



Cisco Jabber 10.6 計画ガイド

初版：2015年01月27日

最終更新：2015年03月05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、すべてユーザー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。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。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)

© 2015 Cisco Systems, Inc. All rights reserved.



目次

Cisco 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

導入シナリオ 3

オンプレミス展開 3

Cisco Unified Communications Manager を使用したオンプレミス展開 4

Cisco Unified Presence によるオンプレミス展開 5

電話機モードでのオンプレミス展開 6

クラウドベース展開 6

クラウドベース展開 7

ハイブリッドクラウドベース展開 7

シングルサインオンを使用した展開 8

シングルサインオンの要件 9

シングルサインオンとリモート アクセス 10

クライアント内の SAML SSO の有効化 11

仮想環境での展開 12

仮想環境の要件 12

仮想環境とローミング プロファイル 13

要件 15

Cisco Jabber for Windows および Cisco Jabber for Mac 向けのオンプレミス サーバ 15

Cisco Jabber for Android 向けのオンプレミス サーバ 16

Cisco Jabber for iPhone and iPad 向けのオンプレミス サーバ 19

デスクトップ クライアントのハードウェア要件 21

Cisco Jabber for Windows でサポートされるオペレーティング システム 21

Cisco Jabber for Mac のオペレーティング システム 22

CTI でサポートされるデバイス 22

Cisco Jabber for Android のハードウェア要件	22
Cisco Jabber for iPhone and iPad のハードウェア要件	24
ネットワークの要件	25
Cisco Jabber for Windows と Cisco Jabber for Mac のポートとプロトコル	26
Cisco Jabber for Android、iPhone、および iPad のポートとプロトコル	28
Cisco Jabber for Windows と Cisco Jabber for Mac でサポートされるコーデック	30
Cisco Jabber for Android、iPhone、および iPad でサポートされるコーデック	31
連絡先ソース	33
オンプレミス連絡先ソース オプション	33
IM アドレス スキーム	33
ディレクトリ サーバ	34
連絡先の写真の形式と寸法	35
連絡先の写真の形式	35
連絡先の写真の寸法	36
連絡先の写真の調整	36
証明書	39
証明書の検証	39
オンプレミス サーバに必要な証明書	40
証明書署名要求の形式と要件	41
失効サーバ	41
証明書のサーバ識別情報	42
クラウドベースのサーバの証明書要件	43
サービス ディスカバリ	45
サービス ディスカバリについて	45
クライアントによるサービスの検索方法	47
Cisco UDS SRV レコード	49
CUP ログイン SRV レコード	50
Collaboration Edge SRV レコード	52
セキュリティ	55
連邦情報処理規格 (FIPS)	55
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	56
インスタントメッセージの暗号化	56

オンプレミス暗号化	56
クラウドベースの暗号化	58
クライアント間の暗号化	59
暗号化アイコン	60
サーバの暗号化対応クライアント用のロックアイコン	60
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	60
ローカルのチャット履歴	61
プランニングの考慮事項	63
DNS の設定	63
クライアントが DNS を使用する方法	63
クライアントがネーム サーバを検索する方法	63
クライアントがサービス ドメインを取得する方法	64
クライアントによる利用可能なサービスの検出方法	65
クライアントによる HTTP クエリーの発行	66
クライアントからのネーム サーバのクエリー	67
クライアントの内部サービスへの接続	67
Expressway for Mobile and Remote Access を介したクライアントの接続	70
ドメイン ネーム システムの設計	71
独立ドメイン設計	71
独立ドメイン構造での SRV レコード導入	72
サービス ドメインへの内部ゾーンの使用	72
同一ドメイン設計	72
同一ドメイン (スプリットブレイン)	72
同一ドメイン (非スプリットブレイン)	73
クライアントによるサービスへの接続方法	73
推奨される接続方法	74
認証ソース	77
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	78
フェールオーバー中のクライアントの動作	79
コンピュータ テレフォニー インテグレーション従属	81



第 1 章

Cisco 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](#)

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（EDI および 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、『*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 製品ファミリーには、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
Cisco Jabber の展開方法を決定する。	導入シナリオ, (3 ページ)	
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, (15 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, (33 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があるかどうかを確認する。	証明書, (39 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, (45 ページ)	
セキュリティ情報を確認する。	セキュリティ, (55 ページ)	
その他の計画に関する考慮事項を確認する。	プランニングの考慮事項, (63 ページ)	



第 2 章

導入シナリオ

- [オンプレミス展開, 3 ページ](#)
- [クラウドベース展開, 6 ページ](#)
- [シングルサインオンを使用した展開, 8 ページ](#)
- [仮想環境での展開, 12 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。

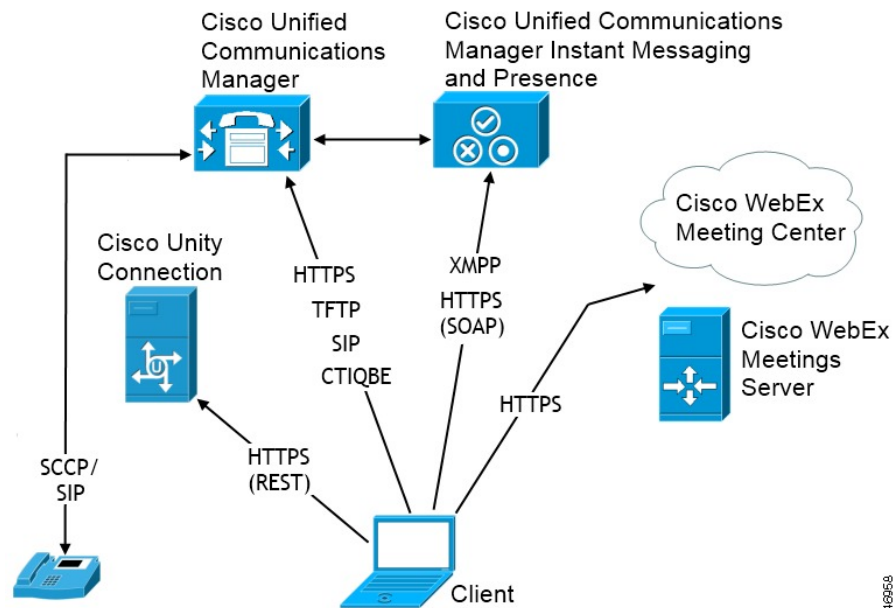
デフォルト製品モードは、ユーザのプライマリ認証が IM and Presence サーバで行われるモードです。

Cisco Unified Communications Manager を使用したオンプレミス展開

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

- **プレゼンス**：Cisco Unified Communications Manager IM and Presence Service 経由で対応可否を公開し、他のユーザの対応可否をサブスクライブします。
- **IM**：Cisco Unified Communications Manager IM and Presence Service 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**：卓上電話機または Cisco Unified Communications Manager 経由のコンピュータを使用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：ホスト型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。



Cisco Unified Presence によるオンプレミス展開

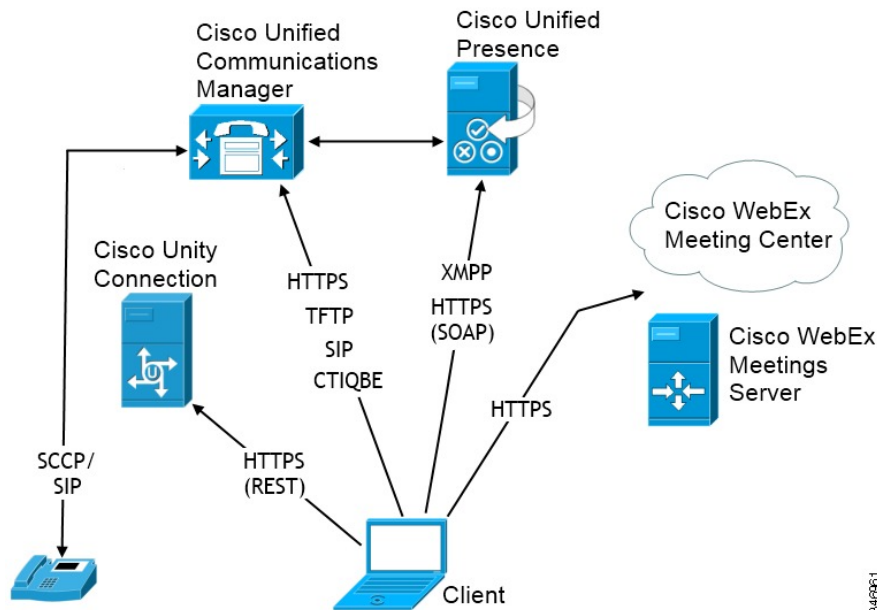
Cisco Unified Presence によるオンプレミスで使用可能なサービスは次のとおりです。

- **プレゼンス**：Cisco Unified Presence 経由で対応可否を公開し、他のユーザの対応可否をサブスクライブします。
- **IM**：Cisco Unified Presence 経由で IM を送受信します。
- **音声コール**：卓上電話機または Cisco Unified Communications Manager 経由のコンピュータを使用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**：ホスト型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) モバイル クライアント用の Cisco Jabber は電話機モード中の会議をサポートしません。

次の図は、Cisco Unified Presence 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。



344261

電話機モードでのオンプレミス展開

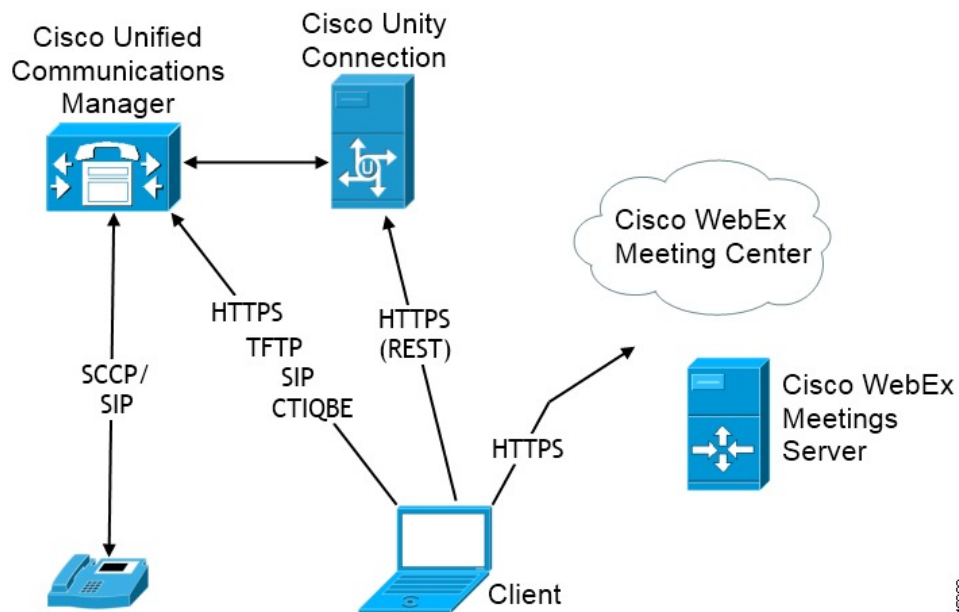
電話機モード展開で使用可能なサービスは次のとおりです。

- **音声コール**：卓上電話機または Cisco Unified Communications Manager 経由のコンピュータを使用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**：ホスト型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 は電話機モードの会議をサポートしません。

