Cisco Jabber 11.5 計画ガイド

初版：2015 年 12 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/

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

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

新機能および変更情報 ix

新機能および変更情報 ix

Jabber の概要 1

このマニュアルの目的 1

Cisco Jabber について 1

Cisco Jabber 計画チェックリスト 2

サポートされる言語 2

要件 7

サーバ要件 7

オペレーティング システム要件 9

Cisco Jabber for Windows のオペレーティング システム 9

Cisco Jabber for Mac のオペレーティング システム 9

Cisco Jabber for Android のオペレーティング システム 9

Cisco Jabber for iPhone and iPad のオペレーティング システム 10

ハードウェア要件 10

デスクトップ クライアントのハードウェア要件 10

CTI でサポートされるデバイス 11

Cisco Jabber for Android のハードウェア要件 11

Cisco Jabber for iPhone and iPad のハードウェア要件 17

ネットワークの要件 18

ポートおよびプロトコル 19

サポートされるコーデック 24

仮想環境の要件 25

音声およびビデオのパフォーマンス参照 26

Cisco Jabber デスクトップ クライアントの音声ビット レート 26

Cisco Jabber モバイル クライアントの音声ビット レート 26

Cisco Jabber デスクトップ クライアントのビデオ ビット レート 27
Cisco Jabber for Android のビデオ ビット レート 27
Cisco Jabber for iPhone and iPad のビデオ ビット レート 28
プレゼンテーションのビデオ ビット レート 28
ネゴシエートされた最大ビット レート 28
COP ファイル 29
帯域幅 30
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 30
Cisco Jabber for Android の帯域幅パフォーマンス予測 31
Cisco Jabber for iPhone and iPad の帯域幅パフォーマンス予測 32
ビデオ レート アダプテーション 33
導入シナリオ 35
オンプレミス展開 35
Cisco Unified Communications Manager IM and Presence Service によるオンプレミス展開 36
コンピュータ テレフォニー インテグレーション従属 37
電話機モードでのオンプレミス展開 38
ソフトフォン 39
デスクフォン 39
Extend and Connect 39
クラウドベース展開 40
クラウドベース展開 40
ハイブリッド クラウドベース展開 41
仮想環境での展開 42
仮想環境とローミング プロファイル 42
リモート アクセス 44
Expressway Mobile and Remote Access 44
サポートされるサービス 44
Cisco AnyConnect の展開 51
シングル サインオンを使用した展開 52
シングル サインオンの要件 53
シングル サインオンとリモート アクセス 55
ユーザ管理 57

Jabber ID 57
IM アドレス スキーム 57
Jabber ID によるサービス ディスカバリ 59
SIP URI 59
LDAP ユーザ ID 59
フェデレーション用ユーザ ID の計画 59
ユーザの連絡先写真のプロキシ アドレス 60
認証 60
Cisco Unified Communications Manager の LDAP 認証 60
WebEx Messenger のログイン認証 60
シングル サインオン認証 60
ボイスメール認証 60
複数リソースのログイン 61
サービス ディスカバリ 63
クライアントによるサービスへの接続方法 63
Cisco WebEx サービス ディスカバリ 64
シスコ クラスタ間検索サービス 64
Expressway for Mobile and Remote Access サービス ディスカバリ 64
推奨される接続方法 64
認証ソース 67
クライアントがサービスを検出する方法 67
方法 1：サービスの検索 69
クライアントによる利用可能なサービスの検出方法 70
クライアントによる HTTP クエリーの発行 71
クライアントからのネーム サーバのクエリー 72
クライアントの内部サービスへの接続 73
Expressway for Mobile and Remote Access を介したクライアントの接続 75
Cisco UDS SRV レコード 76
Collaboration Edge SRV レコード 77
DNS の設定 79
クライアントが DNS を使用する方法 79
クライアントがネーム サーバを検索する方法 79
クライアントがサービス ドメインを取得する方法 79

ドメイン ネーム システムの設計 80
独立ドメイン設計 81
独立ドメイン構造での SRV レコード導入 81
サービス ドメインへの内部ゾーンの使用 82
同一ドメイン設計 82
単一ドメイン（スプリット ブレイン） 82
単一ドメイン（非スプリット ブレイン） 83
方法 2：カスタマイズ 83
サービス ディスカバリのカスタマイズ 83
Cisco Jabber for Windows のカスタム インストール 83
インストーラ スイッチ：Cisco Jabber for Windows 84
Cisco Jabber for Mac/iPhone and iPad/Android のカスタム インストール 84
URL 設定 84
企業モビリティ管理によるモバイルの設定 84
方法 3：手動インストール 85
高可用性 85
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 85
フェールオーバー中のクライアントの動作 87
音声およびビデオのハイ アベイラビリティ 88
Survivable Remote Site Telephony 88
設定のプライオリティ 89
[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 89
連絡先ソース 91
ディレクトリ サーバ 91
連絡先ソースとは 92
ディレクトリ統合を設定するタイミング 92
連絡先ソースが必要な理由 93
連絡先ソース オプション 93
LDAP オプション：EDI と BDI 94
拡張ディレクトリ統合 94
ドメイン名の検索 94
ディレクトリ サーバの検出 95

基本ディレクトリ統合 95
Cisco Unified Communications Manager User Data Service 96
複数のクラスタでの連絡先の解決 97
LDAP の前提条件 98
LDAP サービス アカウント 98
Jabber ID 属性マッピング 99
Jabber ID の検索 99
ローカル連絡先ソース 99
カスタム連絡先ソース 100
連絡先のキャッシュ 100
ダイヤル プランのマッピング 100
Cisco Unified Communication Manager UDS for Mobile and Remote Access 101
クラウドの連絡先ソース 101
Cisco WebEx 連絡先ソース 101
連絡先の写真の形式と寸法 101
連絡先の写真の形式 101
連絡先の写真の寸法 102
連絡先の写真の調整 102
セキュリティおよび証明書 105
暗号化 105
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 105
インスタント メッセージの暗号化 105
オンプレミス暗号化 106
クラウドベースの暗号化 107
クライアント間の暗号化 108
暗号化アイコン 109
サーバの暗号化対応クライアント用のロック アイコン 110
クライアントの暗号化対応クライアント用の鍵アイコン 110
ローカルのチャット履歴 110
音声およびビデオの暗号化 111
連邦情報処理標準規格 111
Secure LDAP 112
証明書 112

証明書の検証 112
オンプレミス サーバに必要な証明書 113
証明書署名要求の形式と要件 114
失効サーバ 115
証明書のサーバ識別情報 115
マルチサーバ SAN の証明書 116
クラウド展開の証明書検証 116
画面共有 119
画面共有 119
Cisco WebEx 画面共有 119
BFCP の画面共有 120
IM 専用画面の共有 120
会議や共有へのエスカレーション 120
フェデレーション 121
ドメイン間フェデレーション 121
ドメイン内フェデレーション 122
フェデレーション用ユーザ ID の計画 122

新機能および変更情報

- 新機能および変更情報，ix ページ

新機能および変更情報

変更の詳細	日付	参照先
モバイル クライアント向け Cisco Jabber： • 「*Hardware Requirements for Cisco Jabber for iPhone and iPad*」の項を更新。 • 「*Hardware Requirements for Cisco Jabber for Android*」の項を更新。	2016 年 1 月 29 日	目次を参照
Cisco Jabber for Android： • 「*Hardware Requirements for Cisco Jabber for Android*」の項を更新。 • 「高解像度のビデオ送信をサポートする *Android* デバイス（*Android Devices That Support Sending High Definition Videos*）」の項を追加。 • 「*Cisco Jabber for Android* の *COP* ファイル（*COP files for Cisco Jabber for Android*）」の項を更新。	2015 年 12 月 22 日	目次を参照

新機能および変更情報

第 1 章

Jabber の概要

- このマニュアルの目的，1 ページ
- Cisco Jabber について，1 ページ
- Cisco Jabber 計画チェックリスト，2 ページ
- サポートされる言語，2 ページ

このマニュアルの目的

『*Cisco Jabber* 計画ガイド』には、Cisco Jabber の展開とインストールの計画を支援する次の情報が記載されています。

- このリリースの製品で使用可能な機能に関する製品概要
- サービス ディスカバリ、暗号化、および連絡先ソース（拡張ディレクトリ統合（EDI）および 基本ディレクトリ統合（BDI））に関する計画の考慮事項。
- オンプレミス展開かクラウド展開かに関係しない、クライアントの展開方法に関する情報。
- ハードウェア、ソフトウェア、ネットワーク、および証明書の要件。

Cisco Jabber を展開してインストールするには、『*Cisco Jabber Deployment and Installation Guide*』を使用します。

Cisco Jabber について

Cisco Jabber は、あらゆる場所から連絡先とのシームレスな対話を実現する Unified Communications アプリケーション スイートです。Cisco Jabber は、IM、プレゼンス、音声およびビデオ通話、ボイスメール、および会議を提供します。

Cisco Jabber 製品ファミリには、次のようなアプリケーションが含まれています。

- Cisco Jabber for Android

- Cisco Jabber for iPhone and iPad
- Cisco Jabber for Mac
- Cisco Jabber for Windows

Cisco Jabber 製品スイートの詳細については、http://www.cisco.com/go/jabber を参照してください。

Cisco Jabber 計画チェックリスト

Cisco Jabber 展開を計画するときにこのチェックリストを使用します。

タスク	参照先	完了
サーバ、ハードウェア、およびネットワークが要件を満たしていることを確認する。	要件, （7 ページ）	
Cisco Jabber の展開方法を決定する。	導入シナリオ, （35 ページ）	
ユーザ管理の計画する。	ユーザ管理, （57 ページ）	
サービスディスカバリを確認して、サービスディスカバリを設定し、必要なサービス ディスカバリ レコードを決定するかどうかを判断する。	サービス ディスカバリ, （63 ページ）	
連絡先ソースの設定方法を決定する。	連絡先ソース, （91 ページ）	
選択した展開オプションに基づいて必要な証明書および保障があるかどうかを確認する。	セキュリティおよび証明書, （105 ページ）	
利用可能な画面共有オプションを確認します。	画面共有, （119 ページ）	
展開で利用可能なフェデレーションを確認します。	フェデレーション, （121 ページ）	

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		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
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

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
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		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		1048
ロシア語（ロシア）	X	X	X	1049
セルビア語	X	X		1050
スロバキア語（スロバキア）	X	X		1051
スロベニア語（スロベニア）	X	X		1060

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
トルコ語	X	X		1055

第 2 章

要件

- サーバ要件，7 ページ
- オペレーティング システム要件，9 ページ
- ハードウェア要件，10 ページ
- ネットワークの要件，18 ページ
- 仮想環境の要件，25 ページ
- 音声およびビデオのパフォーマンス参照，26 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 and Presence	Cisco Unified Communications Manager IM and Presence Service	9.x 以降
	Cisco WebEx Messenger	
テレフォニー	Cisco Unified Communications Manager	9.x 以降
	Cisco Unified Survivable Remote Site Telephony	8.5 以降
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	8.6(2)* 以降

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	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	コラボレーション会議室対応 Cisco WebEx Meetings Server
	Cisco WebEx Meetings Server	2.0 以降 Cisco Jabber for Windows は 1.5 以降に対応
	Cisco WebEx Meeting Center	WBS28 以降
	Cisco WebEx Meetings Client Cisco Jabber for Android にのみ適用。	4.5 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	8.1.1 以降
	Cisco Expressway E	8.1.1 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 Cisco Jabber for Windows 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）
- Microsoft Windows 7

