729a	8	24

Cisco Jabber デスクトップ クライアントのビデオ ビット レート

次のビデオ ビット レート（g.711 音声を使用）は、Cisco Jabber for Windows と Cisco Jabber for Mac に適用されます。この表は、想定される解像度をすべて網羅しているわけではありません。

解像度	ピクセル	g.711 音声で測定されたビット レート（kbit/秒）
w144p	256 x 144	156
w288p これが Cisco Jabber のビデオ レンダリング ウィンドウのデフォルト サイズです。	512 x 288	320
w448p	768 x 448	570
w576p	1024 x 576	890
720p	1,280 X 720	1300
1080p	1920 X 1080	2500-4000

（注） 測定されたビット レートは、実際の使用帯域幅（RTP ペイロード+IP パケットのオーバーヘッド）です。

Cisco Jabber for Android のビデオ ビット レート

ビデオ	解像度	帯域幅
HD	1280 X 720	1024
VGA	640 X 360	512
CIF	488 X 211	310

（注） コール中に HD ビデオを送受信するには、

- Cisco Unified Communications Manager に 1024 kbps を超えるビデオコール用の最大のビットレートを設定します。
- ビデオRTPパッケージを高い優先順位で送信するため、ルータのDSCPを有効にします。

Cisco Jabber for iPhone and iPad のビデオ ビット レート

クライアントは 20 fps でキャプチャおよび送信します。

解像度	ピクセル	g.711 音声でのビット レート（kbit/秒）
w144p	256 x 144	290
w288p	512 x 288	340
w360P	640 X 360	415
w720p	1280 X 720	1024

プレゼンテーションのビデオ ビット レート

Cisco Jabber は 8 fps でキャプチャし、2 ～ 8 fps で送信します。

この表の値には、音声は含まれていません。

ピクセル	2 fps でのワイヤ ビット レートの概算値（kbit/秒）	8 fps でのワイヤ ビット レートの概算値（kbit/秒）
720 x 480	41	164
704 x 576	47	188
1024 X 768	80	320
1280 X 720	91	364

ピクセル	2 fps でのワイヤ ビット レートの概算値（kbit/秒）	8 fps でのワイヤ ビット レートの概算値（kbit/秒）
1280 x 800	100	400
1920 X 1080	150-300	500 ～ 1000

リリース 12.5 では、ビデオ帯域幅全体が 300 kb 未満になっている場合に、メインビデオ品質を向上させるためにビットレート割り当てを変更しました。ただし、この変更はメインビデオの最大ビットレートを 450 キロビット/秒に設定することもできます。

ビデオ帯域幅の合計値が高くなるほど、メインビデオの以前のリリースと比べて低い解像度が表示される場合があります。

ネゴシエートされた最大ビット レート

Cisco Unified Communications Manager の [リージョンの設定（Region Configuration）] ウィンドウで、最大ペイロード ビット レートを指定します。この最大ペイロード ビット レートには、パケット オーバーヘッドは含まれません。したがって、使用される実際のビット レートは、指定した最大ペイロード ビット レートよりも大きくなります。

次の表に、Cisco Jabber による最大ペイロード ビット レートの割り当て方法に関する説明を示します。

デスクトップ共有セッション	音声	双方向ビデオ（メイン ビデオ）	プレゼンテーション ビデオ（デスクトップ共有ビデオ）
X	Cisco Jabber は最大音声ビット レートを使用します。	Cisco Jabber は次のように残りのビット レートを割り当てます。 ビデオ コールの最大ビット レートから音声のビット レートを引きます。	—
あり	Cisco Jabber は最大音声ビット レートを使用します。	Cisco Jabber は音声ビット レートを差し引いた残りの帯域幅の半分を割り当てます。	Cisco Jabber は音声ビット レートを差し引いた残りの帯域幅の半分を割り当てます。

音声	双方向ビデオ（メイン ビデオ）
Cisco Jabber は最大音声ビット レートを使用します。	Cisco Jabber は次のように残りのビット レートを割り当てます。 ビデオ コールの最大ビット レートから音声のビット レートを引きます。

帯域幅

Cisco Unified Communications Manager での領域設定では、クライアントで使用可能な帯域幅を制限できます。

音声コールおよびビデオ コール用のトランスポート非依存の最大ビット レートを指定することにより、領域内および既存の領域間で音声コールおよびビデオ コールに使用される帯域幅を、領域を使用して制限します。領域設定の詳細については、お使いのリリースのCisco Unified Communications Manager のマニュアルを参照してください。

Cisco Jabber デスクトップ クライアントの帯域幅パフォーマンス予測

Cisco Jabber for Mac は、音声用のビット レートを分離してから、残りの帯域幅をインタラクティブ ビデオとプレゼンテーション ビデオに均等に分割します。次の表では、帯域幅ごとに達成できるパフォーマンスを理解するのに役立つ情報について説明します。

アップロード速度	[音声（Audio）]	音声+インタラクティブビデオ（メイン ビデオ）
125 kbps（VPN）	g.711 の帯域幅のしきい値レベルです。帯域幅は g.729a および g.722.1 用に十分です。	帯域幅はビデオ用に不十分です。
384 kbps（VPN）	帯域幅は音声コーデック用に十分です。	W288p（512 X 288）（30 fps）
384 kbps（企業ネットワーク）	帯域幅は音声コーデック用に十分です。	W288p（512 X 288）（30 fps）
1000 kbps	帯域幅は音声コーデック用に十分です。	W576p（1024 X 576）（30 fps）
2000 kbps	帯域幅は音声コーデック用に十分です。	w720p30（1280 x 720）（30 fps）

Cisco Jabber for Windows は、音声用のビット レートを分離してから、残りの帯域幅をインタラクティブ ビデオとプレゼンテーション ビデオに均等に分割します。次の表では、帯域幅ごとに達成できるパフォーマンスを理解するのに役立つ情報について説明します。

アップロード速度	[音声（Audio）]	音声+インタラクティブ ビデオ（メイン ビデオ）	音声 + プレゼンテーション ビデオ（デスクトップ共有ビデオ）	音声+インタラクティブ ビデオ + プレゼンテーション ビデオ
125 kbps（VPN）	g.711 の帯域幅のしきい値レベルです。帯域幅は g.729a および g.722.1 用として十分です。 .	帯域幅はビデオ用に不十分です。	帯域幅はビデオ用に不十分です。	帯域幅はビデオ用に不十分です。
384 kbps（VPN）	帯域幅は音声コーデック用に十分です。	W288p（512 X 288）（30 fps）	1280 x 800（2 fps 以上）	w144p（256 x 144）（30 fps）+ 1280 x 720（2 fps 以上）
384 kbps（企業ネットワーク）	帯域幅は音声コーデック用に十分です。	W288p（512 X 288）（30 fps）	1280 x 800（2 fps 以上）	w144p（256 x 144）（30 fps）+ 1280 x 800（2 fps 以上）
1000 kbps	帯域幅は音声コーデック用に十分です。	W576p（1024 X 576）（30 fps）	1280 x 800（8 fps）	w288p（512 x 288）（30 fps）+ 1280 x 800（8 fps）
2000 kbps	帯域幅は音声コーデック用に十分です。	w720p30（1280 x 720）（30 fps）	1280 x 800（8 fps）	w288p（1024 x 576）（30 fps）+ 1280 x 800（8 fps）

VPN でペイロードのサイズを大きくすると、帯域幅の消費が増えることに注意してください。

Cisco Jabber for Android の帯域幅パフォーマンス予測

VPN でペイロードのサイズを大きくすると、帯域幅の消費が増えることに注意してください。

アップロード速度	[音声（Audio）]	音声+インタラクティブ ビデオ（メイン ビデオ）
125 kbps（VPN）	g.711 の帯域幅のしきい値レベルです。帯域幅はビデオ用に不十分です。 帯域幅は g.729a および g.722.1 用に十分です。	帯域幅はビデオ用に不十分です。

アップロード速度	[音声（Audio）]	音声+インタラクティブビデオ（メインビデオ）
256 kbps	帯域幅は音声コーデック用に十分です。	送信レート（Tx）：15 fps で 256 X 144 受信レート（Rx）：30 fps で 256 X 144
384 kbps（VPN）	帯域幅は音声コーデック用に十分です。	Tx：15 fps で 640 X 360 Rx：30 fps で 640 X 360
384 kbps（企業ネットワーク）	帯域幅は音声コーデック用に十分です。	Tx：15 fps で 640 X 360 Rx：30 fps で 640 X 360

（注） デバイスの機能上の制限により、Samsung Galaxy SII および Samsung Galaxy SIII デバイスでは、この表に示す最大解像度を達成できません。

Cisco Jabber for iPhone and iPad の帯域幅パフォーマンス予測

クライアントは音声のビット レートを分けてから、インタラクティブ ビデオとプレゼンテーション ビデオの間で残りの帯域幅を均等に分けます。次の表では、帯域幅ごとに達成できるパフォーマンスを理解するのに役立つ情報について説明します。

VPN でペイロードのサイズを大きくすると、帯域幅の消費が増えることに注意してください。

アップロード速度	[音声（Audio）]	音声 + インタラクティブ ビデオ（メイン ビデオ）
125 kbps（VPN）	g.711 の帯域幅のしきい値レベルです。帯域幅はビデオ用に不十分です。 帯域幅は g.729a および g.722.1 用に十分です。	帯域幅はビデオ用に不十分です。
290 kbps	帯域幅は音声コーデック用に十分です。	256 X 144（20 fps）
415 kbps	帯域幅は音声コーデック用に十分です。	640 X 360（20 fps）
1024 kbps	帯域幅は音声コーデック用に十分です。	1280 X 720（20 fps）

ビデオ レート アダプテーション

Cisco Jabber は、ビデオ レート アダプテーションを使用して、最適なビデオ品質を調整します。ビデオ レート アダプテーションは、ビデオのビット レートのスループットを動的に増減して、有効な IP パスの帯域幅でリアルタイムの変動を処理します。

Cisco Jabber ユーザは、ビデオ コールが低解像度で始まり、短時間で高解像度になることを期待しているはずです。Cisco Jabber は、後続のビデオ コールが最適な解像度で開始されるように、履歴を保存します。

帯域幅への H.264 プロファイルの影響

以前のリリースでは、H.264 のベースラインプロファイルのみがサポートされていました。リリース 12.8 では、デスクトップクライアント向けに、H.264高プロファイルのサポートが追加されました。VDI またはモバイルクライアントに高レベルのプロファイルを使用することはできません。

高レベルのプロファイルでは、同じビデオ品質を最大10%安い帯域幅で提供できます。また、同じ帯域幅を使用してビデオ品質を向上させることもできます。

Jabber は、H. 264 ベースのプロファイルにデフォルト設定されています。高プロファイルを有効にするには、H264HighProfileEnableパラメータを使用します。

コール管理レコード

通話の終了時に、Jabber は通話のパフォーマンスと品質の情報を Cisco Unified Communications Manager に送信します。シスコ ユニファイド コミュニケーション マネージャーは、シスコ ユニファイド コミュニケーション マネージャーを呼び出す管理レコード (CMR) を設定するのにこれらのメトリックを使用します。Cisco Jabber では、音声通話およびビデオコールの両方で次の情報を送信します。

- 送受信パケット数。
- 送受信オクテット数。
- パケット損失数。
- 平均ジッター。

ビデオの場合、クライアントは、次のビデオ専用の情報を送信します。

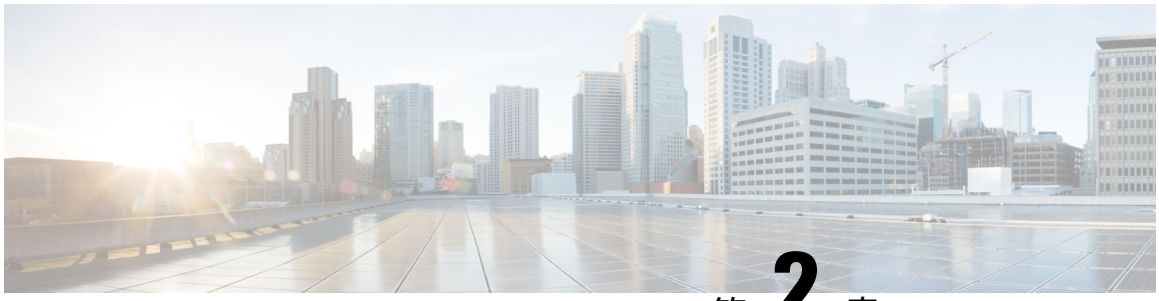
- 送受信で使用したコーデック。
- 送受信の解像度。
- 送受信のフレームレート。
- 平均ラウンドトリップ時間（RTT）

クライアントは、次のオーディオ専用の情報を送信します。

- フレーム損失発生秒数。
- 深刻なフレーム損失発生秒数。

これらの指標は、Cisco Unified Communications Manager の CMR レコード出力にプレーンテキスト形式で表示されます。このデータは直接解読可能で、テレメトリ、分析アプリケーションに読み込ませることもできます。

Cisco Unified Communications Manager CMR レコードの設定の詳細は、Cisco Unified Communications Manager のご使用のリリースの『*Call Detail Records Administration Guide*』の『*Call Management Records*』の章を参照してください。



第 2 章

展開シナリオ

- オンプレミス展開 （41 ページ）
- クラウドベース展開 （46 ページ）
- 仮想環境での展開 （50 ページ）
- リモート アクセス （52 ページ）
- シングル サインオンを使用した展開 （63 ページ）

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Cisco Jabberで展開できます。

- **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。
- **電話機のみのモード**: 電話機のみのモードでは、ユーザのプライマリ認証がCisco Unified Communications Managerになります。電話機専用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。

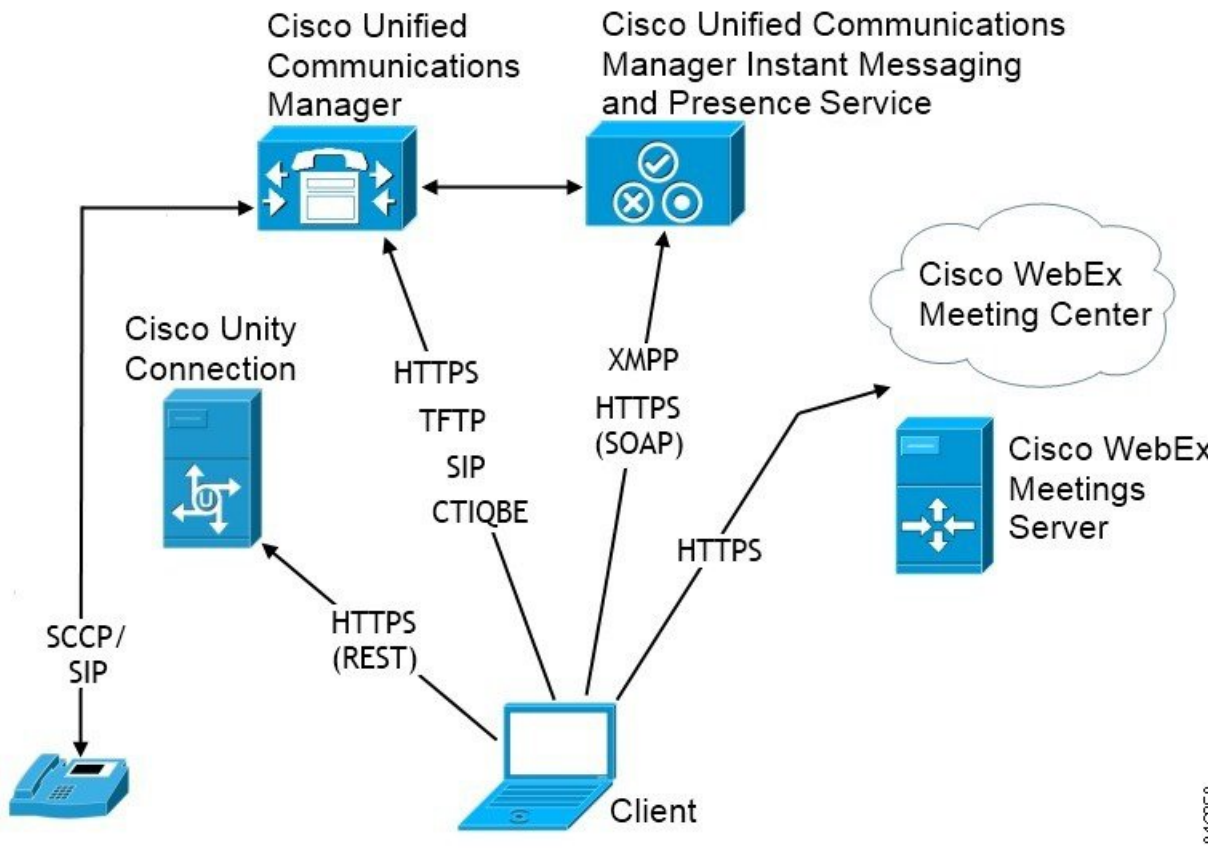
Cisco Unified Communications Manager IM and Presence Service によるオンプレミス展開

Cisco Unified Communications Manager IM and Presence Service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 経由で対応可否を公開し、他のユーザの対応可否をサブスクライブします。
- **IM**：Cisco Unified Communications Manager IM and Presence Service を介して IM を送受信します。
- **ファイル転送**: Cisco Unified Communications Manager IM and Presence Service を介してファイルおよびスクリーンショットを送信および受信します。
- **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を通じてビデオ通話を発信します。
- **ボイスメール**—Cisco Unity Connectionを通じて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 Meetings センター—ホステッド会議機能を実現します。
  - Cisco Webex Meetings サーバーオンプレミス会議能力を提供します。

次の図は、Cisco Unified Communications Manager IM and Presence Serviceを使った 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* : 以下のものを使ったオンプレミスの展開 *Cisco Unified Communications Manager IM and Presence Service*



コンピュータ テレフォニー インテグレーション

Windows 版 Cisco JabberおよびMac 版 Cisco Jabber Mac には、サードパーティ製のアプリケーションからCisco Jabberの CTI をサポートしています。

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*システム ガイド の項を参照してください。または、Cisco Unified Communications Manager API を通じ、CTI コントロールのアプリケーションを作成する方法についての詳細は、次の Cisco Developer Network サイトを参照してください。

- 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

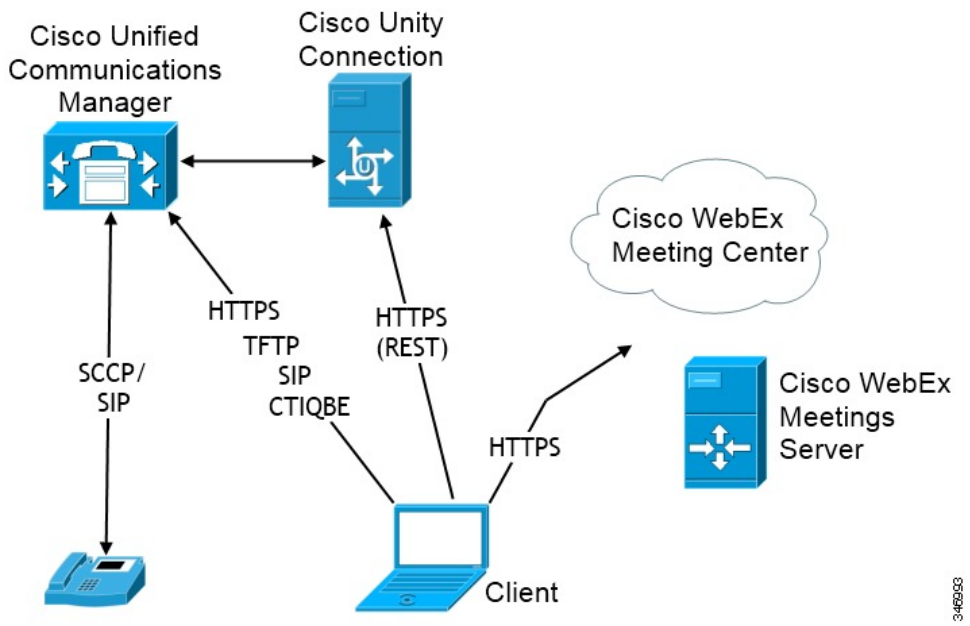
電話機モード展開で使用可能なサービスは次のとおりです。

- **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 Unity Connectionを通じてビデオ通話を発信します。
- **ボイスメール**—Cisco Unity Connectionを通じて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 Meetingsセンター**—ホステッド会議機能を実現します。
  - **Cisco Webex Meetingsサーバー**—オンプレミス会議能力を提供します。

（注） Android 版 Cisco JabberとiPhone および iPad 版 Cisco Jabberは、電話モードでは会議機能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。

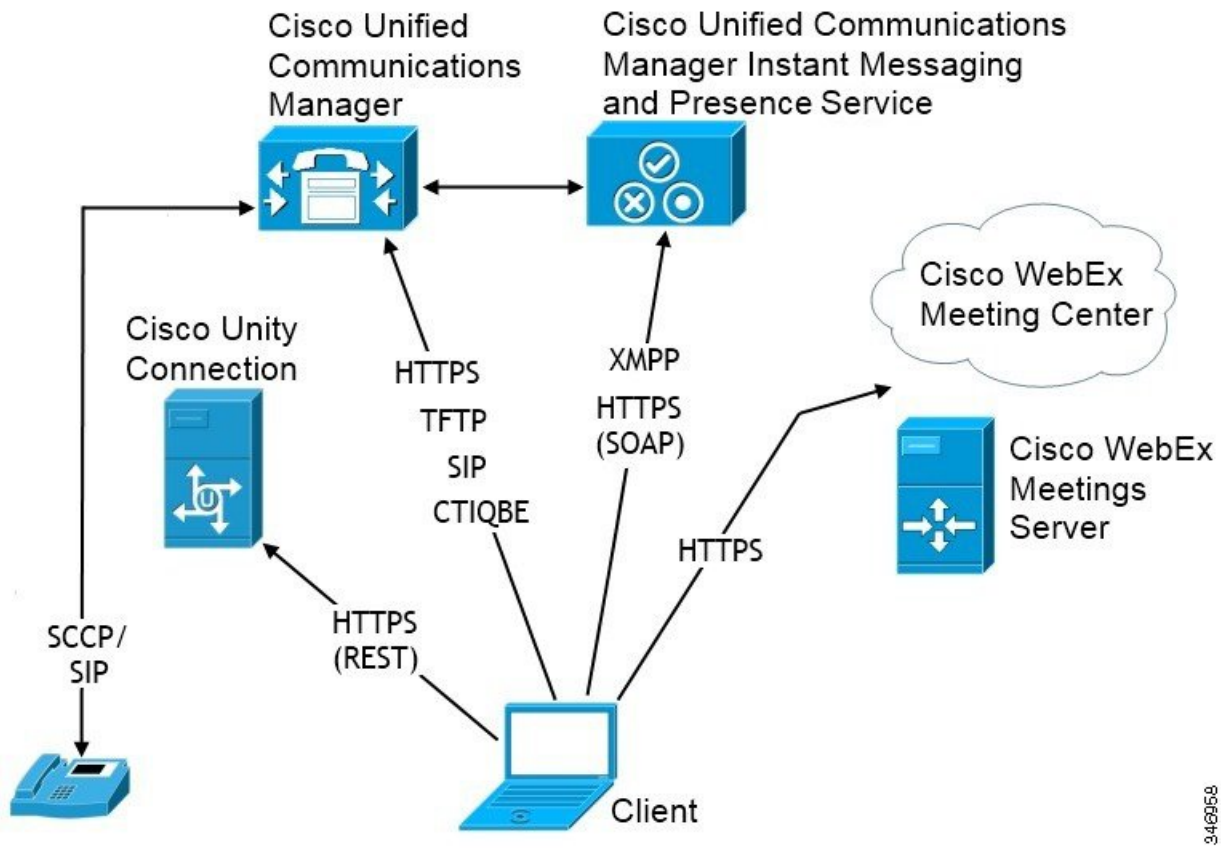
電話モードの展開（連絡先を使用）

連絡先つき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**: Cisco Unified Communications Manager IM and Presence Serviceを通じて連絡先情報を参照できます。
- **プレゼンス**：Cisco Unified Communications Manager IM and Presence Service 経由で対応可否を公開し、他のユーザの対応可否をサブスクライブします。
- **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を通じてビデオ通話を発信します。
- **ボイスメール**—Cisco Unity Connectionを通じて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 Meetings センター—ホステッド会議機能を実現します。
  - Cisco Webex Meetings サーバーオンプレミス会議能力を提供します。