次の図は、電話機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。



34693

クラウドベース展開

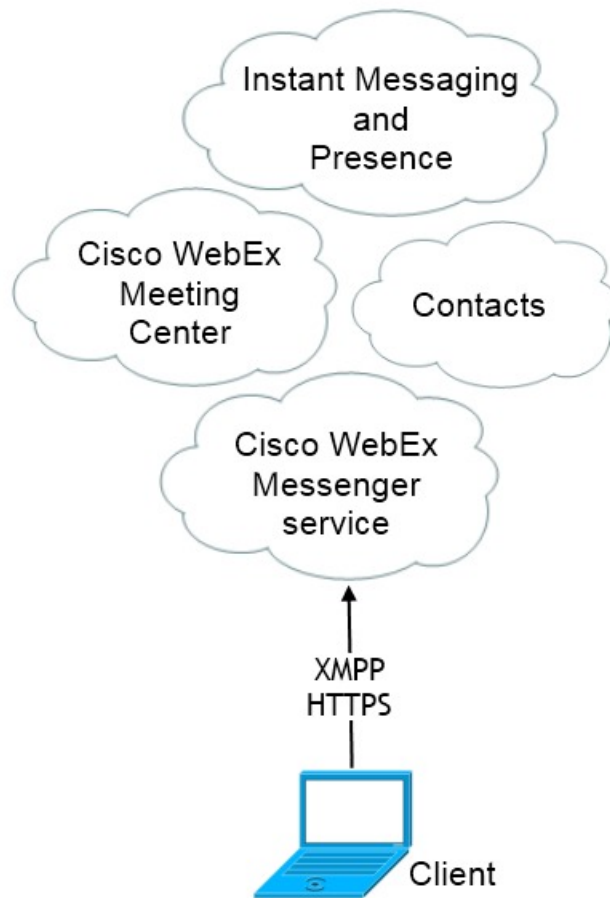
クラウドベース展開は、Cisco WebEx がサービスをホストする展開の 1 つです。Cisco WebEx 管理ツールでクラウドベース展開を管理および監視します。

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 サービスが連絡先を解決します。
- **プレゼンス**：Cisco WebEx Messenger サービスを使用すれば、ユーザは自分の対応可否を公開し、他のユーザの対応可否にサブスクライブできます。
- **インスタント メッセージング**：Cisco WebEx Messenger サービスを使用すれば、インスタントメッセージを送受信することができます。
- **会議**：Cisco WebEx Meeting Center がホスト型ミーティング機能を提供します。

次の図は、クラウドベース展開のアーキテクチャを図示したものです。



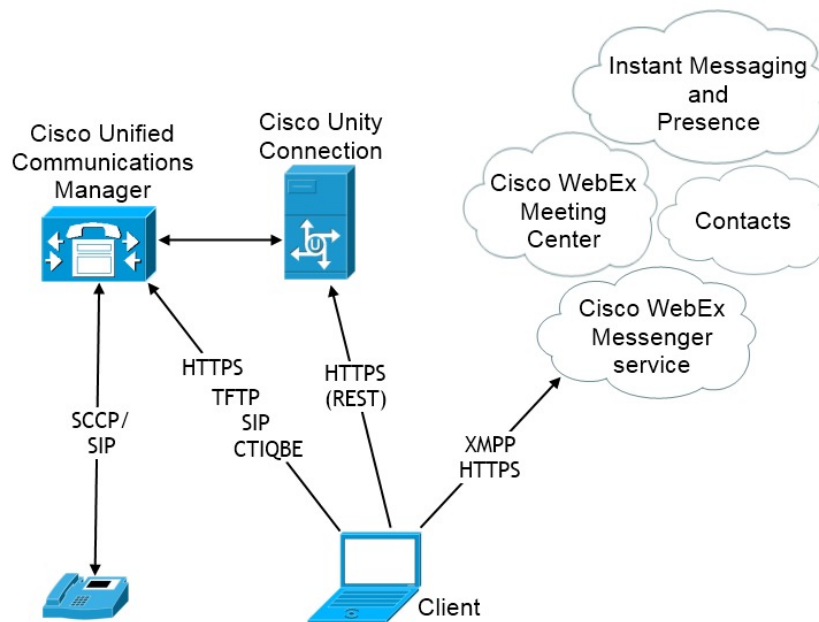
3412655

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 サービスが連絡先を解決します。
- **プレゼンス**：Cisco WebEx Messenger サービスを使用すれば、ユーザは自分の対応可否を公開して、他のユーザの対応可否にサブスクライブできます。
- **インスタントメッセージング**：Cisco WebEx Messenger サービスを使用すれば、インスタントメッセージを送受信することができます。
- **音声**：卓上電話機または Cisco Unified Communications Manager 経由のコンピュータを使用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 がホスト型ミーティング機能を提供します。
- **ボイスメール**：Cisco Unity Connection 経由でボイス メッセージを送受信します。

次の図は、ハイブリッドクラウドベース展開のアーキテクチャを図示したものです。



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。

次の手順では、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について説明します。

- 1 ユーザが Jabber クライアントを起動します。ユーザに Web フォームを使用したサインインを要求するようにアイデンティティプロバイダー（略して *IdP*）を設定した場合は、その形式がクライアントに表示されます。
- 2 Cisco Jabber クライアントが、Cisco WebEx Messenger サービス、Cisco Unified Communications Manager、Cisco Unity Connection などの接続先の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を含むページをユーザに表示する、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）
- 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 SSO のユーザエクスペリエンスに影響します。たとえば、Kerberos を使用する場合は、クライアントがユーザにクレデンシャルを要求しません。これは、ユーザがすでに認証され、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。セッションの期限が切れて、Jabber がそれを自動的に更新できなかった場合は、ユーザ入力が必要なため、再認証を要求するプロンプトが表示されます。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

サポートされるアイデンティティプロバイダー

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

- Ping Federate 6.10.0.4
- Microsoft Active Directory Federation Services (ADFS) 2.0

- Open Access Manager (OpenAM) 10.1



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

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

クッキー

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

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



(注) Android で SSO を使用している場合は、組み込みブラウザが外部ブラウザと 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。

クライアント内の SAML SSO の有効化

はじめる前に

- WebEx Messenger を使用しない場合は、Cisco Unified Communications Applications 10.5.1 Service Update 1 で SSO を有効にします。このサービス上での SAML SSO の有効化方法については、『*SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 10.5*』を参照してください。
- Cisco Unity Connection バージョン 10.5 で SSO を有効にします。このサービス上での SAML SSO の有効化方法については、『*Managing SAML SSO in Cisco Unity Connection*』を参照してください。
- WebEx Messenger を使用する場合は、WebEx Messenger サービスで SSO を有効にして Cisco Unified Communications アプリケーションと Cisco Unity Connection をサポートします。このサービス上での SAML SSO の有効化方法については、『*Cisco WebEx Messenger Administrator's Guide*』の「Single Sign-On」を参照してください。
このサービス上での SAML SSO の有効化方法については、『*Cisco WebEx Messenger Administrator's Guide*』の「Single Sign-On」を参照してください。

手順

-
- ステップ 1** Web ブラウザで証明書を検証できるように、すべてのサーバに証明書を配布してください。これを行わない場合、無効な証明書に関する警告メッセージが表示されます。証明書の検証に関する詳細については、「証明書の検証」を参照してください。
 - ステップ 2** クライアントの SAML SSO のサービス検出を確認します。クライアントは、標準サービス検出を使用してクライアントの SAML SSO を有効化します。次の設定パラメータを使用してサービス検出を有効にします。ServicesDomain、VoiceServicesDomain、および ServiceDiscoveryExcludedServices。サービス検出の有効化方法については、「クライアントがサービスを検出する方法」を参照してください。
 - ステップ 3** セッションの継続時間を定義します。
セッションは、Cookie およびトークン値で構成されます。通常、Cookie はトークンより長く残ります。cookie の寿命はアイデンティティプロバイダーで定義され、トークンの期間はサービスで定義されます。

- ステップ 4** SSO を有効にすると、デフォルトで、すべての Jabber ユーザが SSO を使用してサインインします。管理者は、特定のユーザが SSO を使用する代わりに、Jabber ユーザ名とパスワードを使用してサインインするようにユーザ単位でこの設定を変更できます。Jabber ユーザの SSO を無効にするには、SSO_Enabled パラメータの値を FALSE に設定します。
- ユーザに電子メールアドレスを尋ねないように Jabber を設定した場合は、ユーザの Jabber への最初のサインインが非 SSO になることがあります。展開によっては、パラメータの ServicesDomainSsoEmailPrompt を ON に設定する必要があります。これにより、最初の SSO によるサインインの実行に必要な情報が Jabber に渡されることが保証されます。ユーザが一度でも Jabber にサインインしたことがある場合は、必要な情報が入手できるため、このプロンプトは必要ありません。

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
VMware Horizon View	6.0、5.3、および 5.2

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。

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には、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する必要があります。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** : コールおよびチャット履歴
 - **写真キャッシュ** : ディレクトリ写真をローカルにキャッシュする
- 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維持し、コンフィギュレーションストア キャッシュを保存する
 - **クレデンシャル** : 暗号化されたユーザ名およびパスワード ファイルを保存する

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除外リストに追加します。

個人ユーザ設定を保存するには

- 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** : これは Citrix 環境向けのプロファイルソリューションです。ランダム ホスト型仮想デスクトップ割り当てを使用した展開では、Citrix Profile Management が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** : これは、ユーザ プロファイルを保存し、それらを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、View ユーザプロファイルの管理では 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。



第 3 章

要件

- [Cisco Jabber for Windows および Cisco Jabber for Mac 向けのオンプレミス サーバ](#), 15 ページ
- [Cisco Jabber for Android 向けのオンプレミス サーバ](#), 16 ページ
- [Cisco Jabber for iPhone and iPad 向けのオンプレミス サーバ](#), 19 ページ
- [デスクトップクライアントのハードウェア要件](#), 21 ページ
- [Cisco Jabber for Android のハードウェア要件](#), 22 ページ
- [Cisco Jabber for iPhone and iPad のハードウェア要件](#), 24 ページ
- [ネットワークの要件](#), 25 ページ