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

Microsoft Windows 7 または 8.x の場合は、デスクフォン ビデオで使用するために Cisco Media Services Interface（MSI）4.1.2 をダウンロードできます。

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。

Cisco Jabber for Mac のオペレーティング システム

Cisco Jabber for Mac 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。

- Apple OS X El Capitan 10.11（以降）
- Apple OS X Yosemite 10.10（以降）
- Apple OS X Mavericks 10.9（以降）

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

Cisco Jabber for Android のインストールに必要なオペレーティング システムについては、「*Hardware Requirements for Cisco Jabber for Android*」を参照してください。

（注） Cisco Jabber が Android 6.0 Marshmallow OS 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。

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

Cisco Jabber for iPhone and iPad は次のオペレーティング システムをサポートします。

- iOS 9 以降
- watchOS 2

重要 シスコは、Cisco Jabber for iPhone and iPad 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	Cisco Jabber for Windows	Cisco Jabber for Mac
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

要件	Cisco Jabber for Windows	Cisco Jabber for Mac
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 • Mac Pro • MacBook Pro（Retina Display モデルを含む） • MacBook • MacBook Air • iMac • Mac Mini
GPU	Microsoft Windows 7 上の DirectX11	該当なし
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

コンピュータ テレフォニー インテグレーション（CTI）対応デバイスの一覧を表示するには、Cisco Unified Reporting から、[Unified CM電話機能リスト（Unified CM Phone Feature List）] を選択します。[機能（Feature）] ドロップダウン リストから、[CTI制御（CTI controlled）] を選択します。

Cisco Jabber for Android のハードウェア要件

（注） Cisco Jabber for Android は、ここに記載された Android デバイスによってテストされています。他の Android デバイスは正式にはサポートされていませんが、それらの Android デバイスで Cisco Jabber for Android を使用できる場合もあります。

Android デバイスの CPU およびディスプレイの最小要件は次のとおりです。

- チップセット：Intel チップセットに基づく Android デバイスはサポートされません。
- Android オペレーティング システム：4.1.2 以降
- CPU：1.5 GHz デュアルコア、1.2 GHz クアッドコア以上（クアッドコアを推奨）。
- ディスプレイ：双方向ビデオの場合は、最小ディスプレイ解像度要件が 480 x 800 です。

（注）
- Cisco Jabber for Android は Tegra 2 チップセットをサポートしません。
- 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。この問題が発生した場合は、『*Cisco Jabber for Android User Guide*』の「トラブルシューティング」の章を参照してください。

Cisco Jabber for Android は、次の最小限の仕様を満たす Android デバイスで IM 専用モードをサポートします。

- チップセット：Intel チップセットに基づく Android デバイスはサポートされません。
- Android OS：4.1.2 以降
- CPU：1.5 GHz デュアルコア、1.2 GHz クアッドコア以上（クアッドコアを推奨）。
- ディスプレイ：320 X 480 以上。

Cisco Jabber for Android は、最小ハードウェア要件を満たす Samsung デバイスで、音声およびビデオ対応モードをサポートします。次の Samsung デバイスは、テストおよび認定されています。

Samsung Galaxy	オペレーティング システム
A7	Android OS 4.4.4 以降
A8	Android OS 5.1.1 以降
Rugby Pro	Android OS 4.2.2 以降
Xcover3	Android OS 4.4.4 以降
Note II	Android OS 4.2 以降
Note III	Android OS 4.3 以降
Note IV	Android OS 4.4.4 以降
Note 5	Android OS 5.1.1 以降
Note Edge	Android OS 4.4.4 以降
SII	Android OS 4.1.2 以降
SIII	Android OS 4.2.2 以降
S4	Android OS 4.2.2 以降

Samsung Galaxy	オペレーティング システム
S4 mini	Android OS 4.2.2 以降
S5	Android OS 4.2.2 以降
S5 mini	Android OS 4.2.2 以降
S6	Android OS 5.0.2 以降
S6 Edge	Android OS 5.0.2 以降
S6 Edge+	Android OS 5.1.1 以降
Tab 4 7 インチ、8 インチ、および 10.1 インチ	Android OS 4.4.2 以降
Tab PRO 8.4 インチおよび 10.1 インチ	Android OS 4.4.2 以降
Tab S 8.4 インチおよび 10.5 インチ	Android OS 4.4.2 以降
Tab 3 8 インチ	Android OS 4.4 以降
Note Pro 12.2	Android OS 4.4.2 以降
Note 10.1 インチ（2014 年モデル）	Android OS 4.4.2 以降

Cisco Jabber for Android は、表に示すオペレーティング システムのバージョンを搭載した各デバイスで、音声およびビデオ対応モードをサポートします。

Device	デバイス モデル	オペレーティング システム
Cisco DX	70	バージョン 10.2.x
	80	バージョン 10.2.x
	650	バージョン 10.2.x
HTC	M7	Android OS 4.4.2 以降
	M8	Android OS 4.4.2 以降
	M9	Android OS 5.0.2 以降
	One Max	Android OS 4.4.2 以降
	E9 PLUS	Android OS 5.0.2 以降

Device	デバイス モデル	オペレーティング システム
Google Nexus	4	Android OS 5.1.1 以降
	5	Android OS 4.4 以降
	6	Android OS 5.0.2 以降
	7	Android OS 4.4 以降
	9	Android OS 5.0.2 以降
	10	Android OS 4.4 以降
LG	G2	Android OS 4.2.2 以降
	G3	Android OS 4.4.2 以降
	G4	Android OS 5.1 以降
記号	Moto G	Android OS 4.4.2 以降
	MC40	Android OS 4.1.1 [1]
Sony Xperia	ZR/A	Android OS 4.1.2 以降
	M2	Android OS 4.3 以降
	Z1	Android OS 4.2 以降
	Z2	Android OS 4.4.2 以降
	Z2 tablet	Android OS 4.4.2 以降
	Z3	Android OS 4.4.2 以降
	Z3 Tablet Compact	Android OS 4.4.4 以降
	Z3+/Z4[2]	Android OS 5.0.2 以降
	Z4 TAB	Android OS 5.0 以降
Huawei	G6	Android OS 4.2.2 以降
	Mate 7	Android OS 4.4 以降
	P8	Android OS 4.4.4 以降

Device	デバイス モデル	オペレーティング システム
Sonim	XP7	Android OS 4.4.4
Xiaomi	Mi 4	Android OS 4.4 以降
	Mi Note	Android OS 4.4.4 以降
	Mi Pad	Android OS 4.4.4 以降
Fujitsu	ARROWS M305	Android OS 4.4.2 以降
Honeywell Dolphin	CT50	Android OS 4.4.4 以降

1 Cisco Jabber は MC40 デバイスでのオーディオ モードのみをサポートします。
2 ビデオ コールは Sony Z3+/Z4 には適していません。ビデオ コールのセルフ ビデオを無効にするか、ボイス コールのみを行うことができます。

Cisco Jabber for Android の Android バージョン 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 カーネルをバージョン 3.10 以降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 4.4.2 以降
HTC M8	Android OS 4.4.2 以降
HTC M9	Android OS 5.0.1 以降
HTC One Max	Android OS 4.4.2 以降

デバイス モデル	オペレーティング システム
Sony Xperia M2	Android OS 4.3 以降と 3.10.49 より前のカーネル バージョン [3]
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 4.4 以降）
Xiaomi Mi Note	（Android OS 4.4.4 以降）
Xiaomi Mi Pad	（Android OS 4.4.4 以降）
Sonim XP7	（Android OS 4.4.4）

[3] 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。

サポートされる Bluetooth デバイス

Bluetooth デバイス	便利な情報
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。
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。
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 Wave+	

Bluetooth デバイス	便利な情報
Jabra BIZ 2400	
Jabra Easygo	
Jabra PRO 9470	
Jabra Speak 510	
Jabra Supreme UC	
Jabra Stealth	
Jabra Evolve 65 UC Stereo	
Plantronics Voyager Legend	
Plantronics Voyager Legend UC	
Plantronics Voyager Edge UC	
Plantronics Voyager Edge	
Plantronics PLT Focus	

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

Android Wear

Cisco Jabber は、Android OS 5.0 以降と Google Play Service 8.3 以降が搭載されたすべての Android Wear でサポートされます。Cisco Jabber は、次の Android Wear デバイスでテストされています。

- Samsung Gear live
- LG G Watch R
- Sony SmartWatch 3
- LG Watch Urbane
- Moto 360

Cisco Jabber for iPhone and iPad のハードウェア要件

iOS 8 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。

Apple デバイス	生成
iPod Touch	5 および 6
iPhone	4S、5、5c、5s、6、6 Plus、、6s、6s Plus および Apple Watch
iPad	2、3、4、12.9 inch iPad Pro、および
iPad mini	mini 1、mini 2、mini 3 および mini 4
iPad Air	Air1 と Air 2

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。

Jabra Easygo	Jabra Speak 510
Jabra EXTREME 2	Jawbone ICON（Cisco Bluetooth ヘッドセット用）
Jabra Speak 450 for Cisco	Jabra Stealth
Jabra Supreme UC	Jabra Evolve 65 UC Stereo
Jabra Wave+	Plantronics Voyager Legend
Jabra Motion は、[4]。[5]	Plantronics Voyager Legend UC
Sony Ericsson Bluetooth Headset BW600	Plantronics Voyager Edge
Jabra PRO 9470	Plantronics Voyager Edge UC
Jabra BIZ 2400	

ネットワークの要件

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。

[4] Cisco Jabber の通話に対する Bluetooth 制御をサポートしています
[5] 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。

- 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。

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)*』

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
設定				

	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
	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 Messenger 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 over 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	TCP	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				

	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	UDP	オーディオまたはビデオ用の RTP メディア ストリームを送信する。
	49152 ～ 65535	RDP	TCP	IM 専用画面の共有。Cisco Jabber for Windows にのみ適用されます。
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 Meeting Center に接続する。
	443	HTTPS	TCP	会議用の Cisco WebEx Meeting Center 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）。

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 Server については、『*Administration Guide*』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	コーデック	コーデック タイプ	Cisco Jabber for Android	Cisco Jabber for iPhone and iPad	Cisco Jabber for Mac	Cisco Jabber for Windows
音声	G.711	A-law	○ 通常モードをサポートします。		○	
		μ-law/Mu-law	○ 通常モードをサポートします。		○	
	G.722		○		○	
	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。		○	
	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。		X	
	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。		○	
	Opus		○		○	
ビデオ	H.264/AVC		○		○	

タイプ	コーデック	コーデック タイプ	Cisco Jabber for Android	Cisco Jabber for iPhone and iPad	Cisco Jabber for Mac	Cisco Jabber for Windows
ボイスメール	G.711	A-law	○		X	
		μ-law/Mu-law（デフォルト）	○		X	
	GSM 6.10		○		X	
	PCM リニア		○		X	

Cisco Jabber for Android または Cisco Jabber for iPhone and iPad 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 Cisco Jabber for Windows 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	7.6、7.5、7.1
Citrix XenApp	7.6、公開されたデスクトップ 7.5、公開されたデスクトップ 6.5、公開されたデスクトップ
VMware Horizon View	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、Cisco Virtualization Experience Media Engine（VXME）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。

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
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	1280 X 720	1300