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

図 *3:* 電話モードの展開（連絡先を使用）



クラウドベース展開

クラウドベース展開は、Cisco Webexを使ってサービスをホストします。

Cisco Webex メッセンジャーを使ってクラウドとハイブリッドを展開するには、Cisco Webex 管理ツールでクラウドベースの導入を管理および監視します。ユーザのサービスプロファイルを設定する必要はありません。

クラウド展開およびハイブリッド展開の Cisco Webex Platform サービス場合は、Cisco Control Hub を使用して展開を管理および監視します。

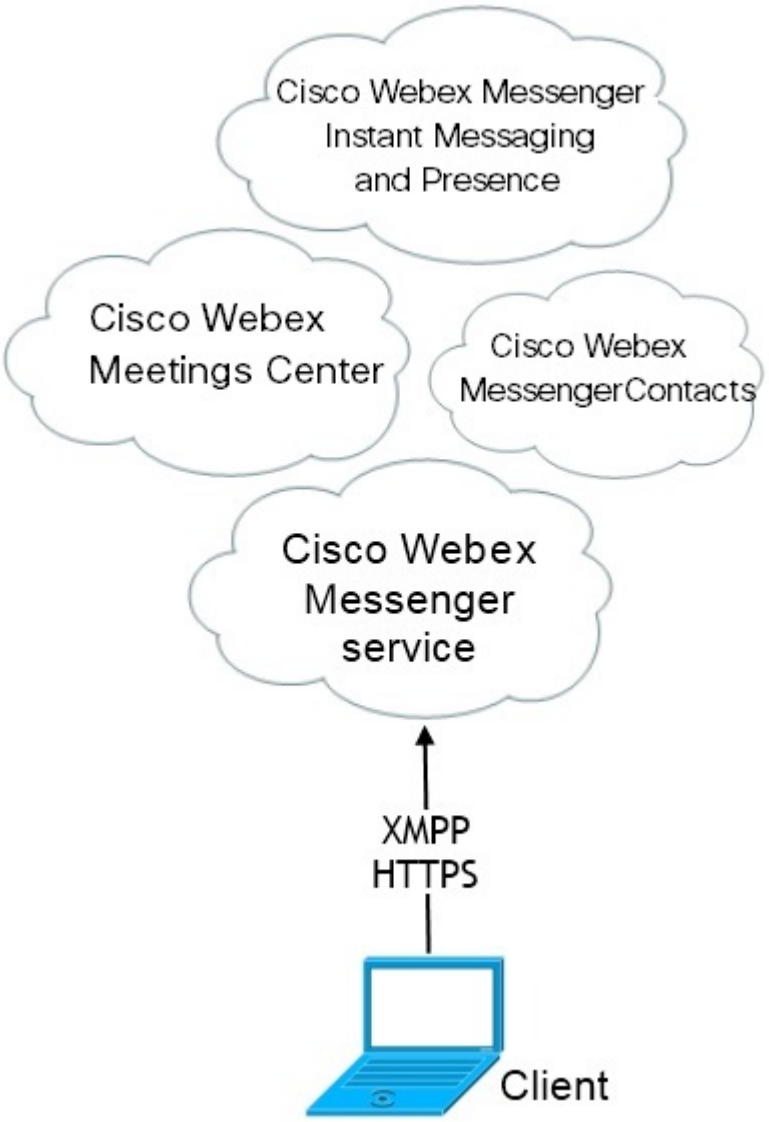
クラウドベース導入での Cisco Webex Messenger サービス。

Webex Messenger を使用したクラウドベースの導入では、次のサービスを利用できます。

- **連絡先ソース**—Cisco Webex Messenger が連絡先の解決を提供します。
- **プレゼンス**—Cisco Webex Messengerによりユーザーは、自分自身のアベイラビリティを表示したり、他のユーザーのアベイラビリティを閲覧したりできます。

- **インスタント メッセージ**—Cisco Webex Messenger ユーザーは、インスタントメッセージを送受信できるようになります。
- **会議**—Cisco Webex Meetings センターは、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。

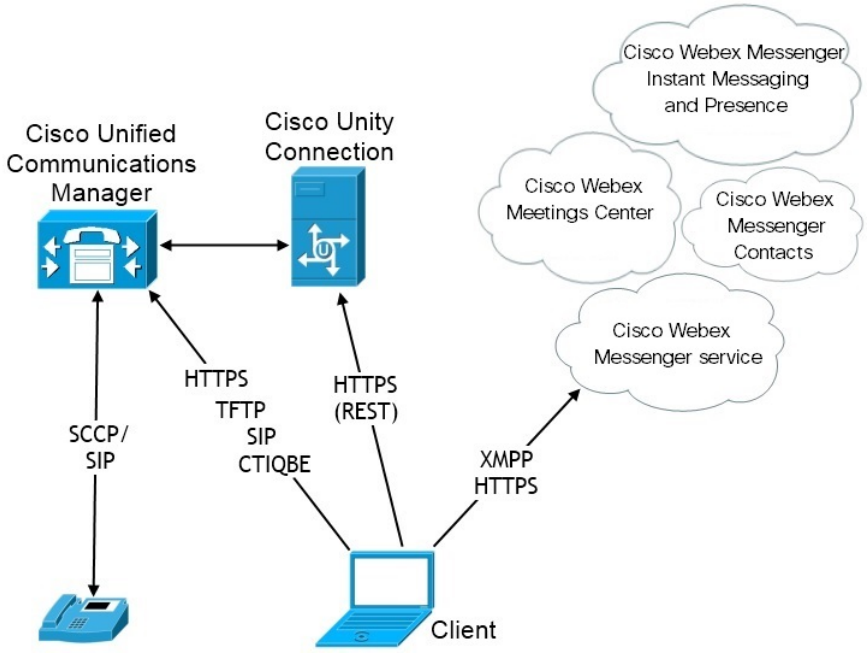


HyDeployメCisco Webex Messenger Serviceを使ったハイブリッド クラウドベース展開

Webex Messenger サービスを使用したハイブリッド クラウドベースの導入では、次のサービスを利用できます。

- **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を通じてビデオ通話を発信します。
- **会議**—Cisco Webex Meetings センターは、ホステッド会議機能を提供します。
- **ボイスメール**—Cisco Unity Connectionを通じて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。



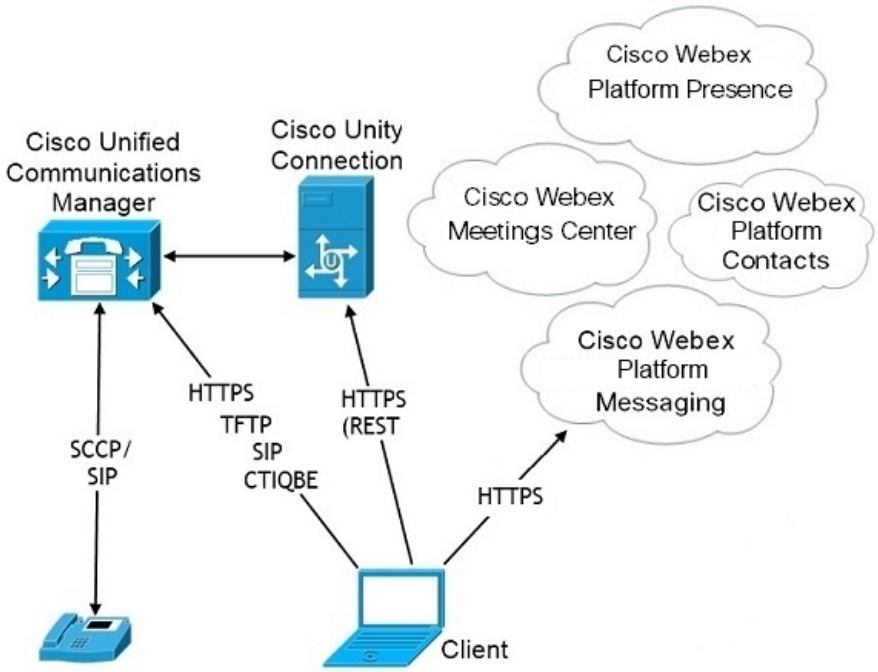
以下のものを使ってハイブリッド クラウドベース展開 Cisco Webex Platform サービス

次の Jabber チームメッセージングモードサービスは、Jabber によるハイブリッドのクラウドベース展開において、 Cisco Webex Platform サービスとともにご利用になれます:

- 連絡先ソース - Cisco Webex Platform サービスが、連絡先を提供します。
- プレゼンス— Cisco Webex Platform サービス によりユーザーは、アベイラビリティを公開したり、他のユーザーのアベイラビリティを閲覧したりできるようになります。

- メッセージング— Cisco Webex Platform サービスによりユーザーは、メッセージの送受信ができるようになります。
- 音声— 卓上電話機またはコンピュータを介して、Cisco UC Managerを使って音声通話を行います。
- ビデオ— Cisco UC Manager を使用してビデオコールを行います。
- 会議— Webex Meeting Center がホスト型ミーティング機能を提供します。
- 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、 Cisco Webex Platform サービスを使った Jabber のハイブリッド クラウドベース展開のアーキテクチャを示しています。



Jabber チーム メッセージング モードにおける連絡先

サインインフロー

Webex Control Hub でチームメッセージモードを有効にしている間に、ユーザの連絡先を移行する必要があります。

このサインインフローは、ユーザの連絡先を移行するプロセスの概略を示しています。フローは、現在の Jabber の展開にログインしているユーザから開始されます。Jabber チームメッセージモードを有効にして、連絡先を移行します。

1. ユーザは現在の Jabber の展開にログインしており、Cisco UC Manager IM & P または Cisco Webex Messenger に接続しています。

2. 管理者は、Webex Control Hub の設定を変更して、Jabber チームのメッセージモード、オプションで移行、および Jabber のコールを有効にします。
3. 翌日、ユーザは現在の Jabber の展開にログインします。5 分以内に、Jabber はサービス検索プロセスを実行し、そのユーザ向け配置 Cisco Webex Platform サービスが検出されたことを検出します。
4. Jabber は、ユーザが Jabber からメッセージをサインアウトするか、"設定の変更が検出された"かを確認します。
5. ユーザが再度サインインすると、その時点でに認証されます Cisco Webex Platform サービス。
6. 連絡先の移行を有効にした場合、ユーザは Jabber の連絡先を取得するようにメッセージが表示されます。[Ok] をクリックすると、Jabber は連絡先リストのキャッシュを取得して Cisco Webex Platform サービスにアップロードします。ユーザが**キャンセル**を選択すると、Jabber は連絡先リストを移行しません。後で連絡先を検索し、その連絡先を個別に追加できます。

   連絡先移行中は、Jabber は、 Cisco Webex Platform サービスが有効になっている連絡先のみを移行します。Jabber には、 Cisco Webex Platform サービスにカスタム連絡先が保存されないため、それらをユーザの連絡先リストに追加することはできません。
7. Jabber は、 Cisco Webex Platform サービスに接続された後、Cisco UC Manager に接続してサービスプロファイルをダウンロードします。SSO が異なる IdPs で Cisco Webex Platform サービスとUC マネージャーの両方で有効化されている場合、または SSO が 1 つのみで有効化されている場合は、ユーザに資格情報の入力を求めるプロンプトが表示されます。ただし、両方の IdP で SSO がオンになっている場合は、サインインは必要ありません。

Jabber チームメッセージモードの導入に関する考慮事項と連絡先の移行

Cisco Webex Platform サービス組織には、サービスドメインと同じドメインを割り当てる必要があります。これらのドメインが異なるドメインである場合、ユーザは連絡先を移行できません。

仮想環境での展開

仮想環境に Windows 版 Cisco Jabber 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 はユーザーデータを、以下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。

VDI 向け Jabber ソフトフォンの展開

コールの発信機能がある仮想環境に Jabber を展開するには、仮想デスクトップインフラストラクチャ用の Jabber ソフトフォンを展開する必要があります。

VDI 用 Jabber ソフトフォンの展開のワークフローは、オンプレミスの環境またはハイブリッド環境で展開している場合に依存するため、アプリケーションがインストールされる前に jabber による展開のワークフローに従い、その時点においては VDI の展開向けJabber のソフトフォン、およびインストールワークフローに従います。

VDI 用 Jabber ソフトフォンのオンプレミスの展開ワークフローを取得するには、*Cisco Jabber* のオンプレミス展開の展開およびインストールワークフローセクションの完全な UC 展開ワークフローを参照してください。

Jabber ソフトフォン向けに VDI のハイブリッド展開ワークフローを取得するには、*Webex Messenger*を使ったハイブリッド展開のワークフロー（クラウド向けワークフローとハイブリッドの展開セクションを参照、Cisco Jabber向けクラウドとハイブリッド展開）をご覧ください。

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。

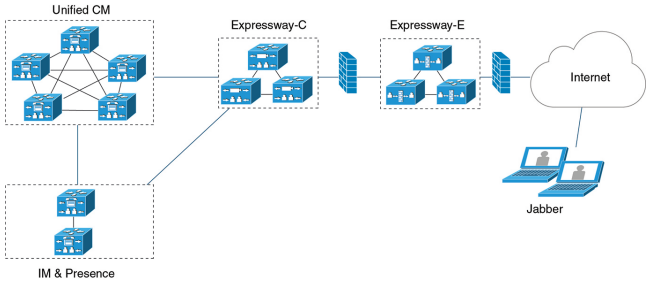
Jabber は、サードパーティ VPN クライアントではテストもサポートもされません。

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。

図 *4 :* クライアントが、*Expressway for Mobile and Remote Access* に接続する方法

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



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。ハイブリッド導入の場合、管理者はVoiceServicesDomainパラメータを設定することができます。*Cisco Jabber* のパラメータリファレンスガイドの最新版を参照してください。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 *2 : 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。	
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	
永続的なチャット	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。	

サービス	サポート対象	非サポート対象
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	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。	

サービス	サポート対象	非サポート対象
共有回線	X 前提条件： • Cisco Expressway 8.9.1 以降 • 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	X
クラウド	X	
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
カスタマイズ		
カスタム HTML タブ		X

サービス	サポート対象	非サポート対象
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		
メディア向け ICE プロトコル	X	
エンドツーエンド暗号化	X	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）		
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	
連絡先の検索	X	

サービス	サポート対象	非サポート対象
連絡先の解決	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。
- 無制限の Cisco ユニファイドコミュニケーションマネージャー IM およびプレゼンスサーバを使用したモバイルおよびリモートアクセスの展開の場合、管理ファイル転送はサポートされていません。

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（Voicemail）]

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。
  - 社内ネットワークの外部では、Jabber で送信されたメディアを暗号化するように、パブリッシング Sway-C または社内 Sway-E サーバ上で ICE パススルーサポートを設定することができます。セットアップの詳細については、*Cisco Expressway*を通じたモバイル・リモートアクセス向け展開ガイドを参照してください。

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クライアントは、Cisco Webex Messengerサービス、Cisco Unified Communications Manager、またはCisco Unity Connectionに接続されているサービスに対して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
Windows 版 Cisco Jabber	Internet Explorer[InternetExplorer]
Mac 版 Cisco Jabber	Safari
iPhone および iPad 版 Cisco Jabber	Safari
Android 版 Cisco Jabber	Chrome または Internet Explorer

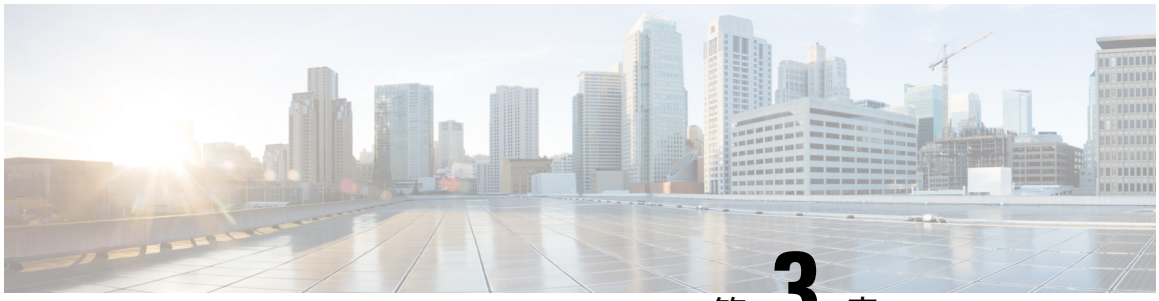
（注） Cisco Jabber for Android で SSO を使用する場合、組み込みブラウザは外部ブラウザと Cookie を共有できません。

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。両方において SSO を有効または無効にする必要があります。

- セキュアな電話機の Expressway for Mobile and Remote Access を介して SSO を使用することはできません。
- 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と外側の間で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。



第 3 章

ユーザ管理

- Jabber ID （67 ページ）
- IM アドレス スキーム （68 ページ）
- Jabber ID によるサービス ディスカバリ （69 ページ）
- SIP URI （69 ページ）
- LDAP ユーザ ID （69 ページ）
- フェデレーション用ユーザ ID の計画 （70 ページ）
- ユーザの連絡先写真のプロキシ アドレス （70 ページ）
- 認証および承認 （70 ページ）
- 複数リソースのログイン （75 ページ）

Jabber ID

Cisco Jabber は Jabber ID を使用して、連絡先ソース内の連絡先情報を識別します。

デフォルトの Jabber ID は、ユーザ ID とプレゼンス ドメインを使用して作成されます。

たとえば、Adam McKenzie が `amckenzie` というユーザ ID を持っており、そのドメインが `example.com` である場合、Jabber ID は `amckenzie@example.com` となります。

次の文字は、Cisco Jabber ユーザ ID または電子メール アドレスでサポートされます。

- 大文字 (A から Z)
- 小文字 (a から z)
- 数字（0 ～ 9）
- ピリオド（.）
- ハイフン（-）
- アンダースコア（_）
- チルダ（~）
- Hashtag (#)

連絡先リストに入力する場合、クライアントは Jabber ID を使用して連絡先ソースを検索し、連絡先を解決して、名、姓、その他の連絡先情報を表示します。

IM アドレス スキーム

Cisco Jabber 10.6 以降は、example-us.com や example-uk.com のユーザのようにドメインが同じプレゼンス アーキテクチャ上に存在する場合は、オンプレミス展開用の複数のプレゼンス ドメイン アーキテクチャ モデルをサポートします。Cisco Jabber は Cisco Unified Communications Manager IM and Presence 10.x 以降を使用して柔軟な IM アドレス スキームをサポートします。IM アドレス スキームは Cisco Jabber ユーザを識別する Jabber ID です。

マルチ ドメイン モデルをサポートするには、展開のすべてのコンポーネントに次のバージョンが必要です。

- Cisco Unified Communications IM and Presence サーバ ノードとコール制御ノード バージョン 10.x 以降。
- Windows、Mac、IOS、および Android のバージョン 10.6 以降で実行中のすべてのクライアント。

次のシナリオでは、複数のドメイン アーキテクチャを使用している Cisco Jabber を展開するだけです。

- Cisco Jabber 10.6 以降は、すべてのプラットフォーム（Windows、Mac、IOS、および Android（DX シリーズなどの Android ベースの IP 電話を含む））上の組織内のすべてのユーザに対する新しいインストールとして展開されます。
- プレゼンス サーバ上でドメインまたは IM アドレスを変更する前に、Cisco Jabber がすべてのプラットフォーム（Windows、Mac、IOS、および Android（DX シリーズなどの Android ベースの IP 電話を含む））上のすべてのユーザに対してバージョン 10.6 以降にアップグレードされます。

詳細プレゼンス設定で使用可能な IM アドレス スキームは次のとおりです。

- UserID@[Default Domain]
- Directory URI

UserID@[Default Domain]

User ID フィールドは LDAP フィールドにマップされます。これがデフォルトの IM アドレス スキームです。

たとえば、ユーザの Anita Perez は、アカウント名が aperez で、User ID フィールドが sAMAccountName LDAP フィールドにマップされます。使用されるアドレス スキームは aperez@example.com です。

Directory URI

ディレクトリ URI は、**mail** または **msRTCSIP-primaryuseraddress** LDAP フィールドにマップされます。このオプションは、認証用のユーザ ID に依存しないスキームを提供します。

たとえば、ユーザの Anita Perez は、アカウント名が aperez で、mail フィールドが Anita.Perez@domain.com で、使用されるアドレス スキームが Anita.Perez@domain.com です。

Jabber ID によるサービス ディスカバリ

サービス ディスカバリは、`[userid]@[domain.com]` の形式で入力された Jabber ID を取得し、デフォルトでは、Jabber ID の `domain.com` 部分を取り出して使用可能なサービスを検出します。プレゼンス ドメインがサービス ディスカバリ ドメインと同じではない展開の場合は、次のようにして、インストール時にサービス ディスカバリ ドメイン情報を含めることができます。

- Cisco Jabber for Windows では、`SERVICES_DOMAIN` コマンドライン引数を使用してこれを行います。
- Cisco Jabber for Mac、Cisco Jabber for Android、Cisco Jabber for iPhone and iPad では、URL 設定で使用される `ServicesDomain` パラメータを使用してサービス ディスカバリ ドメインを設定できます。

.