Cisco Jabber for Windows および Cisco Jabber for Mac 向けのオンプレミス サーバ

Cisco Jabber は次のオンプレミス サーバをサポートします。

- Cisco Unified Communications Manager リリース 8.6(2) 以降
- Cisco Unified Presence リリース 8.6(2) 以降
- Cisco Unity Connection リリース 8.6(2) 以降
- Cisco WebEx Meetings Server バージョン 1.5 以降 (Windows のみ)
- Cisco WebEx Meetings Server バージョン 2.0 以降 (Mac のみ)
- Cisco Expressway Series for Cisco Unified Communications Manager
 - Cisco Expressway-E バージョン 8.1.1 以降
 - Cisco Expressway-C バージョン 8.1.1 以降
- Cisco TelePresence Video Communications Server

- Cisco VCS Expressway バージョン 8.1.1 以降
- Cisco VCS Control バージョン 8.1.1 以降

Cisco Jabber は、Cisco Unified Survivable Remote Site Telephony バージョン 8.5 で次の機能をサポートします。

- 基本コール機能
- コールを保留およびレジュームする機能



制約事項 Cisco Jabber には、Cisco Unified Survivable Remote Site Telephony に正常にフォールバックするためのプレゼンス サーバへのアクティブな接続が必要です。

Cisco Unified Survivable Remote Site Telephony の設定方法については、http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide.html で『Cisco Unified SCCP and SIP SRST System Administrator Guide』を参照してください。

Cisco Unified Communications Manager Express サポートの詳細については、http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_device_support_tables_list.html で Cisco Unified CME のマニュアルを参照してください。

Cisco Jabber for Android 向けのオンプレミス サーバ

Cisco Jabber for Android は次のオンプレミス ノードとサーバをサポートします。

Cisco Unified Communications Manager

- Cisco Unified Communications Manager リリース 8.6(1)
- Cisco Unified Communications Manager リリース 8.6(2)
- Cisco Unified Communications Manager リリース 9.1(1)
- Cisco Unified Communications Manager リリース 9.1(2)
- Cisco Unified Communications Manager リリース 10.0(1)
- Cisco Unified Communications Manager リリース 10.5(1)
- Cisco Unified Communications Manager リリース 10.5(2)

Cisco Unified Presence

- Cisco Unified Presence リリース 8.6(1)
- Cisco Unified Presence リリース 8.6(2)

Cisco Unified Communications Manager IM and Presence Service



(注) Cisco Unified Communications Manager IM and Presence Service は、以前は、Cisco Unified Presence と呼ばれていました。

- Cisco Unified Communications Manager IM and Presence Service リリース 9.1(1)
- Cisco Unified Communications Manager IM and Presence Service リリース 9.1(2)
- Cisco Unified Communications Manager IM and Presence Service リリース 10.0(1)
- Cisco Unified Communications Manager IM and Presence Service リリース 10.5(1)
- Cisco Unified Communications Manager IM and Presence Service リリース 10.5(2)

ビデオ会議ブリッジ

- Cisco TelePresence MCU 5310
- Cisco Telepresence Server 7010
- Cisco Telepresence Server MSE 8710
- Cisco サービス統合型ルータ (PVDM3)



(注) Expressway for Mobile and Remote Access は、シスコサービス統合型ルータ (PVDM3 を搭載) ではサポートされません。

Cisco Unity Connection

- Cisco Unity Connection リリース 8.5
- Cisco Unity Connection リリース 8.6(1)
- Cisco Unity Connection リリース 8.6(2)
- Cisco Unity Connection リリース 9.1(1)
- Cisco Unity Connection リリース 9.1(2)
- Cisco Unity Connection リリース 10.0(1)
- Cisco Unity Connection リリース 10.5(1)
- Cisco Unity Connection リリース 10.5(2)

Cisco WebEx Meetings Server

- Cisco WebEx Meetings Server バージョン 2.0
- Cisco WebEx Meetings Server バージョン 2.5

- Cisco WebEx Meetings client バージョン 4.5 ~ 6.5

Cisco Expressway Series for Cisco Unified Communications Manager (オプション)

クライアントに対してモバイルアクセスとリモートアクセスをセットアップするには、次のサーバを使用します。Expressway サーバは Cisco Jabber にコール制御を提供しないことに注意してください。クライアントは、コール制御に Cisco Unified Communications Manager を使用します。

- Cisco Expressway-E バージョン 8.5
- Cisco Expressway-C バージョン 8.5
- Cisco Expressway バージョン 8.2
- Cisco Expressway バージョン 8.2.1

現在 Cisco TelePresence Video Communications Server (VCS) 環境を展開している場合は、Cisco Expressway for Mobile and Remote Access をセットアップできます。VCS 環境には、Cisco VCS Expressway バージョン 8.1.1 と Cisco VCS Control バージョン 8.1.1 が必要です。

Cisco Adaptive Security Appliance (オプション)

- Cisco ASA (Adaptive Security Appliance) 5500 シリーズ バージョン 8.4(1) 以降
- Cisco Adaptive Security Device Manager (ASDM) バージョン 6.4 以降
- Cisco AnyConnect Secure Mobility Client Integration (オプション) : Android デバイスは Google Play ストアから入手可能な Cisco AnyConnect Secure Mobility Client の最新バージョンを実行する必要があります。



(注) Samsung の AnyConnect を使用している場合にサポートされるバージョンは 4.0.01128 です。

- ASA のライセンス要件：次の組み合わせのいずれかを使用します。
 - AnyConnect Essentials と AnyConnect Mobile ライセンス
 - AnyConnect Premium と AnyConnect Mobile ライセンス
- 証明書ベースの認証を使用する場合の認証局 (CA) : Cisco IOS Certificate Server、Microsoft Windows Server 2008 Enterprise Certificate Authority、または Microsoft Windows Server 2003 Enterprise Certificate Authority

Cisco Jabber for iPhone and iPad 向けのオンプレミス サーバ

Cisco Jabber for iPhone and iPad は次のオンプレミス サーバをサポートします。

Cisco Unified Communications Manager

- Cisco Unified Communications Manager リリース 8.6(2)
- Cisco Unified Communications Manager リリース 9.1(2)
- Cisco Unified Communications Manager リリース 10.0(1)
- Cisco Unified Communications Manager リリース 10.5(1)
- Cisco Unified Communications Manager リリース 10.5(2)

Cisco Unified Presence

- Cisco Unified Presence リリース 8.6(1)
- Cisco Unified Presence リリース 8.6(2)

Cisco Unified Communications Manager Release IM and Presence Service



(注) Cisco Unified Communications Manager IM and Presence Service は、以前は、Cisco Unified Presence と呼ばれていました。

- Cisco Unified Communications Manager IM and Presence Service リリース 9.1(1)
- Cisco Unified Communications Manager IM and Presence Service リリース 9.1(2)
- Cisco Unified Communications Manager IM and Presence Service リリース 10.0(1)
- Cisco Unified Communications Manager IM and Presence Service リリース 10.5(1)
- Cisco Unified Communications Manager IM and Presence Service リリース 10.5(2)

Cisco Unity Connection

- Cisco Unity Connection リリース 8.5
- Cisco Unity Connection リリース 8.6(1)
- Cisco Unity Connection リリース 8.6(2)
- Cisco Unity Connection リリース 9.1(1)

- Cisco Unity Connection リリース 9.1(2)
- Cisco Unity Connection リリース 10.0(1)
- Cisco Unity Connection リリース 10.5(1)
- Cisco Unity Connection リリース 10.5(2)

Cisco WebEx Meetings Server

- Cisco WebEx Meetings Server バージョン 1.5
- Cisco WebEx Meetings Server バージョン 2.0
- Cisco WebEx Meetings Server バージョン 2.5
- Cisco WebEx Meetings Client バージョン 4.5 ~ 6.5

Cisco Adaptive Security Appliance (オプション)

- VPN オンデマンド (オプション) : Apple iOS オンデマンド VPN 機能は、証明書のみ認証が必要です。証明書のみ認証がない状態で (ASA) を設定した場合、ユーザは必要に応じて AnyConnect VPN 接続を手動で開始する必要があります。

iOS デバイスは、Cisco AnyConnect Secure Mobility Client などの VPN クライアントを使用して企業ネットワーク、サーバ、およびテレフォニーエンドポイントにアクセスする必要があります。

- Cisco AnyConnect Secure Mobility Client Integration (オプション)
 - iOS デバイスは、Apple App Store から入手可能な Cisco AnyConnect Secure Mobility Client 3.0.09115 を実行する必要があります。
 - Cisco ASA 5500 Series Adaptive Security Appliance (ASA) バージョン 8.4(1) 以降
 - Cisco Adaptive Security Device Manager (ASDM) バージョン 6.4 以降
 - ASA のライセンス要件 : 次の組み合わせのいずれかを使用します。
 - AnyConnect Essentials と AnyConnect Mobile ライセンス
 - AnyConnect Premium と AnyConnect Mobile ライセンス



(注) Cisco AnyConnect のライセンス要件の詳細については、『*VPN License and Feature Compatibility*』を参照してください。

- 証明書ベースの認証を使用している場合の認証局 (CA) : Cisco IOS Certificate Server、Cisco IOS Certificate Server、または Microsoft Windows Server 2003 Enterprise Certificate Authority

Cisco Jabber は、Cisco Unified Survivable Remote Site Telephony (SRST) バージョン 8.6 で次の機能をサポートします。

- 基本コール機能
- 共有回線でさまざまなクライアントのコールを保留して再開する機能。

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	256MB	300 MB
CPU の速度およびタイプ	モバイル AMD Sempron プロセッサ 3600+ (2 GHz) Intel Core2 CPU 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 <ul style="list-style-type: none"> • 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)

Cisco Jabber for Windows でサポートされる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 8.1 32 ビットおよび 64 ビット：デスクトップ モードでのみサポートされる
- Microsoft Windows 8 32 ビットおよび 64 ビット：デスクトップ モードでのみサポートされる
- Microsoft Windows 7 32 ビットおよび 64 ビット

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 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。

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 Mountain Lion 10.8.1 (以降)
- Apple OS X Mavericks 10.9 (以降)
- Apple OS X Yosemite 10.10 (以降)

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

Cisco Jabber for Android でサポートされるデバイスは次のとおりです。

デバイス	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	One M7	Android OS 4.4.x
	One M8	Android OS 4.4.x
	One Max	Android OS 4.4.x

