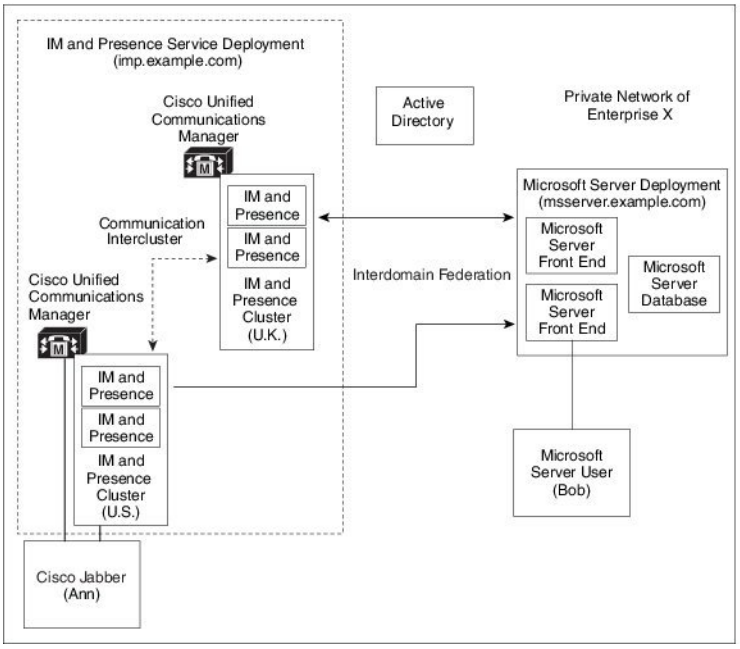
Microsoft Lync へのドメイン間フェデレーション

このセクションでは、Microsoft Lync へのドメイン間フェデレーションについて説明します。

企業内の Microsoft Lync へのドメイン間フェデレーション

図 *1*：企業内の *Microsoft* サーバーへのドメイン間フェデレーション



Microsoft サーバーと IM and Presence Service のドメインが異なる場合は、企業内でフェデレーションを構成できます。サブドメインを使用する必要はありません。個別のドメインも同様に

適用できます。詳細については、フェデレーションとサブドメインに関連するトピックを参照してください。

Microsoft Lync フェデレーションの設定タスク フロー

IM and Presence Service と Microsoft Lync 間のフェデレーションを設定するには、次のタスクを実行します。この設定は、チャットのみの展開とチャット+コールの展開の両方をサポートします。

（注） Expressway ゲートウェイの SIP ブローカを介したドメイン間フェデレーションは、単一の企業ネットワーク（社内）でのみサポートされます。ビジネスツービジネスの場合は、Expressway トラフィック分類または ASA を使用する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	企業内での Microsoft Lync ドメインの追加 （3 ページ）	IM and Presence Service で、Microsoft Lync ドメインのフェデレーション ドメイン エントリを追加します。IM and Presence Service は、フェデレーテッド ドメイン エントリの着信 ACL を自動的に追加します。
ステップ 2	IM and Presenceから Lync へのスタティック ルートの構築 （4 ページ）	IM and Presence Service で、Microsoft Lync サーバ ドメインごとに個別の TLS スタティック ルートを設定します。各ルートは、特定の Microsoft フロントエンド サーバーを指す必要があります。 （注） TLS スタティック ルートを設定する必要があります。TCP は、Microsoft Lync とのフェデレーションではサポートされていません。
ステップ 3	Configure Expressway Gateway for Microsoft Lync Federation （4 ページ）	（**省略可**）チャット+コール展開の場合のみ、Expressway ゲートウェイを追加します。ゲートウェイで、Microsoft の相互運用性と SIP ブローカを設定します。 （注） チャットのみの展開では、Expressway ゲートウェイは必要ありません。
ステップ 4	Lync サーバーで、次のいずれかの手順を使用して TLS 静的ルートを構成します。	チャット + コール展開の場合は、Expressway ゲートウェイへの TLS スタティック ルートを構成します。

