セキュリティおよび証明書

暗号化

ファイル転送および画面キャプチャのコンプライアンスおよびポリシー管理

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

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

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

インスタント メッセージの暗号化

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

オンプレミス暗号化

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

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

サーバとクライアントのネゴシエーション

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

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

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

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

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

XMPP 暗号化

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

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

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

インスタント メッセージのロギング

規制ガイドラインへの準拠のために、インスタント メッセージをログに記録してアーカイブできます。インスタント メッセージをログに記録するには、外部データベースを設定するか、またはサードパーティ製のコンプライアンス サーバと統合します。Cisco Unified Communications Manager

IM and Presence サービスは、外部データベースまたはサードパーティ製コンプライアンス サーバに記録されたインスタント メッセージを暗号化しません。必要に応じて、外部データベースまたはサードパーティ製コンプライアンス サーバを設定し、記録したインスタント メッセージを保護する必要があります。

コンプライアンスの詳細については、次を参照してください。

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

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

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

クラウドベースの暗号化

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

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

サーバとクライアントのネゴシエーション

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

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

XMPP 暗号化

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

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

インスタント メッセージのロギング

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

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

AES などの対称キー アルゴリズムや RSA などの公開キー アルゴリズムを含め、暗号化レベルや暗号化アルゴリズムの詳細については、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 トラフィックは安全です。必要に応じて、Cisco WebEx 管理ツールでポリシーを指定して、クライアント間のインスタント メッセージング トラフィックを保護できます。

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

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

次の表は、これらのポリシーを使用して設定できる組み合わせを示しています。

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

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

（注） Cisco Jabber では、グループ チャットによるクライアント間の暗号化をサポートしていません。Cisco Jabber は、ポイントツーポイント チャットのみに関して、クライアント間の暗号化を使用します。

暗号化および Cisco WebEx ポリシーの詳細については、Cisco WebEx のマニュアルの「*About Encryption Levels*」の項を参照してください。

暗号化アイコン

暗号化レベルを表示するには、クライアントが表示するアイコンを確認します。

サーバの暗号化対応クライアント用のロック アイコン

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

クライアント間暗号化の鍵アイコン

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

ローカルのチャット履歴

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

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

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

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

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

音声およびビデオの暗号化

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

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

連邦情報処理標準規格

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

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

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

Cisco Jabber for Windows 用の FIPS の有効化

（注） FIPS モードを有効にすると、画面共有機能はサポートされません。

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

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

表 *1*：*Cisco Jabber for Windows* の *FIPS* 設定

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

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 非対応	設定なし	FIPS非対応：プラットフォームの設定。

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

Cisco Jabber for Mobile Clients 用の FIPS の有効化

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

重要

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

Secure LDAP

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

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

認証済み UDS 連絡先の検索

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

証明書

証明書の検証

証明書検証プロセス

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

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

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

Cisco JabberはCisco Unified Communications Managerサーバ上の2つのサービスに対して認証を行います。サービス名はCisco TomcatとExtensible Messaging and Presence Protocol（XMPP）です。サービスごとに証明書署名要求（CSR）を生成する必要があります。一部のパブリック認証局は、完全修飾ドメイン名（FQDN）ごとに1つのCSRしか承認しません。そのため、各サービスのCSRを別々のパブリック認証局に送信しなければならない場合があります。

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

署名証明書

証明書は、認証局（CA）で署名することも、自己署名することもできます。

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

（注） 自己署名証明書を使用しないことをお勧めします。

証明書検証オプション

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

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

オンプレミス サーバに必要な証明書

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

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

特記事項

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

  クラスタ内の各ノードの証明書に署名する必要があります。

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

証明書署名要求の形式と要件

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

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

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

CSR の問題を回避するために、CSR を送信するパブリック CA からの形式の要件を確認する必要があります。次に、サーバを構成する際に、入力する情報がパブリック CA が要求する形式に適合していることを保証する必要があります。

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

たとえば、1 つの Cisco Unified Communications Manager IM and Presence Service ノードの HTTP 証明書と XMPP 証明書に署名するには、各 CSR を個別のパブリック CA に送信する必要があります。

失効サーバ

証明書を検証するには、失効情報を提供できる到達可能なサーバの [CDP] または [AIA] フィールドに HTTP URL が証明書に含まれている必要があります。認証局（CA）によって証明書が取り消された場合、クライアントはユーザがそのサーバに接続することを許可しません。

ユーザには次の結果が通知されません。

- 証明書に失効情報が含まれない。
- 失効サーバにアクセスできない。

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

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

証明書のサーバ識別情報

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

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

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

ID フィールド

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

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

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

ID の不一致の防止

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

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

マルチサーバ SAN の証明書

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

クラウド展開の証明書検証

Cisco WebEx Messenger と Cisco WebEx Meeting Center は、デフォルトで次の証明書をクライアントに提示します。

- CAS
- WAPI

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

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

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

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

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