デバイス	デバイス モデル	オペレーティング システム
Google Nexus	5	Android OS 4.4.x および Android OS 5.0
	7	Android OS 4.4.x および Android OS 5.0
	10	Android OS 4.4.x および Android OS 5.1
LG	G2	Android OS 4.2.2 ~ Android OS 4.4.x
	G3	Android OS 4.4.x
Motorola	Moto G	Android OS 4.4.x
Samsung Galaxy	Note II	Android OS 4.2 ~ Android OS 4.4.x
	Note III	Android OS 4.3 ~ Android OS 4.4.x
	Note IV	Android OS 4.4.x
	Note Pro 12.2	Android OS 4.4.x
	Rugby Pro	Android OS 4.2.2 ~ Android OS 4.4.x
	SII	Android OS 4.1.2 ~ Android OS 4.4.x
	SIII	Android OS 4.2 ~ Android OS 4.4.x
	S4	Android OS 4.2.2 ~ Android OS 4.4.x
	S4 mini	Android OS 4.2.2 ~ Android OS 4.4.x
	S5	Android OS 4.4.x
	S5 mini	Android OS 4.4.x
	Tab 3 8 インチ	Android OS 4.4.x
	Tab 4 7 インチ、8 インチ、および 10.1 インチ	Android OS 4.4.x
Tab PRO 8.4 インチおよび 10.1 インチ	Android OS 4.4.x	
Tab S 8.4 インチおよび 10.5 インチ	Android OS 4.4.x	

デバイス	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
	Z1	Android OS 4.2 ~ Android OS 4.4.x
	Z2	Android OS 4.4.x
	Z2 tablet	Android OS 4.4.x
	Z3	Android OS 4.4.x
	ZR/A	Android OS 4.1.2 ~ Android OS 4.4.x

各 Android デバイスが次の CPU とディスプレイの最小要件を満たしている必要があります。

- 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。
- CPU：1.5 GHz デュアルコア以上（クアッドコアを推奨）。
- ディスプレイ：320 x 480 以上。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。

サポートされる Bluetooth デバイス

- Jabra Motion
- 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+
- Jabra Easygo

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。

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	注記
iTouch	5	
iPhone	4S、5、5C、5S、6、および 6 Plus	
iPad	second、third、および fourth	
iPad Mini	mini 1、mini 2、および mini 3	
iPad Air	Air1 と Air 2	

上記すべての Apple デバイスで Bluetooth ヘッドセットがサポートされます。

- Jabra EASYGO
- Jabra EXTREME 2
- Jabra SPEAK 450 for Cisco
- Jabra SUPREME UC
- Jabra WAVE
- Sony Ericsson Bluetooth Headset BW600

ネットワークの要件

電話サービスを展開する場合は、モバイルデバイスを社内ネットワークに接続できる必要があります。

社内の Wi-Fi ネットワークを介した Cisco Jabber 使用時のユーザ エクスペリエンスを最適化するために、シスコは次を推奨します。

- エレベータ、階段、屋外廊下などのエリアを含め、カバレッジのギャップを可能な限り排除するように、Wi-Fi ネットワークを設計します。
- すべてのアクセス ポイントで、モバイルデバイスに同じ IP アドレスが割り当てられることを確認します。コール中に IP アドレスが変更されると、コールが切断されます。
- すべてのアクセス ポイントの 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。シスコでは次を推奨しています。

- 重複しないチャンネルの設定、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、以下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)』

Bluetooth の使用により、音声品質と接続の問題が発生する可能性があります。

ユーザがリモートからネットワークに接続する場合は、モバイルデバイスが安定した広帯域幅接続を使用して、社内ネットワークに接続する必要があります。ビデオと音声の品質は接続品質によって変化し、保証されるものではありません。

Cisco Jabber for Windows と Cisco Jabber for Mac のポートとプロトコル

次の表に、Cisco Jabber で使用される発信ポートとプロトコルを示します。

ポート	プロトコル	説明
443	TCP (XMPP および HTTPS)	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。 (注) Cisco Jabber は、Cisco Unity Connection と Cisco WebEx Meetings Server への HTTPS トラフィックにもこのポートを使用できます。
389	UDP/TCP	LDAP ディレクトリ サーバ
636	LDAPS	LDAP ディレクトリ サーバ (セキュア)
3268	TCP	グローバル カタログ サーバ
3269	LDAPS	グローバル カタログ サーバ (セキュア)

ポート	プロトコル	説明
5070	UDP	ビデオ デスクトップ 共有機能の Binary Floor Control Protocol (BFCP)
5222	TCP (XMPP)	Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence Service への XMPP トラフィック。
8443	TCP (HTTPS)	Cisco Unified Communications Manager と Cisco Unified Communications Manager IM and Presence Service へのトラフィック。
7080	TCP (HTTPS)	ボイス メッセージの通知 (新しいメッセージ、メッセージの更新、およびメッセージの削除) 用の Cisco Unity Connection
53	UDP/TCP	ドメイン ネーム システム (DNS) トラフィック
37200	SOCKS5 バイトストリーム	ピア ツー ピア 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。
5060	UDP/TCP	Session Initiation Protocol (SIP) コール シグナリング
5061	TCP	セキュアな SIP コール シグナリング
49152 ~ 65535	TCP	IM 専用画面の共有 クライアントはこの範囲からランダムにポートを選択します。 実際の範囲は異なる場合があります。実際の範囲を調べるには、次のコマンドを実行します。 netsh interface ipv4 show dynamicportrange tcp SharePortRangeStart パラメータと SharePortRangeSize パラメータを使用して、IM 画面共有に使用される範囲を絞り込むことができます。これらのパラメータの詳細については、『 <i>Deployment and Installation Guide</i> 』で <i>Common Policies</i> パラメータに関するトピックを参照してください。

追加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、展開されたすべてのサービスおよびプロトコルに必要なポートを確認することを保証する必要があります。バージョンに応じて適切なマニュアルを参照してください。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、および Cisco Unified Presence 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。

Cisco Jabber for Android、iPhone、および iPad のポートとプロトコル

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する必要があります。



(注) クライアントで有効にする TCP/IP サービスはありません。

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
着信			
16384 ~ 32766	RTP	UDP	オーディオおよびビデオ用の Real-Time Transport Protocol (RTP) メディア ストリームを受信する。これらのポートは、Cisco Unified Communications Manager で設定します。
発信			
69	TFTP	UDP	Trivial File Transfer Protocol (TFTP) サーバに接続する。
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する。

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
80	HTTP	TCP	会議用の Cisco WebEx Meeting Center やボイスメール用の Cisco Unity Connection などのサービスに接続します。
389	LDAP	TCP、UDP	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。
443	HTTPS	TCP	会議用の Cisco WebEx Meeting Center やボイスメール用の Cisco Unity Connection などのサービスに接続します。
636	LDAPS	TCP	LDAP ディレクトリ サービスにセキュアに接続する。
3269	LDAPS	TCP	グローバル カタログ サーバにセキュアに接続する。
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	セキュアな SIP コール シグナリングを提供する。
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 Presence または Cisco Unified Communications Manager IM and Presence Service に接続します。
5269	XMPP	TCP	XMPP フェデレーション。
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。

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
8443	HTTPS	TCP	8443 は、Cisco Unified Communications Manager に対する Web アクセス用のポートで、次に対する接続が含まれます。 <ul style="list-style-type: none"> • 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)。
16384 ~ 32766	RTP	UDP	オーディオおよびビデオ用の RTP メディア ストリームを送信する。
53	DNS	UDP	ホスト名の解決を提供する。
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。これは、Cisco Unified Communications Manager Certificate Authority Proxy Function (CAPF) 登録用のリスニングポートです。

Expressway for Mobile and Remote Access のポート使用方法については、『*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, Release 10.5(2)*』の「Managed File Transfer」の章を参照してください。

Cisco Jabber for Windows と Cisco Jabber for Mac でサポートされるコーデック

サポートされるオーディオコーデック

- G.722
- G.722.1 : 32k と 24k。 G.722.1 は Cisco Unified Communications Manager 8.6.1 以降でサポートされます。
- G.711 : a-law と u-law
- G.729a

サポートされるビデオ コーデック

- H.264/AVC

Cisco Jabber for Android、iPhone、および iPad でサポートされるコーデック

サポートされるオーディオ コーデック

- G.711 : mu-law
- G.711 : a-law
- G.722.1
- G.729a

狭帯域幅で使用するための最小要件 : G.729a

音声品質に問題が発生した場合、ユーザはクライアント設定の狭帯域幅モードをオン/オフにすることができます。

通常モードでは、G.711、G.722.1、G.729a がサポートされます。

狭帯域幅モードでは、G.729a だけがサポートされます。

サポートされるビデオ コーデック

H.264/AVC

サポートされるボイスメール コーデック

- PCM リニア
- G.711 : mu-law (デフォルト)
- G.711 : a-law
- GSM 6.10



(注) Cisco Jabber は、G.729 を使用したビジュアルボイスメールをサポートしません。ただし、ユーザは G.729 と [ボイスメールに発信 (Call Voicemail)] 機能を使用して自分のボイス メッセージにアクセスできます。



第 4 章

連絡先ソース

- [オンプレミス連絡先ソース オプション](#), 33 ページ

オンプレミス連絡先ソース 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。

- **LDAP** : 社内ディレクトリを使用している場合は、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)** : 社内ディレクトリを使用していない場合は、このオプションを使用できます。

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]
- ディレクトリ 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。

ディレクトリ 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、認証用のユーザー 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。

ディレクトリサーバ

Cisco Jabber では、次のディレクトリサーバを使用できます。



(注)

Cisco Jabber for Mac、Cisco Jabber for iPhone and iPad、Cisco Jabber for Android は、ディレクトリの統合で 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、Cisco Unified Communications Manager の次の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) 以降と COP ファイルの `cmterm-cucm-uds-912-5.cop.sgn`。

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。詳細については、「LDAP ディレクトリ サーバ」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。

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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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、幅が高さと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。
- 縦方向：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。

- 横方向：ディレクトリ内の連絡先写真が横方向である場合、クライアントは両方の側から 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 5 章

証明書

- [証明書の検証, 39 ページ](#)
- [オンプレミス サーバに必要な証明書, 40 ページ](#)
- [クラウドベースのサーバの証明書要件, 43 ページ](#)

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、サービスが 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は、信頼できないものとみなされ、Jabber からその証明書を受け入れるか拒否するかが尋ねられます。

ユーザが証明書を受け入れた場合は、Jabber がサービスに接続して、証明書を証明書ストアまたはデバイスのキーチェーンに保存します。ユーザが証明書を拒否した場合は、Jabber がサービスに接続せず、証明書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は、Jabber が証明書を信頼します。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。

Jabber が 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 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 1 つの FQDN に対する複数の CSR を受け入れません。そのため、サービスごとに CSR を別々のパブリック認証局に送信する必要があります。

IP アドレスまたは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内で 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 Presence または 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な SIP コールシグナリングと CTI 接続検証)
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

- SAML SSO と 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 Presence または 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。
- クラスタ、サブスクライバ、およびパブリッシャのノードごとに、Tomcat サービスが実行され、クライアントに HTTP 証明書が提示されます。
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) には特定の形式に準拠するための証明書署名要求 (CSR) が必要です。たとえば、パブリック CA は、次のような CSR を受け入れる場合があります。