	コマンドまたはアクション	目的
	• Lync から Expressway ゲートウェイへの静的ルートの構成 （5 ページ） • Lync から IM および Presence へのスタティック ルートの構成 （6 ページ）	チャットのみの展開の場合は、 IM and Presence Service ルーティングノードへの TLS スタティック ルートを構成します。
ステップ 5	Lync Server での信頼できるアプリケーションの構成 （9 ページ）	Lync サーバーで、IM and Presence Service を信頼できるアプリケーションとして追加し、各 IM and Presence クラスタ ノードを信頼できるアプリケーション サーバー プールに追加します。
ステップ 6	トポロジの公開 （11 ページ）	Lync サーバーで、トポロジをコミットします。
ステップ 7	Set up Certificates on IM and Presence for Federation with Lync （11 ページ）	IM and Presence Service で、Lync サーバ証明書に署名する CA のルート証明書を IM and Presence Service にアップロードします。また、TLS ピア サブジェクトをセット アップします。

企業内での Microsoft Lync ドメインの追加

Lync サーバーのフェデレーテッド ドメイン エントリを構成すると、 IM and Presence Service は自動的にフェデレーテッド ドメイン エントリの着信 ACL を追加します。フェデレーテッド ドメインに関連付けられている着信 ACL は、IM and Presence Administration で確認できますが、変更や削除はできません。（関連付けられた）フェデレーテッド ドメイン エントリを削除する場合にのみ、着信 ACL を削除できます。

ステップ 1 **Cisco Unified CM IM and Presence Administration** のユーザ インターフェイスにログインします。**[プレゼンス（Presence）] > [ドメイン間フェデレーション（Interdomain Federation）] > [SIP フェデレーション（SIP Federation）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [ドメイン名（Domain Name）] フィールドにフェデレ―テッド ドメイン名を入力します。

ステップ 4 [説明（Description）] フィールドにフェデレ―テッド ドメインを識別する説明を入力します。

ステップ 5 **[ドメイン間（Inter-domain to OCS/Lync）]** を選択します。

ステップ 6 **[直接フェデレーション（Direct Federation）]** チェックボックスをオンにします。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 SIP フェデレーテッド ドメインを追加、編集、または削除した後、Cisco XCP ルータを再起動します。**Cisco Unified IM and Presence Service Serviceability** のユーザー インターフェイスにログインします。**[ツール（Tools）] > [コントロール センター - ネットワーク サービス（Control Center - Network Services）]** を選択します。Cisco XCP ルータを再起動すると、 IM and Presence Serviceのすべての XCP サービスが再起動されます。

（注） Cisco XCP ルータの再起動は、クラスタ内のすべての IM and Presence Service ノードで必要です。

次のタスク

IM and Presenceから Lync へのスタティック ルートの構築 （4 ページ）

IM and Presenceから Lync へのスタティック ルートの構築

Microsoft Lync サーバ ドメインを指す IM and Presence Service で TLS スタティック ルートを設定するには、次の手順を使用します。Microsoft サーバー ドメインごとに個別のスタティック ルートを追加する必要があります。設定する各スタティック ルートは、特定の Microsoft Lync Enterprise Edition フロントエンド サーバーまたは Standard Edition サーバーをポイントする必要があります。

高可用性を実現するために、各 Microsoft サーバー ドメインへの追加のバックアップ スタティック ルートを構成できます。バックアップ ルートのプライオリティは低く、プライマリ スタティック ルートのネクスト ホップ アドレスに到達できない場合にのみ使用されます。

ステップ 1 Cisco Unified CM IM and Presence 管理で、**[プレゼンス（Presence）] > [ルーティング（Routing）] > [スタティック ルート（Static Routes）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 ドメインまたは FQDN が逆になるように、**[接続先パターン（Destination Pattern）]** の値を入力します。たとえば、ドメインが `domaina.com`の場合は、 `.com.domaina.*`と入力します。