（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

クライアントは 15 fps でビデオをキャプチャして送信します。

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

高解像度のビデオ送信をサポートする Android デバイス

Cisco Jabber for Android は、次のデバイスでのビデオ コールを介した高解像度のビデオ送信をサポートします。

- Samsung Galaxy S6
- Samsung Galaxy S6 edge
- Samsung Galaxy S6 edge+
- Samsung Galaxy Note5

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
1280 x 800	100	400

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。

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。

COP ファイル

すべてのクライアントで必要な COP ファイル

- cmterm-bfcp-e.8-6-2.cop.sgn：Cisco Unified Communications Manager リリース 9.x 以降でビデオ デスクトップ共有を設定します。
- cmterm-cucm-uds-912-5.cop.sgn：Cisco Unified Communications Manager 9.1(2)。

Cisco Jabber for Android 用 COP ファイル

- Android タブレット：
  - `cmterm-jabbertablet-install-151020.k3.cop.sgn`：Cisco Unified Communications Manager のすべてのバージョン用。
- Android 電話：
  - `cmterm-android-install-151020.k3.cop.sgn`：Cisco Unified Communications Manager のすべてのバージョン用。

Cisco Jabber for iPhone and iPad 用の COP ファイル

- iPhone
  - `cmterm-iphone-install-151020.k3.cop.sgn`：Cisco Unified Communications Manager のすべてのバージョン用。
- iPad
  - `cmterm-jabbertablet-install-151020.k3.cop.sgn`：Cisco Unified Communications Manager のすべてのバージョン用。

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	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（512x288）（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（512x288）（30 fps）
1000 kbps	帯域幅は音声コーデック用に十分です。	w576p（1024x576）（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	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（512x288）（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（512x288）（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（1024x576）（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	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。
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	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）

アップロード速度	音声	音声+インタラクティブ ビデオ（メイン ビデオ）
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。

第 3 章

導入シナリオ

- オンプレミス展開，35 ページ
- クラウドベース展開，40 ページ
- 仮想環境での展開，42 ページ
- リモート アクセス，44 ページ
- シングル サインオンを使用した展開，52 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。

次のモードで Cisco Jabber を展開できます。

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

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

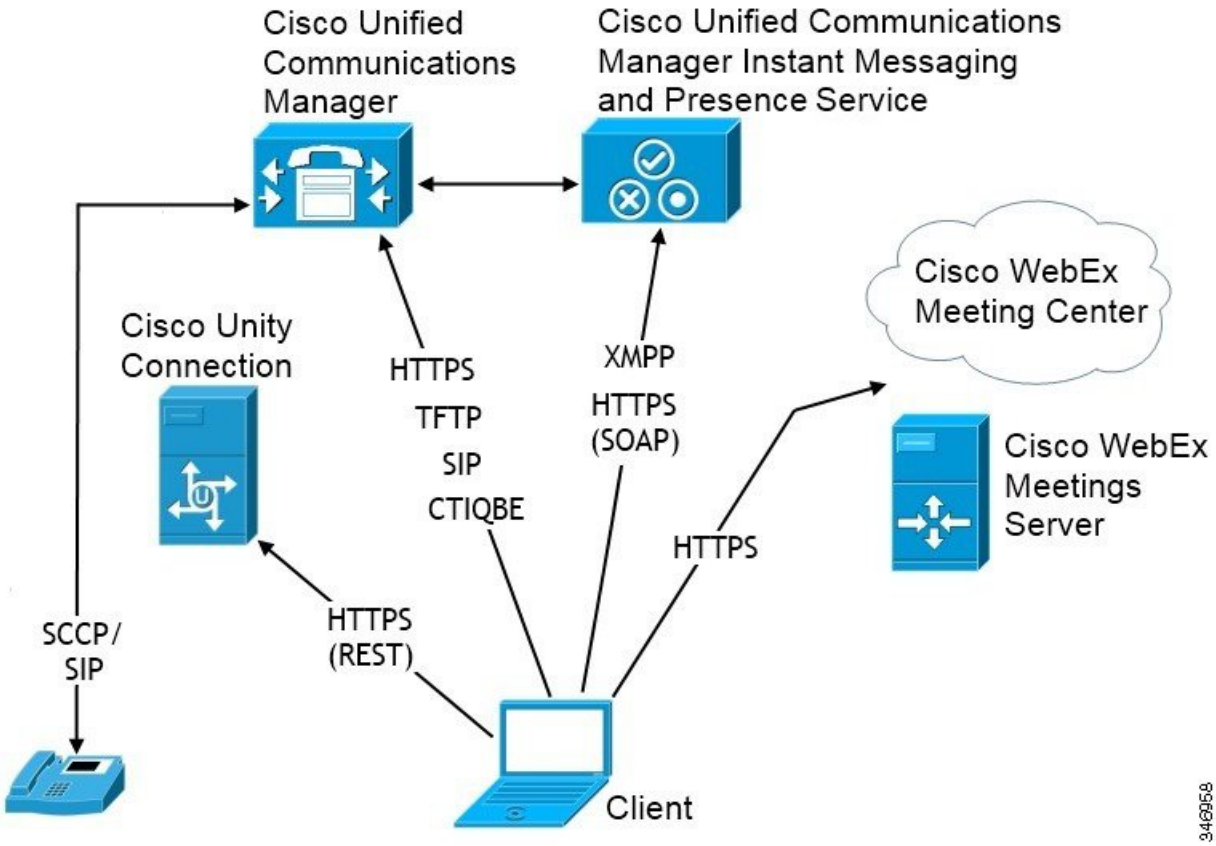
Cisco Unified Communications Manager IM and Presence Service によるオンプレミス展開