- Base 64 エンコードである。
- 組織、OU、その他フィールドに @&! などの特定の文字を含まない。
- サーバの公開キーで特定のビット長を使用する。

同様に、複数ノードから CSR を送信すると、パブリック CA は、すべての CSR で情報の整合性がとれていることを必要とする場合があります。

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 あたり証明書 1 つ : いくつかのパブリック CA は、完全修飾ドメイン名 (FQDN) あたり 1 つの証明書にのみ署名します。

たとえば、単一の 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、それぞれの CSR を別々のパブリック 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 HTTP URL が証明書に含まれている必要があります。CA が証明書を取り消した場合は、クライアントがユーザにそのサーバへの接続を許可しません。

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、認証局（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、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、環境全体の FQDN として各サーバ名を指定する必要があります。

クラウドベースのサーバの証明書要件

Cisco WebEx Messenger と Cisco WebEx Meeting Center はクライアントに次の証明書を提示します。

- CAS
- WAPI



重要

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 が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 for Windows 9.7.2 と Cisco Jabber for Mac 9.6.1 以降では、Cisco Jabber が Cisco WebEx Messenger から受信した XMPP 証明書を検証します。オペレーティングシステムに Cisco WebEx Messenger 用の次の証明書が含まれていない場合は、それらを入力する必要があります。

- VeriSign Class 3 Public Primary Certification Authority : G5 (信頼されたルート認証局に保存される)
- VeriSign Class 3 Secure Server CA : G3 (中間認証局に保存される)

中間認証局に保存されている証明書によって WebEx Messenger サーバ ID が検証されます。

Cisco Jabber for Windows 9.7.2 以降の場合は、

<http://www.identrust.co.uk/certificates/trustid/install-nes36.html> でルート証明書の詳細情報とインストール手順を確認できます。

Cisco Jabber for Mac 9.6.1 以降の場合は、<http://support.apple.com> の Apple サポート Web サイトでルート証明書の詳細情報を確認できます。



第 6 章

サービス ディスカバリ

- [サービス ディスカバリについて, 45 ページ](#)
- [クライアントによるサービスの検索方法, 47 ページ](#)
- [Cisco UDS SRV レコード, 49 ページ](#)
- [CUP ログイン SRV レコード, 50 ページ](#)
- [Collaboration Edge SRV レコード, 52 ページ](#)

サービス ディスカバリについて

サービス ディスカバリにより、クライアントは自動的に企業のネットワークでサービスを検出することができます。サーバロケーションを提供するサービス (SRV) レコードを取得するため、クライアントはドメイン ネーム サーバを問い合わせます。

サービス ディスカバリを使用することの主な利点は次のとおりです。

- 導入までの時間短縮。
- サーバロケーションの一元管理が可能。



重要 Cisco Unified Presence 8.x から Cisco Unified Communications Manager IM and Presence Service 9.0 以降への移行。

Cisco Unified Communications Manager 上で移行された UC サービスに、Cisco Unified Presence サーバの FQDN を指定する必要があります。[Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] インターフェイスを開きます。[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [UC サービス (UC Service)] を選択します。

[IM and Presence (IM and Presence)] タイプの UC サービスの場合は、Cisco Unified Presence 8.x から Cisco Unified Communications Manager IM and Presence Service に移行すると、[ホスト名/IP アドレス (Host Name/IP Address)] フィールドにドメイン名が入力されるため、このドメイン名を Cisco Unified Presence サーバの FQDN に変更する必要があります。

ただし、クライアントは、さまざまなサーバが存在することと、さまざまなサービスを利用できることをクライアントに示す、さまざまな SRV レコードを取得できます。このように、クライアントは、各 SRV レコードを取得するときに、環境に関する特定の情報を取得します。

次の表は、配置可能な SRV レコードを一覧表示し、それぞれのレコードに関する目的とメリットについて説明しています。

SRV レコード	目的	設置の理由
_cisco-uds	<p>Cisco Unified Communications Manager バージョン 9.0 以降の場所を提供します。</p> <p>クライアントは Cisco Unified Communications Manager からサービスプロファイルを取得してオーセンティケータを特定できます。</p>	<ul style="list-style-type: none"> インストール引数を指定する必要性を排除します。 UC サービス プロファイルの設定を集中管理できます。 クライアントは、ユーザのホーム クラスタを検出できます。 <p>その結果、クライアントは自動的にユーザのデバイス設定を取得し、デバイスを登録できます。CCMCIP プロファイルまたは TFTP サーバアドレスのユーザをプロビジョニングする必要はありません。</p> <ul style="list-style-type: none"> 混在製品モードのサポート。 <p>フル UC、IM のみ、もしくは電話機モード機能でユーザを容易に配置できます。</p> <ul style="list-style-type: none"> Expressway for Mobile and Remote Access をサポートします。

SRV レコード	目的	設置の理由
_cuplogin	<p>Cisco Unified Presence の場所を提供します。</p> <p>Cisco Unified Presence をオーセンティケータに設定します。</p>	<ul style="list-style-type: none"> • Cisco Unified Communications Manager と Cisco Unified Presence バージョン 8.x を使用した展開をサポートします。 • すべてのクラスタが Cisco Unified Communications Manager 9 にまだアップグレードされていない展開をサポートします。
_collab-edge	<p>Cisco VCS Expressway または Cisco Expressway-E の場所を提供します。</p> <p>クライアントは Cisco Unified Communications Manager からサービスプロファイルを取得してオーセンティケータを特定できます。</p>	<ul style="list-style-type: none"> • Expressway for Mobile and Remote Access を使用した展開をサポートします。

クライアントによるサービスの検索方法

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は、ネットワーク接続を取得します。
クライアント ホスト コンピュータがネットワーク接続を取得すると、DHCP 設定から DNS ネーム サーバのアドレスを取得します。
- 2 ユーザは最初のサイン イン時に、次のいずれかの方法でサービスを検出します。
 - 手動：ユーザは Cisco Jabber を開始してから、ウェルカム画面で電子メールに似たアドレスを入力します。
 - URL 設定：URL 設定を使用すれば、ユーザは手動で電子メールを入力せずに、Cisco Jabber を相互起動するためのリンクをクリックできます。

URL 設定リンクの作成には、次の手順が含まれます。

- **ServicesDomain**：Cisco Jabber がサービス検出に使用するドメイン。
- **VoiceServicesDomain**：ハイブリッド展開では、Cisco Jabber が DNS SRV レコードを取得するために使用するドメインが Cisco Jabber ドメインの検出に使用される **ServicesDomain** と異なる可能性があります。
- **ServiceDiscoveryExcludedServices**：特定の展開シナリオ サービスは、サービス検出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
- CUP



(注) 3個のパラメータすべてを含む場合、サービスディスカバリは発生せず、ユーザは手動で接続設定を入力するように促されます。

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,CUP

電子メールまたは Web サイトを使用してユーザへのリンクを指定します。



(注) 所属組織が相互起動専用プロトコルまたはカスタム リンクをサポートするメールアプリケーションを使用している場合、電子メールを使用してリンクを提供できます。使用していない場合、Web サイトを使用してユーザに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 クライアントが Cisco WebEx Messenger サービス用の CAS URL に対して HTTP クエリーを発行します。

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

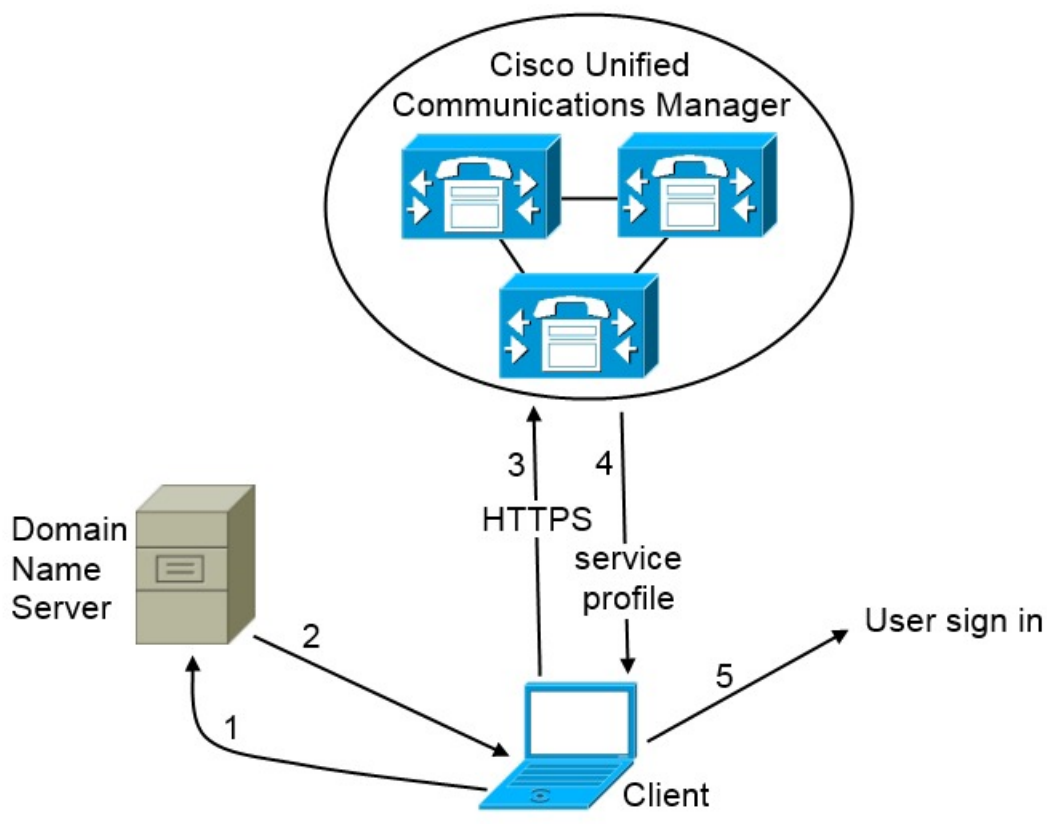
```
_cuplogin._tcp.DOMAIN SRV service location:
priority = 0
weight = 0
```

```
port = 8443
svr hostname=192.168.0.26
```

Cisco UDS SRV レコード

Cisco Unified Communications Manager バージョン9以降の展開では、クライアントが自動的に SRV レコード (`_cisco-uds`) を使用してサービスとコンフィギュレーションを検出できます。

次の図は、クライアントが `_cisco-uds` SRV レコードをどのように使用するかを示しています。



- 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 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。

自動でのユーザのホームクラスタ検索結果として、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、EMCC リモート クラスタのセットアップと同様に、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。