ステップ 4 **[次のホップ（Next Hop）]** フィールドに、 Microsoft Lync サーバーの IP アドレスまたは FQDN を入力します。

ステップ 5 **[次のホップ ポート（Next Hop Port）]** フィールドに **5061**と入力します。

ステップ 6 **[ルート タイプ（Route Type）]** ドロップダウン リストから、**[ドメイン（Domain）]** を選択します。

ステップ 7 **[プロトコル タイプ（Protocol Type）]** ドロップダウン リスト ボックスから、**[TLS]**を選択します。

ステップ 8 [保存（Save）] をクリックします。

次の作業：

チャット + コールの導入、 Configure Expressway Gateway for Microsoft Lync Federation （4 ページ）

チャットのみの展開の場合、 Lync から IM および Presence へのスタティック ルートの構成 （6 ページ）

Configure Expressway Gateway for Microsoft Lync Federation

Chat + calling deployments only. On the Expressway Gateway, configure Microsoft interoperability and enable the SIP broker. For Expressway Gateway configuration, see the *Cisco Expressway and Microsoft Lync Deployment Guide* at:

http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.

Note For chat-only deployments, you do not need to deploy the Expressway Gateway.

What to do next

Lync から Expressway ゲートウェイへの静的ルートの構成, on page 5

Lync から Expressway ゲートウェイへの静的ルートの構成

チャット + コール展開の場合のみ。Lync サーバで、Expressway ゲートウェイの完全修飾ドメイン名（FQDN）を指す TLS スタティック ルートを構成します。

（注） スタティック ルートの FQDN が Lync フロントエンド サーバから解決可能であり、Expressway ゲートウェイの正しい IP アドレスに解決されることを確認します。

ステップ 1 たとえば、Lync Server 管理シェルがインストールされているコンピュータにドメイン管理者としてログインします。

ヒント **New-CsStaticRoute** コマンドレットを割り当てた RTCUniversalServerAdmins グループまたはロールベース アクセス コントロール（RBAC）ロールのメンバーとしてログインする必要があります。

ステップ 2 **[スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync Server 2010] > [Lync Server Management Shell]]** の順に選択します。

ヒント Microsoft Lync Server のバージョンに応じて、Microsoft Lync Server 2010 または 2013 に移動します。

ステップ 3 次のコマンドを入力して、TLS ルートを定義します。

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination expresswayGateway_fqdn -Port
expresswayGateway_TLS_listening_port -usedefaultcertificate $true -MatchUri expresswayGateway_domain
```

定義：

パラメータ	説明
-宛先	Expressway ゲートウェイの完全修飾ドメイン名（FQDN）。例：`expGateway.sip.com`
-ポート	Expressway ゲートウェイの TLS リスニング ポート。デフォルトのリスニング ポートは `65072` です。
-MatchUri	Expressway ゲートウェイのドメイン。たとえば、`sip.com` などです。

例：

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination expGateway.sip.com -Port 65072
-usedefaultcertificate $true -MatchUri sip.com
```

（注）
- ドメインの子ドメインを照合するには、**-MatchUri** パラメータでワイルドカード値（*.sip.com など）を指定できます。この値は、サフィックス sip.com で終わるすべてのドメインと一致します。
- Microsoft Lync server 2013 で IPv6 を使用している場合、* ワイルドカード オプションは **-MatchUri** パラメータではサポートされません。
- **-usedefaultcertificate** を false に設定する場合は、TLSCertIssuer パラメータと TLSCertSerialNumber パラメータを指定する必要があります。これらのパラメータは、スタティック ルートで使用される証明書を発行する認証局（CA）の名前と TLS 証明書のシリアル番号をそれぞれ示します。これらのパラメータの詳細については、「Lync Server 管理シェル」を参照してください。

ステップ 4 新しく作成したスタティック ルートを中央管理ストアで永続的にします。次のコマンドを入力します。

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

ステップ 5 新しいスタティック ルートを永続的にした場合は、コマンドが成功したことを確認します。次のコマンドを入力します。

```
Get-CsStaticRoutingConfiguration | select-object -ExpandProperty Route
```

