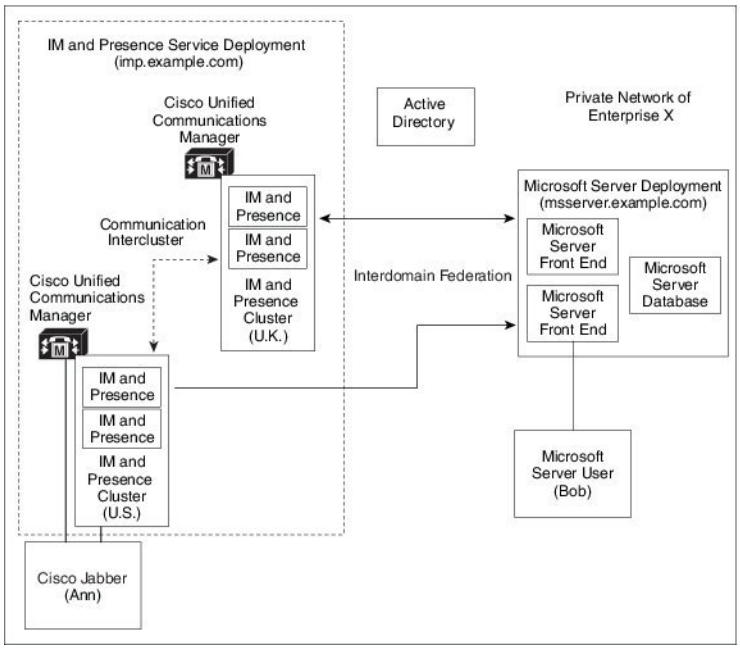
MicrosofOCSへのドメイン間フェデレーション

企業内の Microsoft OCS へのドメイン間フェデレーション

図 *1*：エンタープライズ内のサーバへのドメイン間フェデレーション



Microsoft サーバおよび IM and Presence サービス ドメインが異なる場合、企業内フェデレーションを設定できます。ドメインが異なればそれらは同等に適用することができるため、サブドメイン

を使用する必要はありません。詳細については、フェデレーションとサブドメインのトピックを参照してください。

Microsoft OCS フェデレーションのタスク フローの設定

IM and Presence サービスと Microsoft OCS の間のフェデレーテッド リンクをセットアップする場合に、以下のタスクを実行します。

Access Edge サーバも Cisco Adaptive Security Appliance も使用せずに IM and Presence サービスから OCS に直接フェデレーションを使用している場合は、OCS サーバの各ドメインで TLS または TCP のスタティック ルートを設定する必要があります。これらのスタティック ルートは、IM and Presence サービス ノードをポイントします。Cisco Adaptive Security Appliance や Microsoft Access Edge は必要ではありません。

- Standard Edition では、すべての Standard Edition サーバでスタティック ルートを設定します。
- Enterprise Edition では、すべてのプールでスタティック ルートを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	企業内の Microsoft OCS ドメインの追加, （3 ページ）	IM and Presence サービスで、Microsoft OCS ドメインのフェデレーテッド ドメイン エントリを追加します。IM and Presence サービスは、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	Microsoft サーバ用 の IM and Presence サービスのスタティック ルートの設定, （4 ページ）	IM and Presence サービスで、Microsoft OCS サーバ ドメインごとに個別のスタティック 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 サーバをポイントする必要があります。 （注） OCS では、プロトコル タイプとして TCP と TLS のいずれかを選択できます。
ステップ 3	IM and Presence サービスをポイントする OCS のスタティック ルートの設定, （5 ページ）	OCS サーバで、IM and Presence サービス ドメインをポイントする TCP または TLS スタティック ルートを設定します。各ルートは、特定の IM and Presence サービス ノードをポイントする必要があります。
ステップ 4	ピア認証リスナーの確認, （7 ページ）	IM and Presence サービスで、ピア認証リスナーがポート 5061 として設定されており、サーバ認証リスナーがポート 5061 になっていないことを確認します。
ステップ 5	OCS での IM and Presence サービス ノード用ホスト認証エントリの追加, （7 ページ）	OCS サーバで、IM and Presence サービス ノードごとにホスト認証エントリを設定します。TLS 暗号化を使用する場合は、IM and Presence ノードごとに次の 2 つのエントリを追加する必要があります。