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

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

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



コンピュータ テレフォニー インテグレーション従属

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

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

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

- Cisco TAPI： http://developer.cisco.com/web/tapi/home

- Cisco JTAPI： http://developer.cisco.com/web/jtapi/home

電話機モードでのオンプレミス展開

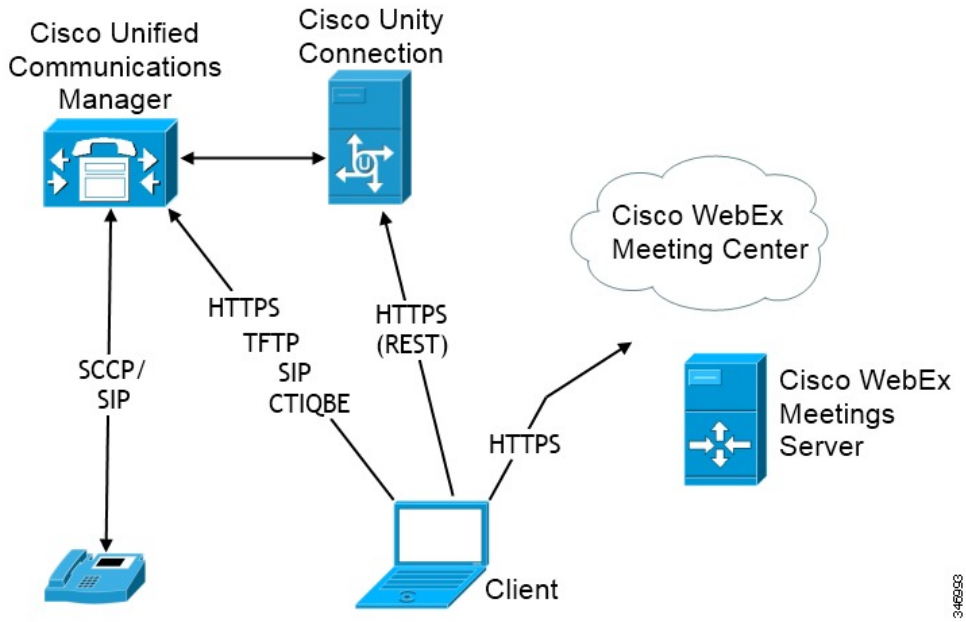
電話機モード展開で使用可能なサービスは次のとおりです。

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

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

次の図は、電話モードでのオンプレミス展開のアーキテクチャを示しています。

図 *2*：電話機モードでのオンプレミス展開



ソフトフォン

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

デスクフォン

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

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

Extend and Connect

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

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

クラウドベース展開

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

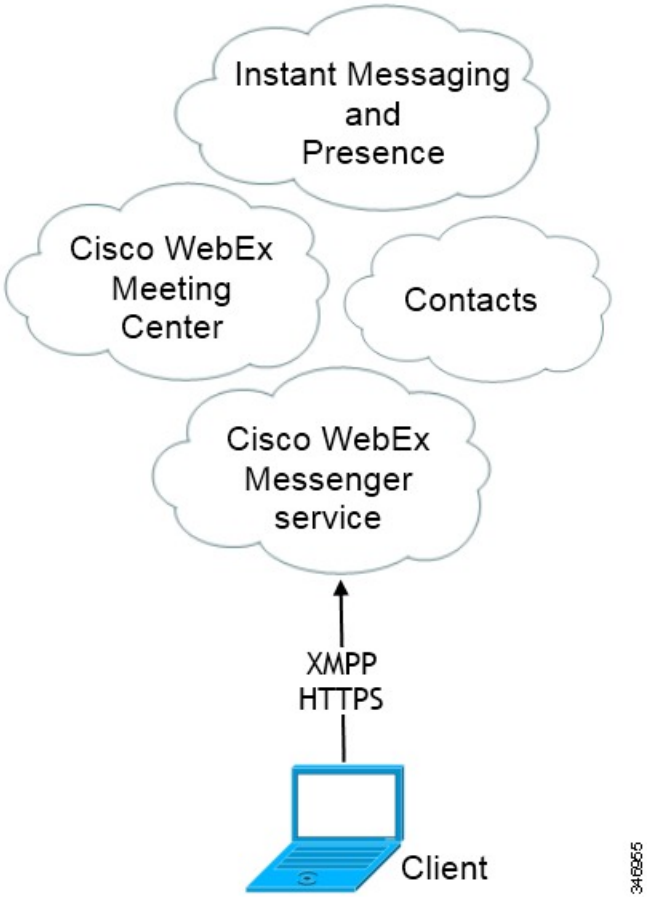
クラウドベース展開

クラウドベース展開で使用可能なサービスは次のとおりです。

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

次の図は、クラウドベース展開のアーキテクチャを示しています。

図 *3*：クラウドベース展開



ハイブリッド クラウドベース展開

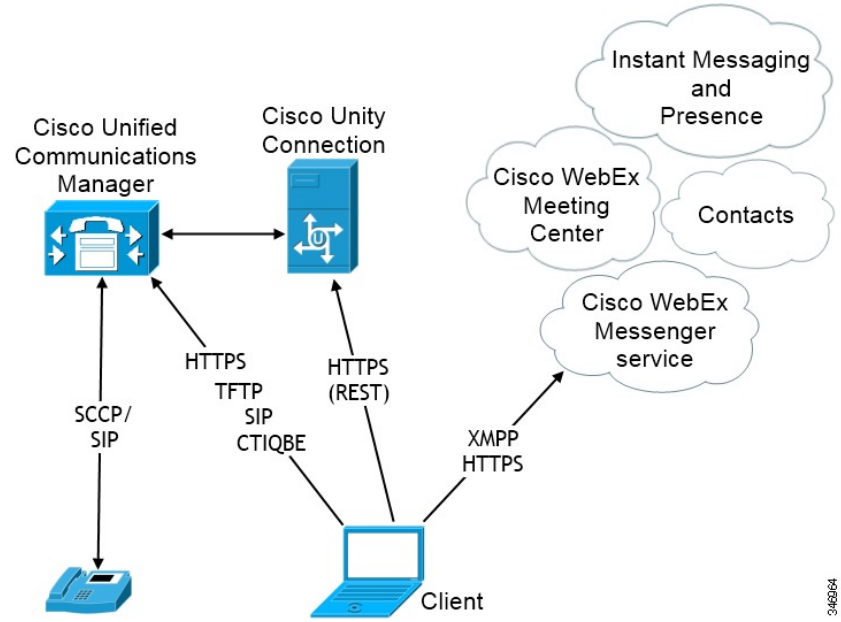
ハイブリッド クラウドベース展開で使用可能なサービスは次のとおりです。

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

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

次の図は、ハイブリッド クラウドベース展開のアーキテクチャを示しています。

図 *4*：ハイブリッド クラウドベース展開



仮想環境での展開

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

仮想環境でサポートされる機能は次のとおりです。

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

仮想環境とローミング プロファイル

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

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

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

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

個人ユーザ設定を保持するには、次を実行する必要があります。

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

リモート アクセス

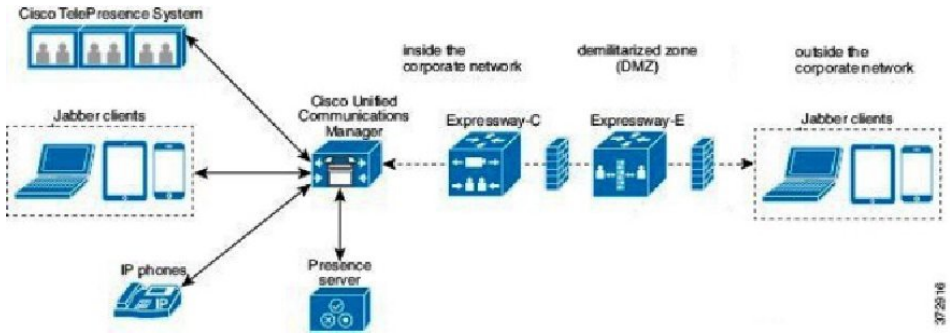
ユーザが企業ネットワークの外部の場所から作業にアクセスしなければならないことがあります。リモート アクセス用のいずれかのシスコ製品を使用して、ユーザが作業にアクセスできるようにします。

Expressway Mobile and Remote Access

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

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

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



サポートされるサービス

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

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

サービス	サポート対象	非サポート対象
ディレクトリ		
UDS ディレクトリ検索	X	
LDAP ディレクトリ検索		X

サービス	サポート対象	非サポート対象
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	
ハイ アベイラビリティ：オンプレミス展開	X	
ファイル転送：オンプレミス展開	X Cisco Unified Communications Manager IM and Presence サービス 10.5(2) 以降を使用したファイル転送に使用可能な高度なオプション、後述の注意を参照してください。	
ファイル転送：クラウド展開	X	
ビデオ画面共有：BFCP	X（モバイル クライアント向け Cisco Jabber は BFCP 受信のみをサポートします）。	
IM 専用画面の共有		x
オーディオとビデオ		

サービス	サポート対象	非サポート対象
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
Dial via Office - リバース（モバイル クライアントのみ）	X	
セッションの永続性		X
アーリー メディア		X
セルフケアポータル アクセス		X
ボイスメール		
ビジュアル ボイスメール	X * Cisco Expressway-C 上で HTTP ホワイト リストを使用	
Cisco WebEx Meetings		
オンプレミス		X
クラウド	X	
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（Cisco Jabber for Windows）		

サービス	サポート対象	非サポート対象
カスタム HTML タブ	X * Cisco Expressway-C 上で HTTP ホワイト リストを使用	
セキュリティ		
エンドツーエンド暗号化	X	
CAPF 登録		X
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	

ディレクトリ

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

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

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

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

- ドメイン内フェデレーション：ドメイン内フェデレーションを展開して、クライアントがファイアウォールの外側から Expressway for Mobile and Remote Access に接続した場合は、連絡先 ID に次の形式のいずれかが使用されている場合にのみ連絡先検索がサポートされます。
  - sAMAccountName@domain
  - UserPrincipleName（UPN）@domain
  - EmailAddress@domain
  - employeeNumber@domain
  - telephoneNumber@domain
- XMPP を使用するドメイン間フェデレーション：Expressway for Mobile and Remote Access は、XMPP ドメイン間フェデレーション自体を有効にするものではありません。Expressway for Mobile and Remote Access 経由で接続された Cisco Jabber クライアントでは、Cisco Unified Communications Manager IM and Presence で有効になっている XMPP ドメイン間フェデレーションを使用できます。

インスタント メッセージおよびプレゼンス

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

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

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

音声コールとビデオ コール

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

- Cisco Unified Communications Manager：Expressway for Mobile and Remote Access は、Cisco Unified Communications Manager バージョン 9.1.2 以降でビデオおよび音声通話をサポートします。
- デスクフォン制御モード（CTI）（デスクトップ クライアントのみ）：クライアントは、エクステンション モビリティを含むデスクフォン制御モード（CTI）をサポートしません。
- Extend and connect（デスクトップ クライアントのみ）：クライアントを以下の目的に使用することはできません。
  - オフィスの Cisco IP Phone でコールを発信および受信する。

- 自宅電話、ホテルの電話、またはオフィスの Cisco IP Phone で、保留と復帰などの通話中制御を実行する。

- セッション永続性：クライアントが使用するネットワークが切り替わると、音声コールおよびビデオ コールが切断され、復帰できません。たとえば、ユーザがオフィス内で Cisco Jabber コールを開始してから、建物を出て Wi-Fi 接続が切断されると、クライアントが Expressway for Mobile and Remote Access を使用するように切り替わるため、コールが切断されます。
- アーリー メディア：アーリー メディアを使用すれば、クライアントは、接続が確立される前にエンドポイント間でデータを交換できます。たとえば、ユーザが同じ組織に属さない通話者にコールを発信し、相手側がこれを拒否したまたはコールに応答しなかった場合、アーリー メディアによってユーザがビジー トーンを受け取るか、ボイスメールがユーザに送信されます。

  Expressway for Mobile and Remote Access を使用している場合は、電話の相手がコールを拒否するか、応答しないと、ビジー トーンが鳴りません。代わりに、ユーザは、コールが終了するまで約 1 分無音を受信します。
- セルフ ケア ポータル アクセス（デスクトップ クライアントのみ）：ユーザは、ファイアウォールの外側にいるときに Cisco Unified Communications Manager のセルフ ケア ポータルにアクセスできません。外部から Cisco Unified Communications Manager のユーザ ページにアクセスできません。

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

ボイスメール

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

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

Cisco WebEx Meetings

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、Cisco WebEx Meeting Center を使用したクラウドベースの会議だけをサポートします。

クライアントは、Cisco WebEx Meetings Server にアクセスしたり、Cisco WebEx の社内会議に参加したり、開始したりできません。

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。

カスタマイゼーション

Cisco Jabber for Windows のみ。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、デスクトップ クライアント用のカスタム HTML タブ設定がサポートされます。

（注） クライアントがカスタム HTML タブ設定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 リストにカスタム HTML タブ設定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。

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、フェールオーバーする Cisco Expressway-E サーバではなく、特定のサービスをセカンダリ サーバ（インスタント メッセージおよびプレゼンスなど）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。

Cisco AnyConnect は、Cisco 5500 シリーズ ASA へのセキュアな IPsec（IKEv2）または SSL VPN 接続をリモート ユーザに提供します。また、Cisco AnyConnect は、ASA からまたは社内ソフトウェア展開システムを使用してリモートユーザに展開できます。ASA から展開する場合は、リモートユーザが、クライアントレス SSL VPN 接続を許可するように設定された ASA のブラウザで IP アドレスまたは DNS 名を入力することによって、ASA への初期 SSL 接続を確立します。その後で、ASA が、ブラウザ ウィンドウにログイン画面を表示し、ユーザがログインと認証を満たした場合に、コンピュータのオペレーティング システムにマッチするクライアントをダウンロードします。ダウンロード後、クライアントは自動的にインストールおよび設定され、ASA への IPsec（IKEv2）接続または SSL 接続が確立されます。

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

関連トピック

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

シングル サインオンを使用した展開

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

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

1. ユーザが Cisco Jabber クライアントを起動します。Web フォームによるサインインをユーザに要求するようにアイデンティティ プロバイダー（IdP）を設定した場合は、クライアント内にそのフォームが表示されます。
2. Cisco Jabber クライアントが、Cisco WebEx Messenger サービス、Cisco Unified Communications Manager、Cisco Unity Connection などの接続先サービスに認証要求を送信します。
3. サービスが IdP に認証を要求するためにクライアントをリダイレクトします。
4. IdP がクレデンシャルを要求します。クレデンシャルは、次のいずれかの方法で指定できます。
   - ユーザ名とパスワードのフィールドがあるフォーム ベースの認証。
   - 統合 Windows 認証（IWA）用 Kerberos（Windows のみ）

- スマート カード認証（Windows のみ）
- HTTP 要求時にクライアントがユーザ名とパスワードを提示する、基本的な HTTP 認証方式。

5 IdP がブラウザまたはその他の認証方式に Cookie を提供します。IdP が SAML を使用して ID を認証すると、サービスはクライアントにトークンを提供できます。
6 クライアントが認証用のトークンを使用してサービスにログインします。

認証方式

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

ユーザ セッション

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

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

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

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

シングル サインオンの要件

SAML 2.0

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

サポートされるアイデンティティ プロバイダー

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

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

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

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

クッキー

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

必要なブラウザ

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

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

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

シングル サインオンとリモート アクセス

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

- シングル サインオン（SSO）は、Cisco Expressway 8.5 と Cisco Unified Communications Manager リリース 10.5.2 以降で使用できます。
- 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から外側にまたはその逆に移動するときに再度サインインするように要求されることがあります。

第 4 章

ユーザ管理

- Jabber ID，57 ページ
- IM アドレス スキーム，57 ページ
- Jabber ID によるサービス ディスカバリ，59 ページ
- SIP URI，59 ページ
- LDAP ユーザ ID，59 ページ
- フェデレーション用ユーザ ID の計画，59 ページ
- ユーザの連絡先写真のプロキシ アドレス，60 ページ
- 認証，60 ページ
- 複数リソースのログイン，61 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。

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。

jabber-config.xml ファイルで、SipUri または BDISipUri パラメータ内のユーザ ID の属性を設定します。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クスがある場合は、UriPrefix または BDIUriPrefix パラメータの値を設定できます。

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

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。

WebEx Messenger のログイン認証

Cisco WebEx Messenger の認証は、Cisco WebEx 管理ツールを使用して設定します。

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。

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。

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 クライアントが中央の IM and Presence サービス ノードに登録されます。これは、オンプレミス展開では Cisco Unified Communications ManagerIM and Presence サービス ノード、クラウドベース展開では Cisco WebEx です。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。

この IM and Presence サービス ノードは、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。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。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。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。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。

Adam は Anita と IM 会話を始めたいと思っています。Anita は、Cisco Jabber for Windows と Cisco Jabber for Android にすでにログインしています。また、Anita は、2 つのクライアントを IM and Presence サービス ノードに登録しています。Adam は次のようなメッセージを送信して会話を開始します。「こんにちは、Anita。今時間がありますか?」