SIP URI

SIP URI は各ユーザに関連付けられます。SIP URI には、電子メール アドレス、IMAddress、または UPN を使用できます。

SIP URI は、Cisco Unified Communications Manager の [ディレクトリ URI（Directory URI）] フィールドを使用して設定されます。使用可能なオプションは次のとおりです。

- メール アドレス
- msRTCSIP-primaryuseraddress

ユーザは、SIP URI を入力して、連絡先を検索したり連絡先に電話をかけることができます。

LDAP ユーザ ID

ディレクトリ ソースから Cisco Unified Communications Manager にユーザを同期させる場合は、ディレクトリ内の属性からユーザ ID を入力できます。ユーザ ID を保持するデフォルトの属性は、`sAMAccountName` です。

フェデレーション用ユーザ ID の計画

フェデレーションでは、連絡先の検索中に連絡先を解決するため、Cisco Jabber はそれぞれの連絡先に対して連絡先 ID またはユーザ ID を必要とします。

ユーザ ID の属性を SipUri パラメータに設定します。デフォルト値は `msRTCSIP-PrimaryUserAddress` です。ユーザ ID から削除するプレフィックスがある場合は、UriPrefix パラメータ内の値を設定することができます。*Cisco Jabber* パラメータリファレンスガイドの最新バージョンを参照してください。

ユーザの連絡先写真のプロキシ アドレス

Cisco Jabber は写真サーバにアクセスして、連絡先の写真を取得します。ネットワーク設定に Web プロキシが含まれている場合は、Cisco Jabber が写真サーバにアクセスできることを確認する必要があります。

認証および承認

Cisco Unified Communications Manager の LDAP 認証

ディレクトリ サーバを使用して認証するには、Cisco Unified Communications Manager に LDAP 認証を設定します。

ユーザがクライアントにサインインすると、プレゼンス サーバがその認証を Cisco Unified Communications Manager にルーティングします。次に、Cisco Unified Communications Manager がその認証をディレクトリ サーバにプロキシします。

Cisco Webex Messenger ログイン認証

Cisco Webex 管理ツールを使用してCisco Webex Messenger 認証が設定されます。

ユーザがクライアントにサインインすると、その情報が Cisco Webex Messenger に送信され、認証トークンがクライアントに返送されます。

シングル サインオン認証

シングル サインオン認証は、アイデンティティ プロバイダー（IdP）とサービスを使用して設定されます。

ユーザがクライアントにサインインすると、その情報が IdP に送信され、クレデンシャルが承認されると、認証トークンが Cisco Jabber に返送されます。

Cisco Jabber for iPhone and iPad 向けの証明書ベースの認証

Cisco Jabber は、クライアント証明書により IdP サーバで認証されます。この証明書認証により、ユーザ クレデンシャルを入力せずにサーバにサインインできます。クライアントは Safari フレームワークを使用してこの機能を実装します。

要件

- Cisco Unified Communications Manager 11.5、IM and Presence Service 11.5、Cisco Unity Connection 11.5 以降。
- Expressway for Mobile and Remote Access サーバ 8.9 以降。
- ユニファイド コミュニケーション インフラストラクチャに対し SSO が有効。
- Cisco Unified Communications Manager、IM およびプレゼンス サービス、Cisco Unity Connection、IdP サーバを含むすべてのサーバ証明書が CA による署名を持つ。iOS デバイスが OS の信頼認証局を使用する場合、Cisco Jabber アプリをインストールする前に CA 証明書をインストールします。
- Cisco Unified Communications Manager で SSO のネイティブ ブラウザ（Safari に付属）を設定します。詳細については、*Cisco Jabber*向けオンプレミス展開における証明書ベースの SSO 認証セクションを参照してください。
- Expressway for Mobile and Remote Access サーバで SSO のネイティブ ブラウザ（Safari に付属）を設定します。詳細については、https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.htmlのCisco Expressway インストールガイドを参照してください。

Cisco 証明書は、EMM ソリューションを用いて iOS デバイスに展開できます。

推奨—Ciscoは、iOS デバイスへの証明書の展開に EMM ソリューションの使用をお勧めします。

Cisco Jabber for Android の証明書ベースの認証

Cisco Jabber は、シングル サインオン サーバへのサインインにクライアント証明書を使用します（Webex メッセンジャー とオンプレミス）。

要件

- Android OS 5.0 以降
- シングル サインオンが有効
- Jabber クライアントは、モバイルおよびリモート アクセス（MRA）と非 MRA 導入モードでサポートされています。
- Jabber は、Android 7.0 以降では無効な証明書に関する通知を常に表示します。Android OS には、カスタム CA 署名付き証明書がインストールされている場合もあります。Android 7.0 を対象とするアプリは、システムによって提供された証明書だけを信頼し、ユーザが追加した認証局を信頼しません。

証明書の導入

Android デバイスでの証明書の展開には EMM ソリューションの使用をお勧めします。

ボイスメール認証

ユーザは Cisco Unity Connection に存在している必要があります。Cisco Unity Connection は、複数の認証タイプをサポートします。Cisco Unified Communications Manager と Cisco Unity Connection が同じ認証を使用している場合、Cisco Jabber は同じクレデンシャルを使用するように設定することをお勧めします。

OAuth

Cisco Jabber が OAuth プロトコルを使用して、サービスに対するユーザのアクセス権を承認するように、Cisco Jabber を設定することができます。ユーザが OAuth 対応環境にサインインする場合、サインインのたびにクレデンシャルを入力する必要がありません。ただし、サーバが OAuth に対応していない場合は、Jabber が適切に機能しないことがあります。

Cisco ユニファイドコミュニケーションマネージャー 12.5 以降を使用している場合は、SIP OAuth を有効にすることもできます。この機能を使用すると、Jabber が SIP に対して承認され、Jabber が TLS を介して SIP サービスに接続できるようになります。また、Jabber はセキュア接続 (sRTP) 経由でメディアを送信できます。SIP OAuth は、セキュリティで保護された SIP およびメディアを有効にするには CAPF 登録が不要であることを意味します。

前提条件：

- 機能するように導入している場合は、OAuth 更新トークンをこれらのすべてのコンポーネントでオンにする必要があります。
- Cisco Unified Communication Manager、Cisco Unified Communication Manager Instant Messaging and Presence、および Cisco Unity Connection のバージョン 11.5(SU3) または 12.0
- Cisco Expressway for Mobile and Remote Access バージョン X8.10 以降
- SIP OAuth向け: Cisco Unified Communication Manager 12.5 以降、Mobile and Remote Access version X12.5 以降向けのCisco Expressway。

OAuth の設定前に、使用する展開の種類を確認します。

- ローカル認証を展開する場合、IdP サーバは不要です。Cisco Unified Communication Manager が認証を行います。
- SSO を設定して、または設定せずに OAuth を設定することができます。SSO を使用している場合は、すべてのサービスで有効になっていることを確認します。If you have an SSO-enabled deployment, then deploy an IdP server, and IdP server is responsible for authentication.

次のサービス上で OAuth を有効にすることができます。

- Cisco Unified Communications Manager
- Cisco Expressway

- Cisco Unity Connection

デフォルトでは、OAuthはこれらのサーバ上で無効です。これらのサーバでOAuthを有効にするには、次の操作を実行します。

- Cisco Unified Communications Manager と Cisco Unity Connection サーバの場合、**[エンタープライズパラメータ設定（Enterprise Parameter configuration）] > [更新ログインフローを使用したOAuth（OAuth with refresh Login Flow）]** に移動します。
- Cisco Expressway-C の場合、**[設定ユニファイドコミュニケーション（Configuration Unified Communication）] > [更新のOAuthトークンで認証する設定（Configuration Authorized by OAuth token with refresh）]** を移動します。

上記のサーバのOAuthの有効と無効を切り替えると、Jabberは設定の再取得間隔でこの切り替えを識別するため、ユーザは Jabber のサインアウトとサインインできます。

サインアウト中、Jabberはキャッシュ内に保存されているユーザ クレデンシャルを削除して通常のサインフローでサインインします。この場合、Jabberは最初にすべての設定情報を取得するため、ユーザは Jabber サービスにアクセスできます。

Cisco Unified Communication Manager で OAuth を設定するには、次の操作を実行します。

1. **[Cisco Unified Communication Managerの管理（Cisco Unified Communication Manager Admin）] > [システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）] > [SSO設定（SSO Configuration）]** に移動します。
2. [O-Authアクセストークン期限タイマー（分）（O-Auth Access Token Expiry Timer(minutes)）] を任意の値に設定します。
3. [O-Auth更新トークン期限タイマー（日）（O-Auth Refresh Token Expiry Timer(days)）] を任意の値に設定します。
4. [保存（Save）] ボタンをクリックします。

Cisco Expressway で OAuth を設定するには、次の操作を実行します。

1. **[設定（Configuration）] > [Unified Communications] > [設定（Configuration）] > [MRAアクセスコントロール（MRA Access Control）]** に移動します。
2. [O-Authローカル認証（O-Auth local authentication）] を [オン（On）] に設定します。

Cisco Unity で OAuth を設定するには、次の操作を実行します。

1. [AuthZサーバ（AuthZ Servers）] に移動して [新規追加（Add New）] を選択します。
2. すべてのフィールドに詳細を入力して、[証明書エラーを無視する（Ignore Certificate Errors）] を選択します。
3. [保存（Save）] をクリックします。

制限事項

Jabber が自動侵入防御をトリガーする

状況：

- モバイルおよびリモートアクセスの展開用の開発者向けの管理者が、OAuth トークン (更新トークンの有無による) に応じた承認用に設定されています。
- Jabber ユーザのアクセス トークンの有効期限が切れています

Jabber は次のいずれかを行います。

- デスクトップの休止状態からの再開
- ネットワーク接続の回復
- 数時間サインアウトした後、高速サインインの試行

動作：

- いくつかの Jabber モジュールが、期限切れのアクセス トークンを使用して Expressway-E で認証を試行します。
- Expressway-E がこれらの要求を（正しく）拒否します。
- 特定の Jabber クライアントからの要求が 6 つ以上ある場合、Expressway-E はその IP アドレスを（デフォルトで）10 分間ブロックします。

症状：

影響を受ける Jabber クライアントの IP アドレスは、HTTP プロキシの認証の失敗カテゴリにある Expressway-E のブロックされたアドレス リストに追加されます。このアドレスは、**システム** > **保護** > **自動検出** > **ブロックされたアドレス** で確認できます。。

回避策：

この問題を回避するには2つの方法があります。つまり、その特定のカテゴリの検出しきい値を上げるか、または影響を受けるクライアントに対して免除を作成できます。免除は実際の環境では実用的でない可能性があるため、ここではしきい値オプションについて説明します。

1. **[システム（System）] > [保護（Protection）] > [自動検出（Automated detection）] > [設定（Configuration）]** に移動します。
2. [HTTPプロキシの認証の失敗（HTTP proxy authorization failure）] をクリックします。
3. [トリガーレベル（Trigger level）] を 5 ～ 10 に変更します。期限が切れたトークンを提示する Jabber モジュールを容認するには 10 で十分です。
4. 設定を保存すると、すぐに有効になります。
5. 影響を受けるクライアントのブロックを解除します。

複数リソースのログイン

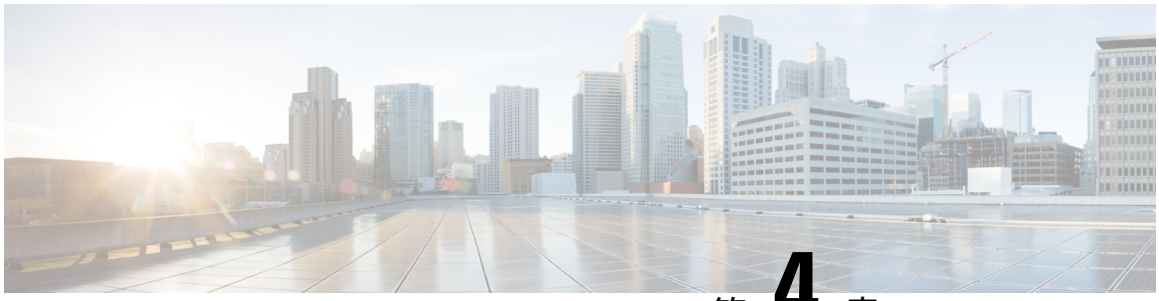
ユーザがシステムにログインすると、すべてのCisco Jabberクライアントが次のいずれかのIM and Presence サービス ノードに一括で登録されます。このノードは、IM and Presence サービス環境のアベイラビリティ、連絡先リスト、およびその他の側面を追跡します。

- オンプレミス展開：Cisco Unified Communications Manager IM and Presence サービス。
- クラウド展開: Cisco Webex

この IM and Presence サービス ノードは、次の順序で一意のネットワーク ユーザに関連付けられた登録済みクライアントのすべてを追跡します。

1. 2人のユーザ間で新しいIMセッションが開始されると、最初の着信メッセージが受信ユーザのすべての登録済みクライアントにブロードキャストされます。
2. その後で、IM and Presence サービス ノードが登録済みクライアントのいずれかからの最初の応答を待機します。
3. 最初に応答したクライアントは、ユーザが別の登録済みクライアントを使用して返信を開始するまで、着信メッセージの残りを受け取ります。
4. その後で、ノードが以降のメッセージをこの新しいクライアントに再ルーティングします。

（注） ユーザが複数のデバイスにログインするときにアクティブなリソースがない場合は、最も高い優先順位を持つクライアントが最優先されます。プレゼンスの優先順位がすべてのデバイスで同じ場合は、最後にユーザがログインしたクライアントが最優先されます。



第 4 章

サービス ディスカバリ

- クライアントがサービスに接続する方法 （77 ページ）
- クライアントがサービスを検出する方法 （81 ページ）
- 方法 1：サービスの検索 （83 ページ）
- 方法 2：カスタマイズ （98 ページ）
- 方法 3：手動インストール （100 ページ）
- 高可用性 （100 ページ）
- 設定のプライオリティ （103 ページ）
- [シスコ サポート フィールド（Cisco Support Field）] によるグループの設定 （103 ページ）

クライアントがサービスに接続する方法

Cisco Jabber は、サービスに接続するために次の情報を必要とします。

- ユーザがクライアントにログインをできるようにする認証ソース。
- サービスのロケーション。

次の方法でクライアントに情報を提供することが可能です。

URL 設定

ユーザには、管理者から電子メールが送信されます。電子メールには、サービスディスカバリに必要なドメインを設定する URL が含まれます。

サービス ディスカバリ

クライアントはサービスを自動的に検出して接続します。

手動接続設定

ユーザは、クライアント ユーザ インターフェイスで接続設定を手動で入力します。

Cisco Webex Platform サービス ディスカバリ

Cisco Jabber は、ユーザがチームのメッセージモードに対応しているかどうかを確認するために、HTTPS 要求を Cisco Webex Platform サービスに送信します。ユーザがチームメッセージングに対して有効になっている場合、Jabber は利用可能なオンプレミスのサービスを引き続きチェックします。

Cisco Webex Messenger Service Discovery

Cisco Jabber は Cisco Webex Messenger サービス用の CAS URL に対してクラウド HTTP 要求を送信します。Cisco Jabber は Cisco Webex Messenger サービスでユーザを認証し、使用可能なサービスに接続します。

サービスは Cisco Webex 管理ツールで設定されます。

シスコ クラスタ間検索サービス

Cisco Unified Communications Manager クラスタが複数存在する環境では、クラスタ間検索サービス（ILS）を設定します。ILS は、クライアントがユーザのホーム クラスタを検索して、サービスを検出できるようにします。

Expressway for Mobile and Remote Access サービス ディスカバリ

Expressway for Mobile and Remote Access は、リモート ユーザによるサービスへのアクセスを有効にします。

クライアントは、SRV レコードのネーム サーバを問い合わせます。`_collab-edge` SRV レコードでは、クライアントはExpressway for Mobile and Remote Access 経由で内部ネットワークに接続して、サービスを検出しようとします。

ネーム サーバは `_collab-edge` SRV レコードを返し、クライアントは Cisco Expressway-E サーバの場所を取得します。その後で、Cisco Expressway-E サーバが内部ネーム サーバに対するクエリの結果をクライアントに提供します。これは `_cisco-uds` SRV レコードに必ず含まれ、クライアントはCisco Unified Communications Manager からサービス プロファイルを受け取ります。

推奨される接続方式

サービスに接続するための必要情報をどのような方法でクライアントに提供するかは、展開タイプ、サーバのバージョン、製品モードによって異なります。次の表では、さまざまな導入方法とクライアントに必要な情報を提供する方法について詳しく示しています。

表 *3 :* 以下に対するオンプレミス展開 *Windows* 版 *Cisco Jabber*

製品モード	サーバのバージョン	検出方法	非 DNS SRV レコード法
フル UC（デフォルト モード）	リリース 9.1.2 以降： • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	_cisco-uds.<domain> に対する DNS SRV 要求	次のインストーラ スイッチと値を使用する。 • AUTHENTICATOR=CUP • CUP_ADDRESS=<presence_server_address>
IM 専用（デフォルト モード）	リリース 9 以降： Cisco Unified Communications Manager IM and Presence Service	_cisco-uds.<domain> に対する DNS SRV 要求	次のインストーラ スイッチと値を使用する。 • AUTHENTICATOR=CUP • CUP_ADDRESS=<presence_server_address>
電話モード	リリース 9 以降： Cisco Unified Communications Manager	_cisco-uds.<domain> に対する DNS SRV 要求	次のインストーラ スイッチと値を使用する。 • AUTHENTICATOR=CUCM • TFTP=<CUCM_address> • CCMCIP=<CUCM_address> • PRODUCT_MODE=phone_mode ハイ アベイラビリティ は、この展開の方法ではサポートされません。

Cisco Unified Communications Manager リリース 9.x 以前：Cisco Extension Mobility を有効にする場合は、CCMCIP に使用される Cisco Unified Communications Manager ノードで `Cisco Extension Mobility` サービスをアクティブにする必要があります。Cisco Extension Mobility の詳細については、使用している Cisco Unified Communications Manager のリリースに応じた『*Feature and Services*』ガイドを参照してください。

（注） Cisco Jabber リリース 9.6 以降では、引き続き `_cuplogin` DNS SRV 要求を使用して、完全な Unified Communications および IM 専用サービスを検出できますが、`_cisco-uds` 要求が提示された場合はその要求が優先されます。

更新インストールの最初のログイン時に電子メール画面をバイパスする場合は、SERVICES_DOMAINインストーラのスイッチを使用してDNSレコードが存在するドメインの値を指定します。

表 *4:* 以下に対するオンプレミス展開 *Mac* 版 *Cisco Jabber*

製品モード	サーバのバージョン	検出方法
フル UC（デフォルト モード）	リリース 9 以降： • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	`_cisco-uds.<domain>` に対する DNS SRV 要求

表 *5: Android* 版 *Cisco Jabber*と *iPhone* および *iPad* 版 *Cisco Jabber*に対するオンプレミス展開

製品モード	サーバのバージョン	検出方法
フルUC（デフォルトモード）	リリース 9 以降： • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	`_cisco-uds.<domain>` と `_cuplogin.<domain>` に対する DNS SRV 要求
IM専用（デフォルトモード）	リリース9以降： Cisco Unified Communications Manager IM and Presence Service	`_cisco-uds.<domain>` と `_cuplogin.<domain>` に対する DNS SRV 要求
電話機モード	リリース9以降： Cisco Unified Communications Manager	`_cisco-uds.<domain>`に対する DNS SRV 要求

（注） Cisco Unified Communications Managerバージョン 9 以降では、引き続き `_cuplogin` DNS SRV 要求を使用して、完全な Unified Communications および IM 専用サービスを検出できますが、`_cisco-uds` 要求が提示された場合はその要求が優先されます。

表 *6:* ハイブリッド クラウド ベースの展開

サーバのバージョン	接続方法
Cisco Webex Messenger	`https://loginp.webexconnect.com/cas/FederatedSSO?org=<domain>` に対する HTTPS 要求

サーバのバージョン	接続方法
Cisco Webex Platform サービス	atlas-a.wbx2.comに対するHTTPS 要求

表 7: クラウドベース展開

展開タイプ	接続方法
シングル サインオン（SSO）	Cisco Webex 管理ツール SSO_ORG_DOMAIN 引数を設定するためのブートストラップ ファイル。
SSO に対しては有効ではありません	Cisco Webex 管理ツール

認証ソース

認証ソースまたはオーセンティケータにより、ユーザはクライアントにログインすることができます。

次の 3 つの認証ソースを使用できます。

- Cisco Unified Communications Manager IM and Presence：フル UC または IM のみでのオンプレミス展開。
- Cisco Unified Communications Manager：電話機モードでのオンプレミス展開。
- Cisco Webex Messenger サービス—クラウドベースまたはハイブリッド クラウド ベースでの展開。
- Cisco Webex Platform サービスクラウドベースまたはハイブリッド クラウド ベースでの展開。

クライアントがサービスを検出する方法

次の手順は、クライアントが SRV レコードでサービスを検索する方法について説明しています。

1. クライアント ホスト コンピュータまたはデバイスがネットワーク接続を取得します。

   クライアントホストコンピュータは、ネットワーク接続を取得するときに、DHCP 設定から DNS（ドメイン ネーム システム）ネーム サーバのアドレスも取得します。

2. ユーザは最初のサイン イン時に、次のいずれかの方法でサービスを検出します。
   - 手動—ユーザは Cisco Jabber を起動し、初期画面で電子メール形式のアドレスを入力します。

- URL の設定：電子メールを手動で入力することなく、リンクをクリックして Cisco Jabber を相互起動できます。
- 企業モビリティ管理を使用してモバイル設定：URL 設定の代わりに、Android for Work（Cisco Jabber for Android の場合）または Apple Managed App Configuration（Cisco Jabber for iPhone and iPad の場合）と共に、企業モビリティ管理（EMM）を使用して Cisco Jabber を設定できます。URL 設定リンクの作成に使用される EMM コンソールで同じパラメータを設定する必要があります。

URL 設定リンクを作成するには、以下のパラメータを含めます。

- ServicesDomain：Cisco Jabber がサービス検出に使用するドメイン。
- VoiceServicesDomain：ハイブリッド展開の場合、Cisco Jabberが DNS SRV レコードの取得に使用するCisco Jabberドメインと、Cisco Jabber ドメインの検出に使用される ServicesDomain が異なることがあります。
- ServiceDiscoveryExcludedServices：特定の展開シナリオでは、サービスをサービス ディスカバリ プロセスから除外できます。これらの値は、次の組み合わせになります。
  - WEBEX
  - CUCM

（注） 3つのパラメータすべてを含めると、サービスディスカバリは実行されず、手動で接続設定を入力するように要求されます。

リンクを次の形式で作成します。

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
```

次に、例を示します。

- `ciscojabber://provision?servicesdomain=example.com`
- `ciscojabber://provision?servicesdomain=example.com &VoiceServicesDomain=VoiceServices.example.com`
- `ciscojabber://provision?servicesdomain=example.com &ServiceDiscoveryExcludedServices=WEBEX,CUCM`

電子メールまたは Web サイトを使用してユーザにリンクを提供します。

（注） 所属組織が相互起動専用プロトコルまたはカスタム リンクに対応したメール アプリケーションを使用している場合は、電子メールを使用してユーザにリンクを提供できます。使用していない場合は、Web サイトを使用してリンクを提供します。

3. クライアントは、DHCP 設定から DNS ネーム サーバのアドレスを取得します。
4. クライアントは、Cisco Webex Messengerサービスについて Central Authentication Service（CAS） URL に HTTP クエリを発行します。

   このクエリーによって、クライアントはドメインが有効な Cisco Webex ドメインかどうかを判定できます。
5. クライアントは、次の SRV レコードのネーム サーバを優先度順に問い合わせます。
   - _cisco-uds
   - _collab-edge

（注） DNS クエリーの結果をキャッシュに格納し、それ以降の起動時にロードします。

（注） DNS クエリーの結果をキャッシュに格納し、それ以降の起動時にロードします。

次は、SRV のレコード エントリの例です。

```
_cisco_uds._tcp.DOMAIN SRV service location:
 priority = 0
 weight = 0
 port = 8443
 svr hostname=192.168.0.26
```

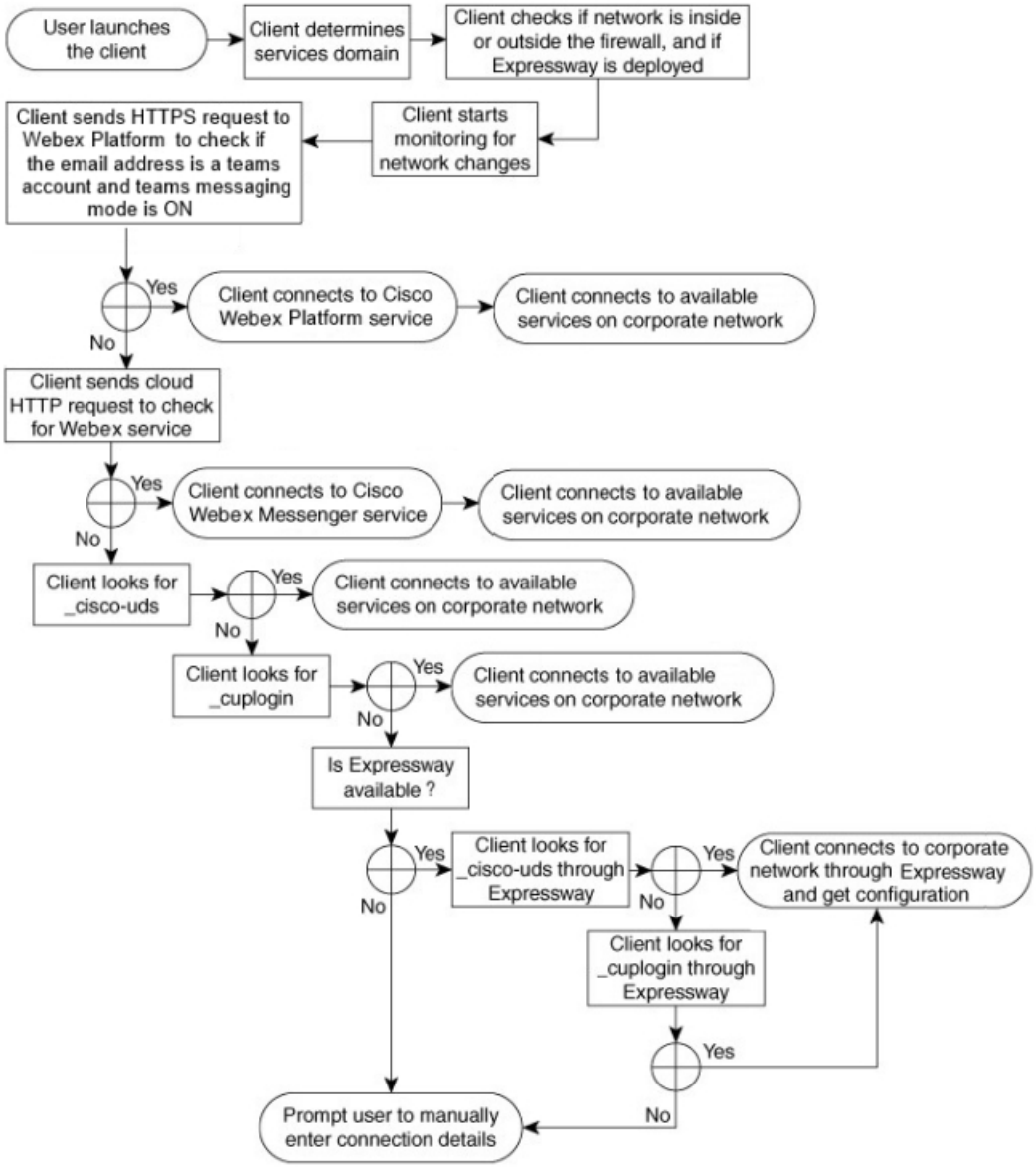
方法 1：サービスの検索

ユーザが使用可能なサービスや機能を Cisco Jabber が検出する方法として、この方式を使用することを推奨します。サービスの検索とは、クライアントがDNSサービス（SRV）レコードを使用して、使用可能なサービスを決定することです。

クライアントによる利用可能なサービスの検出方法

次の図は、クライアントがサービスへの接続に使用するフローを示しています。

図 *5:* サービス ディスカバリのログイン フロー



使用可能なサービスを検出するため、クライアントは次の処理を実行します。

1. ネットワークがファイアウォールの内側に存在するのか、外側に存在するのか、Expressway for Mobile and Remote Access が展開されているかどうかを確認します。ネーム サーバにクエリを送信して、DNS サービス（SRV）レコードを取得します。
2. ネットワーク変更のモニタを開始します。

   Expressway for Mobile and Remote Access が展開されている場合、クライアントはネットワークをモニタして、ネットワークがファイアウォールの内側または外側から切り替わったときに再接続できるようにします。

3. Jabber がチーム Cisco Webex Platform サービスメッセージモードになっているかどうかを確認するために、いくつかの HTTPS 要求を発行します。要求は、ユーザの電子メールアドレスをチェックして、そのユーザが Webex コントロールハブでチームメッセージングが有効になっているかどうかを確認します。

4. Cisco Webex Messenger サービスのため CAS URL に HTTP クエリーを発行します。

   このクエリーによって、クライアントはドメインが有効な Cisco Webex ドメインかどうかを判定できます。

   Expressway for Mobile and Remote Access を展開すると、クライアントはCisco Webex Messenger サービスに接続し、Expressway for Mobile and Remote Access を使用して Cisco Unified Communications Manager に接続します。クライアントが最初に起動すると、電話サービス接続エラーが表示され、クライアント オプション画面でクレデンシャルの入力が求められます。それ以降の起動ではキャッシュされた情報が使用されます。

5. 前回のクエリのキャッシュにDNS サービス（SRV）レコードがない場合、レコードの取得をネーム サーバにクエリーします。

   このクエリーによって、クライアントで次のことが可能になります。

   - どのサービスが利用可能なのかを判定する。
   - Expressway for Mobile and Remote Access 経由で企業ネットワークに接続できるかどうかを判断します。

クライアントが Cisco Webex Messenger Service向けの HTTP クエリを発行します。

使用可能なサービスを検出するために、SRV レコードのネーム サーバへ照会するのに加え、Cisco Jabber は HTTP クエリーに Cisco Webex Messenger の CAS URL を送信します。この要求によって、クライアントは、クラウドベースの導入が可能になり、Cisco Webex Messenger サービスへのユーザ認証が可能になります。

クライアントはユーザからサービス ドメインを取得すると、次の HTTP クエリーへのドメインに追加します。

