



## セキュリティおよび証明書

---

- [暗号化 \(1 ページ\)](#)
- [音声およびビデオの暗号化 \(7 ページ\)](#)
- [セキュアメディア向け認証方法 \(7 ページ\)](#)
- [PIE ASLR サポート \(7 ページ\)](#)
- [連邦情報処理標準規格 \(7 ページ\)](#)
- [Common Criteria \(9 ページ\)](#)
- [Secure LDAP \(9 ページ\)](#)
- [認証済み UDS 連絡先の検索 \(10 ページ\)](#)
- [証明書 \(10 ページ\)](#)
- [マルチテナントのホステッド コラボレーション ソリューション向けの SNI サポート。\(15 ページ\)](#)
- [ウイルス対策の除外 \(15 ページ\)](#)

## 暗号化

### ファイル転送およびスクリーンキャプチャのコンプライアンスおよびポリシー制御

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スクリーン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。

ファイル転送とスクリーン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ー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。

### オンプレミスの暗号化

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。

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ーへ	TLS v1.2 経由の XMPP	X.509 公開キーインフラストラクチャ証明書	AES 256 ビット

#### サーバとクライアントのネゴシエーション

次のサーバは、X.509 公開キーインフラストラクチャ (PKI) 証明書と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 (Version)	キーの長さ (Key Length)
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 Service 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 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 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コンプライアンスサーバを設定し、記録したインスタントメッセージを保護する必要があります。

コンプライアンスの詳細については、次を参照してください。

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

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

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

## クラウドベースの暗号化

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

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

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

### XMPP 暗号化

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

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

### インスタントメッセージのロギング

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、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。

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

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

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

## クライアント間の暗号化

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

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

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

次の表は、これらのポリシーを使用して設定できる組み合わせを示しています。

ポリシーの組み合わせ	クライアント間の暗号化	リモートクライアントがAES暗号化をサポートしている場合	リモートクライアントがAES暗号化をサポートしていない場合
[IM の AES 符号化をサポートする (Support AES Encoding For IM) ] = false  [IM の符号化をサポートしない (Support No Encoding For IM) ] = true	いいえ	Cisco Jabber は暗号化されていないインスタントメッセージを送信します。  Cisco Jabber はキー交換をネゴシエートしません。そのため、他のクライアントは Cisco Jabber の暗号化されたインスタントメッセージを送信しません。	Cisco Jabber は暗号化されていないインスタントメッセージを送受信します。
[IM の AES 符号化をサポートする (Support AES Encoding For IM) ] = True  [IM の符号化をサポートしない (Support No Encoding For IM) ] = true	はい	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	はい	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。  Cisco Jabber 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、にエラーメッセージが表示されます。



(注) Cisco Jabber は、グループチャットの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 チャットだけに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 のマニュアルの暗号化レベルについてを参照してください。

## 暗号化アイコン

暗号化レベルを表示するには、クライアントが表示するアイコンを確認します。

### サーバの暗号化対応クライアント用のロックアイコン

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



### クライアント間暗号化の鍵アイコン

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



## ローカルのチャット履歴

チャット履歴は、参加者がチャット ウィンドウを閉じたあともサインアウトするまで維持されます。参加者がチャット ウィンドウを閉じたらチャット履歴を破棄する場合は、Disable\_IM\_History パラメータを 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。

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

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

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

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

モバイルクライアントでは、チャット履歴ファイルにアクセスできません。

## 音声およびビデオの暗号化

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

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

## セキュアメディア向け認証方法

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

### SIP OAuth

お使いの Cisco Unified Communications Manager がセットアップされたときに 1 回実行されます。これにより、RTP メディアを含む SIP トラフィックの安全性が確保されます。

### 認証モード

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

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

## PIE ASLR サポート

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

## 連邦情報処理標準規格

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

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

FIPS モードではクライアントによる証明書の管理がより厳密になります。FIPS モードでは、サービスの証明書が期限切れになり、ログイン情報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。

### Windows 版 Cisco Jabber の FIPS の有効化

Windows 版 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 1: Windows 版 Cisco Jabber の FIPS 設定