ノードは Anita が 2 つの登録済みクライアントを使用していることを特定して、Adam の メッセージを両方にブロードキャストします。

Anita は自分のデスクで、ノートパソコンと電話の両方に表示される Adam の メッセージを見ます。Anita はノートパソコンを使用して応答することを選択し、次のようなメッセージを返信します。「数分後に会議がありますが、短時間ならチャットできます。」

IM and Presence サービス ノードは、Anita が Cisco Jabber for Windows を使用して応答したことを特定して、それを会話で以降のすべてのメッセージをルーティングするクライアントとしてマーキングします。Adam が「This will only take a minute」と返信すると、この返信が Cisco Jabber for Windows に直接ルーティングされます。会話のある時点から Anita が電話を使用して Adam に応答し始めると、IM and Presence サービス ノードは以降のメッセージを Cisco Jabber for Windows ではなく、電話にルーティングします。

第 5 章

サービス ディスカバリ

- クライアントによるサービスへの接続方法，63 ページ
- クライアントがサービスを検出する方法，67 ページ
- 方法 1：サービスの検索，69 ページ
- 方法 2：カスタマイズ，83 ページ
- 方法 3：手動インストール，85 ページ
- 高可用性，85 ページ
- Survivable Remote Site Telephony，88 ページ
- 設定のプライオリティ，89 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，89 ページ

クライアントによるサービスへの接続方法

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、クライアントのユーザ インターフェイスで手動により接続設定を入力します。

Cisco WebEx サービス ディスカバリ

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。

推奨される接続方法

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 *2*：*Cisco Jabber for Windows* のオンプレミス展開

製品モード	サーバのバージョン	検出方法	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。

（注） Cisco Jabber for Windows 9.2 からアップグレードする場合、サービス ドメインはキャッシュ設定から読み取られます。

表 *3*：*Cisco Jabber for Mac* のオンプレミス展開

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> に対する DNS SRV 要求

表 *4*：*Cisco Jabber for Android* および *Cisco Jabber for iPhone and iPad* のオンプレミス展開

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 5：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	http://loginp.webexconnect.com/cas/FederatedSSO?org=<domain> に対する HTTPS 要求

表 6：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：Cisco Jabber を起動し、ウェルカム画面で電子メール アドレスに似た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 &ServiceDiscoveryExcludeServices=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
- _cuplogin
- _collab-edge

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
```

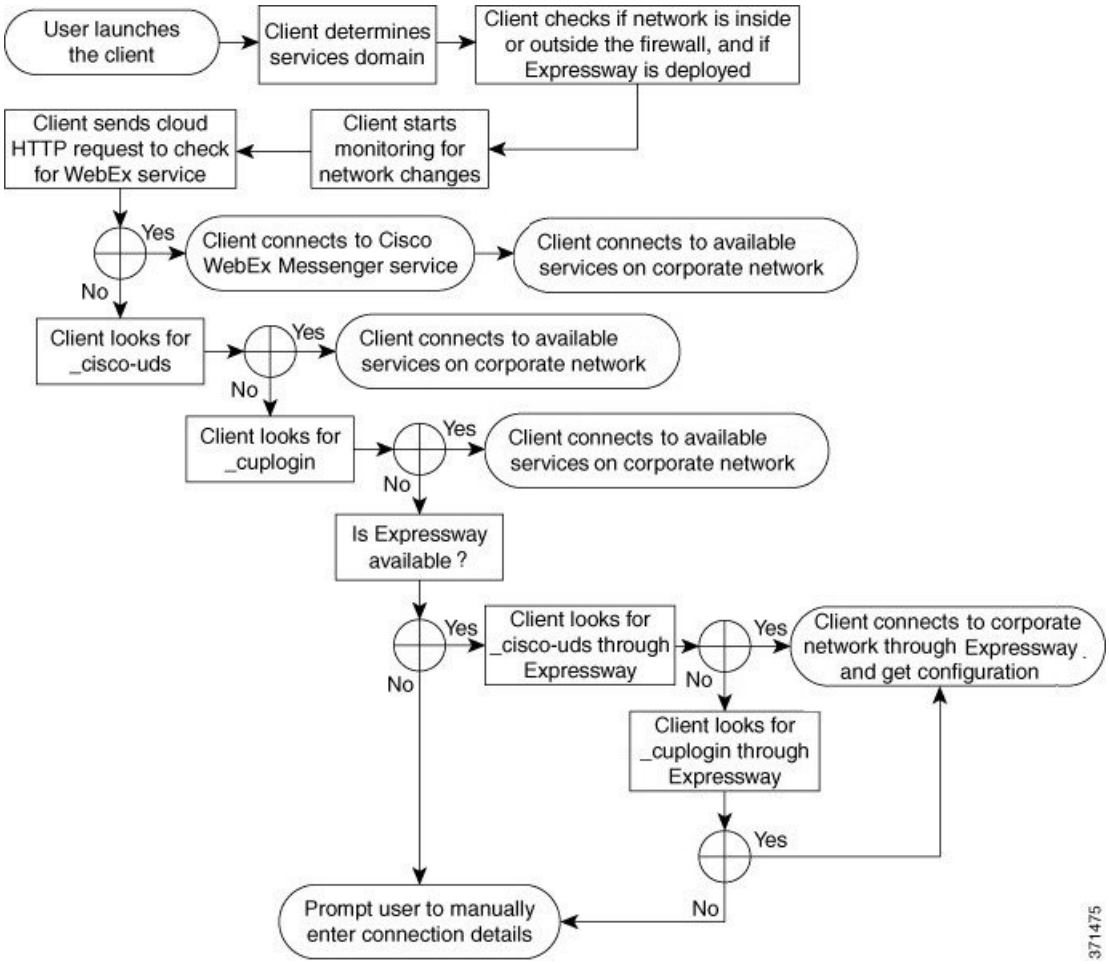
方法 1：サービスの検索

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 *6* : 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. Cisco WebEx Messenger サービス用の CAS URL に対して HTTP クエリを発行します。

このクエリによって、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。

4 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。

クライアントによる HTTP クエリーの発行

利用可能なサービスを検索するためにネーム サーバに SRV レコードを問い合わせるほか、Cisco Jabber は Cisco WebEx Messenger サービス用の CAS URL に対して HTTP クエリーを送信します。この要求により、クライアントはクラウドベース展開を特定して、Cisco WebEx Messenger サービスに対してユーザを認証できるようになります。

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。

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

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

```
http://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。

クライアントはサービス ドメインを有効な Cisco WebEx ドメインとして判定すると、ユーザに Cisco WebEx クレデンシャルの入力を促します。その後で、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 で設定されたコンフィギュレーションと 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「プロキシ設定（*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`

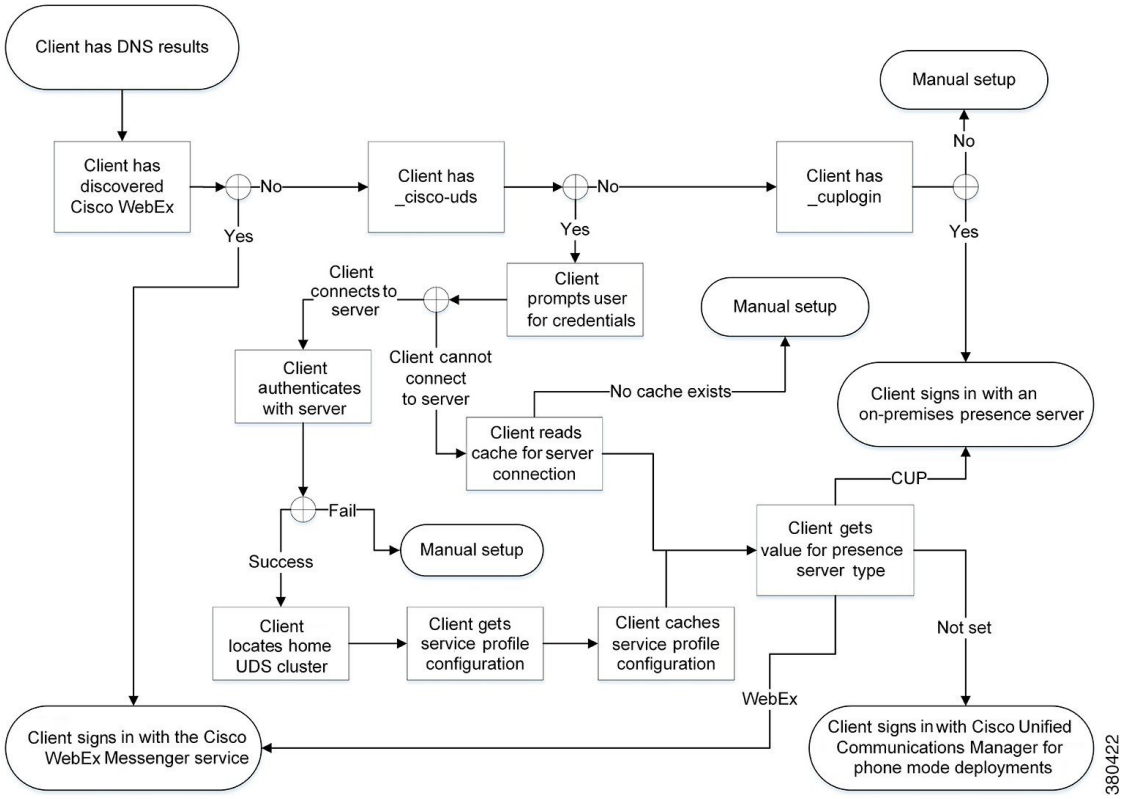
ネーム サーバが次を返した場合：

- `_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 7: 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。

次の 3 つのオーセンティケータによって、ユーザはサインイン画面を通過できます。

- 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 ベースの展開。
- Cisco Unified Communications Manager：電話機モードでのオンプレミス展開。

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. クライアントは、CAS URL ルックアップが 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。
   a. Cisco WebEx Messenger サービスを認証のプライマリ ソースと判定する。
   b. 自動的に Cisco WebEx Messenger サービスに接続する。
   c. ユーザにクレデンシャルの入力を促す。

d クライアント設定とサービス設定を取得する。

2 _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。

1 Cisco Unified Communications Managerにより認証するクレデンシャルの入力をユーザに促します。

2 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。

重要 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）を設定する必要があります。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。

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。

3 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 and Presence）：Cisco WebEx Messenger サービスがオーセンティケータである。

（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。

クラウドベースの展開では、HTTP クエリーの結果、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（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。

- 未設定：サービス プロファイルに IM and Presence サービス設定が含まれていない場合は、Cisco Unified Communications Manager がオーセンティケータになります。