```
https://loginp.webexconnect.com/cas/FederatedSSO?org=
```

たとえば、クライアントは `example.com` をそのユーザからのサービス ドメインとして取得した場合に、次のクエリーを発行します。

```
https://loginp.webexconnect.com/cas/FederatedSSO?org=example.com
```

クエリーは、サービス ドメインが有効な Cisco Webex ドメインであるかどうかを判定するためにクライアントが使用する XML 応答を返します。

クライアントがサービス ドメインを有効な Cisco Webex ドメインとして判定した場合、ユーザに Cisco Webex のクレデンシャルの入力を促します。その後、クライアントは Cisco Webex Messenger サービスから認証を受け、Cisco Webex Org Admin で設定された設定内容と UC サービスを取得します。

サービス ドメインが有効な Cisco Webex ドメインでないと判定した場合、利用可能なサービスの特定にネーム サーバへのクエリー結果を使用します。

CAS URL に HTTP 要求を送信するときに、クライアントは設定されているシステム プロキシを使用します。

詳細については、『*Cisco Jabber Deployment and Installation Guide*』の「*Configure Proxy Settings*」の項を参照してください。

クライアントからのネーム サーバのクエリー

クライアントがネーム サーバをクエリーする場合、ネーム サーバにそれぞれ独立した SRV レコードの要求を同時に送信します。

クライアントは、次の順序で以下の SRV レコードを要求します。

- `_cisco-uds`
- `_collab-edge`

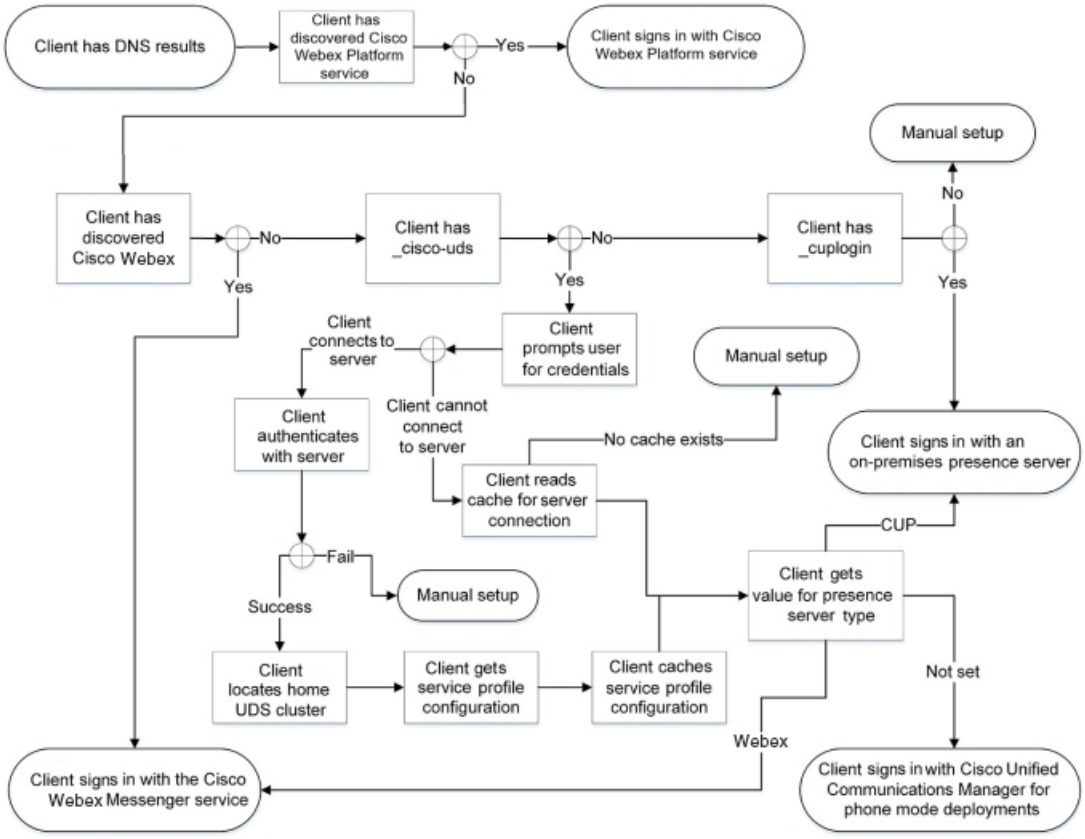
ネーム サーバが次を返した場合：

- `_cisco-uds`：クライアントは、それが企業ネットワーク内に存在することを検出し、Cisco Unified Communications Manager に接続します。
- `_collab-edge`：クライアントは、Expressway for Mobile and Remote Access 経由で内部ネットワークに接続して、サービスを検出しようとします。
- SRV レコードなし：クライアントは、ユーザにセットアップとサインインの詳細を手動で入力するように要求します。

クライアントの内部サービスへの接続

次の図は、クライアントが内部サービスに接続する仕組みを示しています。

図 *6 :* クライアントの内部サービスへの接続



内部サービスに接続する際の目標は、オーセンティケータを決定し、ユーザをサインインし、利用可能なサービスに接続することです。

サインイン画面から、ユーザは次のいずれかのサービスで認証されます。

- Cisco Webex Platform サービス—クラウドまたはハイブリッド展開。
- Cisco Webex Messenger サービス: クラウドまたはハイブリッド展開
- Cisco Unified Communications Manager電話モードでのオンプレミスの展開。

クライアントは検出するサービスに接続します。これは展開によって異なります。

1. クライアントがユーザのチームメッセージモードが有効化されている場合、クライアントは次の処理を実行します。
    1. Cisco Webex Platform サービス が認証のプライマリ ソースであると決定する。
    2. 自動的にCisco Webex プラットフォームサービスに接続されます。
    3. ユーザにクレデンシャルの入力を促す。
2. クライアントは、CAS URL 検索がCisco Webex ユーザを示していることを検出すると、次の処理を実行します。

1. Cisco Webex Messenger サービスを認証のプライマリ ソースと判定する。
2. 自動的に Cisco Webex Messenger サービスに接続する。
3. ユーザにクレデンシャルの入力を促す。
4. クライアント設定とサービス設定を取得する。

3. `_cisco-uds` SRV レコードを検出した場合、クライアントは次の処理を実行します。

   Cisco Unified Communications Manager での認証のためユーザにクレデンシャルの入力を促す。

   1. ユーザのホーム クラスタを特定する。

      ホーム クラスタの特定によって、クライアントは自動的にユーザのデバイス リストを取得し、Cisco Unified Communications Manager に登録することができます。

      複数の Cisco Unified Communications Manager クラスタがある環境では、クラスタ間検索サービス（ILS）が必要です。ILS を使用することで、クライアントはユーザのホーム クラスタの検出が可能になります。

重要 ILS の設定方法については、該当するバージョンの『*Cisco Unified Communications Manager Features and Services Guide*』を参照してください。

   2. サービス プロファイルを取得する。

      サービス プロファイルは、クライアントに対しオーセンティケータと、クライアントおよび UC サービスの設定を準備します。

      クライアントは、[プレゼンス プロファイル（IM and Presence Profile）] の [製品タイプ（Product type）] フィールドの値から、オーセンティケータを次のように決定します。

      - Cisco Unified Communications Manager—Cisco Unified Presence またはCisco Unified Communications Manager IM and Presence Serviceがオーセンティケータである。
      - Webex (IMおよびPresence)—Cisco Webex Messenger サービスがオーセンティケータである。authenticator.

（注） このリリースでは、クライアントは、SRV レコードのクエリーに加え、HTTP クエリーを発行します。HTTP クエリーは、クライアントが Cisco Webex Messenger サービスの認証を受けるかどうかを決定できるようにします。

HTTP クエリーの結果、クラウドベースの展開では、クライアントは Cisco Webex Messenger サービスに接続します。**製品タイプ（Product type）** フィールドの値を [Webex] に設定しても、クライアントが CAS ルックアップを使用してすでに Webex サービスを検出していた場合は、実質的な効果はありません。

- セットされていない-サービス プロファイルに IM およびプレゼンス サービスの設定を含めない場合は、Cisco Unified Communications Manager がオーセンティケータです。

3. オーセンティケータにサイン インします。

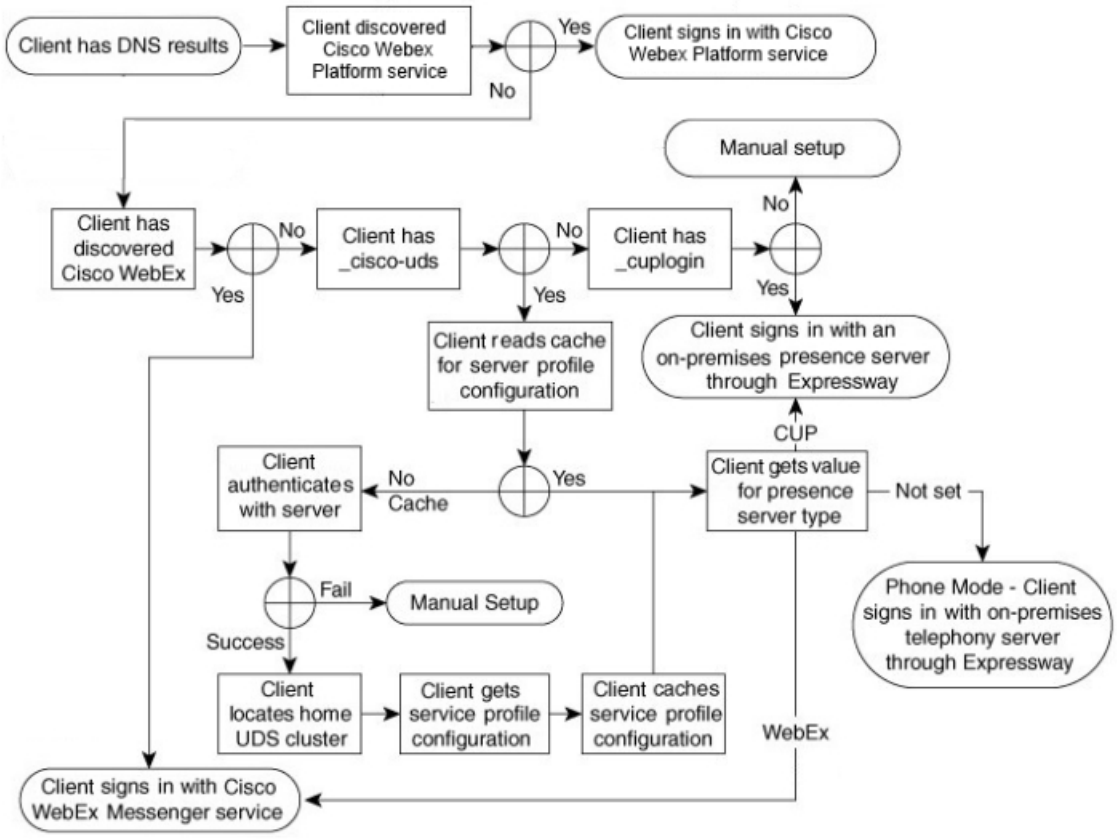
   クライアントにサインインした後、製品モードを判定できます。

Expressway for Mobile and Remote Access を介したクライアントの接続

ネーム サーバが `_collab-edge` SRV レコードを返した場合、クライアントは Expressway for Mobile and Remote Access 経由で内部サーバへの接続を試みます。

次の図は、Expressway for Mobile and Remote Access を介してネットワーク接続したときに、クライアントが内部サービスに接続する仕組みを示しています。

図 *7: Expressway for Mobile and Remote Access* を介したクライアントの接続



ネーム サーバが `_collab-edge` SRV レコードを返すと、クライアントは Cisco Expressway-E サーバの場所を取得します。その後で、Cisco Expressway-E サーバが内部ネーム サーバに対するクエリの結果をクライアントに提供します。

（注） Cisco Expressway-C サーバは内部 SRV レコードを検索し、Cisco Expressway-E サーバにそのレコードを提供します。

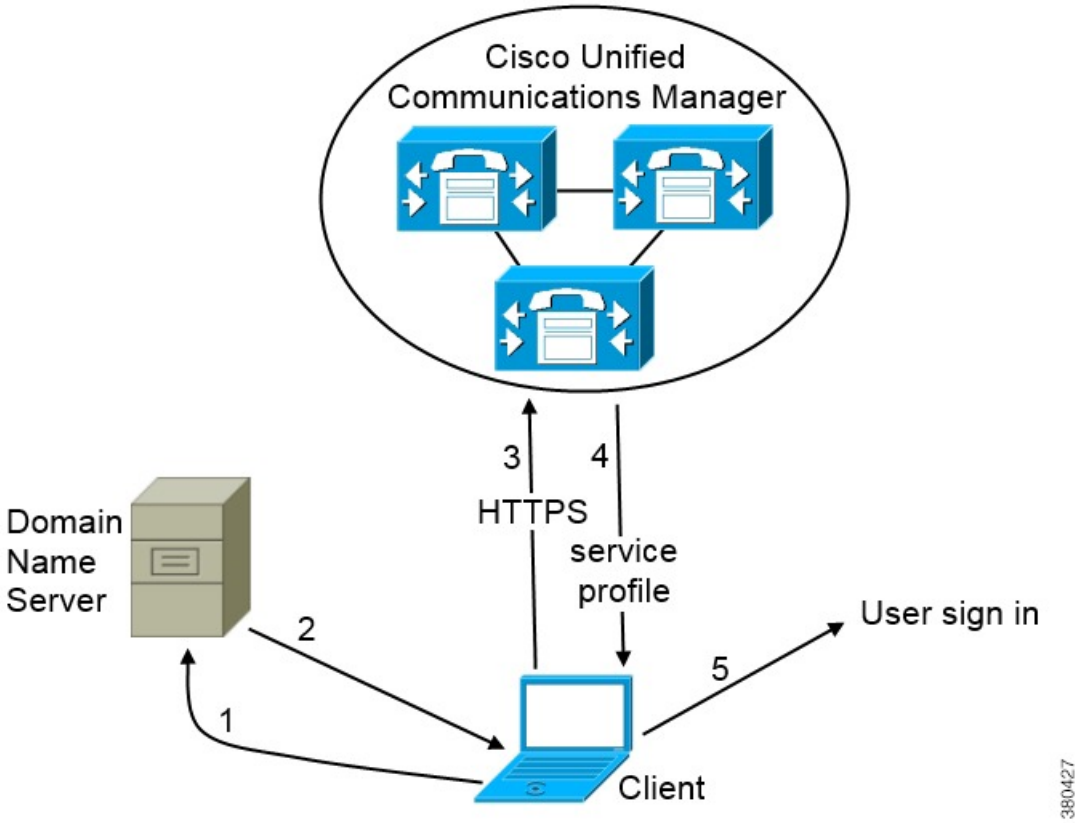
クライアントは、内部 SRV レコードを取得した後（必ず `_cisco-uds`SRV記録が含まれている）、Cisco Unified Communications Managerからサービス プロファイルを取得します。その後、サービス プロファイルはユーザのホーム クラスタ、認証のプライマリ ソース、および設定をクライアントに提供します。

Cisco UDS SRV レコード

Cisco Unified Communications Manager バージョン 9 以降の展開では、クライアントは `_cisco-uds` SRV レコードを使用してサービスと設定を自動的に検出できます。

次の図は、クライアントが `_cisco-uds` SRV レコードを使用する仕組みを示しています。

図 *8 : UDS SRV* レコードのログイン フロー



1. クライアントは、SRV レコードのドメイン ネーム サーバを問い合わせます。
2. ドメイン ネーム サーバが `_cisco-uds` SRV レコードを返します。
3. クライアントは、ユーザのホーム クラスタを検出します。

   その結果、クライアントはユーザのデバイス設定を取得し、自動的にテレフォニー サービスを登録できます。

重要 複数の Cisco Unified Communications Manager クラスタを使用した環境では、クラスタ間検索サービス（ILS）を設定することができます。ILS は、クライアントがユーザのホーム クラスタを検索して、サービスを検出できるようにします。

ILS を設定しない場合は、クラスタ間エクステンション モビリティ（EMCC）リモート クラスタの設定と同様に、リモート クラスタ情報を手動で設定する必要があります。リモート クラスタ設定の詳細については、『*Cisco Unified Communications Manager Features and Services Guide*』を参照してください。

4. クライアントはユーザのサービス プロファイルを取得します。

ユーザのサービス プロファイルには、UC サービスのアドレスと設定およびクライアント構成が含まれます。

また、クライアントはサービス プロファイルからオーセンティケータを決定します。

5. クライアントは、オーセンティケータにユーザをログインさせます。

次に、_cisco-uds SRV レコードの例を示します。

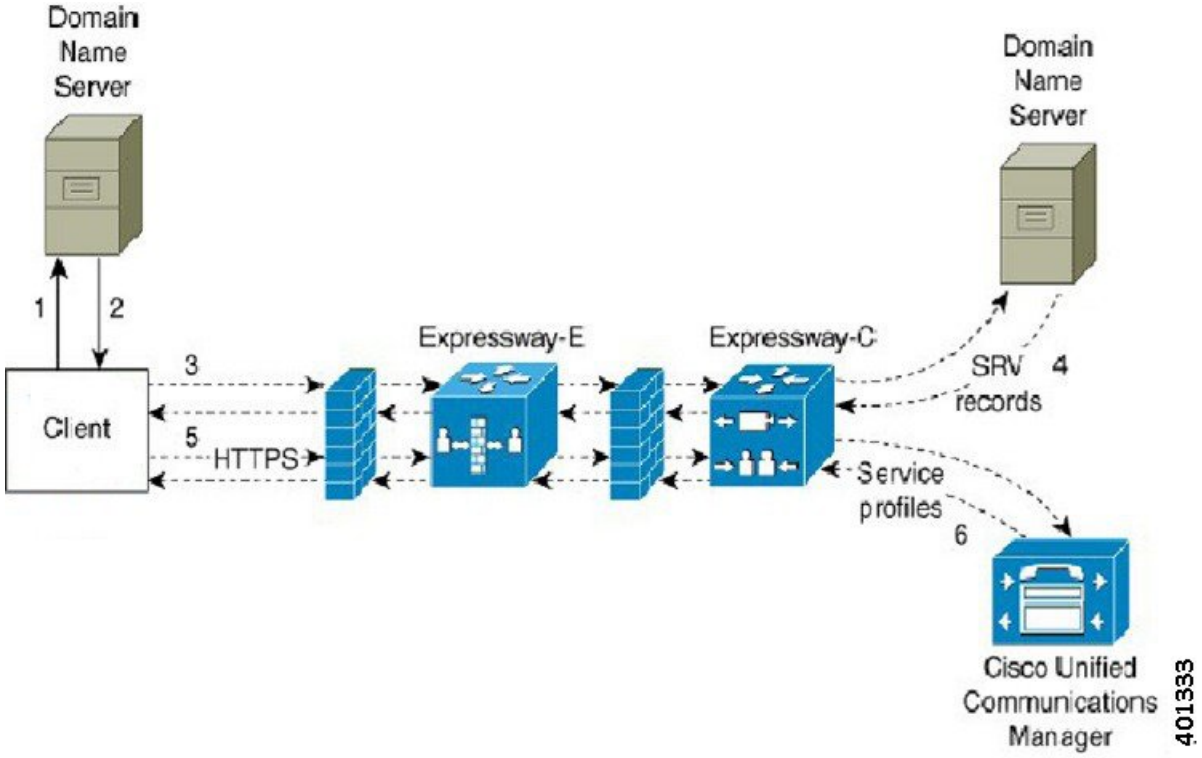
```
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 6
          weight         = 30
          port           = 8443
          svr hostname   = cucm3.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 2
          weight         = 20
          port           = 8443
          svr hostname   = cucm2.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 1
          weight         = 5
          port           = 8443
          svr hostname   = cucm1.example.com
```

Collaboration Edge SRV レコード

Cisco Jabber は、Expressway for Mobile and Remote Access 経由で内部サーバに接続し、以下の _collab-edgeSRV レコードを使用してサービスの検出を試みます。

次の図は、クライアントが _collab-edge SRV レコードを使用する仕組みを示しています。

図 *9 : Collaboration Edge* レコードのログイン フロー



1. クライアントは外部ドメイン ネーム サーバに SRV レコードについて問い合わせます。
2. ネーム サーバは、`_collab-edge` SRV レコードを返しますが、`_cuplogin` や `_cisco-uds` SRV レコードを返しません。

   その結果、Cisco Jabber は Cisco Expressway-E サーバを検出できます。
3. クライアントは、（Expressway 経由で）内部ドメイン ネーム サーバに内部 SRV レコード要求します。

   これらの SRV レコードには `_cisco-uds` SRV レコードが含まれている必要があります。
4. クライアントは、（Expressway 経由で）内部 SRV レコードを取得します。

   その結果、クライアントは Cisco Unified Communications Manager サーバを検出できます。
5. クライアントは、（Expressway 経由で）Cisco Unified Communications Manager にサービス プロファイルを要求します。
6. クライアントは（Expressway 経由で）Cisco Unified Communications Manager からサービス プロファイルを取得します。

   サービス プロファイルには、ユーザのホーム クラスタ、認証のプライマリ ソース、クライアント設定が含まれています。

DNS の設定

クライアントが DNS を使用する方法

Cisco Jabber は、ドメイン ネーム サーバを使用して次の内容を実行します。

- クライアントが社内ネットワークの内部か外部かを判定する。
- 社内ネットワーク内のオンプレミス サーバを自動的に検出する。
- パブリック インターネットで Expressway for Mobile and Remote Access 用のアクセス ポイントを検索する。

（注） Android OS の制限：DNS サービスを使用している Android OS 4.4.2 および 5.0 が解決できるのはドメイン名だけで、ホスト名は解決できません。

詳細については、「Android developer link」を参照してください。

クライアントがネーム サーバを検索する方法

Cisco Jabber は次の場所から DNS レコードを検索します。

- 社内ネットワーク内の内部ネーム サーバ。
- パブリック インターネット上の外部ネーム サーバ。

クライアントのホスト コンピュータまたはデバイスがネットワーク接続を取得すると、ホスト コンピュータまたはデバイスは DHCP 設定から DNS ネーム サーバのアドレスも取得します。ネットワーク接続によりますが、そのネーム サーバが社内ネットワークの内部の場合と外部の場合があります。

Cisco Jabber は、ホスト コンピュータまたはデバイスが DHCP 設定から取得するネーム サーバをクエリーします。

クライアントがサービス ドメインを取得する方法

サービス ドメインは、 クライアントによってさまざまな方法で検出されます。

新規インストール：

- クライアント ユーザ インターフェイスで `username@example.com` の形式でアドレスを入力。
- サービス ドメインを含む構成 URL をクリック。このオプションは、次のバージョンのクライアントでのみ使用できます。
  - Cisco Jabber for Android リリース 9.6 以降
  - Cisco Jabber for Mac リリース 9.6 以降
  - Cisco Jabber for iPhone and iPad リリース 9.6.1 以降

- クライアントが、ブートストラップ ファイルのインストール スイッチを使用。このオプションは、次のバージョンのクライアントでのみ使用できます。
  - Cisco Jabber for Windows リリース 9.6 以降

既存のインストール：

- クライアントが、キャッシュ設定を使用。
- ユーザが、クライアント ユーザ インターフェイスで、手動でアドレスを入力。

ハイブリッド展開では、Central Authentication Service（CAS）ルックアップによる Cisco Webex ドメインの検出で必要なドメインと、DNS レコードが配布されるドメインが異なる場合があります。このような場合は、Cisco Webex の検出に使用されるドメインとして ServicesDomain を設定し、DNS レコードが配布されるドメインとして VoiceServicesDomain を設定します。音声サービス ドメインは、次のように設定されます。

- クライアントが、設定ファイルの VoiceServicesDomain パラメータを使用。このオプションは、`Jabber config.xml` ファイルをサポートしているクライアントで使用できます。
- ユーザが、VoiceServicesDomain を含む構成 URL をクリック。このオプションは、次のクライアントで使用できます。
  - Cisco Jabber for Android リリース 9.6 以降
  - Cisco Jabber for Mac リリース 9.6 以降
  - Cisco Jabber for iPhone and iPad リリース 9.6.1 以降
- クライアントが、ブートストラップ ファイルの Voice_Services_Domain インストール スイッチを使用。このオプションは、次のバージョンのクライアントでのみ使用できます。
  - Cisco Jabber for Windows リリース 9.6 以降

Cisco Jabber はサービス ドメインを取得した後、クライアント コンピュータまたはデバイスに設定されているネーム サーバをクエリします。

ドメイン ネーム システムの設計

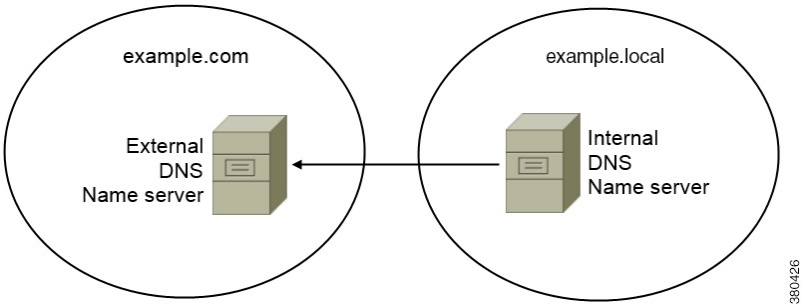
DNS サービス（SRV）レコードの導入場所は、DNS ネームスペースの設計に依存します。通常、2 種類の DNS 設計があります。

- 社内ネットワークの内外で独立したドメイン名。
- 社内ネットワークの内外で同一のドメイン名。

独立ドメイン設計

次の図は、独立ドメイン設計を示しています。

図 *10* : 独立ドメイン設計



独立ドメインの一例として、組織が example.com を外部ドメインとしてインターネット名前登録機関に登録したとします。

会社はまた、次のいずれかの内部ドメインも使用します。

- 外部ドメインのサブドメイン。example.local など。
- 外部ドメインと異なるドメイン。exampledomain.com など。

独立ドメイン設計には、次の特性があります。

- 内部ネーム サーバには、内部ドメインのリソース レコードを含むゾーンがあります。内部ネーム サーバには、内部ドメインに対する権限があります。
- 内部ネーム サーバは、DNS クライアントが外部ドメインをクエリーすると、要求を外部ネーム サーバへ転送します。
- 外部ネーム サーバには、組織の外部ドメインのリソース レコードを含むゾーンがあります。外部ネーム サーバには、そのドメインに対する権限があります。
- 外部ネーム サーバは、要求を他の外部ネーム サーバに転送できます。ただし、外部のネーム サーバは内部ネーム サーバに要求を転送できません。

独立ドメイン構造での *SRV* レコード導入

独立ネーム設計では、内部ドメインと外部ドメインの2つのドメインがあります。クライアントは、サービス ドメインで SRV レコードをクエリーします。内部ネーム サーバがサービス ドメインのレコードを扱う必要があります。しかし、独立ネーム設計では、サービス ドメイン用のゾーンが内部ネーム サーバにない可能性があります。

サービス ドメインが内部ドメイン ネーム サーバで現在扱われていない場合、次のように処理できます。

- サービス ドメイン用の内部ゾーンにレコードを導入する。
- 内部ネーム サーバ上のピンポイント サブドメイン ゾーンにレコードを導入する。

サービス ドメインへの内部ゾーンの使用

内部ネーム サーバにサービス ドメイン用のゾーンがまだない場合、作成できます。この方式では、内部ネーム サーバにサービス ドメインに対する権限を持たせます。内部ネーム サーバは権限を持っているので、他のネーム サーバにクエリーを転送しません。

この方式は、ドメイン全体のフォワーディング関係を変え、内部 DNS 構造を混乱させることがあります。サービス ドメインの内部ゾーンを作成できない場合、内部ネーム サーバにピンポイント サブドメイン ゾーンを作成できます。

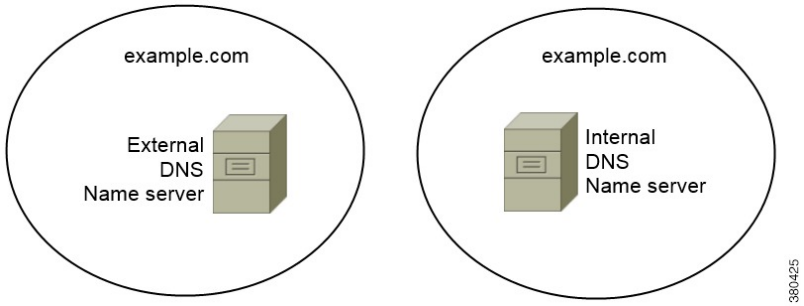
同一ドメイン設計

同一ドメインの設計の例として、組織が`example.com`を外部ドメインとしてインターネット名前登録機関に登録しているとします。組織は`example.com`を内部ドメイン名としても使用します。

単一ドメイン（スプリット ブレイン）

次の図は、スプリット ブレイン ドメインがある単一ドメイン設計を示しています。

図 *11* : 単一ドメイン（スプリット ブレイン）



2 つの DNS ゾーンが同一のドメインを表します。内部ネーム サーバ内の DNS ゾーンと外部ネーム サーバ内の DNS ゾーンです。

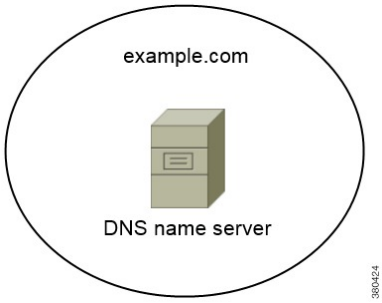
内部ネーム サーバと外部ネーム サーバは、どちらも単一ドメインに対して権限がありますが、異なるホスト コミュニティに対応します。

- 社内ネットワーク内のホストは、内部ホスト ネーム サーバだけにアクセスします。
- パブリック インターネットのホストは、外部ネーム サーバだけにアクセスします。
- 社内ネットワークとパブリック インターネットを行き来するホストは、時によって異なるネーム サーバにアクセスします。

単一ドメイン（非スプリット ブレイン）

次の図は、スプリット ブレイン ドメインがない単一ドメイン設計を示しています。

図 *12：*単一ドメイン（非スプリット ブレイン）



単一ドメイン（非スプリットブレイン）設計では、内部および外部ホストは1セットのネームサーバとして扱われ、同じ DNS 情報にアクセスできます。

重要　この設計は、内部ネットワークに関する多くの情報を公開し攻撃にさらすことになるため、一般的ではありません。

方法 2：カスタマイズ

インストール パラメータ、URL の設定、または企業モビリティ管理を使用してサービス検出をカスタマイズできます。

サービス ディスカバリのカスタマイズ

Cisco Jabber for Windows のカスタム インストール

Cisco Jabber for Windows は、次のように使用可能な MSI インストール パッケージを提供します。

- コマンド ラインを使用する：コマンド ライン ウィンドウで引数を指定して、インストール プロパティを設定できます。

  複数のインスタンスをインストールする場合は、このオプションを選択します。

- MSI を手動で実行する：クライアントの起動時に、クライアント ワーク ステーションのファイル システム上で MSI を手動で実行してから、接続プロパティを指定します。

  テストまたは評価用に単一インスタンスをインストールする場合は、このオプションを選択します。

- カスタム インストーラを作成する：デフォルト インストール パッケージを開いて、必要なインストール プロパティを指定してから、カスタム インストール パッケージを保存します。

同じインストール プロパティを持つインストール パッケージを配布する場合は、このオプションを選択します。

- グループ ポリシーを使用して展開する：同じドメイン内の複数のコンピュータにクライアントをインストールします。

インストーラ スイッチ :Cisco Jabber for Windows

