証明書検証の設定

- オンプレミス展開用の証明書の設定 （1 ページ）
- クライアントへの CA 証明書の展開 （2 ページ）

オンプレミス展開用の証明書の設定

証明書は、Jabber クライアントが接続するサービスごとに必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence Serviceを使用している場合は、該当する HTTP（tomcat）証明書と XMPP 証明書をダウンロードします。	詳細については、『Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager』の「*Security Configuration on IM and Presence Service*」の章を参照してください。
ステップ 2	Cisco Unified Communications Manager と Cisco Unity Connection 用の HTTPS（tomcat）証明書をダウンロードします。	詳細については、ここで『*Cisco Unified Communications Manager Security Guide*』と『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。
ステップ 3	Cisco Webex Meetings サーバ用の HTTP（tomcat）をダウンロードします。	詳細については、ここで『*Cisco Cisco Webex Meetings Server Administration Guide*』を参照してください。
ステップ 4	リモート アクセスを設定する場合は、Cisco VCS Expressway と Cisco Expressway-E のサーバ証明書をダウンロードします。このサーバ証明書は、HTTP と XMPP の両方に使用されます。	詳細については、『Configuring Certificates on Cisco VCS Expressway』を参照してください。

	コマンドまたはアクション	目的
ステップ 5	証明書署名要求（CSR）を生成します。	
ステップ 6	サービスに証明書をアップロードします。	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。
ステップ 7	クライアントへの CA 証明書の展開 （2 ページ)	証明書を承認または却下するためのプロンプトを表示せずに証明書の検証が行われることを保証するには、クライアントのローカル証明書ストアに証明書を展開します。

クライアントへの CA 証明書の展開

証明書を承認または却下するためのプロンプトを表示せずに証明書検証が実施されることを保証するには、エンドポイント クライアントのローカル証明書ストアに証明書を展開します。

既存のパブリック CA を使用している場合は、CA 証明書がクライアント証明書ストアまたはキーチェーン上に存在している可能性があります。その場合は、CA 証明書をクライアントに展開する必要はありません。

CA 証明書がクライアント証明書ストアまたはキーチェーン上に存在しない場合は、CA 証明書をクライアントに展開します。

展開規模	推奨内容
ローカル マシンが多数の場合	グループ ポリシーや証明書展開管理アプリケーションなどの証明書展開ツールを使用する。
ローカル マシンが少数の場合	手動で CA 証明書を展開する。

Windows 版 Cisco Jabber クライアントへの CA 証明書の手動展開

手順

ステップ 1 Windows 版 Cisco Jabber クライアント マシンで CA 証明書を使用できるようにします。

ステップ 2 Windows マシンで、証明書ファイルを開きます。

ステップ 3 証明書をインストールしてから、[次へ（Next）] をクリックします。

ステップ 4 [証明書をすべて次のストアに配置する（Place all certificates in the following store）] を選択してから、[参照（Browse）] を選択します。

ステップ 5 [信頼されたルート証明機関（Trusted Root Certification Authorities）] ストアを選択します。
ウィザードを終了すると、正常な証明書インポートを確認するためのメッセージが表示されます。

次のタスク

Windows Certificate Manager ツールを起動することによって、証明書が正しい証明書ストアにインストールされていることを確認します。**[信頼されたルート証明機関（Trusted Root Certification Authorites）] > [証明書（Certificates）]** を参照します。CA ルート証明書が証明書ストアに一覧表示されます。

Mac 版 Cisco Jabber クライアントへの CA 証明書の手動展開

手順

ステップ 1 Mac 版 Cisco Jabber クライアント マシンで CA 証明書を使用できるようにします。

ステップ 2 Mac マシンで、証明書ファイルを開きます。

ステップ 3 現在のユーザのみのログイン キーチェーンに追加して、[追加（Add）] を選択します。

次のタスク

キーチェーン アクセス ツールを開いて、[証明書（Certificates）] を選択することによって、証明書が正しいキーチェーンにインストールされていることを確認します。キーチェーン内の CA ルート証明書が一覧表示されます。

モバイル クライアントへの CA 証明書の手動展開

CA 証明書を iOS クライアントに展開するには、証明書展開管理アプリケーションが必要です。CA 証明書をユーザに電子メールで送信することも、ユーザがアクセス可能な Web サーバ上で証明書を公開することもできます。ユーザは証明書展開管理ツールを使用して証明書をダウンロードしてインストールできます。

ただし、Cisco Jabber for Android には証明書管理ツールが付属していないため、次の手順を実行する必要があります。

手順

ステップ 1 CA 証明書をデバイスにダウンロードします。

ステップ 2 デバイスで **[設定（Settings）] > [セキュリティ（Security）] > [デバイスストレージからインストール（Install from device storage）]** の順にタップして、画面上の指示に従います。