4 オーセンティケータにサイン インします。

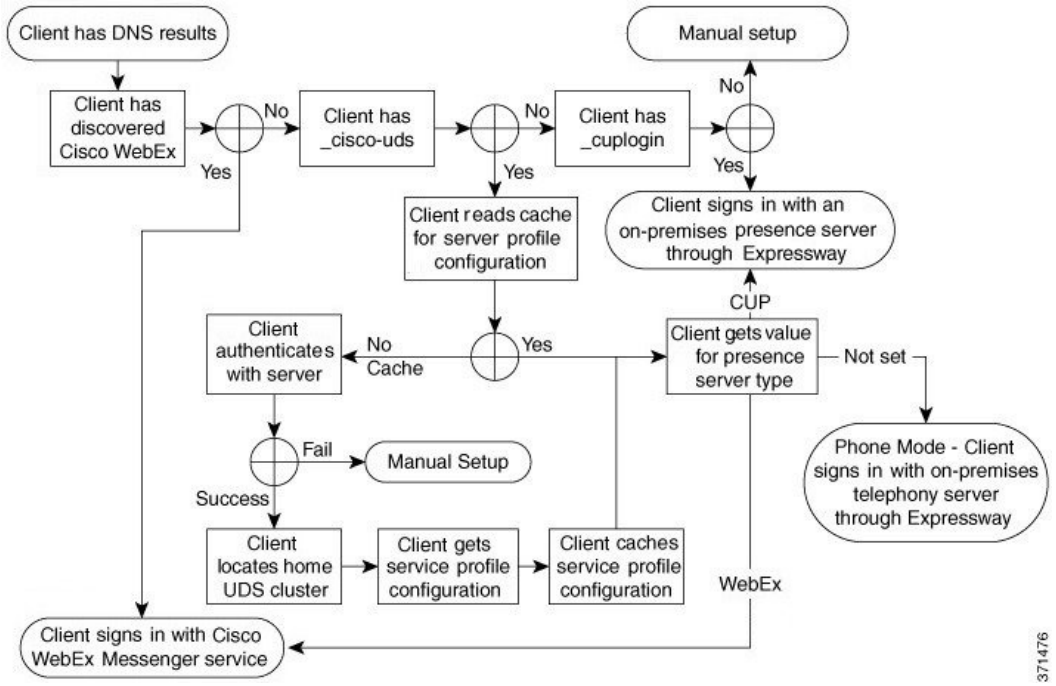
クライアントにサインインした後、製品モードを判定できます。

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 *8*：*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。

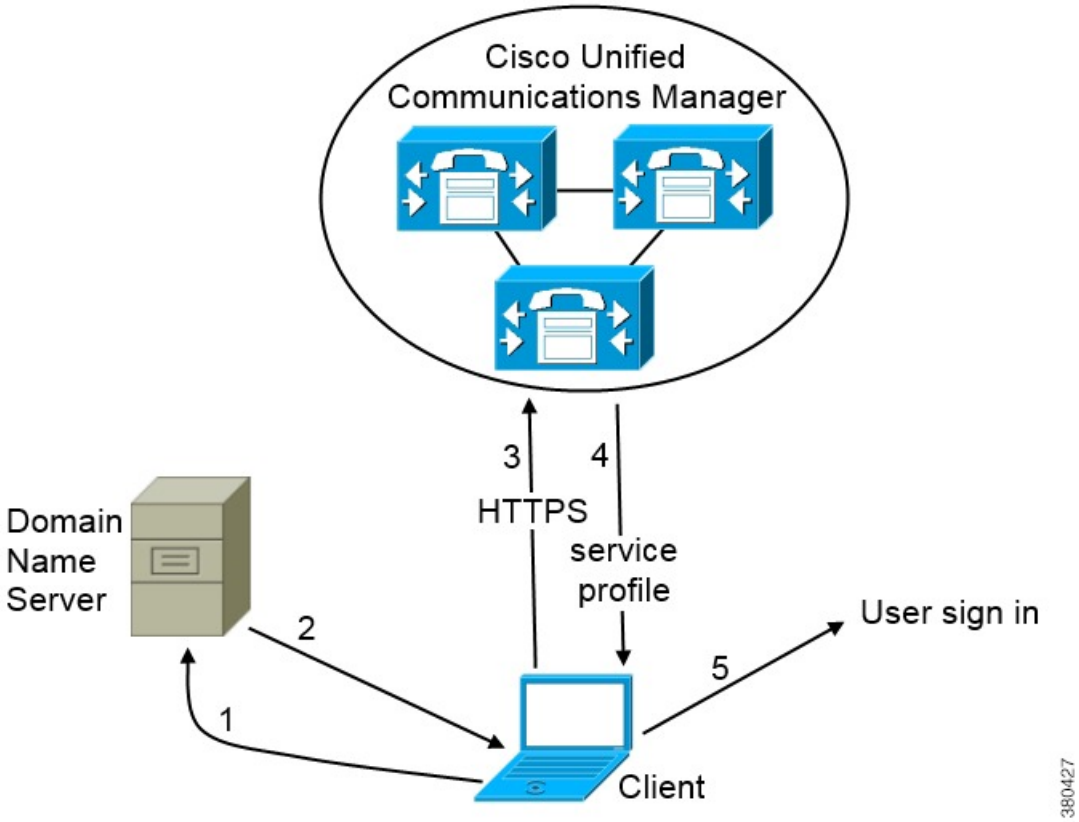
_cisco-uds SRV レコードが含まれている内部 SRV レコードを取得すると、クライアントは Cisco Unified Communications Manager からサービス プロファイルを受け取ります。その後、サービス プロファイルはユーザのホーム クラスタ、認証のプライマリ ソース、および設定をクライアントに提供します。

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 SRV レコード（_cisco-uds）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 *9*： *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 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 サービスおよびクライアント設定のアドレスと設定が含まれます。

