証明書の検証設定

Cisco Jabber では、証明書の検証を使用して、サーバとのセキュア接続を確立します。

セキュア接続を確立しようとする場合、サーバは Cisco Jabber に証明書を提示します。

Cisco Jabber では、Microsoft Windows 証明書ストアの証明書に対して証明書を検証します。

クライアントが証明書を検証できない場合、ユーザに証明書を受け入れるかどうか確認するよう指示されます。

オンプレミス サーバ

オンプレミス サーバがどの証明書をクライアントに提示するかを確認し、また、署名された証明書の取得作業も確認します。

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	HTTP（Tomcat） XMPP
Cisco Unified Communications Manager	HTTP（Tomcat）
Cisco Unity Connection	HTTP（Tomcat）
Cisco WebEx Meetings Server	HTTP（Tomcat）

特記事項

- 証明書の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。
- クラスタ、サブスクライバおよびパブリッシャの各ノードは、Tomcat サービスを実行し、HTTP の証明書でクライアントを提示できます。

  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。

認証局により署名された証明書の取得

シスコは、次の認証局（CA）のいずれかにより署名されたサーバ証明書を使用することを推奨します。

パブリック CA

サードパーティ企業が、サーバの識別情報を確認し、信頼できる証明書を発行します。

プライベート CA

自身でローカルの CA を作成および管理し、信頼できる証明書を発行します。

署名プロセスは、各サーバごとに異なり、サーバのバージョン間でも異なります。 各サーバのすべてのバージョンに関する詳細な手順については、このマニュアルの範囲外になります。 CA により署名された証明書を取得する方法の詳細な指示については、該当するサーバのマニュアルを参照してください。 ただし、手順の概要を次に示します。

手順

ステップ 1 クライアントに証明書を提示できる各サーバで証明書署名要求（CSR）を作成します。

ステップ 2 CA に各 CSR を送信します。

ステップ 3 CA が各サーバに発行する証明書をアップロードします。

証明書署名要求の形式と要件

パブリック CA は、通常 CSR に特定の形式に確認するよう要求します。 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 Cisco Unified Communications Manager IM and Presence 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る場合があります。

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。

（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、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。

クライアントへの XMPP ドメインの提供

クライアントは、FQDN ではなく XMPP ドメインを使用して、XMPP 証明書を識別します。 XMPP の証明書は ID フィールドに XMPP ドメインを含める必要があります。

クライアントがプレゼンス サーバに接続しようとすると、プレゼンス サーバはクライアントに XMPP ドメインを提供します。 その際に、クライアントは XMPP 証明書に対するプレゼンス サーバの識別情報を検証します。

プレゼンス サーバがクライアントに XMPP ドメインを提供することを保証するため、次の手順を実行します。

手順

ステップ 1 次のとおり、プレゼンス サーバの管理インターフェイスを開きます。

Cisco Unified Communications Manager IM and Presence

[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] インターフェイスを開きます。

Cisco Unified Presence

[Cisco Unified Presence の管理（Cisco Unified Presence Administration）] インターフェイスを開きます。

ステップ 2 [システム（System）] > [セキュリティ（Security）] > [設定（Settings）] を選択します。

ステップ 3 [XMPP 証明書の設定（XMPP Certificate Settings）] セクションを検索します。

ステップ 4 [XMPP サーバ間証明書のサブジェクト代替名のドメイン ネーム（Domain name for XMPP Server-to-Server Certificate Subject Alternative Name）] フィールドにプレゼンス サーバのドメインを指定します。

ステップ 5 [MPP サーバ証明書のサブジェクト代替名のドメイン ネームを使用（Use Domain Name for XMPP Certificate Subject Alternative Name）] チェックボックスを選択します。

ステップ 6 [保存（Save）] を選択します。

クライアント コンピュータのルート証明書のインポート

サーバ証明書はクライアント コンピュータの信頼ストアに存在する関連のルート証明書が必要です。 Cisco Jabberは、サーバが信頼ストアのルート証明書に対して提示する証明書を検証します。