プラットフォームモード	ブートストラップ設定	Cisco Jabber クライアントの設定
FIPS を使う (DHCP Enabled)	FIPS を使う (DHCP Enabled)	FIPS 対応：ブートストラップの設定。
FIPS を使う (DHCP Enabled)	RFC2833が無効(FIPS Disabled)	FIPS 非対応：ブートストラップの設定。
FIPS を使う (DHCP Enabled)	設定なし	FIPS 対応：プラットフォームの設定。
RFC2833が無効(FIPS Disabled)	FIPS を使う (DHCP Enabled)	FIPS 対応：ブートストラップの設定。
RFC2833が無効(FIPS Disabled)	RFC2833が無効(FIPS Disabled)	FIPS 非対応：ブートストラップの設定。
RFC2833が無効(FIPS Disabled)	設定なし	FIPS 非対応：プラットフォームの設定。



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

### Cisco Jabber for Mobile Clients 用の FIPS の有効化

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



**重要**

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

## Common Criteria

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

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

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

共通基準モードで Jabber が実行されるように設定する方法の詳細については、『Cisco Jabber 12.5 のオンプレミス導入ガイド』に Cisco Jabber アプリケーションを導入する方法を参照してください。

## Secure LDAP

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

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

## 認証済み UDS 連絡先の検索

Cisco Unified Communications Manager での UDS 連絡先検索のための認証を有効にします。Cisco Jabber は連絡先検索のための UDS 認証のログイン情報を提供します。

## 証明書

### 証明書の検証

#### 証明書検証プロセス

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

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

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

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

#### 署名証明書

証明書は、認証局 (CA) で署名することも、自己署名することもできます。

- CA 署名証明書 (推奨) —ユーザが自分自身で証明書をデバイスにインストールしているため、プロンプトが表示されません。CA 署名証明書はプライベート CA またはパブリック CA で署名できます。パブリック CA で署名された証明書の多くは証明書ストアまたはデバイスのキーチェーンに保存されます。Android 7.0 以降の devices、CA 署名付き証明書のみを認識します。

- 自己署名証明書：証明書は、証明書を提示しているサービスによって署名され、ユーザは必ずその証明書を受け入れるか拒否するかを尋ねられます。

### 証明書検証オプション

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

- オンプレミス展開とクラウドベース展開のどちらかに証明書を展開しようとしているか。
- 証明書の署名に使用している方法。
- CA 署名証明書を展開している場合は、パブリック CA とプライベート CA のどちらを使用するか。
- どのサービスの証明書を取得する必要があるか。

## オンプレミス サーバに必要な証明書

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

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

### 特記事項

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

クラスタ内の各ノードの証明書に署名する必要があります。

- クライアントと Cisco Unified Communications Manager 間の SIP シグナリングを確立するには、Certification Authority Proxy Function (CAPF) 登録を使用する必要があります。

## 証明書署名要求の形式と要件

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

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

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

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

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

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

## 失効サーバ

失効サーバにアクセスできない場合、Cisco Jabber は Cisco Unified Communications Manager サーバに接続できません。また、認証局 (CA) が証明書を取り消した場合、Cisco Jabber 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。

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

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

- **[CRL Distribution Point]** (CDP) フィールドに、失効サーバ上の認証失効リスト (CRL) への HTTP URL が含まれていることを確認します。

- **[Authority Information Access]** (AIA) フィールドに、オンライン証明書ステータス プロトコル (OCSP) サーバの HTTP URL が含まれていることを確認します。

## 証明書のサーバ識別情報

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

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



- (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、クライアントは、信頼できるポートとサーバを識別できないため、ユーザにとって良い結果をもたらしません。

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

## マルチサーバ SAN の証明書

マルチサーバ SAN を使用している場合は、クラスタと tomcat 証明書ごとに一度ずつとクラスタと XMPP 証明書ごとに一度ずつサービスに証明書をアップロードする必要があります。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

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

- CAS
- WAPI



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

Cisco Jabber は、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

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

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

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

Cisco Jabberは、マルチテナントのホステッドコラボレーションソリューションでのモバイルおよび Remote Access (MRA) の導入で、SNI をサポートしています。

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

マルチテナント展開の詳細については、ドメイン証明書を使用したエンドポイントサービスの検出とドメイン証明を使用しない *Jabber* サービスの検出（『[Cisco Hosted Collaboration Solution](#)』、リリース 11.5 マルチテナント Expressway の構成ガイド）を参照してください。

## ウイルス対策の除外

アンチウイルスソフトウェアを展開する場合は、ウイルス対策の除外一覧に次のフォルダの場所を含めます。

- C:\Users\\AppData\Local\Cisco\Unified Communications\Jabber
- C:\Users\\AppData\Roaming\Cisco\Unified Communications\Jabber
- C:\ProgramData\Cisco Systems\Cisco Jabber





## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。