Cisco Jabber をインストールすると、オーセンティケータおよびサーバ アドレスを指定できます。インストーラは、ブートストラップ ファイルにこれらの詳細を保存します。ユーザがクライアントを初めて起動した際に、ブートストラップ ファイルを読み取ります。サービス ディスカバリが展開されている場合は、ブートストラップ ファイルが優先されます。

ブートストラップ ファイルは、サービス ディスカバリが展開されていない場合やユーザに手動で自分の接続設定を指定させたくない場合に、サービス ディスカバリのフォールバック メカニズムを提供します。

クライアントは、最初に起動したときのみ、ブートストラップ ファイルを読み取ります。クライアントは、最初の起動後にサーバ アドレスと設定をキャッシュし、以降の起動ではキャッシュからロードします。

Cisco Unified Communications Managerリリース 9.x 以降を使用したオンプレミス展開では、ブートストラップ ファイルを使用せず、代わりに、サービス ディスカバリを使用することをお勧めします。

Cisco Jabber for Mac/iPhone and iPad/Android のカスタム インストール

URL 設定を使用して、Cisco Jabber for Mac またはモバイル クライアントのカスタム インストールを作成できます。モバイル クライアントの場合、エンタープライズ モビリティ管理も使用できます。これらのカスタム インストールは、サービスを有効化するインストール パラメータによって異なります。

URL 設定

ユーザが手動でサービス ディスカバリ情報を入力しなくても Cisco Jabber を起動できるようにするには、構成 URL リンクをユーザに配布してクライアントをインストールするようにします。

電子メールで直接、ユーザにリンクを送信するか、Web サイトにリンクを掲載することで、ユーザに構成 URL リンクを提供します。

企業モビリティ管理によるモバイルの設定

企業モビリティ管理（EMM）を使用して、Cisco Jabber for Android や Cisco Jabber for iPhone and iPad に Cisco Jabber を設定できます。EMM の設定の詳細については、EMM プロバイダーから提供される管理者用の説明書を参照してください。

Jabber をマネージド デバイスでのみ実行する場合、証明書ベースの認証を展開し、EMM を使用してクライアント証明書を登録できます。

EMMの展開方法の詳細については、*Cisco Jabber*向けオンプレミス展開内の*Cisco Jabber*アプリケーションの展開、または*Cisco Jabber*向けクラウドとハイブリッド展開のセクションを参照してください。

方法 3：手動インストール

詳細オプションとして、サインイン画面でサービスに手動で接続できます。

高可用性

インスタント メッセージおよびプレゼンスのハイ アベイラビリティ

ハイ アベイラビリティとは、インスタント メッセージおよびプレゼンス サービスに対してフェールオーバー機能を提供するために複数のノードがサブクラスタに存在する環境を意味します。サブクラスタ内の1つのノードが利用できなくなった場合、インスタントメッセージおよびプレゼンスがそのノードからサブクラスタ内の別のノードにフェールオーバーします。このようにして、ハイ アベイラビリティにより、Cisco Jabber のインスタント メッセージおよびプレゼンス サービスの信頼できる継続性が保証されます。

ハイ アベイラビリティは LDAP でサポートされています。UDS 連絡先ソースを使用する場合は、ハイ アベイラビリティはサポートされません。

Cisco Jabber は、次のサーバを使用したハイ アベイラビリティをサポートします。

Cisco Unified Communications Manager IM and Presence Service リリース 9.0 以降

ハイ アベイラビリティの詳細については、次の Cisco Unified Communications Manager IM and Presence Service のドキュメントを使用します。

『Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager』

「High Availability Client Login Profiles」

「Troubleshooting High Availability」

フェールオーバー中の保留状態アクティブ コール

Cisco Unified Communications Manager のプライマリ インスタンスからセカンダリ インスタンスへのフェールオーバーが発生した場合、アクティブ コールを保留状態にすることはできません。

クライアントのハイ アベイラビリティ

フェールオーバー中のクライアントの動作

ハイ アベイラビリティがサーバに設定されている場合、プライマリ サーバがセカンダリ サーバにフェールオーバー後、クライアントは最大1分間プレゼンス ステータスを一時的に失います。サーバに再ログインを試行する前にクライアントが待機する時間を定義するため、再ログイン パラメータを設定します。

ログイン パラメータの設定

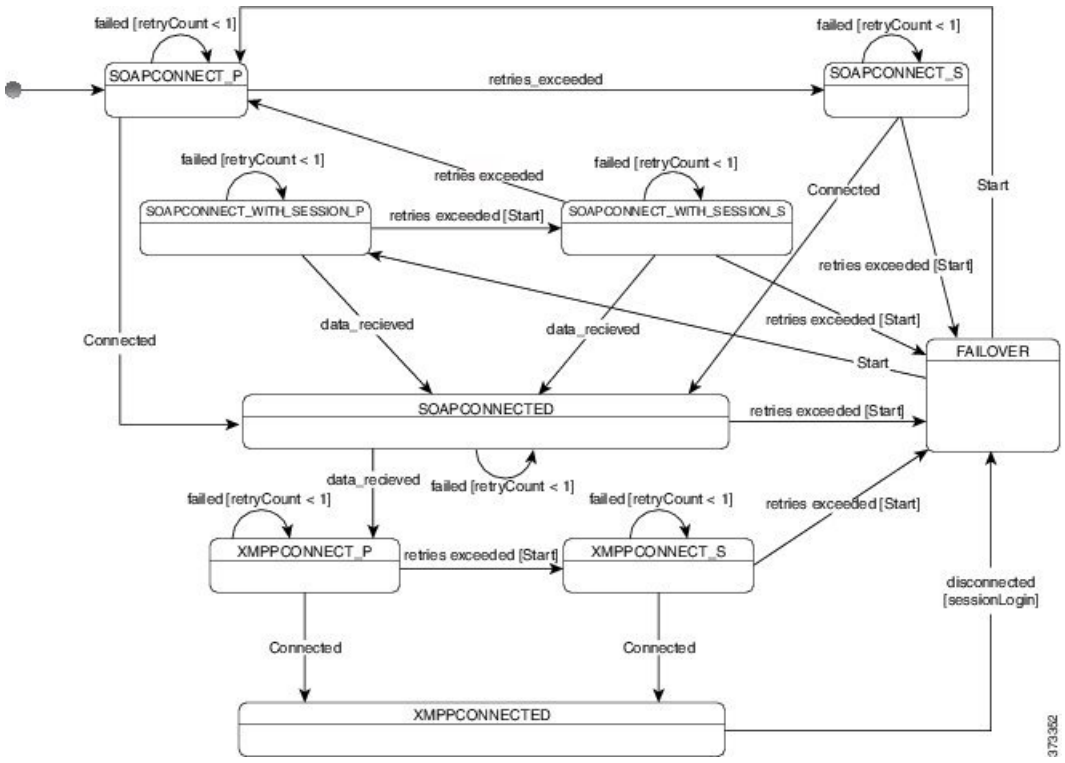
Cisco Unified Communications Manager IM and Presence サービスでは、Cisco Jabber がサーバへの再ログインを試みるまでに待機する最大秒数と最小秒数を設定できます。サーバで、次のフィールドに再ログイン パラメータを指定します。

- **クライアントの再ログインの下限（Client Re-Login Lower Limit）**
- **クライアントの再ログインの上限（Client Re-Login Upper Limit）**

フェールオーバー中のクライアントの動作

次の図は、Cisco Unified Communications Manager IM and Presence サービスがフェールオーバーした場合のクライアントの動作を示しています。

図 *13 :* フェールオーバー中のクライアントの動作



1. クライアントがアクティブ サーバから切断されると、クライアントはXMPPCONNECTED状態から FAILOVER 状態になります。

2. FAILOVER 状態から、クライアントは（プライマリ サーバとして）SOAPCONNECT_SESSION_P を試み、それが失敗すると、（セカンダリ サーバとして）SOAPCONNECT_SESSION_S を試みることによって、SOAPCONNECTED 状態に移行しようとします。
   - SOAPCONNECT_SESSION_P または SOAPCONNECT_SESSION_S に移行できなかった場合は、クライアントが再び FAILOVER 状態になります。
   - FAILOVER 状態から、クライアントは SOAPCONNECT_P 状態に移行しようとし、それが失敗すると、SOAPCONNECT_S 状態に移行しようとします。
   - クライアントが SOAPCONNECT_P または SOAPCONNECT_S 状態に移行できなかった場合は、ユーザがログイン試行を開始するまで、それ以上 IM&P サーバへの自動接続を試みません。
3. SOAPCONNECT_SESSION_P、SOAPCONNECT_SESSION_S、SOAPCONNECT_P、または SOAPCONNECT_S 状態から、クライアントは現在のプライマリ セカンダリ XMPP サーバアドレスを取得します。このアドレスはフェールオーバー中に変化します。
4. SOAPCONNECTED 状態から、クライアントは XMPPCONNECT_P 状態に接続することによって XMPPCONNECTED 状態に移行しようとし、それが失敗すると、XMPPCONNECT_S 状態を試みます。
   - クライアントが XMPPCONNECT_P または XMPPCONNECT_S 状態に移行できなかった場合は、ユーザがログイン試行を開始するまで、それ以上 IM&P サーバへの自動接続を試みません。
5. クライアントが XMPPCONNECTED 状態に移行すると、IM&P 機能を使用できます。

音声およびビデオのハイ アベイラビリティ

サブクラスタ内の 1 つのノードが利用できなくなった場合、音声およびビデオはそのノードからサブクラスタ内の別のノードにフェールオーバーします。

デフォルトでは、ソフトフォンデバイスまたはデスクフォンが別のノードに登録されるまで最大 120 秒かかります。このタイムアウト間隔が長すぎる場合、ノードの SIP Station KeepAlive Interval サービス パラメータの値を調整します。SIP Station KeepAlive Interval サービス パラメータは、 Cisco Unified Communications Manager のすべての電話機を変更します。間隔を調整する前に、Cisco Unified Communications Manager サーバへの影響を分析します。

ノードのサービス パラメータを設定するには、Cisco Unified Communications Manager 管理で**システム** > **サービスパラメータ**を使用します。

非 DNS SRV レコード法での電話モード展開では、Cisco Unified Communications Manager ノードが 1 つしか指定されていないため、音声およびビデオはフェールオーバーできません。

パーシステント チャットの高可用性

パーシステント チャットの高可用性をサポートしています。フェールオーバーのウィンドウで、メッセージを送信できないと表示されることがあります。ノードのフェールオーバー時、ユーザは自動的にチャット ルームに再接続され、メッセージを送信できます。

連絡先検索と連絡先の解決策の高可用性

Cisco ユニファイドコミュニケーションマネージャーのユーザデータサービス (UDS) によって提供される連絡先検索と連絡先解決では、高可用性がサポートされています。プライマリ UDS サーバが使用できない場合、Jabber は 2 台目の UDS サーバに自動的にフェールオーバーするか、設定されている場合は 3 台目の UDS サーバにフェールオーバーされます。

ボイスメールの高可用性

セカンダリ ボイスメール サーバが設定されると、プライマリ サーバが使用不能または到達不能になった場合には、すべてのクライアントが自動的にセカンダリ ボイスメール サーバへフェールオーバーします。

設定のプライオリティ

次の表は、サービス プロファイルとコンフィギュレーション ファイルの両方が存在する場合に優先されるパラメータ値を示しています。

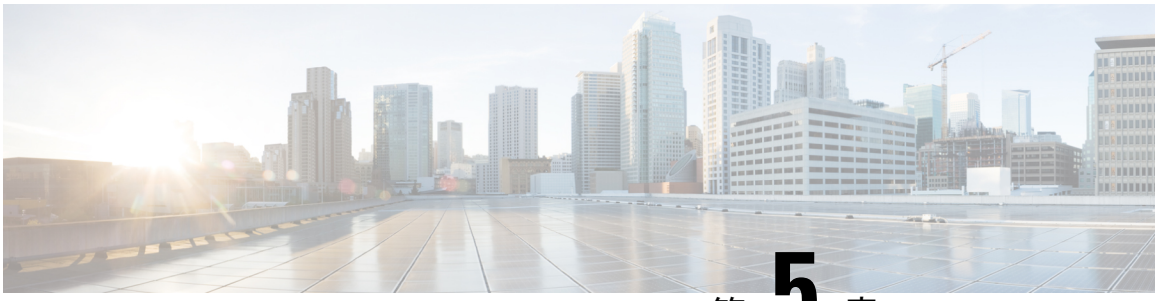
サービス プロファイル	設定ファイル	優先されるパラメータ値
パラメータ値が設定済み	パラメータ値が設定済み	サービス プロファイル
パラメータ値が設定済み	パラメータ値が空白	サービス プロファイル
パラメータ値が空白	パラメータ値が設定済み	設定ファイル
パラメータ値が空白	パラメータ値が空白	サービス プロファイルの空白（デフォルト）値

[シスコ サポート フィールド（Cisco Support Field）] によるグループの設定

グループ設定ファイルは、ユーザのサブセットに適用されます。CSF のデバイスを持つユーザをプロビジョニングする場合、デバイス設定で [シスコ サポート フィールド（Cisco Support Field）] フィールドにグループ設定ファイル名を指定できます。ユーザが CSF デバイスを所有

していない場合は、インストール中に TFTP_FILE_NAME 引数を使用してグループごとに一意の設定ファイル名を設定できます。

グループ設定は、14122 バージョン以降のCOP ファイルを備えた TCT および BOT でサポートされます。



第 5 章

連絡先ソース

- 連絡先ソースとは （105 ページ）
- 連絡先ソースが必要な理由 （106 ページ）
- 連絡先の送信元サーバを設定するタイミング （106 ページ）
- Cisco Directory Integration 向け連絡先ソースのオプション。 （107 ページ）
- LDAP の前提条件 （115 ページ）
- Jabber ID 属性マッピング （116 ページ）
- ローカル連絡先ソース （117 ページ）
- カスタム連絡先ソース （117 ページ）
- 連絡先のキャッシュ （117 ページ）
- 重複する連絡先の解決 （117 ページ）
- ダイヤル プランのマッピング （118 ページ）
- Cisco Unified Communication Manager UDS for Mobile and Remote Access （118 ページ）
- クラウドの連絡先ソース （119 ページ）
- 連絡先の写真の形式と寸法 （119 ページ）

連絡先ソースとは

連絡先ソースとはユーザに関するデータの集合です。ユーザが連絡先を検索したり、Cisco Jabber クライアントに連絡先を追加するときに、連絡先ソースから連絡先情報が読み取られます。

Cisco Jabber は連絡先ソースから連絡先情報を取り出して連絡先リストに入力し、クライアントの連絡先カードと連絡先情報を表示する他の領域を更新します。インスタントメッセージや音声/ビデオ コールなどの着信をクライアントが受信したときに、連絡先ソースを使用して連絡先情報が解決されます。

連絡先ソースサーバー

（注） Jabber のすべてのクライアントで、ディレクトリ統合の LDAPv3 標準がサポートされます。この標準をサポートするディレクトリ サーバは、次のクライアントと互換性があります。

Cisco Jabberで、次の連絡先ソースサーバーを使用できます:

- Active Directory Domain Services for Windows Server 2012 R2
- Active Directory Domain Services for Windows Server 2008 R2
- Cisco Unified Communications Managerユーザデータサーバ(UDS)Cisco Jabberは、Cisco Unified Communications Managerのバージョン 10.5以降を使用して UDS をサポートします。
- OpenLDAP
- Active Directory ライトウェイト ディレクトリ サービス（AD LDS）または Active Directory アプリケーション モード（ADAM）

連絡先ソースが必要な理由

Cisco Jabber は連絡先ソースを次のように使用します。

- 連絡先のユーザの検索：クライアントは入力された情報を取得して、連絡先ソースを検索します。情報は連絡先ソースから取得され、クライアントはその連絡先とやり取りするために使用可能な方法を表示します。
- クライアントが着信通知を受信：クライアントは着信通知から情報を取得して、URI 番号を解決し、連絡先ソースから連絡先と JabberID を取得します。クライアントはアラートに連絡先の詳細を表示します。

連絡先の送信元サーバを設定するタイミング

（注） Active Directory ドメインに登録されているワークステーションにCisco Jabber をインストールします。この環境では、Cisco Jabber をディレクトリに接続するように設定する必要がありません。クライアントはディレクトリを自動的に検出し、そのドメイン内のグローバルカタログ サーバに接続します。

次のいずれかのサービスを連絡先ソースとして使用する場合は、Cisco Jabber をディレクトリ サービスに接続するように設定します。

- Active Directoryサービス

- Cisco Unified Communications Manager User Data Service
- OpenLDAP
- Active Directory ライトウェイト ディレクトリ サービス
- Active Directory Application Mode; Active Directory アプリケーション モード

オプションで、次のようにディレクトリ統合を設定できます。

- デフォルト属性マッピングを変更します。
- ディレクトリのクエリー設定を調整します。
- クライアントが連絡先写真を取得する方法を指定します。
- イントラドメイン フェデレーションを実行します。

Cisco Directory Integration 向け連絡先ソースのオプション。

オンプレミス展開では、クライアントがユーザ情報のディレクトリ検索を解決するために次の連絡先ソースのいずれかを要求します。

- Lightweight Directory Access Protocol（LDAP）：社内ディレクトリがある場合は、次のLDAPベースの連絡先ソース オプションを使用してディレクトリを連絡先ソースとして設定できます。
  - Ciscoディレクトリ統合（CDI）：すべてのクライアントを展開する場合に、この連絡先ソース オプションを使用します。
- Cisco Unified Communications Manager User Data Service(UDS)：社内ディレクトリがない場合、または展開に Expressway Mobile and Remote Access と接続しているユーザが含まれている場合は、このオプションを使用できます。

軽量ディレクトリ アクセス プロトコル

Cisco Directory IntegrationがLDAPと協力する方法

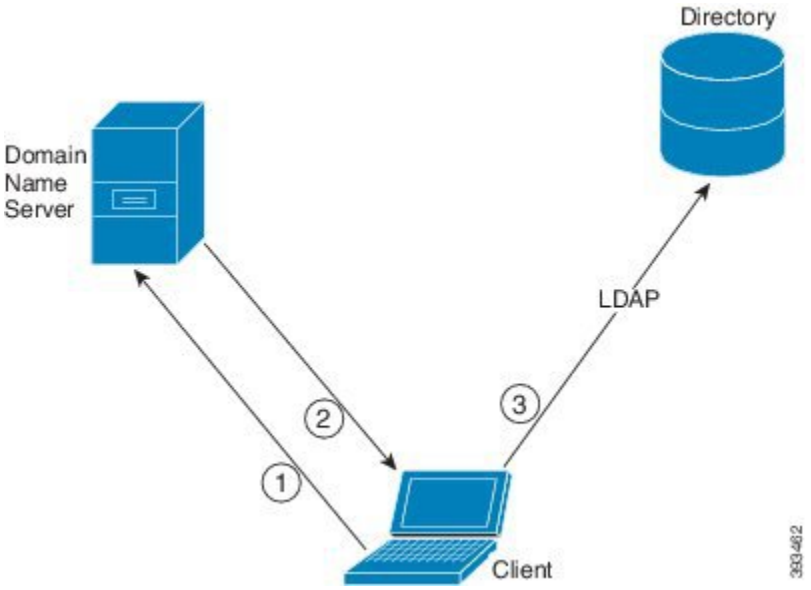
CDI はサービス検出を使用して LDAP サーバを決定します。

CDI を使用したオンプレミス展開用のデフォルト設定は次のとおりです。

- Cisco Jabber は連絡先ソースとして Active Directory と統合します。
- Cisco Jabber は自動的にグローバル カタログを検出して接続します。

自動サービス検出: 推奨

サービス検出を使用し、グローバルカタログ (GC) サーバまたはLDAP サーバに自動的に接続および認証することをお勧めします。展開をカスタマイズする場合は、LDAP サーバ情報を提供するオプションと使用可能な認証オプションを確認します。Jabber は最初に GC ドメインに DNS クエリを送信して GC サーバを検出します。GC サーバが検出されない場合、Jabber は ldap ドメインに DNS クエリを送信して LDAP サーバを検出します。



GC がある場合、クライアントは次のように実行します。

1. DNS ドメインをワークステーションから取得し、GC の SRV レコードを検索します。
2. SRV レコードから GC のアドレスを取得します。
3. ログインしているユーザのクレデンシャルで GC に接続します。

グローバルカタログドメインを使用した探索

Jabber は、DNS SRV クエリを使用して GC サーバを検出しようとします。まず、Jabber は GC ドメインを取得します。

1. 利用可能な場合、Jabber はGCドメインとしてDNSFORESTNAME環境変数を使用します。
2. DNSFORESTNAMEが利用できない場合、JABBER は GC ドメインについて次のことを確認します。
   - Windows では、Jabber は Windows `DsGetDcName` API を呼び出して、`DnsForestName`を取得します。
   - Windows 以外のプラットフォームでは、Jabberはjabber-configを`LdapDNSForestDomain`から読み取ります。

Jabber は GC ドメインを取得すると、次のように DNS SRV クエリを送信して GC サーバアドレスを取得します。

- Windows では、Jabber は`SiteName`が Windows `DsGetSiteName` API を通じて利用可能かどうかを確認します。
  - `SiteName`が存在する場合、JABBER は DNS SRV クエリを送信して、`_gc _tcp` を送信します。`_Sites`。`GCDomain`は、GC サーバアドレスを取得します。
  - `SiteName`が存在しない場合、または`_gc._tcp.SiteName._sites.GCDomain`に対して SRV レコードが返されない場合、Jabber は DNS SRV クエリ _gc を`_gc._tcp.GCDomain`に送信し、GC サーバアドレスを取得します。
- Windows 以外のプラットフォームでは、Jabber は DNS SRV クエリ`_gc._tcp.GCDomain`を送信して、GC サーバアドレスを取得します。

LDAP ドメインを使用した検出

Jabber が GC サーバを検出できない場合は、次のようにして LDAP ドメインを検出します。

1. 利用可能な場合、Jabber は LDAP ドメインとしてUSERDNSDOMAIN 環境変数を使用します。
2. USEDNSDOMAINが利用できない場合、jabber はLdapUserDomainを`jabber-config.xml`から読み取ります。
3. LdapUserDomainが利用できない場合、jabber は、ユーザが LDAP ドメインとしてログインに使用した電子メールドメインを使用します。

Jabber がLDAP ドメインを取得すると、次のように DNS SRV クエリを送信して LDAP サーバアドレスを取得します。

- Windows では、Jabber は、 SiteName が Windows `DsGetSiteName` API を介して利用可能かどうかを確認します。
  - `SiteName` が存在する場合、Jabber は DNS SRV クエリ`_ldap._tcp.SiteName.sites.LdapDomain`を送信して、LDAP サーバアドレスを取得します。
  - `SiteName`が存在しない場合、または `_ldap._tcp.SiteName.sites.LdapDomain`に対して SRV レコードが返されない場合、Jabber は DNS SRV クエリを送信し、`_ldap._tcp.LdapDomain`LDAP サーバアドレスを取得します。
- Windows 以外のプラットフォームでは、Jabber は DNS SRV クエリを送信して、`_ldap._tcp.LdapDomain`LDAP サーバアドレスを取得します。

Jabber が LDAP サーバに接続したら、使用する認証メカニズムのリストと順序が指定された `SupportedSaslMechanisms` 属性を読み取ります。

LDAPサービスに対する手動設定

LDAPサービスに対する手動設定

1. PrimaryServerName パラメータを設定すると、Jabber が接続する特定の LDAP サーバを定義できます。
2. `jabber-config.xml` ファイルの LdapSupportedMechanisms パラメータを設定すると、supportedSaslMechanisms 属性のリストを上書きできます。

   連絡先サービスとLDAPサーバーは、これらメカニズムのそれぞれをサポートする必要があります。複数の値はスペースで区切ります。

   • GSSAPI – Kerberos v5

   • EXTERNAL – SASL external

   • PLAIN（デフォルト）–LDAP シンプル バインド。匿名はシンプル バインドの一部です。

   例：

   ```
   <LdapSupportedMechanisms>GSSAPI EXTERNAL PLAIN</LdapSupportedMechanisms>
   ```
3. 必要であれば、Jabber が LDAP サーバの認証に使用するドメインを設定するために、LdapUserDomain パラメータを設定してください。次に例を示します。

   ```
   CUCMUsername@LdapUserDomain
   ```

LDAP の考慮事項

基本ディレクトリ統合（BDI）と拡張ディレクトリ統合（EDI）の各パラメータは、Cisco ディレクトリ統合（CDI）パラメータに置き換えられます。CDI パラメータはすべてのクライアントに適用されます。

Cisco Jabberの展開シナリオ

シナリオ 1：Jabber 11.8 を初めて使用する場合