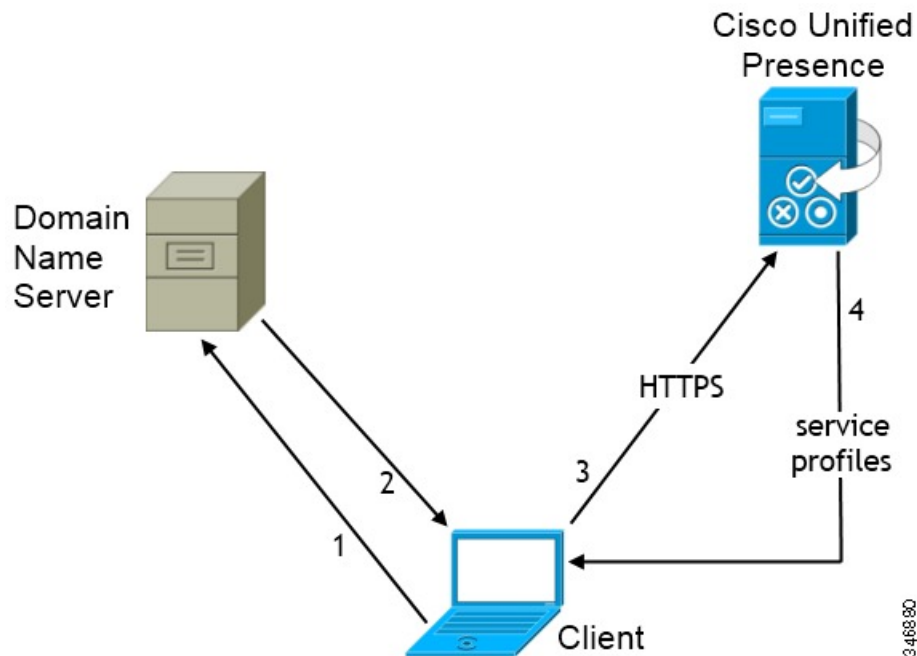
次に、_cisco-uds SRV レコードの例を示します。

```
_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
```

CUP ログイン SRV レコード

Cisco Jabber は、SRV レコード (_cuplogin) を使用して、Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence Service を自動的に検出して接続できます

次の図は、クライアントが _cuplogin SRV レコードをどのように使用するかを示しています。



- 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 ネーム サーバが `_cuplogin SRV` レコードを返します。
その結果として、Cisco Jabber は、プレゼンス サーバを検索して、Cisco Unified Presence がオーセンティケータであることを特定できます。
- 3 クライアントは、クレデンシヤルについてユーザに指示し、プレゼンス サーバを認証します。
- 4 クライアントは、プレゼンス サーバからサービス プロファイルを取得します。



ヒント

`_cuplogin SRV` レコードは、[詳細設定 (Advanced Settings)] ウィンドウのデフォルト サーバアドレスも設定します。

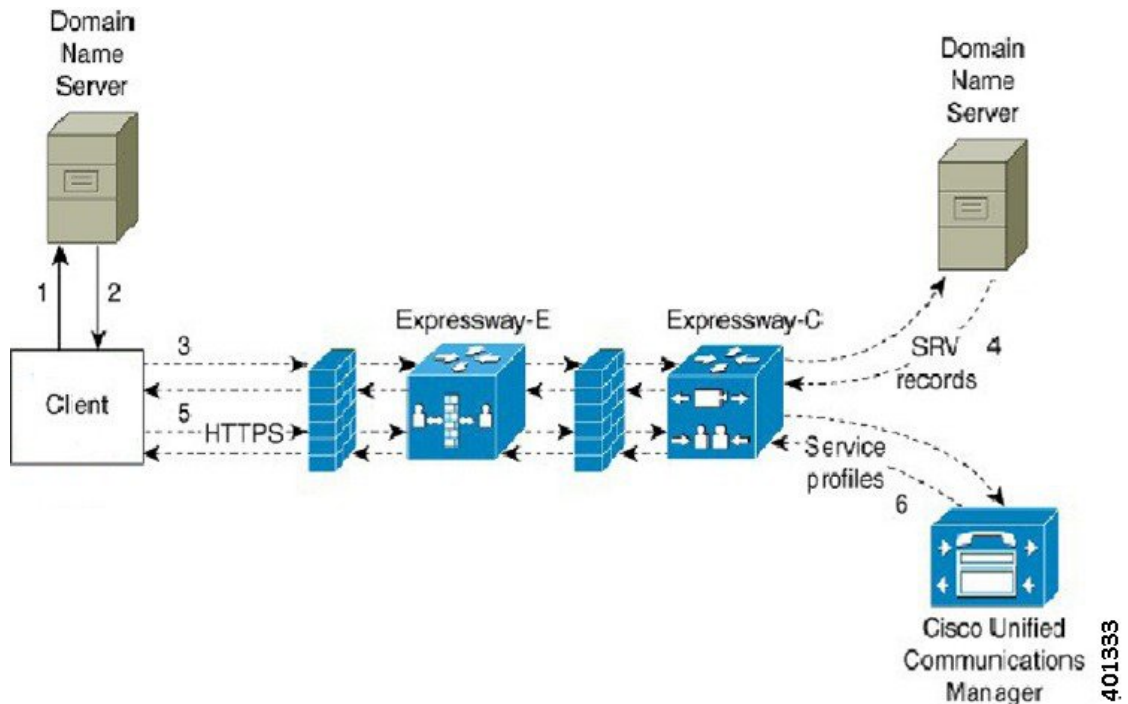
次に、`_cuplogin SRV` レコードの例を示します。

```

_cuplogin._tcp.example.com      SRV service location:
  priority      = 8
  weight       = 50
  port        = 8443
  svr hostname  = cup3.example.com
_cuplogin._tcp.example.com      SRV service location:
  priority      = 5
  weight       = 100
  port        = 8443
  svr hostname  = cup1.example.com
_cuplogin._tcp.example.com      SRV service location:
  priority      = 7
  weight       = 4
  port        = 8443
  svr hostname  = cup2.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て SRV レコード (`_collab-edge`) を使用してサービスを検出しようとしています。



- 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`または`_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 Cisco Unified Communications Manager からサービス プロファイル (Expressway 経由) 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。



第 7 章

セキュリティ

- [連邦情報処理規格 \(FIPS\) , 55 ページ](#)
- [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, 56 ページ](#)
- [インスタントメッセージの暗号化, 56 ページ](#)

連邦情報処理規格 (FIPS)

Cisco Jabber for Windows のみ。

連邦情報処理規格 (FIPS) 140 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を含む暗号モジュールのセキュリティ要件を規定した米国およびカナダ政府の標準です。

FIPS では、Cisco Jabber for Windows 内部で使用される暗号化、キー交換、デジタル署名、ハッシュ、および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。

Cisco Jabber for Windows は FIPS 140.2 に準拠しています。クライアントを FIPS モードで実行するには、Windows オペレーティングシステム上で FIPS を有効にする必要があります。クライアントは、オペレーティングシステムが FIPS モードになっており、それに応じて FIPS モードで動作していることを検出します。

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。サービスの証明書が期限切れになり、その前に FIPS モードのユーザが自分のクレデンシャルを再入力しなかった場合は、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。

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、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 XMPP トラフィックを保護します。また、ポイントツーポイント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 v2	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 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 Presence と Cisco Unified Communications Manager IM and Presence Service の PKI 証明書キー長を示します。

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
Cisco Unified Presence バージョン 8.6.4	2048 ビット
Cisco Unified Presence バージョン 8.6.4 以前	1024 ビット

XMPP 暗号化

Cisco Unified Presence と Cisco Unified Communications Manager IM and Presence Service はどちらも、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するために 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 Presence または Cisco Unified Communications Manager IM and Presence Service 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、次のドキュメントを参照してください。

- Cisco Unified Presence : 『*Configuring Security on Cisco Unified Presence*』
- 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

必要に応じて、規制ガイドラインへのコンプライアンスのためにインスタントメッセージをログに記録し、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 Presence と Cisco Unified Communications Manager IM and Presence Service 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のコンプライアンスサーバを設定し、ログに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、次のドキュメントを参照してください。

- Cisco Unified Presence : 『*Instant Messaging Compliance Guide*』
- 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。

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。

クラウドベースの暗号化

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

接続	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

次のサーバが Cisco WebEx Messenger サービスと 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 Cisco Jabber と Cisco WebEx Messenger サービス間のインスタントメッセージングトラフィックを保護する AES アルゴリズムで暗号化された 128 ビット長のセッション キーを使用します。

必要に応じて、256 ビットのクライアント間の AES 暗号化を有効にしてクライアント間のトラフィックを保護します。

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、それらの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。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 クライアント間暗号化が有効になっていると、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、クライアントと Cisco WebEx Messenger サービス間のインスタント メッセージング トラフィックは保護されます。必要に応じて、Cisco WebEx 管理ツールで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するためのポリシーを指定できます。

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：送信クライアントが 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。受信クライアントはインスタント メッセージを復号化します。
- IM の符号化をサポートしない：クライアントは暗号化をサポートし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。

次の表に、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	No	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 で暗号化されたインスタントメッセージを送信しません。	Cisco Jabber は、暗号化されていないインスタントメッセージを送受信します。
[IM の AES 符号化をサポートする (Support AES Encoding For IM)] = true [IM の符号化をサポートしない (Support No Encoding For IM)] = true	Yes	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 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を表示します。	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。

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)] = false	Yes	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 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を表示します。	Cisco Jabber は、リモートクライアントとインスタントメッセージを送受信しません。 Cisco Jabber は、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したときにエラーメッセージを表示します。



(注)

- Cisco Jabber は、グループチャットでのクライアント間暗号化をサポートしません。Cisco Jabber は、ポイントツーポイントチャットでのみクライアント間暗号化を使用します。

暗号化と Cisco WebEx ポリシーの詳細については、Cisco WebEx のマニュアルで「*About Encryption Levels*」のトピック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 true 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。



第 8 章

プランニングの考慮事項

- [DNS の設定, 63 ページ](#)
- [クライアントによるサービスへの接続方法, 73 ページ](#)
- [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, 78 ページ](#)
- [コンピュータ テレフォニー インテグレーション従属, 81 ページ](#)

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

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、CAS ルックアップによる Cisco WebEx ドメインの検出に必要なドメインと、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。

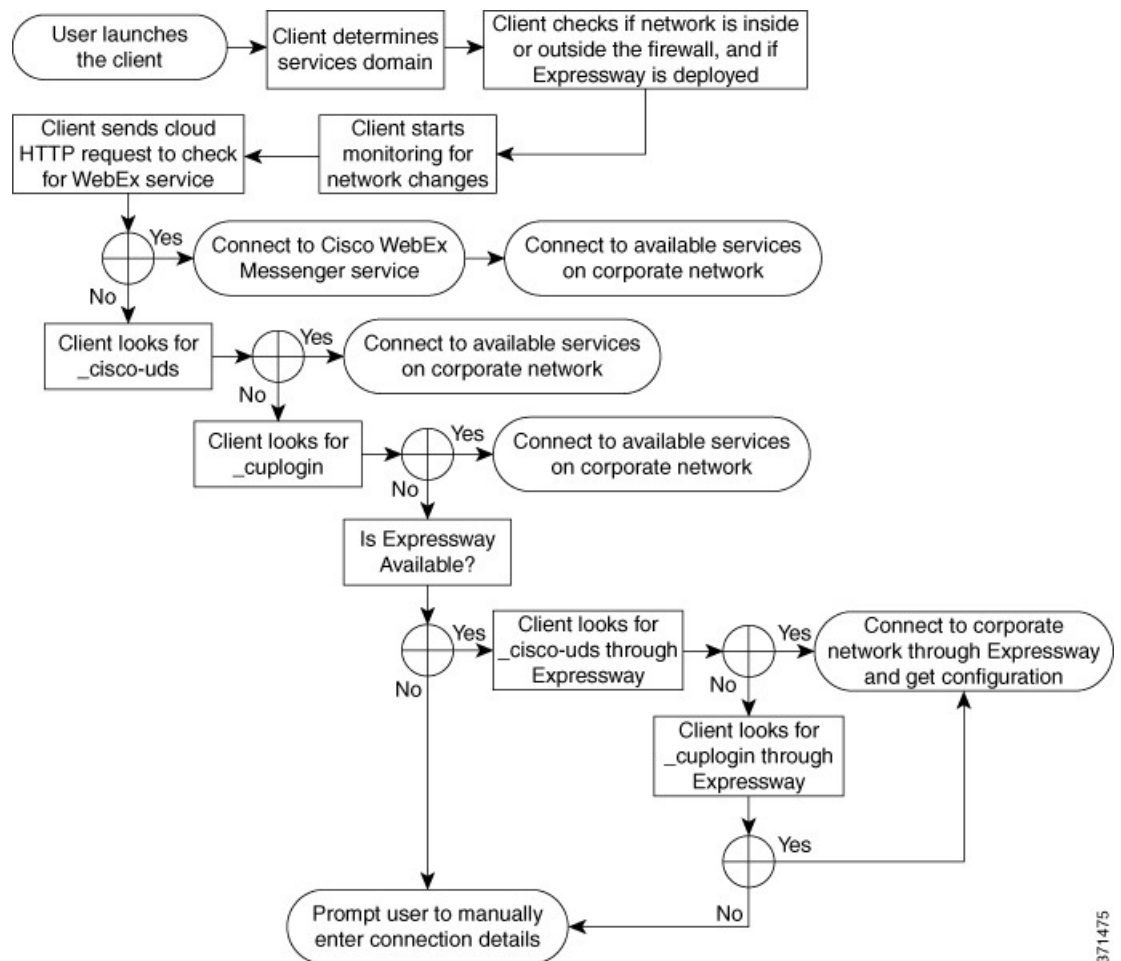
- クライアントが、設定ファイルの `VoiceServicesDomain` パラメータを使用。このオプションは、Jabber `config.xml` ファイルをサポートしているクライアントで使用できます。
- ユーザが、`VoiceServicesDomain` を含む構成 URL をクリック。このオプションは、次のクライアントで使用できます。
 - Cisco Jabber for Android リリース 9.6 以降
 - Cisco Jabber for Mac リリース 9.6 以降
 - Cisco Jabber for iPhone and iPad リリース 9.6.1 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。

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。



371475

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ことを実行します。

- 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。DNS サービス (SRV) レコードを取得するために、ネーム サーバにクエリが送信されます。

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。

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