パブリック CA によって署名されたサーバ証明書を取得する場合、パブリック CA はすでにクライアントコンピュータの信頼ストアで提示されるルート証明書を持っている必要があります。この場合、クライアント コンピュータのルート証明書をインポートする必要はありません。

次の場合、Microsoft Windows 証明書ストアにルート証明書をインポートする必要があります。

- 証明書がプライベート CA などの信頼ストアではない CA によって署名されます。

  [信頼されたルート証明機関（Trusted Root Certification Authorities）] ストアにプライベート CA 証明書をインポートします。

- 証明書には自己署名します。

  [エンタープライズ信頼（Enterprise Trust）] ストアに自己署名した証明書をインポートします。

重要 ルート証明書が信頼ストアにない場合、Cisco Jabberは環境内の各サーバからの証明書を受け入れるようユーザに指示します。

クライアントがユーザ証明書を受け入れるよう指示すると、ユーザは次のことを実行することができます。

証明書の受け入れ

クライアントは、[エンタープライズ信頼（Enterprise Trust）] ストアに証明書を保存します。

証明書の拒否

クライアントは、次のことを実行しません。

- 証明書を保存する。
- サーバに接続する。
- エラー通知を表示する。

ユーザがクライアントを再起動した場合、再度証明書を受け入れるように指示します。

次のことを含め、Microsoft Windows 証明書ストアに証明書をインポートする適切な方式を使用できます。 証明書のインポートの詳細については、適切なMicrosoftマニュアルを参照してください。

- 個別に証明書をインポートするために、[証明書のインポート ウィザード（Certificate Import Wizard）] を使用します。
- Microsoft Windows Server で `CertMgr.exe` コマンドライン ツールを持つユーザに証明書を展開します。

（注） このオプションでは、Microsoft 管理コンソールの `CertMgr.msc` ではなく、Certificate Manager ツールの `CertMgr.exe` を使用する必要があります。

- Microsoft Windows Server でグループ ポリシー オブジェクト（GPO）でユーザに証明書を展開します。

クラウドベースのサーバ

Cisco WebEx Messenger および Cisco WebEx Meeting Center は、Cisco Jabber に対して次の証明書を提示します。

- `CAS`
- `WAPI`

重要 Cisco WebEx は、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 サービスのセキュアな接続を確立します。 ただし、クラウド サービスを使用する場合に、証明書を発行したり、署名したりする必要はありません。

プロファイル写真の URL の更新

クラウド ベースの展開では、ユーザを追加またはインポートする際に、Cisco WebEx により、プロファイル写真に一意の URL が割り当てられます。 Cisco Jabber により連絡先情報が解決される場合、写真がホスティングされている URL の Cisco WebEx からプロファイル写真が取得されます。

プロファイル写真の URL は、HTTP セキュア（`https://server_name/`）を使用して、クライアントに証明書を提示します。 URL のサーバ名が次の場合：

Cisco WebEx ドメインを含む完全修飾ドメイン名（FQDN）

クライアントは、Cisco WebEx 証明書に対してプロファイル写真をホスティングしている Web サーバを検証します。

IP アドレス

クライアントは、Cisco WebEx 証明書に対してプロファイル写真をホスティングしている Web サーバを検証しません。

この場合、プロファイル写真の URL の IP アドレスで連絡先をルックアップする場合は常に、証明書を受け入れるようクライアントがユーザに指示します。

重要 シスコは、サーバ名としての IP アドレスを含むすべてのプロファイル写真の URL を更新することを推奨します。 クライアントが証明書を受け入れるようにユーザに指示しないことを保証するために、Cisco WebEx ドメインを含む FQDN と IP アドレスを置き換える必要があります。

プロファイル写真の URL を更新するには、次の手順を実行します。 詳細については、該当する Cisco WebEx マニュアルを参照してください。

手順

ステップ 1 Cisco WebEx 管理ツール を使用して、CSV ファイルのユーザ連絡先データを CSV ファイル形式でエクスポートします。

ステップ 2 必要に応じて、userProfilePhotoURL フィールドのCisco WebEx ドメインと IP アドレスを置き換えます。

ステップ 3 CSV ファイルを保存します。

ステップ 4 Cisco WebEx 管理ツール を使用して、CSV ファイルをインポートします。