サービス検出を使用し、LDAP サーバに自動的に接続および認証することをお勧めします。展開をカスタマイズする場合は、LDAP サーバ情報を提供するオプションと使用可能な認証オプションを確認します。

シナリオ 2：EDI 設定から 11.8 にアップグレードする場合

EDI パラメータのみを使用する設定の場合、Jabber は EDI パラメータを読み取り、ディレクトリ ソース統合でこのパラメータを使用します。EDI パラメータをアップグレードして、同等の CDI パラメータで置き換えることをお勧めします。

シナリオ 3：BDI 設定から 11.8 にアップグレードする場合

BDI パラメータのみを使用する設定の場合、BDI パラメータを同等の CDI パラメータに更新する必要があります。たとえば、BDIPrimaryServerName の場合、このパラメータを PrimaryServerName で置き換える必要があります。BDIEnableTLS は UseSSL パラメータに置き換えられます。

シナリオ 4：EDI と BDI の混合設定から 11.8 にアップグレードする場合

EDI と BDI の両方を使用する設定の場合、Jabber が LDAP サーバに接続する場合に EDI パラメータを使用しているかを BDI の設定を確認する必要があります。

ディレクトリ パラメータ

次の表に、BDI と EDI のパラメータを示し、CDI パラメータ名、または Jabber 11.8 以降に適用されないかどうかも示します。

BDI パラメータ	EDI パラメータ	CDI パラメータ
-	DirectoryServerType	DirectoryServerType
-	ConnectionType	-
BDILDAPServerType	-	-
BDIPresenceDomain	PresenceDomain	PresenceDomain
BDIPrimaryServerName	PrimaryServerName	PrimaryServerName
-	SecondaryServerName	SecondaryServerName
BDIServerPort1	ServerPort1	ServerPort1
-	ServerPort2	ServerPort2
-	UseWindowCredentials	-
BDIUseJabberCredentials	-	-
BDIConnectionUsername	ConnectionUsername	ConnectionUsername
BDIConnectionPassword	ConnectionPassword	ConnectionPassword
BDIEnableTLS	UseSSL	UseSSL
-	UseSecureConnection	-
BDIUseANR	UseANR	UseANR
BDIBaseFilter	BaseFilter	BaseFilter
BDIGroupBaseFilter	GroupBaseFilter	GroupBaseFilter
BDIUseANR	-	-
BDIPredictiveSearchFilter	PredictiveSearchFilter	PredictiveSearchFilter
-	DisableSecondaryNumberLookups	DisableSecondaryNumberLookups
-	SearchTimeout	SearchTimeout
-	UseWildcards	UseWildcards

BDI パラメータ	EDI パラメータ	CDI パラメータ
-	MinimumCharacterQuery	MinimumCharacterQuery
BDISearchBase1	SearchBase1、SearchBase2、SearchBase3、SearchBase4、SearchBase5	SearchBase1、SearchBase2、SearchBase3、SearchBase4、SearchBase5
BDIGroupSearchBase1	GroupSearchBase1、GroupSearchBase2、GroupSearchBase3、GroupSearchBase4、GroupSearchBase5	GroupSearchBase1、GroupSearchBase2、GroupSearchBase3、GroupSearchBase4、GroupSearchBase5
BDIUseSipUriToResolveContacts	UseSipUriToResolveContacts	UseSipUriToResolveContacts
BDIUriPrefix	UriPrefix	UriPrefix
BDISipUri	SipUri	SipUri
BDIPhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled
BDIPhotoUriSubstitutionToken	PhotoUriSubstitutionToken	PhotoUriSubstitutionToken
BDIPhotoUriWithToken	PhotoUriWithToken	PhotoUriWithToken
BDIPhotoSource	PhotoSource	PhotoSource
LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom
LDAPUserDomain	LDAPUserDomain	LDAPUserDomain
-	-	LdapSupportedMechanisms
BDICommonName	CommonName	CommonName
BDIDisplayName	DisplayName	DisplayName
BDIFirstname	Firstname	Firstname
BDILastname	Lastname	Lastname
BDIEmailAddress	EmailAddress	EmailAddress
BDISipUri	SipUri	SipUri
BDIPhotoSource	PhotoSource	PhotoSource
BDIBusinessPhone	BusinessPhone	BusinessPhone
BDIMobilePhone	MobilePhone	MobilePhone
BDIHomePhone	HomePhone	HomePhone

BDI パラメータ	EDI パラメータ	CDI パラメータ
BDIOtherPhone	OtherPhone	OtherPhone
BDIDirectoryUri	DirectoryUri	DirectoryUri
BDITitle	Title	Title
BDICompanyName	CompanyName	CompanyName
BDIUserAccountName	UserAccountName	UserAccountName
BDIDomainName	DomainName	DomainName
BDICountry	Country	Country
BDILocation	Location	Location
BDINickname	Nickname	Nickname
BDIPostalCode	PostalCode	PostalCode
BDICity	City	City
BDIState	状態	State
BDIStreetAddress	StreetAddress	StreetAddress

Cisco Unified Communications Manager User Data Service

User Data Service（UDS）は、連絡先解決を提供する Cisco Unified Communications Manager の REST インターフェイスです。

UDS は次のような状況で連絡先解決に使用されます。

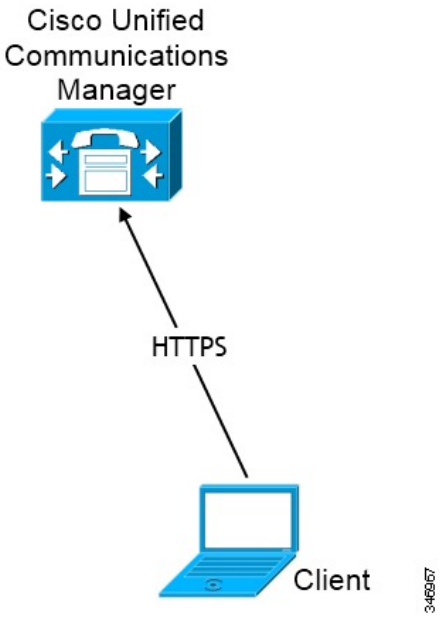
- クライアント コンフィギュレーション ファイルの UDS の値を使用するように DirectoryServerType パラメータを設定した場合。

  この設定では、企業のファイアウォールの内側または外側のクライアントが連絡先解決に UDS を使用します。

- Expressway for Remote and Mobile Access を展開した場合。

  この設定では、企業のファイアウォールの外側のクライアントが自動的に連絡先解決に UDS を使用します。

ディレクトリ サーバから Cisco Unified Communications Manager に連絡先データを同期します。そうすると、Cisco Jabber が自動的に UDS からその連絡先データを取得します。



複数のクラスタでの連絡先の解決

複数の Cisco Unified Communications Manager クラスタを使用した連絡先解決では、社内ディレクトリ上のすべてのユーザを各クラスタに同期させます。該当するクラスタでそのようなユーザのサブセットをプロビジョニングします。

たとえば、組織のユーザが 40,000 人とします。20,000 人のユーザが北米にいます。20,000 人のユーザがヨーロッパにいます。組織は、拠点ごとに次の Cisco Unified Communications Manager クラスタを配置しています。

- `cucm-cluster-na`（北米）
- `cucm-cluster-eu`（ヨーロッパ）

この例では、40,000 人のユーザすべてを両方のクラスタに同期させます。北米の 20,000 人のユーザを `cucm-cluster-na` に、ヨーロッパの 20,000 人のユーザを `cucm-cluster-eu` にプロビジョニングします。

ヨーロッパのユーザが北米のユーザに発信すると、Cisco Jabber が `cucm-cluster-na` からヨーロッパのユーザの連絡先詳細を取得します。

北米のユーザがヨーロッパのユーザに発信すると、Cisco Jabber が `cucm-cluster-eu` から北米のユーザの連絡先詳細を取得します。

UDS 拡張連絡先ソース

UDS から LDAP サーバに連絡先検索を拡張します。Cisco Unified Communications Manager 11.5(1) 以降では、Jabber が LDAP サーバを検索するかどうかを設定できます。

LDAP の前提条件

Cisco Jabber はさまざまな属性を使用して連絡先ソースを検索しますが、これらの属性すべてがデフォルトでインデックス化されるわけではありません。効率的に検索するために、Cisco Jabber で使用される属性をインデックス化する必要があります。

デフォルトの属性マッピングを使用する場合は、次の属性が LDAP サーバ上でインデックス化されていることを確認します。

- sAMAccountName
- displayName
- sn
- 名前
- proxyAddresses
- [mail]
- 部署
- givenName
- telephoneNumber
- otherTelephone
- mobile
- homePhone
- msRTCSIP-PrimaryUserAddress

LDAP サービス アカウント

Jabber を LDAP サーバに接続するには、LDAP による Jabber ユーザの認証方法を定義する必要があります。

- サービス プロファイルまたは `jabber-config.xml` ファイルでクレデンシャルを定義した場合、常にデフォルト オプションが優先されます。デフォルト オプションは、Jabber は Kerberos またはクライアント証明書（SASL External）を使用して連絡先サーバーに自動的に接続されます。このオプションは安全性に優れているため使用することをお勧めします。
- LdapSupportedMechanisms パラメータに PLAIN 値を設置しても、ディレクトリ プロファイルのユーザ名またはパスワードを設定しなければ、ユーザはディレクトリ クレデンシャルをクライアント ディレクトリに入力できます。
- それ以外の場合、セキュア ポートをサービス プロファイルに接続したら、`jabber-config.xml` ファイルの LDAP_UseCredentialsFrom 設定パラメータの Cisco Unified

Communications Manager クレデンシャルを指定することで、Jabber をディレクトリ サーバに接続する方法を定義できます。

- 前述のオプションが使用できない場合は、サービス プロファイルまたは `jabber-config.xml` ファイルで提供される既知のクレデンシャルセットを使用します。これは安全性が最も低いオプションです。Cisco Jabber は、アカウントを使用して連絡先ソースサーバーを認証します。このアカウントは、ディレクトリへの読み取りアクセス専用にして、一般的なパブリック クレデンシャル セットにすることを推奨します。この場合、すべての Jabber ユーザは、これらの資格情報を検索に使用します。

（注） Cisco Unified Communications Manager 12.0 以降では、サービス プロファイルでユーザ名とパスワードを設定することはできません。Jabberユーザは、ディレクトリ サービスを使用して自身を認証するためのオプションを取得します。ユーザがJabberに初めてサインインすると、ユーザに通知が送信されます。最初に自分自身を認証しない場合、連絡先リストにアクセスしようとすると警告が表示されます。

Jabber ID 属性マッピング

ユーザ ID の LDAP 属性は sAMAccountName です。これがデフォルト属性です。

ユーザ ID の属性が sAMAccountName 以外の場合で、Cisco Unified Communications Manager IM and Presence サービス でデフォルトの IM アドレス スキームが使用されている場合は、次のようにクライアント コンフィギュレーション ファイルでパラメータの値として属性を指定する必要があります。

CDI パラメータはUserAccountNameです。<UserAccountName>attribute-name</UserAccountName>

設定で属性を指定せず、属性が sAMAccountName 以外の場合、クライアントはディレクトリ内の連絡先を解決できません。この結果、ユーザはプレゼンスを取得せず、インスタントメッセージを送信または受信できません。

Jabber ID の検索

Cisco Jabber は Jabber ID を使用して、ディレクトリ内の連絡先情報を検索します。ディレクトリ内の検索を最適化するオプションがいくつかあります。

- **検索ベース**—デフォルトでは、クライアントはディレクトリ ツリーのルートから検索を開始します。検索ベースを使用して、別の検索開始を指定したり、特定のグループに対する検索を制限したりできます。たとえば、ユーザのサブセットにはインスタントメッセージング機能だけがあります。これらのユーザを OU に含め、この OU を検索ベースとして指定します。
- **ベース フィルタ**—ディレクトリのサブキー名のみを指定し、ディレクトリへのクエリーの実行時にユーザ オブジェクト以外のオブジェクトを取得します。

- **予測検索フィルタ**—検索クエリーをフィルタするために、複数のカンマ区切り値を定義できます。デフォルト値は ANR（Ambiguous Name Resolution）です。

これらオプションについての詳細については、*Cisco Jabber*向けパラメータリファレンスガイドのディレクトリ統合に関する章を参照してください。

ローカル連絡先ソース

Cisco Jabber には、ローカル連絡先ソースにアクセスして検索する機能があります。これらのローカル連絡先ソースには次のものがあります。

- Microsoft Outlook に保存されているローカル連絡先には Cisco Jabber for Windows からアクセスします。
- IBM Notes に保存されているローカル連絡先には Cisco Jabber for Windows（リリース 11.1 以降）からアクセスします。
- ローカル アドレス帳の連絡先には、Cisco Jabber for Mac、Cisco Jabber for Android、Cisco Jabber for iPhone and iPad からアクセスします。

カスタム連絡先ソース

すべてのクライアントの Cisco Jabber は、クライアントにカスタム連絡先をインポートする機能をユーザに提供します。

連絡先のキャッシュ

Cisco Jabber は、ローカルキャッシュを作成します。特に、キャッシュには、ユーザの連絡先リストが保存されています。ユーザが連絡先リストで連絡先を検索するとき、Jabber はローカル キャッシュで一致する連絡先を検索してから、ディレクトリ検索を開始します。

ユーザが連絡先リストに存在しない連絡先を検索している場合、Jabber はまずローカルキャッシュを検索し、その後社内ディレクトリを検索します。そしてユーザがその連絡先とチャットまたは通話を開始すると、Jabber は連絡先情報をローカル キャッシュに追加します。

ローカル キャッシュ情報は 24 時間で期限切れになります。

重複する連絡先の解決

Jabber の連絡先は異なるソースから取得できます。Jabber では、複数の連絡先ソースで同じ連絡先の一致が検出される可能性があります。この場合、Jabber は、同じ人物に一致するレコードを判断し、その人物のすべてのデータを結合します。いずれかの連絡先ソースのレコードが

連絡先に一致しているかどうかを確認するために、Jabberは次の順序でこれらのフィールドを探します。

1. **Jabber ID (JID)**: レコードにJIDが含まれている場合、Jabberはそのベースのレコードに一致します。Jabberは、メールまたは電話番号のフィールドに基づいた比較は行いません。
2. **メール**: レコードにメールフィールドがある場合、Jabberはその基準に一致するレコードを検索します。Jabberは、電話番号に基づいてレコードをそれ以上比較することはありません。
3. **電話番号**：レコードに電話番号が含まれる場合、Jabberは電話番号に基づいて照合されます。

Jabberは、レコードを比較し、同じ人物に一致するレコードを特定するため、連絡先のデータを結合して1つの連絡先レコードを作成します。

ダイヤル プランのマッピング

Cisco Unified Communications Managerのダイヤル ルールがディレクトリのダイヤル ルールと確実に一致するように、ダイヤル プランのマッピングを設定します。

アプリケーション ダイヤル ルール

アプリケーション ダイヤル ルールにより、ユーザがダイヤルする電話番号の桁数の追加および削除が自動的に行われます。アプリケーション ダイヤル ルールにより、ユーザがクライアントからダイヤルする番号が操作されます。

たとえば、7桁の電話番号の先頭に自動的に9を追加して外線にアクセスするように、ダイヤル ルールを設定できます。

ディレクトリ検索ダイヤル ルール

ディレクトリ検索ダイヤル ルールによって、発信者IDの番号が、クライアントがディレクトリで検索できる番号に変換されます。定義する各ディレクトリ検索ルールには、先頭の数字および番号の長さに基づいてどの数字を変換するかを指定します。

たとえば、10桁の電話番号から市外局番と2桁の局番を自動的に削除するディレクトリ検索ルールを作成できます。このタイプのルールでは、たとえば、`4089023139` を `23139` に変換します。

Cisco Unified Communication Manager UDS for Mobile and Remote Access

Cisco Unified Communication Manager UDSは、Cisco JabberがExpressway Mobile and Remote Accessを使用して接続している際に使用される連絡先ソースです。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。

クラウドの連絡先ソース

Cisco Webex 連絡先ソース

クラウド展開では、連絡先データは Cisco Webex Messenger 管理ツールで設定されるか、またはユーザの更新によって設定されます。連絡先情報は Cisco Webex Messenger 管理ツールを使用してインポートすることができます。詳細については、Cisco Webex Messenger 管理ガイドのユーザー管理のセクションを参照してください。

連絡先の写真の形式と寸法

Cisco Jabber で最適な結果を得るには、連絡先写真を特定の形式と寸法にする必要があります。サポートされる形式と最適な寸法を確認してください。クライアントが連絡先の写真に対して行う調整について説明します。

連絡先の写真の形式

Cisco Jabber は、ディレクトリ内の連絡先写真に関する次の形式をサポートしています。

- JPG
- PNG
- BMP

重要 Cisco Jabber では、GIF 形式の連絡先写真のレンダリングを向上させるための変更は適用されません。その結果、GIF 形式の連絡先写真が不正にレンダリングされたり最適な品質にならない場合があります。最適な品質を得るには、連絡先写真として PNG 形式を使用します。

連絡先の写真の寸法

ヒント 連絡先写真の最適な寸法は、アスペクト比 1:1 の 128 x 128 ピクセルです。

Microsoft Outlook でのローカル連絡先写真の最大寸法は 128 X 128 ピクセルです。

次の表に、Cisco Jabber での連絡先写真のさまざまな寸法を示します。

参照先	寸法
音声コール ウィンドウ	128 x 128 ピクセル
次のような招待やリマインダ • 着信コール ウィンドウ • 会議リマインダ ウィンドウ	64 x 64 ピクセル
次のような連絡先のリスト • 連絡先リスト • 参加者リスト • コール履歴 • ボイスメール メッセージ	32 x 32 ピクセル

連絡先の写真の調整

Cisco Jabber は次のように連絡先写真を調整します。

- サイズ変更：ディレクトリ内の連絡先写真が 128 X 128 ピクセル以外のサイズである場合、クライアントによって写真のサイズが自動的に変更されます。たとえば、ディレクトリ内の連絡先写真が 64 x 64 ピクセルであるとします。Cisco Jabber でディレクトリから連絡先写真を取得すると、その写真のサイズが 128 X 128 ピクセルに変更されます。

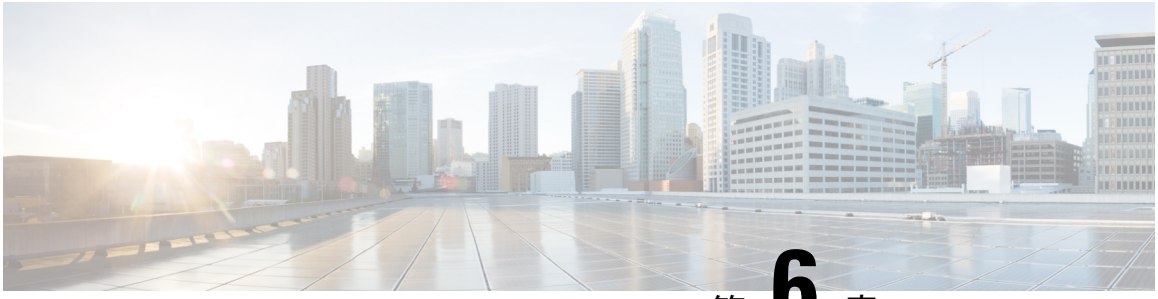
  ヒント 連絡先写真のサイズ変更により、最適な解像度が得られない場合があります。このため、クライアントによって連絡先写真のサイズが自動的に変更されないように、128 X 128 ピクセルの連絡先写真を使用してください。

- トリミング：Cisco Jabber では、正方形以外の連絡先写真を正方形のアスペクト比（つまり、幅と高さが同じであるアスペクト比 1:1）に自動的にトリミングします。
- ディレクトリ内の連絡先写真が縦方向である場合、クライアントは上端から 30 %、下端から 70 % をトリミングします。

  たとえば、ディレクトリ内の連絡先写真が幅 100 ピクセル、高さ 200 ピクセルである場合、アスペクト比が 1:1 となるように Cisco Jabber では高さから 100 ピクセルをトリミングする必要があります。この場合、クライアントは写真の上端から 30 ピクセルを、写真の下端から 70 ピクセルをトリミングします。

- ディレクトリ内の連絡先写真が横方向である場合、クライアントで両方の側から 50 % をトリミングします。

たとえば、ディレクトリ内の連絡先写真が幅 200 ピクセル、高さ 100 ピクセルである場合、アスペクト比が 1:1 となるように Cisco Jabber では幅から 100 ピクセルをトリミングする必要があります。この場合、クライアントは写真の右側から 50 ピクセルを、写真の左側から 50 ピクセルをトリミングします。



第 6 章

セキュリティおよび証明書

- 暗号化（Encryption） （123 ページ）
- 音声およびビデオの暗号化 （129 ページ）
- セキュアメディア向け認証方法。 （129 ページ）
- PIE ASLRサポート （129 ページ）
- 連邦情報処理標準規格 （129 ページ）
- コモン クライテリア （131 ページ）
- Secure LDAP （131 ページ）
- 認証済み UDS 連絡先の検索 （131 ページ）