```
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 サービスに対して認証し、Cisco WebEx Org Admin で設定されたコンフィグレーションと 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。



(注) 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。Internet Explorer の [LAN の設定 (LAN Settings)] でプロキシを設定するには、.pac ファイルの URL を自動設定スクリプトとして指定するか、[プロキシサーバ (Proxy server)] で明示的なプロキシアドレスを指定する必要があります。

次の制限は、これらの HTTP 要求にプロキシを使用する場合に適用されます。

- Web Proxy Auto-Detection (WPAD) プロトコル検索はサポートされません。
- プロキシ認証はサポートされていません。
- バイパスリストのワイルドカードはサポートされません。たとえば、*.example.com の代わりに example.com を使用します

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。

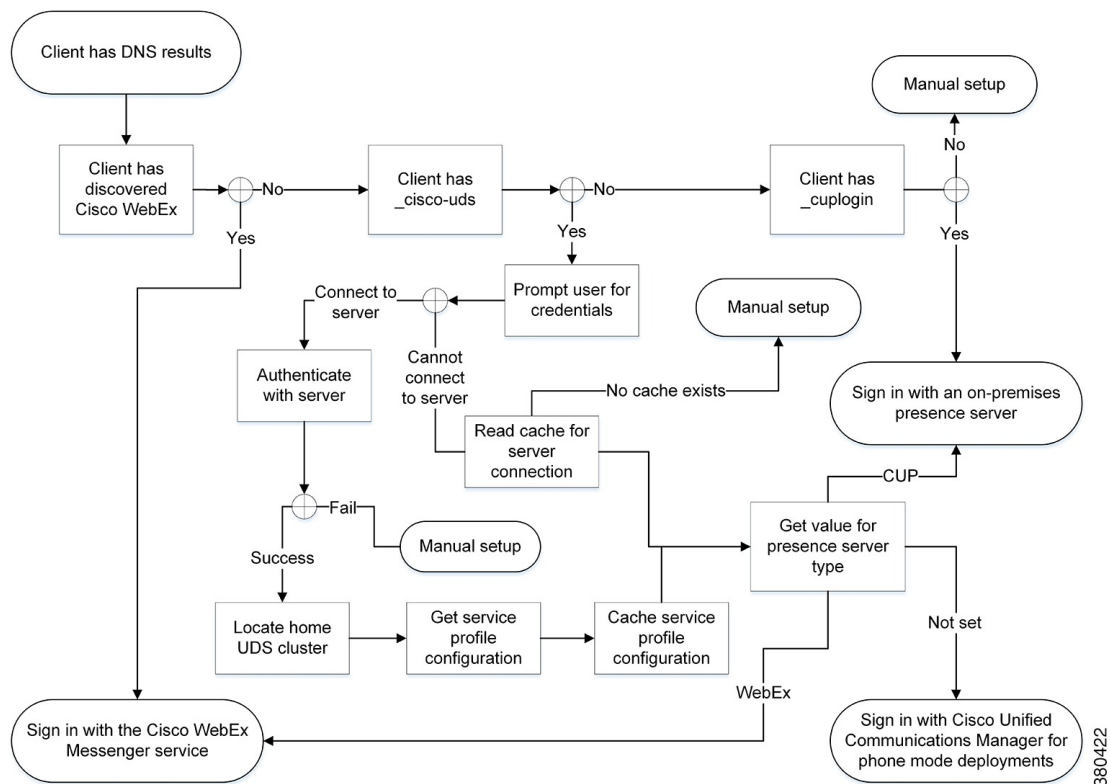
- _cisco-uds
- _cuplogin
- _collab-edge

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。
- _cuplogin：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 Presence 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

次の図に、クライアントの内部サービスへの接続方法を示します。



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。

ユーザにサインイン画面を通過させることが可能なオーセンティケータとして、次の3つが考えられます。

- Cisco WebEx Messenger サービス：クラウドベース展開またはハイブリッドクラウドベース展開。
- Cisco Unified Presence：デフォルト製品モードでのオンプレミス展開。デフォルト製品モードはフル UC または IM のみのいずれかです。
- 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 サービスが認証のプライマリ ソースであることを確認します。
 - b 自動的に Cisco WebEx Messenger サービスに接続されます。
 - 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 クライアントが `_cisco-uds` レコードを検出すると、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す。
 - WebEx (IM and Presence) : Cisco WebEx Messenger サービスがオーセンティケータです。



(注) このリリースの時点では、クライアントは SRV レコードのクエリーに加えて HTTP クエリーを発行します。HTTP クエリーを使用すれば、クライアントが Cisco WebEx Messenger サービスを認証するかどうかを決定できます。

クラウドベース展開では、HTTP クエリーの結果として、クライアントが 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 検索を使用してすでに 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。

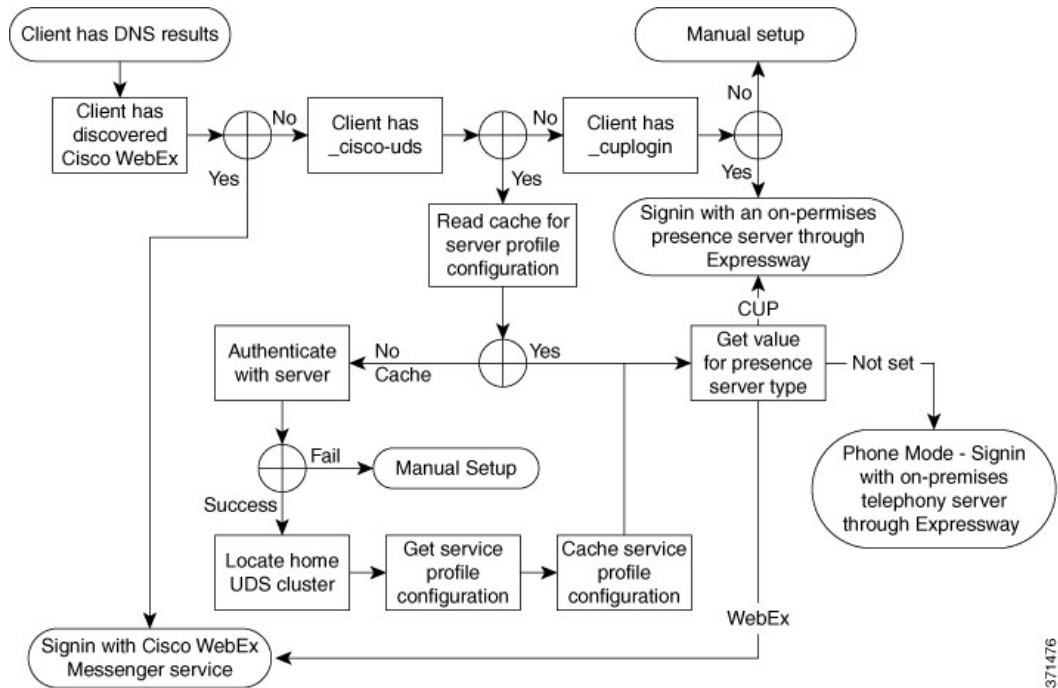
- 未設定 : サービス プロファイルに IM and Presence サービス設定が含まれていない場合は、オーセンティケータが Cisco Unified Communications Manager になります。
- 4 オーセンティケータにサイン インします。
クライアントにサイン インした後、製品モードを判定できます。