また、クライアントは、サービス プロファイルからの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。

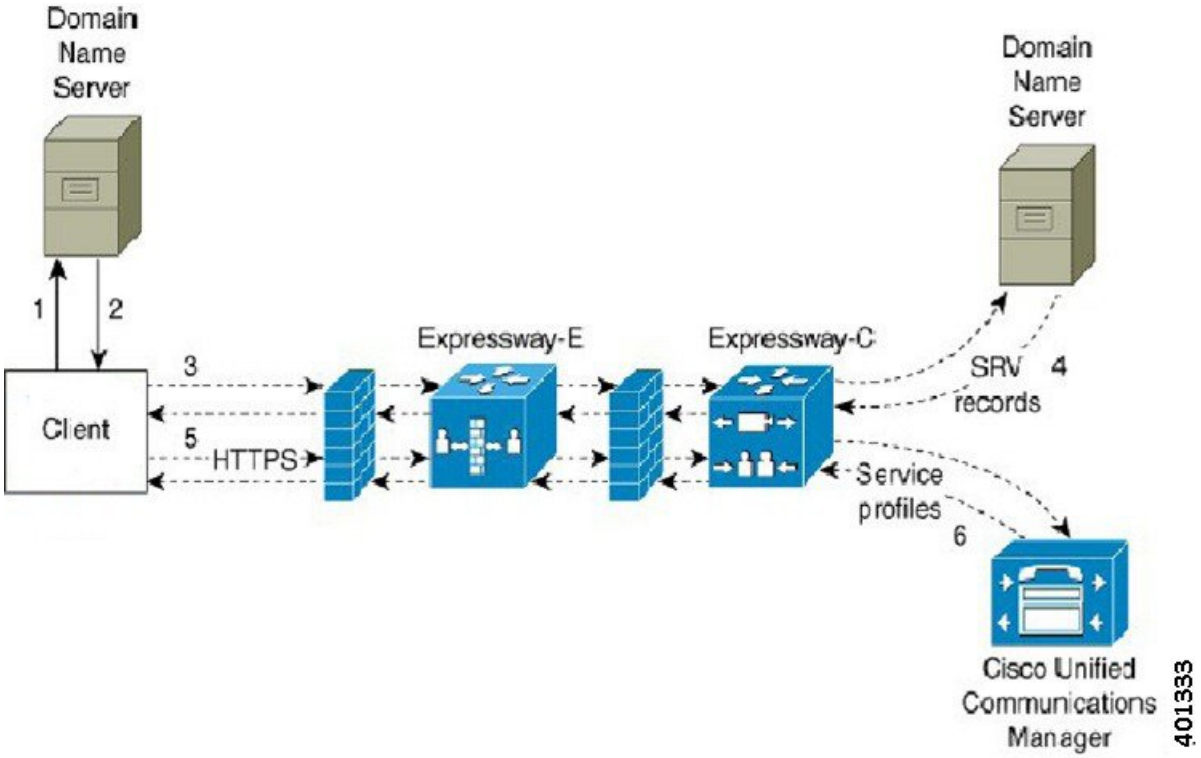
```
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 6
          weight         = 30
          port           = 8443
          svr hostname   = cucm3.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 2
          weight         = 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、SRV レコード（_collab-edge）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 *10*： *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。

   その結果として、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。
   その結果として、クライアントは Cisco Unified Communications Manager サーバを検出できます。
5. クライアントが Cisco Unified Communications Manager にサービス プロファイル（Expressway 経由）を要求します。
6. クライアントが（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処理を実行します。

- 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。

クライアントがネーム サーバを検索する方法

Cisco Jabber は次の場所で 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、Cisco Jabber 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

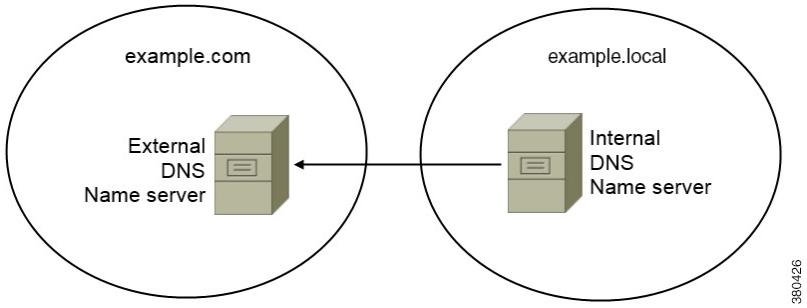
DNS サービス（SRV）レコードの導入場所は、DNS ネームスペースの設計に依存します。通常、2 種類の DNS 設計があります。

- 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 *11*：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。

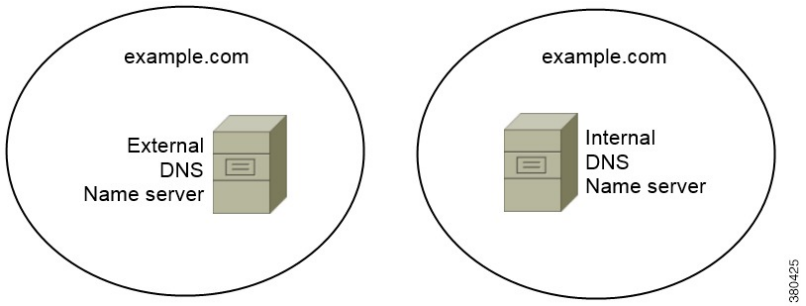
同一ドメイン設計

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 *12*：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。

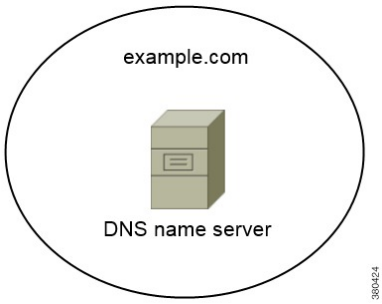
内部ネームサーバと外部ネームサーバは、どちらも単一ドメインに対して権限がありますが、異なるホスト コミュニティに対応します。

- 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 *13*：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きに、オーセンティケータと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 ファイルが無視されます。

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 設定または企業モビリティ管理を使用して、Mac やモバイル クライアント向け Cisco Jabber のカスタムインストールを作成できます。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）を使用する前に、以下を確認してください。

- EMM ベンダーが Android for Work または Apple Managed App Configuration をサポートしている。

- Android デバイスに Android OS 5.0 以降が搭載されているか、IOS デバイスに iOS 8.0 以降が搭載されている。

EMM を使用して、Cisco Jabber for Android や Cisco Jabber for iPhone and iPad に Cisco Jabber を設定することができます。EMM は、URL の設定に代わる方法を提供します。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。

サポートされる EMM ソフトウェア：

- Airwatch by VMware

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。

Cisco Jabber for Mac およびモバイル クライアント向け Cisco Jabber で LDAP または UDS 連絡先ソースを使用している場合、ハイ アベイラビリティはサポートされません。ハイ アベイラビリティは、Cisco Jabber for Windows の LDAP（EDI）でのみサポートされます。

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。

再ログイン パラメータの設定

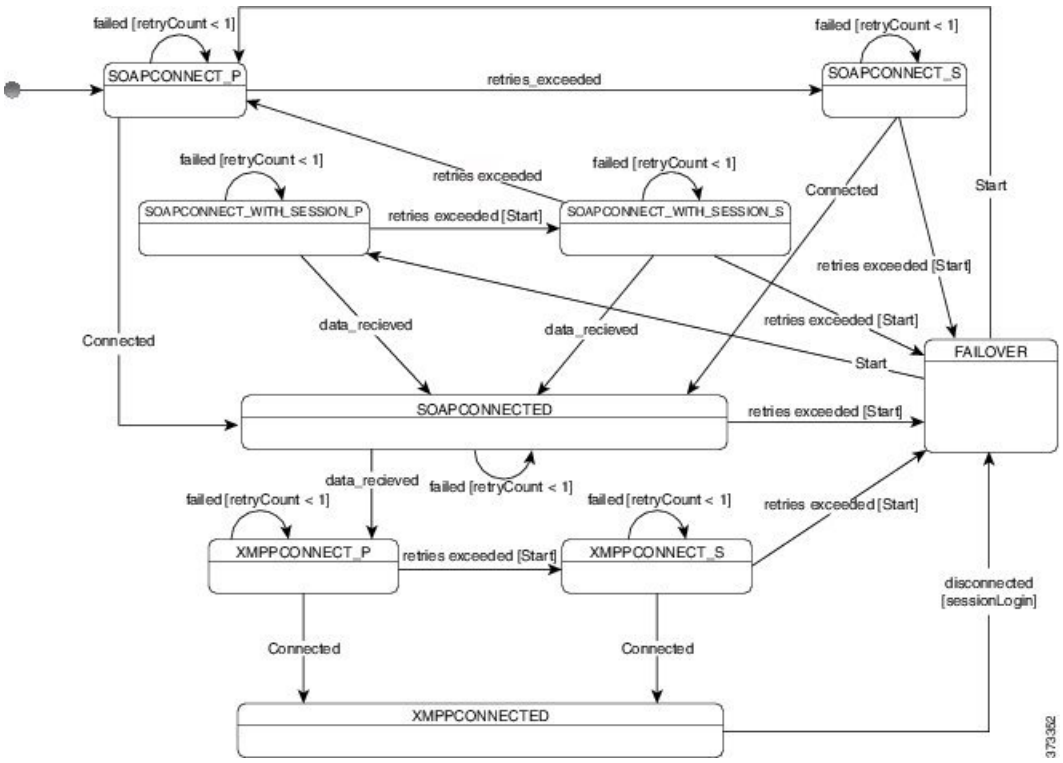
Cisco Unified Communications Manager IM and Presence サービスでは、Cisco Jabber がサーバへの再ログインを試みるまでに待機する最大秒数と最小秒数を設定できます。サーバで、次のフィールドに再ログイン パラメータを指定します。

- 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 *14*：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（Administration）]で、[システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。

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。

Survivable Remote Site Telephony

Cisco Unified Communications Manager アプリケーションが到達不能または WAN がダウンしている場合は、Cisco Unified Survivable Remote Site Telephony（SRST）を使用して、リモート ユーザの基本的なテレフォニー サービスを維持します。接続が失われた場合は、クライアントがリモート サイトのローカル ルータにフェールオーバーします。

（注） SRST バージョン 8.5 および 8.6 がサポートされます。

SRST が基本的なコール制御を提供し、システムがフェールオーバー中は、開始、終了、保留、保留解除、ミュート、ミュート解除、およびデュアルトーン マルチ周波数シグナリング（DTMF）のみが有効になります。

次のサービスは、フェールオーバー中に使用できません。

- ビデオ
- 通話中機能（転送、iDivert、コール パーク、会議、モバイルへの送信）
- Dial via Office（DvO）
- アドホック会議
- Binary Floor Control Protocol（BFCP）共有

SRST の設定方法については、該当するリリースの『*Cisco Unified Communication Manager Administration Guide*』を参照してください。

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 6 章

連絡先ソース

- ディレクトリ サーバ，91 ページ
- 連絡先ソースとは，92 ページ
- ディレクトリ統合を設定するタイミング，92 ページ
- 連絡先ソースが必要な理由，93 ページ
- 連絡先ソース オプション，93 ページ
- LDAP の前提条件，98 ページ
- Jabber ID 属性マッピング，99 ページ
- ローカル連絡先ソース，99 ページ
- カスタム連絡先ソース，100 ページ
- 連絡先のキャッシュ，100 ページ
- ダイヤル プランのマッピング，100 ページ
- Cisco Unified Communication Manager UDS for Mobile and Remote Access，101 ページ
- クラウドの連絡先ソース，101 ページ
- 連絡先の写真の形式と寸法，101 ページ

ディレクトリ サーバ

次のディレクトリを Cisco Jabber で使用できます。

（注） Cisco Jabber for Windows、Cisco Jabber for Mac、Cisco Jabber for iPhone and iPad、および Cisco Jabber for Android はディレクトリ統合用の LDAPv3 標準をサポートしています。この標準をサポートするディレクトリ サーバは、これらのクライアントと互換性がある必要があります。

- Windows Server 2012 R2 の Active Directory Domain Services
- Windows Server 2008 R2 の Active Directory Domain Services
- Cisco Unified Communications Manager User Data Server（UDS）

  Cisco Jabber は、次の Cisco Unified Communications Manager バージョンを使用して UDS をサポートします。

  Cisco Unified Communications Manager バージョン 9.1(2)（Cisco Options Package（COP）ファイル `cmterm-cucm-uds-912-5.cop.sgn` を使用）。

  Cisco Unified Communications Manager バージョン 10.0(1)。COP ファイルは必要ありません。

- OpenLDAP
- Active Directory Lightweight Directory Service（AD LDS）または Active Directory Application Mode（ADAM）

制約事項 OpenLDAP、AD LDS、または ADAM とのディレクトリ統合では、Cisco Jabber コンフィギュレーション ファイルで固有のパラメータを定義する必要があります。

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。

ディレクトリ統合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 for Windows をインストールします。この環境では、Cisco Jabber for Windows 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 をディレクトリに接続するように設定します。

- ドメイン コントローラ

- 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。

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。

連絡先ソース 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。
  - 拡張ディレクトリ統合（EDI）：Cisco Jabber for Windows を展開する場合に、このオプションを選択します。
  - 基本ディレクトリ統合（BDI）：Cisco Jabber for Mac、iOS、および Android を展開する場合に、このオプションを選択します。
- 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。

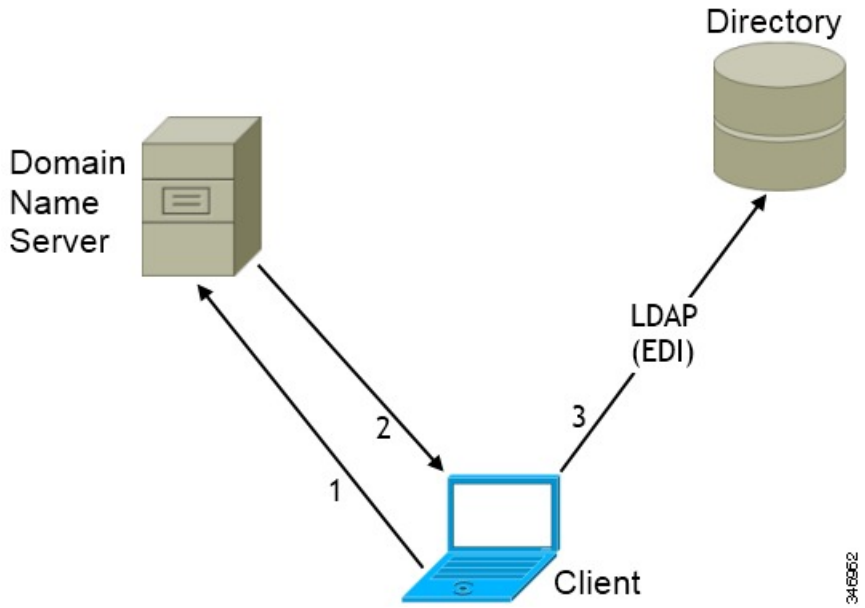
LDAP オプション：EDI と BDI

拡張ディレクトリ統合

EDI は、ネイティブな Microsoft Windows API を使用してディレクトリ サービスから連絡先データを取得します。

EDI 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。



上記の図では、クライアントは次をデフォルトで実行します。

1. ワークステーションから DNS ドメインを取得して、グローバル カタログの SRV レコードを検索します。
2. SRV レコードからグローバル カタログ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グローバル カタログに接続します。

ドメイン名の検索

Cisco jabber for Windows は、クライアント ワークステーション上の `USERDNSDOMAIN` 環境変数から完全修飾 DNS ドメインを取得します。

クライアントが DNS ドメインを取得したら、ドメイン ネーム サーバを見つけて SRV レコードを取得できます。

場合によっては、USERDNSDOMAIN 環境変数の値は、フォレスト全体のドメインに対応する DNS ドメインに解決されません。たとえば、組織がサブドメインまたはリソース ドメインを使用しているとします。この場合、USERDNSDOMAIN 環境変数は、親ドメインではなく子ドメインに解決されます。このため、クライアントは組織のすべてのユーザの情報にアクセスできません。

USERDNSDOMAIN 環境変数が子ドメインに解決される場合は、次のいずれかのオプションを使用して、Cisco jabber for Windows が親ドメイン内のサービスに接続できるようにします。

- グローバル カタログまたは LDAP ディレクトリ サーバが組織内のすべてのユーザにアクセスできることを確認します。
- Cisco jabber for Windows がグローバル カタログまたは LDAP ディレクトリ サーバを要求したときに、組織内のすべてのユーザにアクセス可能なサーバにクライアントをルーティングするように、DNS サーバを設定します。
- 親ドメインの FQDN を使用するように Cisco jabber for Windows を設定します。

  次のように、クライアント設定で PrimaryServerName パラメータの値として親ドメインの FQDN を指定します。
  `<PrimaryServerName>parent-domain-fqdn</PrimaryServerName>`

ディレクトリ サーバの検出

Cisco Jabber は、次の場合にディレクトリ サーバを自動的に検出して接続できます。

- Cisco Jabber がインストールされたワークステーションが Microsoft Windows ドメイン内に存在する場合。
- クライアントが DNS SRV レコードからディレクトリ サーバのアドレスを取得できる場合。

ディレクトリ サーバ	SRV レコード
グローバル カタログ	_gc._msdcs._tcp.*domain.com*
ドメイン コントローラ LDAP ベースのディレクトリ サーバ	_ldap._msdcs._tcp.*domain.com*

基本ディレクトリ統合

基本ディレクトリ統合（BDI）を使用している場合は、次のように、クライアントがディレクトリ サービスから連絡先データを取得します。

1 クライアントが Cisco Unified Communications Manager IM and Presence サービス ノードに接続します。

2 クライアントが Cisco Unified Communications Manager IM and Presence サービス ノードからサービス プロファイル内の LDAP プロファイル設定セクションを取得します。

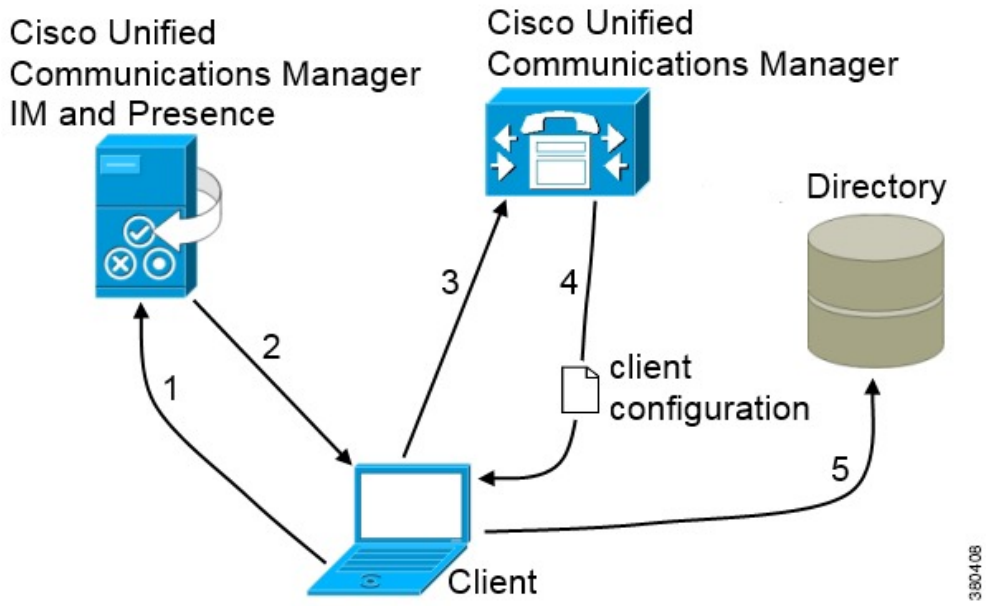
サービス プロファイルに、Cisco Unified Communications Manager（TFTP）ノードの場所が含まれています。設定によっては、サービスプロファイルにディレクトリで認証を受けるためのクレデンシャルが含まれる場合もあります。

3 クライアントが Cisco Unified Communications Manager ノードに接続します。

4 クライアントが Cisco Unified Communications Manager ノードからクライアント コンフィギュレーション ファイルをダウンロードします。

クライアントの設定ファイルには、ディレクトリの場所が含まれます。設定によっては、クライアントの設定ファイルにディレクトリで認証を受けるためのクレデンシャルが含まれる場合もあります。

5 クライアントはディレクトリの場所と認証クレデンシャルを使用し、ディレクトリに接続します。