- 証明書 （132 ページ）
- マルチテナントのホステッド コラボレーション ソリューション向けの SNI サポート。 （136 ページ）

暗号化（Encryption）

ファイル転送および画面キャプチャのコンプライアンスおよびポリシー管理

Cisco Unified Communications Manager IM and Presence 10.5(2) 以降の管理されたファイル転送オプションを使用してファイル転送と画面キャプチャを送信する場合は、監査およびポリシー強制用のコンプライアンス サーバにファイルを送信できます。

コンプライアンスの詳細については、『*Instant Messaging Compliance for IM and Presence Service on Cisco Unified Communications Manager*』ガイドを参照してください。

ファイル転送と画面キャプチャの詳細については、『*Cisco Unified Communications Manager IM and Presence Deployment and Installation Guide*』を参照してください。

インスタント メッセージの暗号化

Cisco Jabber は、Transport Layer Security（TLS）を使用して、クライアントとサーバ間のネットワーク上で Extensible Messaging and Presence Protocol（XMPP）トラフィックを保護します。Cisco Jabber は、ポイント・トゥ・ポイントのインスタントメッセージを暗号化します。

オンプレミス暗号化

次の表に、オンプレミス展開におけるインスタント メッセージ暗号化の詳細を示します。

接続	[プロトコル(Protocol)]	ネゴシエーション証明書	想定される暗号化アルゴリズム
クライアントからサーバへ	XMPP over TLS v1.2	X.509 公開キー インフラストラクチャ証明書	AES 256 ビット

サーバとクライアントのネゴシエーション

次のサーバは、X.509 公開キー インフラストラクチャ（PKI）証明書と次のものを使用して Cisco Jabber と TLS 暗号化をネゴシエートします。

- Cisco Unified Communications Manager IM and Presence
- Cisco Unified Communications Manager

サーバとクライアントが TLS 暗号化をネゴシエートした後、インスタント メッセージのトラフィックを暗号化するためにクライアントとサーバの両方がセッション キーを生成して交換します。

次の表に、Cisco Unified Communications Manager IM and Presence Service の PKI 証明書キーの長さを示します。

バージョン	キーの長さ
Cisco Unified Communications Manager IM and Presence Service バージョン 9.0.1 以降	2048 ビット

XMPP 暗号化

Cisco Unified Communications Manager IM and Presence サービスは、AES アルゴリズムで暗号化された 256 ビット長のセッション キーを使用して Cisco Jabber とプレゼンス サーバ間のインスタント メッセージ トラフィックを保護します。

サーバ ノード間のトラフィックのセキュリティを強化する必要がある場合は、Cisco Unified Communications Manager IM and Presence サービス上で XMPP セキュリティ設定を構成できます。セキュリティ設定の詳細については、次を参照してください。

- Cisco Unified Communications Manager IM and Presence Service：『*Security configuration on IM and Presence*』

インスタント メッセージのロギング

規制ガイドラインへの準拠のために、インスタントメッセージをログに記録してアーカイブできます。インスタントメッセージをログに記録するには、外部データベースを設定するか、またはサードパーティ製のコンプライアンス サーバと統合します。Cisco Unified Communications Manager IM and Presence サービスは、外部データベースまたはサードパーティ製コンプライアンス サーバに記録されたインスタントメッセージを暗号化しません。必要に応じて、外部データベースまたはサードパーティ製コンプライアンス サーバを設定し、記録したインスタントメッセージを保護する必要があります。

コンプライアンスの詳細については、次を参照してください。

- Cisco Unified Communications Manager IM and Presence Service：『*Instant Messaging Compliance for IM and Presence Service*』

AES などの対称キー アルゴリズムや RSA などの公開キー アルゴリズムを含め、暗号化レベルや暗号化アルゴリズムの詳細については、リンク https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html の「*Next Generation Encryption*」を参照してください。

X.509 公開キー インフラストラクチャ証明書の詳細については、リンク https://www.ietf.org/rfc/rfc2459.txt の『*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*』のドキュメントを参照してください。

クラウドベースの暗号化

次の表に、クラウドベース展開におけるインスタント メッセージ暗号化の詳細を示します。

接続先	[プロトコル(Protocol)]	ネゴシエーション証明書	想定される暗号化アルゴリズム
クライアントからサーバへ	TLS 内の XMPP	X.509 公開キー インフラストラクチャ証明書	AES 128 ビット
クライアント間	TLS 内の XMPP	X.509 公開キー インフラストラクチャ証明書	AES 256 ビット

サーバとクライアントのネゴシエーション

次のサーバは、X.509 公開キー インフラストラクチャ（PKI）証明書と Cisco Webex Messenger サービスを使用して Cisco Jabber で TLS 暗号化をネゴシエートします。

サーバとクライアントが TLS 暗号化をネゴシエートした後、インスタント メッセージのトラフィックを暗号化するためにクライアントとサーバの両方がセッション キーを生成して交換します。

XMPP 暗号化

Cisco Webex Messenger サービスは AES アルゴリズムで暗号化された 128 ビット長のセッション キーを使用し、Cisco Jabber と Cisco Webex Messenger サービス間のインスタント メッセージのトラフィックを保護します。

必要に応じて、256 ビットのクライアント間 AES 暗号化を有効化し、クライアント間のトラフィックを保護できます。

インスタント メッセージのロギング

Cisco Webex Messenger サービスはインスタント メッセージをログに記録できますが、暗号化形式のインスタントメッセージはアーカイブされません。ただし、Cisco Webex Messenger サービスは、SAE-16 や ISO-27001 監査などの厳重なデータセンター セキュリティを使用して、記録したインスタント メッセージを保護します。

Cisco Webex Messenger サービスは、AES 256 ビットのクライアント間の暗号化を有効にした場合は、インスタント メッセージをログに記録できません。

AES などの対称キー アルゴリズムや RSA などの公開キー アルゴリズムを含め、暗号化レベルや暗号化アルゴリズムの詳細については、リンク https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html の「*Next Generation Encryption*」を参照してください。

X.509 公開キー インフラストラクチャ証明書の詳細については、リンク https://www.ietf.org/rfc/rfc2459.txt の『*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*』のドキュメントを参照してください。

クライアント間の暗号化

デフォルトでは、クライアントと Cisco Webex Messenger サービス間のインスタント メッセージ トラフィックはセキュアです。必要に応じて、Cisco Webex 管理ツールでポリシーを指定して、クライアント間のインスタント メッセージング トラフィックを保護できます。

次のポリシーは、クライアント間のインスタント メッセージの暗号化を指定します。

- IM の AES 符号化をサポートする（Support AES Encoding For IM）：送信側クライアントは、AES 256 ビット アルゴリズムを使用してインスタント メッセージを暗号化します。受信側クライアントは、インスタント メッセージの暗号を解除します。
- IM の符号化をサポートしない（Support No Encoding For IM）：クライアントは、暗号化をサポートしていない他のクライアントとインスタント メッセージを送受信できます。

次の表は、これらのポリシーを使用して設定できる組み合わせを示しています。

ポリシーの組み合わせ	クライアント間の暗号化	リモートクライアントが**AES**暗号化をサポートしている場合	リモートクライアントが**AES**暗号化をサポートしていない場合
[IM の AES 符号化をサポートする（Support AES Encoding For IM）] = false [IM の符号化をサポートしない（Support No Encoding For IM）] = true	なし	Cisco Jabber は暗号化されていないインスタントメッセージを送信します。 Cisco Jabber はキー交換をネゴシエートしません。そのため、他のクライアントは Cisco Jabber の暗号化されたインスタントメッセージを送信しません。	Cisco Jabber は暗号化されていないインスタントメッセージを送受信します。
[IM の AES 符号化をサポートする（Support AES Encoding For IM）] = True [IM の符号化をサポートしない（Support No Encoding For IM）] = true	あり	Cisco Jabber は暗号化されたインスタントメッセージを送受信します。 Cisco Jabber には、インスタントメッセージが暗号化されていることを示すアイコンが表示されます。	Cisco Jabber は暗号化されたインスタントメッセージを送信します。 Cisco Jabber は暗号化されていないインスタントメッセージを受信します。
[IM の AES 符号化をサポートする（Support AES Encoding For IM）] = True [IM の符号化をサポートしない（Support No Encoding For IM）] = false	あり	Cisco Jabber は暗号化されたインスタントメッセージを送受信します。 Cisco Jabber には、インスタントメッセージが暗号化されていることを示すアイコンが表示されます。	Cisco Jabber は、リモートクライアントに対してインスタントメッセージの送受信を行いません。 ユーザがリモートクライアントにインスタントメッセージを送信しようとすると、Cisco Jabber にエラー メッセージが表示されます。

（注） Cisco Jabberグループのチャットを使用したクライアントからクライアントへの暗号化をサポートしていません。Cisco Jabberは、ポイントツーポイントのチャットの場合、クライアントからクライアントへの暗号化のみを使用します。

暗号化および Cisco Webex ポリシーの詳細については、Cisco Webex のマニュアルの暗号化レベルについてを参照してください。

暗号化アイコン

暗号化レベルを表示するには、クライアントが表示するアイコンを確認します。

サーバの暗号化対応クライアント用のロック アイコン

オンプレミス展開とクラウドベース展開の両方で、Cisco Jabber はクライアント/サーバ間暗号化を示す次のアイコンを表示します。

クライアント間暗号化の鍵アイコン

クラウドベース展開で、Cisco Jabber はクライアント間暗号化を示す次のアイコンを表示します。

ローカルのチャット履歴

チャット履歴は、参加者がチャット ウィンドウを閉じたあともサインアウトするまで維持されます。参加者がチャット ウィンドウを閉じたらチャット履歴を破棄する場合は、Disable_IM_History パラメータを ture に設定します。このパラメータは、IM 専用ユーザを除く、すべてのクライアントで使用できます。

Cisco Jabber for Mac のオンプレミス展開の場合、Cisco Jabber for Mac の [チャットの設定（Chat Preferences）] ウィンドウで [チャットのアーカイブを次に保存：（Save chat archives to:）] オプションを選択すると、チャット履歴は Mac ファイル システムにローカルに保存され、Spotlight を使用して検索できるようになります。

Cisco Jabber は、ローカル チャット履歴が有効の場合は、アーカイブされたインスタント メッセージを暗号化しません。

デスクトップ クライアントの場合、次のディレクトリにアーカイブを保存すると、チャット履歴へのアクセスを制限できます。

- Windows の場合：`%USERPROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\History\uri.db`
- Mac：`~/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/History/uri.db`.

モバイル クライアントでは、チャット履歴ファイルにアクセスできません。

音声およびビデオの暗号化

オプションで、すべてのデバイスに対してセキュアな電話機能をセットアップできます。セキュア電話機能により、セキュア SIP シグナリング、セキュア メディア ストリーム、および暗号化デバイス設定ファイルが提供されます。

ユーザのセキュアな電話機能を有効にした場合は、Cisco Unified Communications Manager へのデバイス接続がセキュアになります。ただし、他のデバイスとのコールは、両方のデバイスがセキュアな接続を備えている場合にのみセキュアになります。

セキュアメディア向け認証方法。

トークンベースの認証でセキュアメディアを有効にするには、SIP oAuth を使用します。Jabber のオンプレミス、クラウド、およびハイブリッド展開の場合は、セキュリティ認証のための CAPF 登録ではなく、SIP oAuth を設定することができます。

SIP OAuth

お使いの Cisco ユニファイドコミュニケーションマネージャーがセットアップされたときに 1 回実行されます。これにより、RTP メディアを含む SIP トラフィックの安全性が確保されます。

認証モード

CAPF enrolment を有効にするためのワークフローは次のようになっています。

- Jabber デバイスの作成と設定
- 認証文字列
- 電話セキュリティ プロファイルの設定

PIE ASLRサポート

Cisco Jabber for Android、iPhone および iPad では、各場所に独立した実行可能アドレススペースレイアウトのランダム化 (パイ ASLR) がサポートされています。

連邦情報処理標準規格

連邦情報処理標準（FIPS）140 は、暗号モジュールのセキュリティ要件を規定する米国およびカナダ政府の基準です。これらの暗号化モジュールには、承認されたセキュリティ機能を実装し、暗号境界内に存在するハードウェア、ソフトウェア、およびファームウェアのセットが含まれます。

FIPS では、クライアント内部で使用される暗号化、キー交換、デジタル署名、およびハッシュと乱数生成関数のすべてが暗号モジュールのセキュリティに関する FIPS 140.2 要件に準拠している必要があります。

FIPS モードではクライアントによる証明書の管理がより厳密になります。FIPS モードでは、サービスの証明書が期限切れになり、クレデンシャルが再入力されていなかった場合、クライアントに証明書エラーが表示されます。ハブ ウィンドウにも、クライアントが FIPS モードで実行中であることを示す FIPS アイコンが表示されます。

Cisco Jabber for Windows 用の FIPS の有効化

Cisco Jabber for Windows では、FIPS を有効にする 2 つの方法をサポートしています。

- オペレーティング システム対応：Windows オペレーティング システムは FIPS モードです。
- Cisco Jabber のブートストラップの設定：FIPS_MODE インストーラ スイッチを設定します。Cisco Jabber は、FIPS 対応ではないオペレーティング システムでも FIPS モードにすることができます。このシナリオでは、Windows API 以外による接続のみ FIPS モードになります。

表 8 : Cisco Jabber for Windows の FIPS 設定

プラットフォームモード	ブートストラップ設定	Cisco Jabber クライアントの設定
FIPS 対応	FIPS 対応	FIPS 対応：ブートストラップの設定。
FIPS 対応	FIPS 非対応	FIPS 非対応：ブートストラップの設定。
FIPS 対応	設定なし	FIPS 対応：プラットフォームの設定。
FIPS 非対応	FIPS 対応	FIPS 対応：ブートストラップの設定。
FIPS 非対応	FIPS 非対応	FIPS 非対応：ブートストラップの設定。
FIPS 非対応	設定なし	FIPS 非対応：プラットフォームの設定。

（注） Jabber ボイスメール サービスは、SSL 接続中に **FIPS を有効にした HTTP 要求**（**https://164.62.224.15/vmrest/version**）の TLS バージョン TLS 1.2 のみを受け入れます。

Cisco Jabber for Mobile Clients 用の FIPS の有効化

Cisco Jabber for mobile clients 用の FIPS を有効にするには、Enterprise Mobility Management（EMM）で、FIPS_MODE パラメータを True に設定します。

重要

- FIPS を有効にすると、ユーザは信頼できない証明書を受け入れられなくなります。この場合、ユーザは一部のサービスを使用できなくなる可能性があります。証明書信頼リスト（CTL）または ITL ファイルは、これには該当しません。サーバの証明書が正常に署名されるか、サイドローディングによってクライアントでサーバ証明書を信頼する必要があります。
- FIPS は TLS1.2 を強制的に適用するため、古いプロトコルが無効となります。
- Cisco Jabber for mobile clients では、プラットフォーム モードはサポートされていません。

コモン クライテリア

情報技術セキュリティ評価の共通基準は、IT 製品のセキュリティ属性を評価するために使用される一連の国際標準を構成しています。共通の条件証明要件に準拠したモードで、Cisco Jabber を実行できます。これを行うには、各クライアントでそれを有効にする必要があります。

一般的な条件が有効になっている環境で Jabber を実行するには、次のようにします。

- Jabber for Windows: CC_MODE のインストール引数を TRUE に設定します。
- Jabber for Android および Jabber for iPhone および iPad の場合: Enterprise Mobility Management (EMM) で、CC_MODE パラメータを TRUE に設定します。
- RSA キー長は、少なくとも 2048 ビットである必要があります。RSA キー長を設定するには、*Cisco Jabber* を作成して設定する方法（*Cisco Jabber 12.5* のオンプレミス導入ガイド内）を確認します。

共通基準モードで Jabber が実行されるように設定する方法の詳細については、*Cisco Jabber*プリケーションを導入する方法（*Cisco jabber 12.5* のオンプレミス導入ガイド内）でご確認ください。

Secure LDAP

Secure LDAP の通信は LDAP over SSL/TLS です。

LDAPS は SSL/TLS 接続を介して LDAP 接続を開始します。SSL セッションを開いてから LDAP プロトコルを使用して開始します。これには、個別のポート 636 またはグローバル カタログ ポート 3269 が必要です。

認証済み UDS 連絡先の検索

Cisco Unified Communications Manager での UDS 連絡先検索のための認証を有効にします。Cisco Jabber は連絡先検索のための UDS 認証のクレデンシャルを提供します。

証明書

証明書の検証

証明書検証プロセス

OS Cisco Jabber は、サービスの認証時に有効なサーバ証明書上で起動します。セキュアな接続の確立を試みるときに、サービスは Cisco JabberconrefCisco Jabber に証明書を提示します。OS は、提示された証明書をクライアントデバイスのローカル証明書ストア内の証明書に照らして検証します。証明書が証明書ストア内に存在しない場合、その証明書は信頼できないものとみなされ、Cisco Jabber はユーザに証明書を受け入れるか拒否するかを尋ねます。

ユーザが証明書を受け入れた場合、Cisco Jabber はサービスに接続して、デバイスの証明書ストアまたはキーチェーンに証明書を保存します。ユーザが証明書を拒否した場合、Cisco Jabber はサービスに接続せず、証明書はデバイスの証明書ストアにもキーチェーンにも保存されません。

証明書がデバイスのローカル証明書ストア内に存在する場合、Cisco Jabber はその証明書を信頼します。Cisco Jabber はユーザに証明書を受け入れるか拒否するかを尋ねることなく、サービスに接続します。

Cisco Jabber 組織に展開している内容に応じて、複数のサービスを認証できます。サービスごとに証明書署名要求（CSR）を生成する必要があります。一部のパブリック認証局は、完全修飾ドメイン名（FQDN）ごとに 1 つの CSR しか承認しません。そのため、各サービスの CSR を別々のパブリック認証局に送信しなければならない場合があります。

IP アドレスやホスト名の代わりに、各サービスのサービス プロファイルで FQDN が指定されていることを確認します。

署名証明書

証明書は、認証局（CA）で署名することも、自己署名することもできます。

- CA 署名証明書 （推奨）—ユーザが自分自身で証明書をデバイスにインストールしているため、プロンプトが表示されません。CA 署名証明書はプライベート CA またはパブリック CA で署名できます。パブリック CA で署名された証明書の多くは証明書ストアまたはデバイスのキーチェーンに保存されます。Android 7.0 以降の devicies、CA 署名付き証明書のみを認識します。
- 自己署名証明書：証明書は、証明書を提示しているサービスによって署名され、ユーザは必ずその証明書を受け入れるか拒否するかを尋ねられます。

証明書検証オプション

証明書検証をセットアップする前に、証明書の検証方法を決定する必要があります。

- オンプレミス展開とクラウドベース展開のどちらかに証明書を展開しようとしているか。

- 証明書の署名に使用している方法。
- CA 署名証明書を展開している場合は、パブリック CA とプライベート CA のどちらを使用するか。
- どのサービスの証明書を取得する必要があるか。

オンプレミス サーバに必要な証明書

オンプレミス サーバは、Cisco Jabber とのセキュアな接続を確立するために、次の証明書を提示します。

