IM and Presence と Microsoft Lync とのセキュリティ設定

この章は、IM and Presence サービスと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。

Microsoft Lync のセキュリティ証明書の設定

CA 証明書チェーンをダウンロード

次の手順を実行し、CA 証明書チェーンをダウンロードします。

手順

ステップ 1 [スタート（Start）] > [実行（Run）] を選択します。

ステップ 2 `http://<発行 CA サーバの名前>/certsrv` と入力し、[OK] を選択します。

ステップ 3 [タスクの選択（Select a task）] から、[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 [CA 証明書チェーンのダウンロード（Download CA certificate chain）] を選択します。

ステップ 5 [ファイルのダウンロード（File Download）] ダイアログボックスで [保存（Save）] を選択します。

ステップ 6 サーバのハード ディスク ドライブにファイルを保存します。

（注） 証明書ファイルの拡張子は .p7b です。 この .p7b ファイルを開くと、チェーンに次の 2 つの証明書が含まれるようになります。

- スタンドアロンのルート CA 証明書の名前
- スタンドアロンの下位 CA 証明書の名前（ある場合）

次の作業

CA 証明書チェーンをインストール, （2 ページ）

CA 証明書チェーンをインストール

次の手順を実行し、CA 証明書チェーンをインストールします。

はじめる前に

CA 証明書チェーンをダウンロードします。

手順

ステップ 1 [スタート（Start）] > [実行（Run）] を選択します。
ステップ 2 mmc と入力し、[OK] をクリックします。
ステップ 3 [ファイル（File）] > [スナップインの追加と削除（Add/Remove Snap-in）] を選択します。
ステップ 4 [スナップインの追加と削除（Add/Remove Snap-in）] ダイアログボックスで [追加（Add）] を選択します。
ステップ 5 [利用できるスタンドアロン スナップイン（Available Standalone Snap-ins）] のリストで [証明書（Certificates）] を選択し、続いて [追加（Add）] を選択します。
ステップ 6 [コンピュータ アカウント（Computer account）] を選択し、[次へ（Next）] をクリックします。
ステップ 7 [コンピュータの選択（Select Computer）] ダイアログ ボックスで、自分のコンピュータ（このコンソールを実行中のコンピュータ）が選択されていることを確認します。
ステップ 8 [終了（Finish）] を選択し、[閉じる（Close）] を選択し、最後に [OK] を選択します。
ステップ 9 [証明書（Certificates）] コンソールの左ペインで、[証明書（ローカル コンピュータ）（Certificates (Local Computer)）] を展開します。
ステップ 10 [信頼されたルート証明機関（Trusted Root Certification Authorities）] を展開し、[証明書（Certificates）] を右クリックします。
ステップ 11 [すべてのタスク（All Tasks）] をポイントして、[インポート（Import）] を選択します。
ステップ 12 インポート ウィザードで [次へ（Next）] を選択します。
ステップ 13 [参照（Browse）] を選択し、自分のコンピュータ上で証明書チェーンがある場所に移動します。
ステップ 14 [開く（Open）] を選択し、[次へ（Next）] を選択します。
ステップ 15 [証明書をすべて次のストアに配置する（Place all certificates in the following store）] をデフォルト値のままオンにしておきます。
ステップ 16 [証明書ストア（Certificate store）] の下に [信頼されたルート証明機関（Trusted Root Certification Authorities）] が表示されていることを確認します。
ステップ 17 [次へ（Next）] を選択し、[終了（Finish）] を選択します。

次の作業

CA サーバで証明書要求を送信, （3 ページ）

関連トピック

CA 証明書チェーンをダウンロード, （1 ページ）

CA サーバで証明書要求を送信

次の手順を実行し、CA サーバで証明書要求を送信します。

はじめる前に

CA 証明書チェーンをインストールします。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync Server 2010] > [Lync Server 管理シェル（Lync Server Management Shell）] を選択します。

ステップ 2 次のコマンドを実行し、Microsoft Lync Server の証明書要求を送信します。

```
Request-CsCertificate -New -Type Default -DomainName <FQDN of Lync Server> -Output c:\cert.csr
-ClientEku $true
```