ステップ 6 Lync コントロールパネルを開きます。**[外部ユーザーアクセス（External User Access）]** 領域で、次の手順を実行します。

a) **[新規 （New）]** をクリックし、Lync がフェデレーションしているドメイン（Expressway ゲートウェイ ドメイン）と Expressway ゲートウェイの FQDN のパブリック プロバイダを作成します。

b) 新しいパブリックプロバイダーで、ユーザの検証レベルを設定し、このプロバイダーとの[すべて]の通信を許可するように変更します。

次のタスク

Lync Server での信頼できるアプリケーションの構成 （9 ページ）

Lync から IM および Presence へのスタティック ルートの構成

チャットのみの展開の場合は、Lync サーバで IM および Presence サービス ルーティング ノードへの TLS スタティック ルートを構成します。IM および Presence サービス の展開に複数のクラスタがある場合でも、サブスクライバ ノードやクラスタ間ピア ノードへのスタティック ルートを作成する必要はありません。

ただし、IM および Presence サービス ドメインごとにスタティック ルートが必要です。

次の表に、この手順で使用する構成パラメータの例を示します。

表 *1 : Microsoft Lync* での *TLS* スタティック ルートのサンプル パラメータ

説明	パラメータの例
IM および Presence サービス ノードの FQDN（IM および Presence サービス ノードのルーティング） FQDN が正しい IP アドレスに解決できることを確認します。	impserverPub.sip.com
IM および Presence サービス ノードの IP アドレス（IM および Presence サービス ノードのルーティング）	10.10.1.10
IM および Presence サービス ノード TLS ポート TLS ポートの値は、ユーザー インターフェイスで構成されている値と一致する必要があります。値を確認するには、 **Cisco Unified CM IM および Presence 管理**のユーザー インターフェイスにログインし、**[システム（System）] > [アプリケーション リスナー（Application Listeners）] > [デフォルト Cisco SIP プロキシ TLS リスナー - ピア認証（Default Cisco SIP Proxy TLS Listener - Peer Auth）]** を選択します。 （注） Cisco ではポート 5061 を推奨しています。ただし、ポート 5062 を使用できます。	5061
IM および Presence サービス ノード ドメイン	sip.com
Lync 登録サーバー	lyncserver.synergy.com

（注）
- Transport Layer Security（TLS）を使用する場合、スタティック ルートの接続先パターンで使用される FQDN は、Lync フロントエンド サーバから解決可能である必要があります。FQDN が、スタティック ルートが指す IM および Presence サービス ノードの IP アドレスに解決されることを確認します。
- Lync FQDN は、パーティション化されたドメイン内フェデレーションに使用される IM および Presence サービス ドメインと一致させることはできません。

ステップ 1 たとえば、Lync Server 管理シェルがインストールされているコンピュータにドメイン管理者としてログインします。

ヒント **New-CsStaticRoute** コマンドレットを割り当てた RTCUniversalServerAdmins グループまたはロールベース アクセス コントロール（RBAC）ロールのメンバーとしてログインする必要があります。

ステップ 2 **[スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync Server 2010] > [Lync Server Management Shell]]** の順に選択します。

ヒント Microsoft Lync Server のバージョンに応じて、Microsoft Lync Server 2010 または 2013 に移動します。

ステップ 3 次のコマンドを入力して、TLS ルートを定義します。

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination fqdn_of_imp_routing_node -Port
listening_port_imp_routing_node -usedefaultcertificate $true -MatchUri destination_domain
```

例：

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination impserverPub.sip.com -Port 5061
-usedefaultcertificate $true -MatchUri sip.com
```

定義：

パラメータ	説明
-宛先	IM および Presence サービス ルーティングの FQDN。
-ポート	IM および Presence サービス ルーティング ノードのリスニング ポート。
-MatchUri	宛先 IM および Presence サービス ドメイン。