サーバ	証明書
Cisco Unified Communications Manager IM and Presence Service	HTTP（Tomcat） XMPP
Cisco Unified Communications Manager	HTT（Tomcat）と CallManager 証明書（セキュアな電話機用のセキュア SIP コール シグナリング）
Cisco Unity Connection	HTTP（Tomcat）
Cisco Webex Meetings サーバ	HTTP（Tomcat）
Cisco VCS Expressway Cisco Expressway-E	サーバ証明書（HTTP、XMPP、および SIP コール シグナリングに使用）

特記事項

- Security Assertion Markup Language（SAML）シングル サインオン（SSO）およびアイデンティティ プロバイダー（IdP）には X.509 証明書が必要です。
- 証明書の署名プロセスを開始する前に、Cisco Unified Communications Manager IM and Presence Serviceの最新の Service Update（SU）を適用する必要があります。
- 必要な証明書は、すべてのサーバ バージョンに適用されます。
- 各クラスタ ノード、サブスクライバ、およびパブリッシャは Tomcat サービスを実行し、クライアントに HTTP 証明書を提示できます。

  クラスタ内の各ノードの証明書に署名する必要があります。
- クライアントとCisco Unified Communications Manager間の SIP シグナリングを確立するには、Certification Authority Proxy Function（CAPF）登録を使用する必要があります。

証明書署名要求の形式と要件

通常、パブリック認証局（CA）は、特定の形式に準拠する証明書署名要求（CSR）を必要とします。たとえば、パブリック CA は、次のような要件を持つ CSR だけを承認する場合があります。

- Base 64 エンコードである。
- [組織（Organization）] フィールド、[OU] フィールド、またはその他フィールドに特定の文字（@&! など）が含まれていない。
- サーバの公開キーで特定のビット長を使用する。

複数ノードから CSR を送信すると、パブリック CA で全 CSR の情報の整合性が求められることがあります。

CSR の問題を回避するために、から形式の要件を、 CSR の提出を計画するパブリック CA 検討が必要です。次に、サーバを構成することがパブリック CA が要求する形式に適合している場合にユーザが入力した情報ことを保障する必要があります。

FQDN ごとに 1 つの証明書：一部のパブリック CA は、完全修飾ドメイン名（FQDN）ごとに 1 つの証明書にだけ署名します。

たとえば、単一 Cisco Unified Communications Manager IM and Presence Service ノードの HTTP および XMPP の証明書に署名するには、異なる各パブリック CA に各 CSR を送信する必要がある場合があります。

失効サーバ

失効サーバにアクセスできない場合、Cisco Jabber は Cisco ユニファイドコミュニケーションマネージャサーバに接続できません。Also, if a certificate authority (CA) revokes a certificate, Cisco Jabber does not allow users to connect to that server.

ユーザには次の結果が通知されません。

- 証明書に失効情報が含まれない。
- 失効サーバにアクセスできない。

証明書を検証するには、失効情報を提供できる到達可能なサーバの [CDP] または [AIA] フィールドに HTTP URL が証明書に含まれている必要があります。

証明書が検証済みであることを確認するには、CA が発行した証明書を取得したときに、次の要件のいずれかを満たしている必要があります。

- [**CRL Distribution Point**]（CDP）フィールドに、失効サーバ上の認証失効リスト（CRL）への HTTP URL が含まれていることを確認します。
- [**Authority Information Access**]（AIA）フィールドに、オンライン証明書ステータス プロトコル（OCSP）サーバの HTTP URL が含まれていることを確認します。

証明書のサーバ識別情報

署名プロセスの一部として、CA は証明書のサーバ識別情報を指定します。クライアントがその証明書を検証する場合、次のことを確認します。

- 信頼できる機関が証明書を発行している。
- 証明書を提示するサーバの識別情報は、証明書に明記されたサーバの識別情報と一致します。

（注） パブリック CA は、通常、サーバの識別情報として、IP アドレスではなく、ドメインを含む完全修飾ドメイン名（FQDN）を必要とします。

ID フィールド

クライアントは、識別情報の一致に関して、サーバ証明書の次の識別子フィールドを確認します。

- XMPP 証明書
  - `SubjectAltName\OtherName\xmppAddr`
  - `SubjectAltName\OtherName\srvName`
  - `SubjectAltName\dnsNames`
  - `Subject CN`
- HTTP 証明書
  - `SubjectAltName\dnsNames`
  - `Subject CN`

ヒント [件名 CN（Subject CN）] フィールドには、左端の文字（たとえば、`*.cisco.com`）としてワイルドカード（*）を含めることができます。

ID の不一致の防止

ユーザが IP アドレスまたはホスト名でサーバに接続し、サーバ証明書が FQDN でサーバを識別しようとすると、クライアントは、信頼できるポートとサーバを識別できないため、ユーザにとって良い結果をもたらしません。

サーバ証明書が FQDN でサーバを識別する場合、サーバの多くの場所の FQDN として各サーバ名を指定する必要があります。詳細については、『Troubleshooting TechNotes』の「*Prevent Identity Mismatch*」の項を参照してください。

マルチサーバ SAN の証明書

マルチサーバ SAN を使用している場合は、クラスタと tomcat 証明書ごとに一度ずつと クラスタと XMPP 証明書ごとに一度ずつサービスに証明書をアップロードする必要があるだけです。マルチサーバ SAN を使用していない場合は、すべての Cisco Unified Communications Manager ノードのサービスに証明書をアップロードする必要があります。

クラウド展開の証明書検証

Cisco Webex MessengerおよびCisco Webex Meetingsセンターは、クライアントにデフォルトで次の証明書を提示します。

- CAS
- WAPI

（注） Cisco Webex は、証明書はパブリックな認証局（CA）によって署名されます。Cisco Jabber はこれらの証明書を検証し、クラウドベース サービスとのセキュアな接続を確立します。

Cisco Jabber は、Cisco Webex Messengerから受信した次の XMPP 証明書を検証します。これらの証明書がオペレーティング システムに付属していない場合は、ユーザが入力する必要があります。

- VeriSign Class 3 Public Primary Certification Authority - G5：この証明書は信頼できるルート認証局に保存されます。
- VeriSign Class 3 Secure Server CA - G3：この証明書は Webex メッセンジャー サーバ ID の検証に使用され、中間認証局に保存されます。
- AddTrust 外部 CA ルート
- GoDaddy Class 2 Certification Authority Root Certificate

Cisco Jabber for Windows のルート証明書の詳細については、https://www.identrust.co.uk/certificates/trustid/install-nes36.htmlを参照してください。

Cisco Jabber for Mac のルート証明書の詳細については、https://support.apple.comを参照してください。

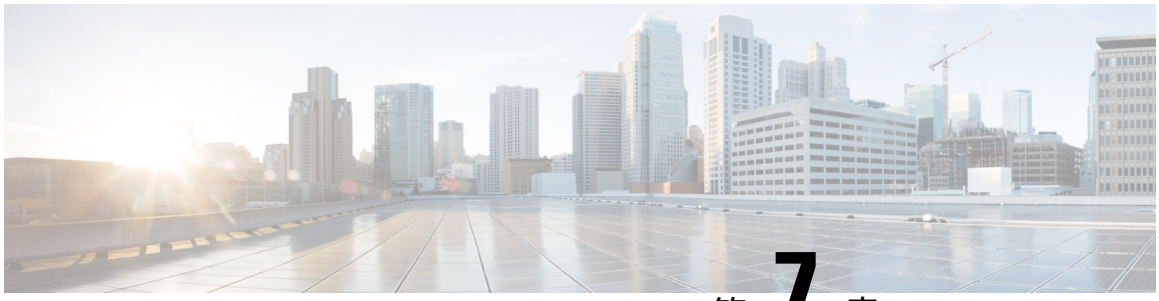
マルチテナントのホステッドコラボレーションソリューション向けの SNI サポート。

Cisco Jabberは、マルチテナントのホステッド コラボレーション ソリューションでの モバイル・リモートアクセス（MRA）の導入で 、SNI をサポートしています。

Cisco Jabber は、SNI を使用して、ドメイン情報をExpressway に送信します。この証明書ストレージを検索して、ドメイン情報が含まれている証明書を検索し、その証明書を Cisco Jabber に対する検証用に返します。

マルチテナント展開の詳細については、ドメイン証明書を使用したエンドポイントサービスの検出とドメイン証明を使用しない *Jabber* サービスの検出（『Cisco ホステッドコラボレーションソリューション』、リリース 11.5 マルチテナントExpresswayの構成ガイド』から）を参照してください。

マルチテナントのホステッド コラボレーション ソリューション向けの **SNI** サポート。



第 7 章

構成管理

• 高速サインイン （139 ページ）

高速サインイン

この機能を使用すると、以前使用していた順次サインイン プロセスとは異なり、Cisco Jabber のすべてのサービスに同時にサインインできます。各サービスはそれぞれのサーバに独立して接続し、キャッシュされたデータに基づいてユーザを認証します。これにより、サインインプロセスが迅速かつダイナミックになります。ただし、この機能は、Jabber への 2 回目のサインインからのみ有効です。

すべてのクライアントに対してSTARTUP_AUTHENTICATION_REQUIREDパラメータを使用して、高速サインインを設定できます。ただし、モバイルクライアントの場合は、STARTUP_AUTHENTICATION_REQUIREDとcachepasswordmobileの両方のパラメータを設定する必要があります。このパラメータの設定の詳細については、最新の*Cisco Jabber* パラメータ リファレンス ガイドを参照してください。

設定の再取得：高速サインインでは、サインインまたはサインアウトのたびにサーバ側の設定を取得しません。これは、以前の Jabber リリースで初回にサインインする場合にのみ発生します。

その後のログインでは、ユーザがサインイン後 7 ~ 9 時間以内 (サインイン後)、または設定を取得するために手動リフレッシュを実行した後で、1 ~ 5 分以内に、サーバから新しい設定を取得するよう要求が送信されます。

7 ～ 8 時間ごとにサーバから設定をフェッチするように、ConfigRefetchInterval パラメータを設定できます。このパラメータの詳細については、最新の*Cisco Jabber* パラメータ リファレンス ガイドを参照してください。

動的な設定変更に対するアクション

Jabber 11.9 では、コンポーネントとサービスが設定変更に対して動的に対応しています。次のような場合は、通知プロンプトが表示されます。

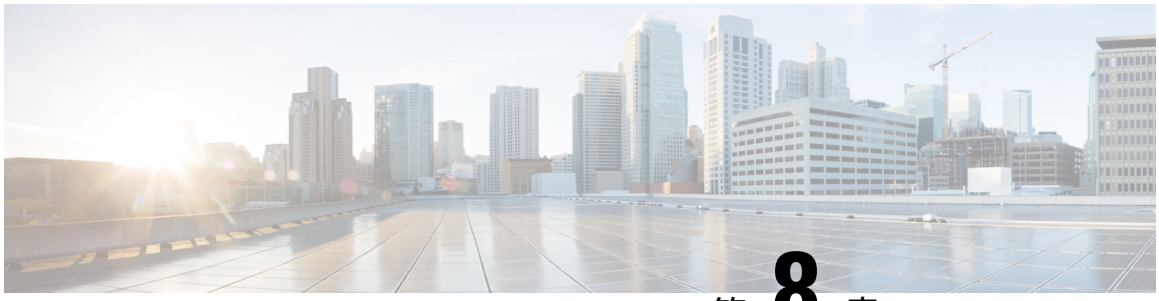
Jabberのリセット：基本サービスを変更した場合は、Jabberのリセットに関する通知プロンプトを受信します。たとえば、IM&P とテレフォニーのアカウントが電話のみのアカウントに変更された場合は、Jabber のリセットが要求されます。

Jabberからのサインアウト：次の表の設定キーを変更した場合は、新しい設定を使用するために、サインアウトとログインのプロンプトが表示されます。

- **Windows**：設定が変更されたことを示すポップアップ通知が表示されます。この通知を無視するか、新しい設定を使用するにはサインアウトとログインを行います。
- **モバイルクライアント**:jabberが自動的にサインアウトします。すると、設定が変更されたことを示すポップアップ通知が表示されます。[OK] をクリックして設定変更を承認すると、Jabber に自動的にサインインされます。

キー名	プラットフォーム	サインアウト
RemoteAccess	すべてのクライアント	サインアウト
Meetings_Enabled	すべてのクライアント	サインアウト
DirectoryServerType	すべてのクライアント	サインアウト
DirectoryUri	すべてのクライアント	サインアウト
UseSipUriToResolveContacts	すべてのクライアント	サインアウト
SipUri	すべてのクライアント	サインアウト
UriPrefix	すべてのクライアント	サインアウト
DirectoryUriPrefix	すべてのクライアント	サインアウト
SwapDisplayNameOrder	すべてのクライアント	サインアウト
PresenceDomain	すべてのクライアント	サインアウト
Support_SSL_Encoding	すべてのクライアント	サインアウト
Support_No_Encoding	すべてのクライアント	サインアウト
IM_Logging_Enabled	すべてのクライアント	サインアウト
IGS_CUP_ENABLESECURE	すべてのクライアント	サインアウト
DISALLOW_FILE_TRANSFER_ON_MOBILE	すべてのクライアント	サインアウト
Persistent_Chat_Enabled	デスクトップ クライアント	Sign out
Persistent_Chat_Mobile_Enabled	モバイル クライアント	サインアウト
Disable_MultiDevice_Message	すべてのクライアント	サインアウト
Location_Enabled/Location_Matching_Mode	すべてのクライアント	サインアウト
IP_MODE	すべてのクライアント	サインアウト

キー名	プラットフォーム	サインアウト
Telephony_Enabled	すべてのクライアント	サインアウト
Voicemail_Enabled	すべてのクライアント	サインアウト
EnableLoadAddressBook	モバイル クライアント	サインアウト
ShowRecentsTab	Jabber Windows のみ	サインアウト
IM_Enabled	すべてのクライアント	サインアウト
Disallow-jaibreak-device	モバイル クライアント	サインアウト
EnableChats	Jabber Windows のみ	サインアウト



第 8 章

画面共有

• 画面共有 （143 ページ）

画面共有

画面共有には次の 4 種類があります。

- Cisco Webex 共有
- BFCP の共有
- IM 専用の共有
- 会議や共有へのエスカレーション

Cisco Webex 画面共有

クラウド展開でのデスクトップ クライアント向け Cisco Jabber に適用されます。

クラウド展開では、BFCP および IM 専用画面共有オプションが使用できない場合、連絡先の選択後に Cisco Webex 画面共有が自動的に選択されます。

Cisco Webex 画面共有を開始するには、次のいずれかの方法を使用します。

- ハブ ウィンドウで連絡先を右クリックし、メニュー オプションから [画面の共有..（Share screen..）] を選択します。
- ハブ ウィンドウで連絡先を選択し、[設定（Settings）] をクリックします。[通信（Communicate）] を選択し、メニュー オプションから [画面の共有..（Share screen..）] を選択します。
- BFCP および IM 専用画面共有オプションが使用できない場合、対話ウィンドウで、メニュー オプションから **... を選択します。** > **メニューオプション**から画面を共有します。

BFCP の画面共有

Cisco Jabberデスクトップ クライアントに適用され、モバイル クライアント向けの Cisco Jabber は BFCP の画面共有の受信のみ可能です。

Binary Floor Control Protocol（BFCP）の画面共有は、Cisco Unified Communications Manager によって制御されます。Cisco Unified Communications Manager は、ビデオ デスクトップ共有機能使用時にユーザが送信する BFCP パケットを処理します。コールの場合、**...を選択します。** > **画面を共有**すると、BFCP 画面の共有が始まります。

リモート スクリーン制御はこの機能でサポートされていません。

BFCP を使用したビデオ デスクトップ共有は、[信頼できるリレーポイント（Trusted Relay Point）] または [メディアターミネーションポイント（Media Termination Point）] がソフトフォン デバイスで有効にされている場合、サポートされません。

（注） Jabber for Windows では、**Screen share**ボタンはデフォルトで bfcp 画面共有を開始します。BFCP ベースの共有が利用できない場合、可能であればボタンにより IM のみのスクリーン共有が開始します。

IM 専用画面の共有

Cisco Jabber for Windows に適用されます。

IM のみのスクリーン共有は、RDP を使用する 1 対 1 のスクリーン共有です。EnableP2PDesktopShare パラメータでは、IM のみのスクリーン共有が利用可能であるかどうかを制御します。PreferP2PDesktopShare パラメータでは、jabber がビデオ共有または IM のみの画面共有を優先するかどうかを制御します。

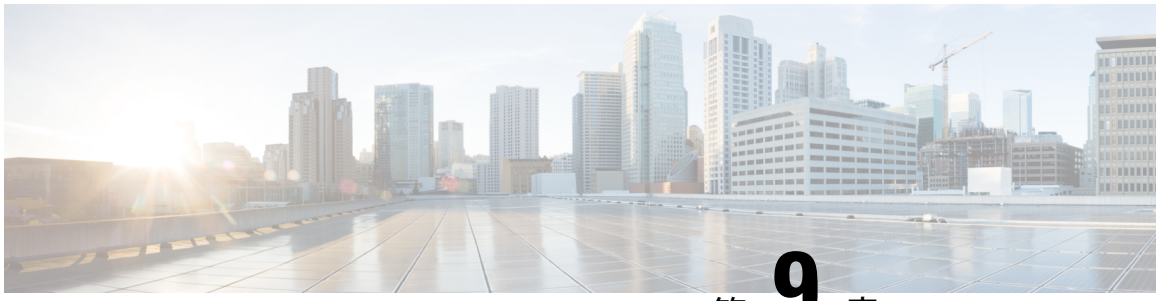
導入時に IM のみのスクリーン共有が許可している場合は、**...を選択します画面の共有を開始するための、チャットウインドウ内での** > **画面の共有**。

デフォルトでは、RDP でポート 3389 が開いている必要があります。Jabber は、IM 専用の画面共有に対して、デフォルトポート範囲の 49152～65535 を備えています。SharePortRangeStart パラメータと SharePortRangeSize パラメータを使用して、ポート幅を制限することができます。

会議や共有へのエスカレーション

すべての Cisco Jabber クライアントに適用されます。

インスタント Cisco Webex Meetings にエスカレーションでき、Cisco Webex Meetings 制御を使用して画面を共有できます。



第 9 章

フェデレーション

- ドメイン間フェデレーション （145 ページ）
- ドメイン内フェデレーション （146 ページ）

ドメイン間フェデレーション

ドメイン間フェデレーションでは、エンタープライズ ドメイン内の Cisco Jabber ユーザは、他のドメイン内のユーザとアベイラビリティを共有し、それらのユーザにインスタント メッセージを送信できます。

- Cisco Jabber ユーザは他のドメインの連絡先を手動で入力する必要があります。
- Cisco Jabber がサポートしているフェデレーション先は次のとおりです。
  - Microsoft Office Communications Server
  - Microsoft Lync
  - IBM Sametime
  - Google Talk などの XMPP 標準ベースの環境

（注） 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。

  - AOL Instant Messenger

Cisco Unified Communications Manager IM and Presence サービスで、Cisco Jabber に対してドメイン間フェデレーションを設定します。詳細については、該当するサーバのドキュメント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では、同じドメイン内のユーザはアベイラビリティを共有し、Cisco Unified Communications Manager IM and Presence サービスと Microsoft Office Communications Server、Microsoft Live Communications Server、または他のプレゼンス サーバとの間でインスタント メッセージを送信できます。

ドメイン内フェデレーションを使用すると、ユーザを別のプレゼンス サーバから Cisco Unified Communications Manager IM and Presence サービスに移行できます。そのために、プレゼンス サーバ上で Cisco Jabber 用のドメイン内フェデレーションを設定します。詳細については、次の各項を参照してください。

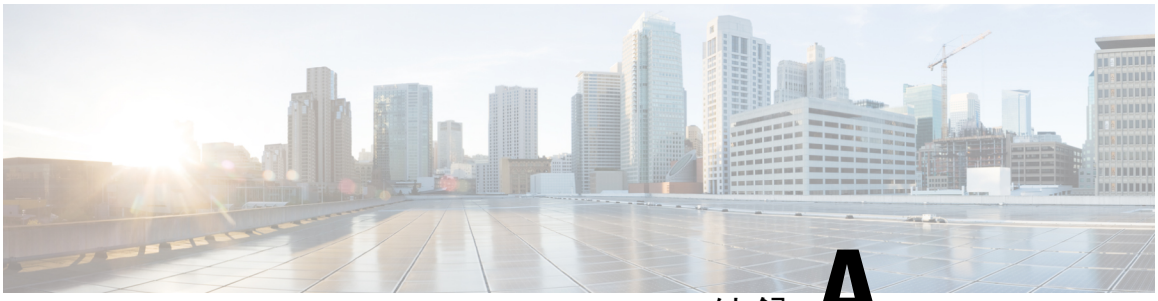
- Cisco Unified Communications Manager IM and Presence サービス：『*Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』

付 録

Jabber がサポートされている言語

- サポートされる言語 （149 ページ）

Jabber がサポートされている言語



付録 A

サポートされる言語

次の表に、Cisco Jabber クライアントがサポートするロケール ID（LCID）または言語 ID（LangID）を示します。

サポートされる言語	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android、Cisco Jabber for iPhone and iPad	LCID/LangID
アラビア語（サウジアラビア）	X		X	1025
ブルガリア語（ブルガリア）	X	X		1026
カタロニア語（スペイン）	X	X		1027
簡体字中国語（中国）	X	X	X	2052
繁体字中国語（台湾）	X	X	X	1028
クロアチア語（クロアチア）	X	X	X	1050
チェコ語（チェコ共和国）	X	X		1029
デンマーク語（デンマーク）	X	X	X	1030
オランダ語（オランダ）	X	X	X	1043
英語（米国）	X	X	X	1033

サポートされる言語	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android、Cisco Jabber for iPhone and iPad	LCID/LangID
フィンランド語（フィンランド）	X	X		1035
フランス語（フランス）	X	X	X	1036
ドイツ語（ドイツ）	X	X	X	1031
ギリシャ語（ギリシャ）	X	X		1032
ヘブライ語（イスラエル）	X			1037
ハンガリー語（ハンガリー）	X	X	X	1038
イタリア語（イタリア）	X	X	X	1040
日本語（日本）	X	X	X	1041
韓国語（韓国）	X	X	X	1042
ノルウェー語（ノルウェー）	X	X		2068
ポーランド語（ポーランド）	X	X		1045
ポルトガル語（ブラジル）	X	X	X	1046
ポルトガル語（ポルトガル）	X	X		2070
ルーマニア語（ルーマニア）	X	X	X	1048
ロシア語（ロシア）	X	X	X	1049
セルビア語	X	X		1050

サポートされる言語	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android、Cisco Jabber for iPhone and iPad	LCID/LangID
スロバキア語（スロバキア）	X	X	X	1051
スロベニア語（スロベニア）	X	X		1060
スペイン語（スペイン（インターナショナル ソート））	X	X	X	3082
スウェーデン語（スウェーデン）	X	X	X	5149
タイ語（タイ）	X	X		1054
Turkish	X	X	X	1055