ステップ 3 Microsoft Lync Server から URL `http://<発行 CA サーバの名前>/certsrv` を入力します。

ステップ 4 [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 5 [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 6 ステップ 2, （4 ページ） のファイル cert.csr を開き、ファイル内のすべての情報をクリップボードにコピーします。

ステップ 7 ファイル cert.csr の情報を認証権限サーバの [保存された要求（Saved Request）] ボックスに貼り付け、[送信（Submit）] を選択します。

次の作業

証明書を承認し、インストール, （4 ページ）

関連トピック

CA 証明書チェーンをインストール, （2 ページ）

証明書を承認し、インストール

次の手順を実行し、証明書の承認およびインポートを行います。

はじめる前に

CA サーバで証明書要求を送信します。

手順

ステップ 1 認証権限サーバで、[管理ツール（Administrative Tools）]>[証明機関（Certificate Authority）] を選択します。

ステップ 2 [保留中の要求（Pending Requests）] を選択し、リスト内で新しい証明書を見つけます。

ステップ 3 新しい証明書を右クリックして、[すべてのタスク（All Tasks）]>[証明書の発行（Issue Certificate）] を選択します。

ステップ 4 Microsoft Lync Server から URL `http://<発行 CA サーバの名前>/certsrv` を入力します。

ステップ 5 [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 6 [Base 64 エンコード（Base 64 encoded）] を選択し、証明書を cer ファイル拡張子のファイルとして Microsoft Lync サーバのローカル ドライブにダウンロードします。

ステップ 7 証明書要求を作成した Microsoft Lync Server に、管理者グループのメンバーとしてサインインします。

ステップ 8 Lync Server 展開ウィザードを開始し、Lync Server システムの [インストール（Install）] または [更新（Update）] を選択します。

ステップ 9 [再実行（Run Again）] を選択します（手順 3：証明書の要求、インストール、または割り当てに加えて）。

ステップ 10 [利用可能な証明書タスク（Available Certificate Tasks）] ページで [インポート（Import）] を選択し、.p7b、.pfx または .cer ファイルから証明書をインポートします。

ステップ 11 [証明書のインポート（Import Certificate）] ページで、ステップ 6, （5 ページ）で証明機関から取得した証明書のフルパスとファイル名を入力します。 または、[参照（Browse）] を選択してファイルを指定し、選択することもできます。

次の作業

インポートされた証明書の割り当て, （5 ページ）

関連トピック

CA サーバで証明書要求を送信, （3 ページ）

インポートされた証明書の割り当て

次の手順を実行し、インポート済みの証明書を割り当てます。

はじめる前に

証明書を承認し、インストールします。

手順

ステップ 1 Microsoft Lync Server で、Lync Server 展開ウィザードを開始します。

ステップ 2 Lync Server システムの [インストール（Install）] または [更新（Update）] を選択します。

ステップ 3 手順 3：証明書の要求、インストール、または割り当ての [再実行（Run Again）] を選択します。

ステップ 4 [利用可能な証明書タスク（Available Certificate Tasks）] ページで、[既存の証明書の割り当て（Assign an existing certificate）] を選択します。

ステップ 5 [証明書の割り当て（Certificate Assignment）] ページで、[次へ（Next）] を選択します。

ステップ 6 [証明書の利用詳細設定（Advanced Certificate Usages）] ページから、すべてのチェックボックスをオンにして、証明書をすべての利用に割り当てます。

ステップ 7 [証明書ストア（Certificate Store）] ページから、要求およびインポートした証明書を選択します。

ステップ 8 [証明書の割り当ての概要（Certificate Assignment Summary）] ページで設定を確認し、[次へ（Next）] を選択して証明書を割り当てます。

ステップ 9 ウィザードの終了ページで、[終了（Finish）] を選択します。

ステップ 10 各サーバで証明書スナップインを開き、[証明書（ローカル コンピュータ）（Certificates (Local Computer)）]>[個人用（Personal）]>[証明書（Certificates）] を選択し、証明書が [詳細（Details）] ウィンドウに表示されていることを確認します。