（注）
- ドメインの子ドメインを照合するには、**-MatchUri** パラメータでワイルドカード値（*.sip.com など）を指定できます。この値は、サフィックス sip.com で終わるすべてのドメインと一致します。
- Microsoft Lync server 2013 で IPv6 を使用している場合、* ワイルドカード オプションは **-MatchUri** パラメータではサポートされません。
- **-usedefaultcertificate** を false に設定する場合は、TLSCertIssuer パラメータと TLSCertSerialNumber パラメータを指定する必要があります。これらのパラメータは、スタティック ルートで使用される証明書を発行する認証局（CA）の名前と TLS 証明書のシリアル番号をそれぞれ示します。これらのパラメータの詳細については、「Lync Server 管理シェル」を参照してください。

ステップ 4 新しく作成したスタティック ルートを中央管理ストアで永続的にします。次のコマンドを入力します。

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

（注） この手順は、ルーティング IM および Presence サービス ノードに対してのみ実行します。

ステップ 5 新しいスタティック ルートを永続的にした場合は、コマンドが成功したことを確認します。次のコマンドを入力します。

```
Get-CsStaticRoutingConfiguration | select-object -ExpandProperty Route
```

ステップ 6 Lync コントロールパネルを開きます。**[外部ユーザーアクセス（External User Access）]** 領域で、次の手順を実行します。

a) **[新規作成（New）]** をクリックし、Lync と連携するドメイン（IM および Presence サービス ドメイン）と、IM および Presence サービス ノードの FQDN パブリック プロバイダを作成します。

b) 新しいパブリックプロバイダーで、ユーザの検証レベルを設定し、このプロバイダーとの[すべて]の通信を許可するように変更します。

次のタスク

Lync Server での信頼できるアプリケーションの構成 （9 ページ）

Lync Server での信頼できるアプリケーションの構成

Lync サーバで、 IM and Presence Service を信頼できるアプリケーションとして追加し、各 IM and Presence クラスタ ノードを信頼できるアプリケーション サーバ プールに追加します。この手順は、Enterprise Edition と Standard Edition の両方の Lync 展開に適用されます。

ステップ 1 次のコマンドを使用して、 IM and Presence Service 展開用の信頼できるアプリケーション サーバー プールを作成します。

ヒント **Get-CsPool** を入力して、プールのレジストラーサービスの FQDN 値を確認できます。

```
New-CsTrustedApplicationPool -Identity trusted_application_pool_name_in FQDN_format -Registrar
Lync_Registrar_service_FQDN -Site ID_for_the_trusted_application_pool_site -TreatAsAuthenticated
$true -ThrottleAsServer $true -RequiresReplication $false -OutboundOnly $false -Computerfqdn
first_trusted_application_computer
```

例：

```
New-CsTrustedApplicationPool -Identity trustedpool.sip.com -Registrar lyncserver.synergy.com -Site
1 -TreatAsAuthenticated $true -ThrottleAsServer $true -RequiresReplication $false -OutboundOnly
$false -Computerfqdn impserverPub.sip.com
```

定義：

パラメータ	説明
-Identity	IM and Presence Service 展開用の信頼できるアプリケーション プールの名前を入力します。これはFQDN形式である必要があります。例：`trustedpool.sip.com`。 **ヒント** Active Directory でマシンが見つからないことに関する警告メッセージを無視し、変更の適用に進みます。
-Registrar	プールのレジストラーサービスのサービス ID または FQDN。例：`lyncserver.synergy.com`。 **Get-CsPool** コマンドを使用して、この値を確認できます。
-Site	信頼できるアプリケーション プールを作成するサイトの数値。 **ヒント** **Get-CsSite** 管理シェル コマンドを使用します。
-Computerfqdn	IM および Presence サービス ルーティングの FQDN。例：`impserverPub.sip.com` • impserverPub = IM and Presence Service のホスト名。 • sip.com = IM and Presence Service ドメイン。

