IM and Presence のセキュリティ証明書の設定

この章は、IM and Presence とMicrosoft Lync との間のセキュアな接続が必要な場合のみ適用されます。

この章では、スタンドアロンの CA を使用したセキュリティ証明書の設定について説明します。エンタープライズ CA を使用する場合は、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』の、エンタープライズ CA を使用した証明書交換手順の例を参照してください。

（注） SIP プロキシ証明書（所有および信頼）は、X.509 バージョン 3 に準拠する必要があります。

スタンドアロン ルート認証局（CA）の設定

次の手順を実行し、スタンドアロン ルート CA を設定します。

手順

ステップ 1 ドメイン管理者権限で CA サーバにサイン インします。

ステップ 2 Windows Server 2003 CD を挿入します。

ステップ 3 [スタート（Start）]>[設定（Settings）]>[コントロール パネル（Control Panel）] を選択し、[プログラムの追加と削除（Add or Remove Programs）] をダブルクリックします。

ステップ 4 [Windows コンポーネントの追加と削除（Add/Remove Windows Components）] を選択します。

ステップ 5 [アプリケーション サーバ（Application Server）] を選択し、[Internet Information Services（IIS）] を選択します。

ステップ 6 インストール手順を完了します。

ステップ 7 [Windows コンポーネントの追加と削除（Add/Remove Windows Components）] を選択します。

ステップ 8 [証明書サービス（Certificate Services] を選択し、[次へ（Next）] を選択します。

ステップ 9 [スタンドアロンのルート CA（Standalone root CA）] を選択し、[次へ（Next）] を選択します。

ステップ 10 CA ルートの名前を入力します。

（注） この名前は、フォレストルートの CA ルートをわかりやすくした名前にすることができます。

ステップ 11 時間を、この証明書に必要な年数に変更し、[次へ（Next）] を選択してインストールを開始します。

ステップ 12 証明書データベースおよび証明書データベース ファイルの場所を選択します。

ステップ 13 [次へ（Next）] を選択します。

ステップ 14 IIS を停止するように求められたら、[はい（Yes）] を選択します。

ステップ 15 Active Server Pages に関するメッセージが表示されたら [はい（Yes）] を選択し、[終了（Finish）] を選択します。

次の作業

CA サーバからルート証明書をダウンロード, （2 ページ）

CA サーバからルート証明書をダウンロード

次の手順を実行し、CA サーバからルート証明書をダウンロードします。

はじめる前に

スタンドアロン ルート Certificate Authority（CA; 認証局）を設定します。

手順

ステップ 1 CA サーバにサイン インし、Web ブラウザを開きます。

ステップ 2 URL `http://<ca_server_IP_address>/certsrv` を開きます。

ステップ 3 [CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain, or CRL）] を選択します。

ステップ 4 [エンコード方式（Encoding Method）] で [Base 64] を選択します。

ステップ 5 [CA 証明書のダウンロード（Download CA Certificate）] を選択します。

ステップ 6 証明書ファイル certnew.cer をローカル ディスクに保存します。

重要 ルート証明書のサブジェクトの Common Name（CN; 共通名）がわからない場合は、外部の証明書管理ツールを使用して探すことができます。 Windows オペレーティング システムでは、拡張子が .cer の証明書ファイルを右クリックして、証明書のプロパティを開くことができます。

次の作業

ルート証明書を IM and Presence にアップロード, （3 ページ）

関連トピック

スタンドアロン ルート認証局（CA）の設定, （1 ページ）

ルート証明書を IM and Presence にアップロード

次の手順を実行し、ルート証明書をIM and Presence にアップロードします。

はじめる前に

CA サーバからルート証明書をダウンロードします。

手順

ステップ 1 IM and Presence の管理に使用するローカル コンピュータに certnew.cer ファイルをコピーします。

ステップ 2 [Cisco Unified オペレーティングシステムの管理（Cisco Unified Operating System Administration）] > [セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 3 [証明書のアップロード（Upload Certificate）] を選択します。

ステップ 4 [証明書の名前（Certificate Name）] メニューから [cup-trust] を選択します。

（注） [ルート名（Root Name）] フィールドは空白のままにしておきます。

ステップ 5 [参照（Browse）] を選択し、自分のコンピュータ上で certnew.cer ファイルのある場所に移動します。

（注） 証明書ファイルの拡張子を .pem に変更することが必要になる場合があります。

ステップ 6 [ファイルのアップロード（Upload File）] を選択します。

ヒント [証明書の管理（Certificate Management）] の検索画面を使用して、cup-trust にアップロードした新規 CA 証明書ファイル名を書き留めます。 この証明書ファイル名（拡張子の .pem または .der 以外）が、CA 署名済み SIP プロキシ証明書をアップロードするときにルート CA のフィールドに入力する値となります。

次の作業

IM and Presence の証明書署名要求の生成, （4 ページ）

関連トピック

CA サーバからルート証明書をダウンロード, （2 ページ）
署名済み証明書を IM and Presence にアップロード, （7 ページ）

IM and Presence の証明書署名要求の生成

次の手順を実行し、IM and Presence の証明書署名要求（CSR）を生成します。

はじめる前に

ルート証明書を IM and Presence にアップロードします。

手順

ステップ 1 [Cisco Unified オペレーティングシステムの管理（Cisco Unified Operating System Administration）] > [セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 2 [CSR の作成（Generate CSR）] を選択します。