次の作業

サーバとのクライアントの認証の証明書設定の確認, （6 ページ）

関連トピック

証明書を承認し、インストール, （4 ページ）

サーバとのクライアントの認証の証明書設定の確認

次の手順を実行し、サーバとクライアントの認証の証明書が正しく設定されていることを確認します。

手順

ステップ 1 Microsoft Lync Server で、Lync Server 展開ウィザードを開始します。

ステップ 2 Lync Server システムの [インストール（Install）] または [更新（Update）] を選択します。

ステップ 3 手順 3：証明書の要求、インストール、または割り当ての [再実行（Run Again）] を選択します。

ステップ 4 [証明書ウィザード（Certificate Wizard）] ウィンドウで、デフォルトの証明書を強調表示し、[表示（View）] を選択します。

ステップ 5 [証明書の表示（View Certificate）] ウィンドウで、[証明書の詳細を表示（View Certificate Details）] を選択します。

ステップ 6 [証明書（Certificate）] ダイアログボックスで、[詳細（Details）] タブを選択します。

ステップ 7 [表示（Show）] ドロップダウン リストで、[拡張機能のみ（Extensions Only）] を選択します。

ステップ 8 [拡張キー使用（Enhanced Key Usage）] を選択し、次の情報が表示されていることを確認します。サーバ認証（1.3.6.1.5.5.7.3.1）、クライアント認証（1.3.6.1.5.5.7.3.2）。

ステップ 9 [スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync Server 2010] > [Lync Server 管理シェル（Lync Server Management Shell）] を選択します。

ステップ 10 次のコマンドを実行し、Microsoft Lync Server からの証明書を表示します。`Get-CsCertificate`

ステップ 11 次のようなデフォルト証明書があることを確認します。

```
Issuer    : CN=ne001a-lynccaNotAfter
NotAfter          : 6/16/2012 2:18:20 PM
NotBefore         : 6/16/2011 2:08:20 PM
SerialNumber      : 152E466D00000000000C
Subject           : CN=pool1.rcdnlync.com
AlternativeNames : {sip.rcdnlync.com, ne011a-lyncent.rcdnlync.com, pool1.rcdnlync.com}
Thumbprint        : 84BED88F2BFBB463CB4CBC328DAA6FD3A5E0677B
Use               : Default
```

次の作業

Microsoft Lync の TLS ルートの設定, （7 ページ）

Microsoft Lync の TLS ルートの設定

次のアイテムを設定し、Microsoft Lync で IM and Presence の TLS ルートを設定します。

- スタティック ルート
- アプリケーション プール
- RCC アプリケーション

Microsoft Lync で、IM and Presence の TLS ルートを設定した後は、トポロジを確定し、フロントエンド サービスを再起動します。

スタティック ルートの設定

次の手順を実行し、スタティック ルートを設定します。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync Server 2010] > [Lync Server 管理シェル（Lync Server Management Shell）] を選択します。

ステップ 2 TCP ルートが存在する場合は、次のコマンドを実行して削除します。

```
Remove-CsStaticRoutingConfiguration -Identity Global
```

ステップ 3 次のコマンドを実行し、スタティック TLS ルートを作成します。

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination <FQDN CUP Server> -Port 5062 -MatchUri
*.rcdnlync.com -UseDefaultCertificate $true
```

ステップ 4 プロンプトで次のコマンドを実行し、スタティック ルートを Lync サーバに読み込みます。

```
Set-CsStaticRoutingConfiguration -Route @{Add=$tlsRoute}
```

ステップ 5 次のコマンドを実行し、新しいシステム設定を確認します。