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。

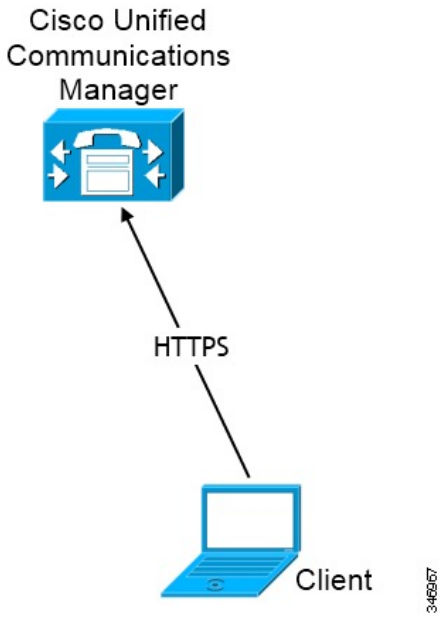
- クライアント コンフィギュレーション ファイルの UDS の値を使用するように DirectoryServerType パラメータを設定した場合。

  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。

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、次の属性がインデックス化されていることを確認します。

- sAMAccountName
- displayName
- sn
- name
- proxyAddresses
- mail
- department
- givenName
- telephoneNumber
- otherTelephone
- mobile
- homePhone
- msRTCSIP-PrimaryUserAddress

LDAP サービス アカウント

Cisco Jabber は、アカウントを使用してディレクトリ サーバを認証します。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。

サービス プロファイルまたは jabber-config.xml ファイルのパラメータを使用して、Cisco Jabber がディレクトリ サーバに接続するように設定します。Cisco Jabber for Windows はデフォルトでグローバル カタログ サーバに接続します。これは Cisco Jabber for Windows 向けの推奨方式であり、ディレクトリに接続するために Cisco Jabber for Windows を設定する必要はありません。

Jabber ID 属性マッピング

ユーザ ID の LDAP 属性は sAMAccountNameで、これはデフォルトの属性です。

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。

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

BDI パラメータは BDIUserAccountName です。
<BDIUserAccountName>attribute-name</BDIUserAccountName>

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がインスタントメッセージの機能だけを持っているとします。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。

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

Cisco Jabber for Windows 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。詳細については、『Cisco Jabber for Windows User Guide』の「連絡先リストのインポート（*Import contact lists*）」のトピックを参照してください。

連絡先のキャッシュ

Cisco Jabberはユーザ連絡先リストのローカル キャッシュを作成します。ユーザが連絡先リストで連絡先を検索するとき、Cisco 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、Cisco Jabber はローカル キャッシュを検索してから、社内ディレクトリを検索します。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、連絡先情報がローカル キャッシュに追加されます。その後この連絡先を検索することによって、連絡先情報が連絡先または最新リストに返されます。

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。

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（Application Dial Rules）

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（Directory Lookup Dial Rules）

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 Administration Guide』の「*User Management*」の項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 7 章

セキュリティおよび証明書

- 暗号化，105 ページ
- 音声およびビデオの暗号化，111 ページ
- 連邦情報処理標準規格，111 ページ
- Secure LDAP，112 ページ
- 証明書，112 ページ

暗号化

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 ツー 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	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、「*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、『*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。

Connection	プロトコル	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、Cisco WebEx Messenger サービスで X.509 公開キー インフラストラクチャ（PKI）証明書を使用して、Cisco Jabber と 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 ビットの長さのセッション キーを使用して、Cisco Jabber 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、「*Next Generation Encryption*」を参照してください。

X509 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、『*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 トラフィックは安全です。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。

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）] = 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 では、グループ チャットによるクライアント間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 チャットのみに関して、クライアント間の暗号化を使用します。

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「*About Encryption Levels*」の項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。

クライアントの暗号化対応クライアント用の鍵アイコン

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

ローカル チャット履歴が有効になっている場合、Cisco Jabber for iPhone and iPad は、モバイル デバイスにローカルに格納されるアーカイブインスタントメッセージを暗号化しません。暗号化されていないインスタントメッセージをローカルに格納することを望まない場合は、ローカルチャット履歴を無効にしてください。

ローカル チャット履歴が有効になっている場合、Cisco Jabber for Android は、モバイル デバイスにローカルに格納されるアーカイブインスタントメッセージを暗号化しません。暗号化されていないインスタントメッセージをローカルに格納することを望まない場合は、ローカルチャット履歴を無効にしてください。

ローカル チャット履歴を有効にすると、Cisco Jabber for Windows はインスタント メッセージを暗号化形式でアーカイブしません。チャット履歴へのアクセスを制限するために、クライアントはアーカイブを `%USERPROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\History\uri.db` ディレクトリに保存します。

ローカル チャット履歴を有効にすると、Cisco Jabber for Mac はインスタント メッセージを暗号化形式でアーカイブしません。チャット履歴へのアクセスを制限するために、Cisco Jabberはアーカイブを `~/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/History/uri.db` ディレクトリに保存します。

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。

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。

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。

連邦情報処理標準規格

（注） ここで説明する内容は、Cisco Jabber for Windows スイッチにのみ適用されます。

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 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 *7*：*FIPS* 向け *Cisco Jabber* クライアントの設定。

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。

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 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。

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。これには別のポートである 636 が必要です。

証明書

証明書の検証

証明書検証プロセス

Cisco Jabber は、サービスの認証時にサーバ証明書を検証します。セキュアな接続の確立を試みるときに、サービスは Cisco Jabber に証明書を提示します。Cisco Jabber 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ずにサービスに接続します。

Cisco Jabber は Cisco Unified Communications Manager サーバ上の 2 つのサービスに対して認証を行います。サービス名は Cisco Tomcat と Extensible Messaging and Presence Protocol（XMPP）です。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：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。
- 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。

（注） 自己署名証明書を使用しないことをお勧めします。

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	HTTP（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 Server	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。
- 証明書署名プロセスを開始する前に、Cisco Unified Communications Manager IM and Presence Service に対して最新のサービス更新（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 シグナリングを保護するには、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、CSR を送信するパブリック CA からの形式の要件を確認する必要があります。次に、サーバを構成する際に、入力する情報がパブリック CA が要求する形式に適合していることを保証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、1 つの Cisco Unified Communications Manager IM and Presence Service ノードの HTTP 証明書と XMPP 証明書に署名するには、各 CSR を個別のパブリック CA に送信する必要があります。

失効サーバ

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HTTPURLが証明書に含まれている必要があります。認証局（CA）によって証明書が取り消された場合、クライアントはユーザがそのサーバに接続することを許可しません。

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「*ID* の不一致の防止（*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 と Cisco WebEx Meeting Center は、デフォルトで次の証明書をクライアントに提示します。

- `CAS`
- `WAPI`

（注） Cisco WebEx 証明書はパブリック認証局（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 Messenger 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、http://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、http://support.apple.comを参照してください。

第 8 章

画面共有

- 画面共有，119 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 の共有
- 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、これがデフォルトの画面共有です。たとえば、BFCP および IM 専用画面共有が無効であるか、または共有しようとしているユーザがこれらのオプションを所有していない場合です。

このオプションは、次のいずれかの方法を使用して、クライアントで使用することができます。

- ハブ ウィンドウで連絡先を選択し、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 [...] > [画面の共有（Share screen）] を選択します。

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。コール中に [...] > [画面の共有（Share screen）] を選択して、BFCP の画面共有を開始します。

IM 専用画面の共有

Cisco Jabber for Windows に適用されます。

IM 専用画面の共有は、1 対 1 の画面共有であり、jabber-config.xml ファイル内での EnableP2PDesktopShare パラメータの使用を有効にします。ユーザは、チャット ウィンドウで [...] > [画面の共有（Share screen）] を選択します。

このオプションのポート範囲は 49152 ～ 65535 ですが、このポート範囲は jabber-config.xml ファイル内で SharePortRangeStart および SharePortRangeSize パラメータを使用して減らすことができます。

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 Meeting にエスカレーションでき、Cisco WebEx Meeting 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，121 ページ
- ドメイン内フェデレーション，122 ページ
- フェデレーション用ユーザ ID の計画，122 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*』

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。

`jabber-config.xml` ファイルで、SipUri または BDISipUri パラメータ内のユーザ ID の属性を設定します。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クスがある場合は、UriPrefix または BDIUriPrefix パラメータの値を設定できます。