- 3 クライアントが `_cuplogin` レコードを検出すると、クライアントは次の処理を実行します。
 - 1 Cisco Unified Presence が認証のプライマリ ソースであることを確認します。
 - 2 自動的にサーバに接続する。
 - 3 ユーザにクレデンシャルの入力を促す。
 - 4 クライアント設定とサービス設定を取得する。

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 レコードを返す場合は、クライアントが Expressway for Mobile and Remote Access 経由で内部サーバに接続しようとします。

次の図は、Expressway for Mobile and Remote Access を介してネットワーク接続されているときに、クライアントが内部サービスに接続する方法を示しています。



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



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

クライアントが `_cisco-uds` が含まれているはずの内部 SRV レコードを取得したら、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 クラスター、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。

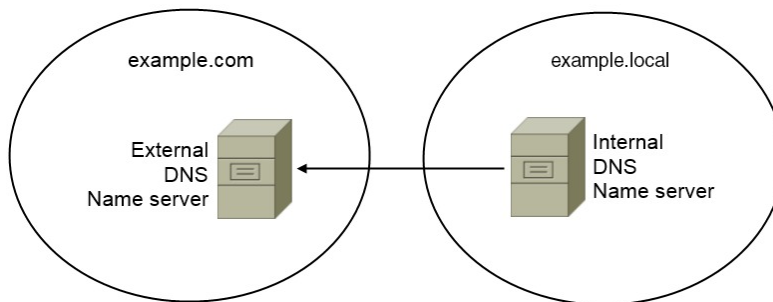
ドメイン ネーム システムの設計

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。



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。

独立ドメイン設計の場合：

- 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。

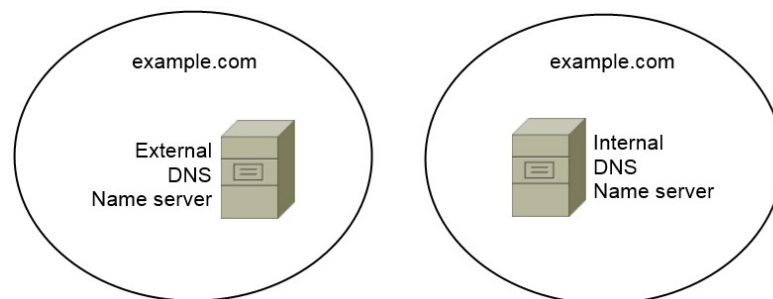
この方式は、ドメイン全体のフォワーディング関係を変え、内部DNS構造を混乱させることがあります。サービスドメインの内部ゾーンを作成できない場合、内部ネームサーバにピンポイントサブドメインゾーンを作成できます。

同ドメイン設計

同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。

同ドメイン (スプリットブレイン)

次の図は、同ドメイン (スプリットブレイン) 設計を示しています。



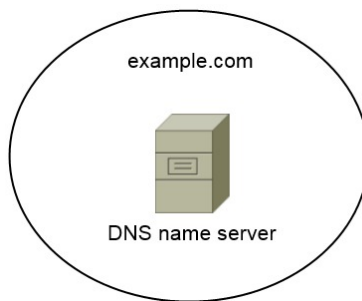
2つの DNS ゾーンが同一のドメインを表します。内部ネーム サーバ内の DNS ゾーンと外部ネーム サーバ内の DNS ゾーンです。

内部ネーム サーバと外部ネーム サーバは、両方ともに単一のドメインに対する権限がありますが、異なるホストのコミュニティを扱います。

- 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。

同ドメイン（非スプリット ブレイン）

次の図は、同ドメイン（非スプリットブレイン）設計を示しています。



同ドメイン（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。

クライアントによるサービスへの接続方法

サービスに接続するには、Cisco Jabber に次の情報が必要です。

- 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、自動的にサービスを探し出し、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。

推奨される接続方法

サービスの接続に必要な情報をクライアントに提供するために使用する必要がある方法は、導入タイプ、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。

Cisco Jabber for Windows 向け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	Non-DNS 方式
フル UC (デフォルトモード)	リリース 9.1.2 以降 : <ul style="list-style-type: none"> • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service 	<code>_cisco-uds.<domain></code> 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。 <ul style="list-style-type: none"> • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>
フル UC (デフォルトモード)	リリース 8.x : <ul style="list-style-type: none"> • Cisco Unified Communications Manager • Cisco Unified Presence 	<code>_cuplogin.<domain></code> 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。 <ul style="list-style-type: none"> • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>

製品モード	サーバのバージョン	検出方法	Non-DNS 方式
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。 <ul style="list-style-type: none"> • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>
IM 専用 (デフォルトモード)	リリース 8.x： Cisco Unified Presence	_cuplogin.<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。 <ul style="list-style-type: none"> • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>
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	次のインストーラスイッチと値を使用する。 <ul style="list-style-type: none"> • AUTHENTICATOR=CUCM • TFTP=<CUCM_address> • CCMCIP=<CUCM_address> • PRODUCT_MODE=phone_mode
電話機モード	リリース 8.x： Cisco Unified Communications Manager	手動接続設定	次のインストーラスイッチと値を使用する。 <ul style="list-style-type: none"> • AUTHENTICATOR=CUCM • TFTP=<CUCM_address> • CCMCIP=<CUCM_address> • PRODUCT_MODE=phone_mode



(注) Cisco Jabber リリース 9.6 以降では、まだ、_cuplogin DNS SRV 要求を使用して完全な Unified Communications およびインスタントメッセージング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。

新規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、DNS レコードが存在するドメインの値を指定するために SERVICES_DOMAIN インストーラのスイッチを使用します。



(注) Cisco Jabber for Windows 9.2からアップグレードしている場合、サービスドメインがキャッシュ設定から読み取られます。

Cisco Jabber for Mac 向け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 : <ul style="list-style-type: none"> • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service 	_cisco-uds.<domain> に対する DNS SRV 要求
フル UC (デフォルトモード)	リリース 8.x : <ul style="list-style-type: none"> • Cisco Unified Communications Manager • Cisco Unified Presence 	_cuplogin.<domain> に対する DNS SRV 要求

Cisco Jabber for Android および Cisco Jabber for iPhone and iPad 向け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 : <ul style="list-style-type: none"> • 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
フル UC (デフォルトモード)	リリース 8.x : <ul style="list-style-type: none"> • Cisco Unified Communications Manager • Cisco Unified Presence 	_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

製品モード	サーバのバージョン	検出方法
IM 専用 (デフォルト モード)	リリース 8.x : Cisco Unified Presence	_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
電話機モード	リリース 8.x : Cisco Unified Communications Manager	手動接続設定またはブートストラップファイル 手動接続設定



(注) Cisco Unified Communications Manager バージョン 9 以降では、まだ、_cuplogin DNS SRV 要求を使用して完全な Unified Communications およびインスタント メッセージング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。

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

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。

認証ソースには、次の 3 つがあります。

- Cisco Unified 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 : クラウドベース展開またはハイブリッドクラウドベース展開。

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 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 Presence リリース 8.5 と 8.6

ハイアベイラビリティの詳細については、次の Cisco Unified Presence のマニュアルを参照してください。

『Configuration and Administration of Cisco Unified Presence Release 8.6』

「Multi-node Deployment Administration」

「Troubleshooting High Availability」

『Deployment Guide for Cisco Unified Presence Release 8.0 and 8.5』

「Planning a Cisco Unified Presence Multi-Node Deployment」

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。

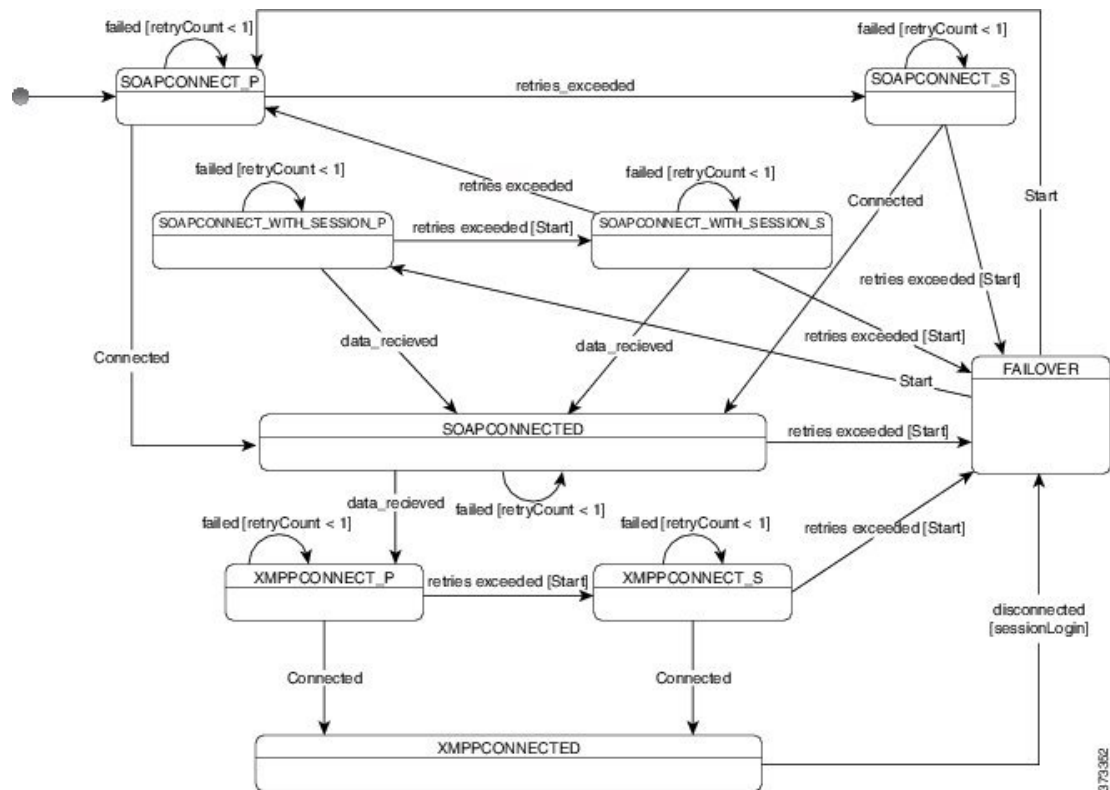
再ログインパラメータの設定

Cisco Unified Presence と Cisco Unified Communications Manager IM and Presence Service 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

次のワークフローでは、Cisco Unified Presence サーバがフェールオーバーした場合のクライアントの動作について説明します。



- 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。

コンピュータ テレフォニー インテグレーション 従属

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。

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。

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>