```
Get-CsStaticRoutingConfiguration
```

次の表に、Lyncサーバに新しいスタティックルートを挿入する際に使用するパラメータを示します。

表 *1*：スタティック ルートのパラメータ

パラメータ	説明
$tlsRoute	変数の名前。 好きな名前をつけることができますが、$ で始まり、Set コマンドの参照に一致している必要があります。
New-CsStaticRoute	スタティック ルートから変数に設定する内部コマンド。
-TLSRoute	このパラメータはルートを TLS として設定します。
-Destination	IM and Presence サーバの FQDN。
-Port	IM and Presence サーバがリッスンするポート。 TLS の場合、ポートは 5062 です。
-MatchUri	この値はワイルドカードで、アスタリスク（*）に続いてドメインを表示します。 Lync のコントロール パネルで各ユーザに指定した Line サーバの URI と比較されます。 Lync Server のコントロール パネルでユーザを有効にするを参照してください。
-UseDefaultCertificate	スタティック ルートがデフォルトの証明書を使用するようにするため、この値は True に設定されています。

パラメータ	説明
-CsStaticRoutingConfiguration	パラメータ値をルーティング データベースに移動するための内部コマンド。
-Route	このパラメータは、変数のパラメータを取得し、スタティック ルートを追加します。

次の作業

アプリケーション プールの設定, （9 ページ）

アプリケーション プールの設定

次の手順を実行し、Lync サーバ（レジストラ）が参照するアプリケーション プールを設定します。 サイトの情報をこのプールへとリンクします。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync Server 2010] > [Lync Server 管理シェル（Lync Server Management Shell）] を選択します。

ステップ 2 次のコマンドを実行し、既存の TCP アプリケーション プールを削除します。

```
Remove-CsTrustedApplicationPool -Identity TrustedApplicationPool:<IP_Address_CUPserver>
```

ステップ 3 次のコマンドを実行し、アドレス プールを作成します。

```
New-CsTrustedApplicationPool -Identity <FQDN CUP Server> -Registrar <FQDN of Pool> -site 1
-ThrottleAsServer $true -TreatAsAuthenticated $true
```

ステップ 4 プロンプトで、[Y] を選択します。

ステップ 5 次のコマンドを実行し、新しいシステム設定を確認します。

```
Get-CsTrustedApplicationPool
```

次の表に、アプリケーション プールの設定の際に使用するパラメータを示します。

表 *2*：アプリケーション プールのパラメータ

パラメータ	説明
New-CsTrustedApplicationPool	アプリケーション プールを追加する内部コマンド。
-Identity	IM and Presence サーバの FQDN。
-Registrar	プールの参照名。 Lync サーバの FQDN とすることもできます。

パラメータ	説明
-Site	サイトを数値で表した値。 **ヒント** Get-CsSite 管理シェル コマンドを使用してサイトの ID を検索できます。
-TreatAsAuthenticated	このパラメータの値は常に `$True` に設定します。
-ThrottleAsServer	このパラメータの値は常に `$True` に設定します。

次の作業

RCC アプリケーションの設定, （10 ページ）

RCC アプリケーションの設定

次の手順を実行し、プールに RCC アプリケーションを追加します。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync Server 2010] > [Lync Server 管理シェル（Lync Server Management Shell）] を選択します。

ステップ 2 次のコマンドを実行し、既存の TCP アプリケーションを削除します。

```
Remove-CsTrustedApplication -Identity <IM and Presence サーバの FQDN>/urn:application:rcc
```

ステップ 3 次のコマンドを実行し、プールに RCC アプリケーションを追加します。

```
New-CsTrustedApplication -ApplicationID RCC -TrustedApplicationPoolFqdn <IM and Presence サーバの FQDN> -Port 5062
```

ステップ 4 プロンプトで、[Y] を選択します。

ステップ 5 次のコマンドを実行し、新しいシステム設定を確認します。

```
Get-CsTrustedApplication
```

次の表に、アプリケーション プールの設定の際に使用するパラメータを示します。

表 *3*：アプリケーション設定パラメータ

パラメータ	説明
New-CsTrustedApplication	RCC アプリケーションを追加する内部コマンド。
-ApplicationID	RCC などのアプリケーション名。
-TrustedApplicationPoolFQDN	IM and Presence サーバの FQDN。

パラメータ	説明
-Port	IM and Presence サーバの SIP TLS のリスニング ポート。 TLS の場合、ポートは 5062 です。

次の作業

Lync Server の設定の確定, （11 ページ）

Lync Server の設定の確定

ここでは、トポロジを確定し、フロントエンド サービスを再起動する方法を説明します。

手順

ステップ 1 Lync Server 管理シェルで次のコマンドを実行し、トポロジを有効にします。

```
Enable-CsTopology
```

ステップ 2 次のコマンドを実行し、トポロジを rcc.xml という XML ファイルに書き出し、ファイルを C ドライブに保存します。