ステップ 3 [証明書の名前（Certificate Name）] メニューから [cup] を選択します。

ステップ 4 [CSR の作成（Generate CSR）] を選択します。

次の作業

IM and Presence からの CSR のダウンロード, （5 ページ）

関連トピック

ルート証明書を IM and Presence にアップロード, （3 ページ）

IM and Presence からの CSR のダウンロード

次の手順を実行し、IM and Presence から CSR をダウンロードします。

はじめる前に

IM and Presence の CSR を生成します。

手順

ステップ 1 [Cisco Unified オペレーティングシステムの管理（Cisco Unified Operating System Administration）] > [セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 2 [CSR のダウンロード（Download CSR）] を選択します。

ステップ 3 [証明書の名前（Certificate Name）] メニューから [cup] を選択します。

ステップ 4 [CSR のダウンロード（Download CSR）] を選択します。

ステップ 5 [保存（Save）] を選択して、cup.csr ファイルをローカル コンピュータに保存します。

次の作業

CA サーバで証明書署名要求を送信, （5 ページ）

関連トピック

IM and Presence の証明書署名要求の生成, （4 ページ）

CA サーバで証明書署名要求を送信

次の手順を実行し、CA サーバで CSR を送信します。

はじめる前に

IM and Presence から CSR をダウンロードします。

手順

ステップ 1 証明書要求ファイル cup.csr を CA サーバにコピーします。

ステップ 2 URL `http://local-server/certserv` または `http://127.0.0.1/certsrv` を開きます。

ステップ 3 [証明書を要求する（Request a certificate）] を選択し、[証明書の要求の詳細設定（Advanced certificate request）] を選択します。

ステップ 4 [Base 64 エンコード CMC または PKCS #10 ファイルを使用して証明書の要求を送信するか、または Base 64 エンコード PKCS #7 ファイルを使用して更新の要求を送信する。（Submit a certificate

request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.）] を選択します。

ステップ 5 メモ帳などのテキスト エディタを使用して、生成した cup 自己証明書を開きます。

ステップ 6 次の行から、
-----BEGIN CERTIFICATE REQUEST

次の行までの情報をすべてコピーします。

END CERTIFICATE REQUEST-----

ステップ 7 証明書要求の内容を [証明書要求（Certificate Request）] テキスト ボックスに貼り付けます。

ステップ 8 [送信（Submit）] を選択します。
要求 ID 番号が表示されます。

ステップ 9 [管理ツール（Administrative Tools）] で [証明機関（Certificate Authority）] を開きます。
[認証局（Certificate Authority）] ウィンドウの [保留中の要求（Pending Requests）] の下に、送信したばかりの要求が表示されます。

ステップ 10 証明書要求を右クリックし、[すべてのタスク（All Tasks）] > [発行（Issue）] を選択します。

ステップ 11 [発行済み証明書（Issued certificates）] を選択し、証明書が発行されていることを確認します。

次の作業

CA サーバから署名済み証明書をダウンロード, （6 ページ）

関連トピック

IM and Presence からの CSR のダウンロード, （5 ページ）

CA サーバから署名済み証明書をダウンロード

次の手順を実行し、CA サーバから署名済み証明書をダウンロードします。

はじめる前に

CA サーバで CSR を送信します。

手順

ステップ 1 CA が実行されている Windows サーバで `http://<local_server>/certsrv` を開きます。
ステップ 2 [保留中の証明書の要求の状態（View the status of a pending certificate request）] を選択します。
ステップ 3 直前に送信された要求を表示するオプションを選択します。
ステップ 4 [Base 64 エンコード（Base 64 encoded）] を選択します。
ステップ 5 [証明書のダウンロード（Download certificate）] を選択します。
ステップ 6 署名済み証明書をローカル ディスクに保存します。
ステップ 7 証明書 cup.pem の名前を変更します。
ステップ 8 cup.pem ファイルをローカル コンピュータにコピーします。

次の作業

署名済み証明書を IM and Presence にアップロード, （7 ページ）

関連トピック

CA サーバで証明書署名要求を送信, （5 ページ）

署名済み証明書を IM and Presence にアップロード

次の手順を実行し、署名済み証明書をIM and Presence にアップロードします。

はじめる前に

CA サーバから署名済み証明書をダウンロードします。

手順

ステップ 1 [Cisco Unified オペレーティングシステムの管理（Cisco Unified Operating System Administration）] > [セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。
ステップ 2 [証明書のアップロード（Upload Certificate）] を選択します。
ステップ 3 [証明書の名前（Certificate Name）] メニューから [cup] を選択します。
ステップ 4 ルート証明書の名前を指定します。 ルート証明書の名前には、拡張子 .pem または .der が含まれている必要があります。
ステップ 5 [参照（Browse）] を選択し、自分のコンピュータ上で署名済みの cup.pem 証明書のある場所に移動します。
ステップ 6 [ファイルのアップロード（Upload File）] を選択します。

次の作業

Lync Remote Call Control プラグインのインストール

関連トピック

CA サーバから署名済み証明書をダウンロード, （6 ページ）