ステップ 2 IM and Presence Service ノードごとに、次のコマンドを入力して、ノードの FQDN を信頼できるアプリケーション コンピュータとして新しいアプリケーション プールに追加します。

New-CsTrustedApplicationComputer -Identity *imp_FQDN* **-Pool** *new_trusted_app_pool_FQDN*

例：

New-CsTrustedApplicationComputer -Identity *impserver2.sip.com* **-Pool** *trustedpool.sip.com*

定義：

パラメータ	説明
-Identity	IM および Presence サービス ノードの FQDN。例： `impserver2.sip.com` （注） このコマンドを使用して、 IM and Presence Service ルーティング ノードを信頼できるアプリケーション コンピュータとして追加しないでください。
-Pool	IM and Presence Service の展開に使用される信頼できるアプリケーション プールの FQDN。例： `trustedpool.sip.com`。

ステップ 3 次のコマンドを入力して、新しい信頼できるアプリケーションを作成し、新しいアプリケーション プールに追加します。

New-CsTrustedApplication -ApplicationID *new_application_name* **-TrustedApplicationPoolFqdn** *new_trusted_app_pool_FQDN* **-Port 5061**

例：

New-CsTrustedApplication -ApplicationID *imptrustedapp.sip.com* **-TrustedApplicationPoolFqdn** *trustedpool.sip.com* **-Port 5061**

定義：

パラメータ	説明
-ApplicationID	アプリケーションの名前。任意の値を指定できます。例：imptrustedapp.sip.com
-TrustedApplicationPoolFqdn	IM and Presence Serviceの信頼できるアプリケーション プール サーバーの FQDN。例： `trustedpool.sip.com`。
-Port	IM and Presence Service ノードの SIP リスニング ポート。TLS の場合、ポートは 5061 です。

次のタスク

トポロジの公開 （11 ページ）

トポロジの公開

ステップ 1 Lync Server 管理シェルにログインします。

ステップ 2 **Enable-CsTopology** コマンドを入力して、トポロジを有効にします。

次のタスク

Set up Certificates on IM and Presence for Federation with Lync （11 ページ）

Set up Certificates on IM and Presence for Federation with Lync

Use this procedure to set up certificates on your IM and Presence Service nodes for Federation with Microsoft Lync.

ステップ 1 On the IM and Presence Service, upload the root certificate for the CA that signs the Microsoft server certificate.

- Upload the certificate as a cup-trust certificate.
- Leave the **Root Certificate** field blank.
- Import the self-signed certificate onto the IM and Presence Service.

ステップ 2 Generate a CSR for the IM and Presence Service so that the certificate can be signed by a CA. Upload the CSR to the CA that signs your certificate.

Important
- The CA must sign the certificate so that it has "Enhanced Key Usage" with both "Server Authentication" and "Client Authentication".
- If this is Microsoft Windows Server CA, it must use a certificate template that has "Server Authentication" and "Client Authentication".

ステップ 3 When you have retrieved the CA-signed certificate and the CA root certificate, upload the CA-signed certificate and the root certificate to the IM and Presence Service node.

- Upload the root certificate as a cup-trust certificate.
- Upload the CA-signed cup certificate. Specify the root certificate .pem file as the root certificate.

ステップ 4 Add a TLS Peer subject on IM and Presence Service for the Microsoft server. Use the FQDN of the Microsoft server.

ステップ 5 Add the TLS Peer to the Selected TLS Peer Subjects list.

- Make sure that the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher is chosen for the TLS Context Configuration.
- Make sure that you disable empty TLS fragments.

What to do next

Set up certificates on the Microsoft Lync server that have "Enhanced Key Usage" with "Server Authentication" and "Client Authentication" values. For details, see:

- CA サーバーからの証明書の要求
- Microsoft TechNet Library, Windows Server — Implementing and Administering Certificate Templates at http://technet.microsoft.com/en-us/library/cc731256(v=ws.10).aspx.

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。