```
Get-CsTopology -AsXml | Out-File C:\rcc.xml
```

（注） トポロジ情報を出力するファイルの名前と保存場所は自由に設定できます。

ステップ 3 rcc.xml ファイルを開きます。

ステップ 4 [クラスタ FQDN（Cluster Fqdn）] セクションで、IPAddress パラメータを「<0.0.0.0>」から IM and Presence サーバの IP アドレスに変更します。

ステップ 5 rcc.xml ファイルを保存します。

ステップ 6 Lync Server 管理シェルで次のコマンドを実行します。

```
Publish-CsTopology -FileName C:\rcc.xml
```

ステップ 7 次のコマンドを実行して、フロントエンド サービスを再起動します。

```
Restart-Service RtcSrv
```

次の作業

TLSv1 のための Microsoft Lync の設定, （12 ページ）

TLSv1 のための Microsoft Lync の設定

IM and Presence は TLSv1 のみをサポートしているため、Microsoft Lync が TLSv1 を使用するように設定する必要があります。 この手順では、Microsoft Lync が TLS 暗号 TLS_RSA_WITH_3DES_EDE_CBC_SHA で TLSv1 を送信できるように、Microsoft Lync で FIPS 準拠のアルゴリズムを設定する方法について説明します。 この手順では、Microsoft Lync がドメイン コントローラに設定されています。

手順

ステップ 1 [スタート（Start）] > [管理ツール（Administrative Tools）] > [ローカル セキュリティ ポリシー（Local Security Policy）] を選択します。

ステップ 2 コンソール ツリーで [セキュリティの設定（Security Settings）] を選択します。

ステップ 3 [ローカル ポリシー（Local Policies）] を選択します。

ステップ 4 [セキュリティ オプション（Security Options）] を選択します。

ステップ 5 [詳細（Details）] ウィンドウで FIPS セキュリティ設定をダブルクリックします。

ステップ 6 [OK] を選択します。

ステップ 7 Windows Server を再起動し、FIPS セキュリティ設定への変更を有効にします。

次の作業

Microsoft Lync のための新しい TLS ピア サブジェクトの作成, （12 ページ）

Microsoft Lync のための新しい TLS ピア サブジェクトの作成

次の手順を実行し、IM and Presence で Microsoft Lync のための新しい TLS ピア サブジェクトを作成します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [IM and Presence] > [セキュリティ（Security）] > [TLS ピア サブジェクト（TLS Peer Subjects）] を選択します。

ステップ 2 [新規追加（Add New）] を選択します。

ステップ 3 [ピア サブジェクト名（Peer Subject Name）] フィールドで、Microsoft Lync が提示する証明書のサブジェクト CN を入力します。

ステップ 4 [説明（Description）] フィールドに、Microsoft Lync サーバの名前を入力します。

ステップ 5 [保存（Save）] を選択します。

次の作業

TLS ピア サブジェクト リストへの TLS ピアの追加, （13 ページ）

TLS ピア サブジェクト リストへの TLS ピアの追加

次の手順を実行し、IM and Presence の選択した TLS ピア サブジェクトのリストに TLS ピアを追加します。

はじめる前に

IM and Presence に、Microsoft Lync のための新しい TLS ピア サブジェクトを作成します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [TLS コンテキスト設定（TLS Context Configuration）] を選択します。

ステップ 2 [検索（Find）] を選択します。

ステップ 3 [Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context] を選択します。
[TLS コンテキスト設定（TLS Context Configuration）] ウィンドウが表示されます。

ステップ 4 使用可能な TLS 暗号のリストから、[TLS_RSA_WITH_3DES_EDE_CBC_SHA] を選択します。

ステップ 5 右矢印を選択して、この暗号を [選択された TLS 暗号（Selected TLS Ciphers）] に移動します。

ステップ 6 [空の TLS フラグメントの無効化（Disable Empty TLS Fragments）] をオンにします。

ステップ 7 使用可能な TLS ピア サブジェクトのリストから、設定した TLS ピア サブジェクトを選択します。

ステップ 8 右矢印を選択して、[選択された TLS ピア サブジェクト（Selected TLS Peer Subjects）] に移動します。

ステップ 9 [保存（Save）] 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