	コマンドまたはアクション	目的
		• IM and Presence ノードの IP アドレスを指定する 1 つのエントリ • IM and Presence ノードの FQDN を指定する 1 つのエントリ TLS 暗号化を使用しない場合は、IM and Presence サービス ノードごとに、ノードの IP アドレスを指定する 1 つのホスト認証エントリを設定します。
ステップ 6	ドメイン間フェデレーション用の OCS 上の証明書の設定, （8 ページ）	OCS と IM and Presence サービスの間で TLS が設定されている場合は、OCS 上で IM and Presence サービスとのドメイン間フェデレーション用の証明書を設定します。 （注） TLS を使用しない場合は、このステップを省略できます。
ステップ 7	OCS サーバでのポート 5060/5061 の有効化, （9 ページ）	OCS サーバで、TLS 用のリスナー ポート（トランスポートとして MTLS または TLS を使用可能）または TCP 用のリスナー ポートが設定されていることを確認します。。 • OCS サーバへの TLS スタティック ルートの場合は、ポート 5061 を使用します。 • OCS サーバへの TCP スタティック ルートの場合は、ポート 5060 を使用します。
ステップ 8	FIPS を使用するための OCS の設定, （10 ページ）	TLS を使用する場合は、FIPS を使用するように OCS を設定します。
ステップ 9	Microsoft サーバとの TLS 経由のフェデレーションに関連する IM and Presence サービス ノード上の証明書の設定, （10 ページ）	TLS を使用する場合は、OCS サーバ証明書に署名する CA のルート証明書を IM and Presence サービスにアップロードします。

企業内の Microsoft OCS ドメインの追加

OCS サーバ用のフェデレーテッド ドメイン エントリを設定すると、IM and Presence サービスがフェデレーテッド ドメイン エントリの着信 ACL を自動的に追加します。この着信 ACL がフェデレーテッド ドメインと関連付けられたことを [IM and Presence Administration] で確認できますが、

着信 ACL は変更したり削除したりすることはできません。着信 ACL を削除できるのは、（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だけです。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] 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（Inter Domain 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ーテッド 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ーテッド ドメインを識別する説明を入力します。

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

ステップ 6 [ダイレクト 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 Serviceability]** ユーザ 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 センタのネットワーク 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 サービス のすべての XCP サービスが再起動されます。

（注） クラスタ内のすべての IM and Presence サービス ノードで Cisco XCP ルータを再起動する必要があります。

次の作業

Microsoft サーバ用 の IM and Presence サービスのスタティック ルートの設定, （4 ページ）

Microsoft サーバ用 の IM and Presence サービスのスタティック ルートの設定

IM およびアベイラビリティをフェデレーテッド Microsoft サーバ ドメインと交換するときに TLS を使用する、または OCS ドメインの場合は TCP を使用するように IM and Presence サービスを設定するには、Microsoft サーバをポイントし、Microsoft Access Edge の外部エッジはポイントしないスタティック ルートを IM and Presence サービスに設定する必要があります。

各 Microsoft サーバ ドメイン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。Microsoft サーバ ドメインのスタティック ルートは、特定の Microsoft サーバの Enterprise Edition フロントエンド サーバまたはスタンダード エディション サーバの IP アドレスをポイントする必要があります。

ハイ アベイラビリティを得るために、各 Microsoft サーバ ドメインの追加バックアップ スタティック ルートを設定できます。バックアップ ルートの優先順位は低く、プライマリ スタティック ルートの次のホップ アドレスに到達できない場合にのみ使用されます。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] 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）] > [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、つまり FQDN が元に戻るよう [宛先パターン（Destination Pattern）] 値を入力します。次に例を示します。

- ドメインが `domaina.com` の場合は、宛先パターンの値として `.domaina.* .com` を入力します。

ステップ 4 その他のパラメータは次のように入力します。

a) [ネクストホップ（Next Hop）] 値には Microsoft サーバの IP アドレスまたは FQDN を入力します。

b) [ネクスト ホップ ポート（Next Hop Port）] の番号および [プロトコル タイプ（Protocol Type）] の値を次のように設定します。

- TCP では、[プロトコルタイプ（Protocol Type）] に TCP、[ネクストホップポート（Next Hop Port）] の番号として 5060 を選択します。
- TLS では、[プロトコル タイプ（Protocol Type）] に [TLS]、[ネクスト ホップ ポート（Next Hop Port）] の番号として [5061] を選択します。

（注） Microsoft OCS サーバは、TCP または TLS 経由のフェデレーションをサポートします。

c) [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 5 [保存（Save）] をクリックします。

次の作業

IM and Presence サービスをポイントする OCS のスタティック ルートの設定, （5 ページ）

IM and Presence サービスをポイントする OCS のスタティック ルートの設定

ダイレクト フェデレーション用に OCS が IM and Presence サービスに要求をルーティングできるようにするには、各 IM and Presence サービス ドメインについて OCS サーバで TLS または TCP のスタティック ルートを設定する必要があります。これらのスタティック ルートは IM and Presence サービス ノードをポイントします。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのプールでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 適宜 Enterprise Edition プール名または Standard Edition サーバ名を右クリックします。

ステップ 3 [プロパティ（Properties）] > [フロント エンド プロパティ（Front End Properties）] を選択します。

ステップ 4 [ルーティング（Routing）] タブを選択し、[追加（Add）] をクリックします。

ステップ 5 foo.com など、IM and Presence サービス ノードのドメインを入力します。

ステップ 6 [電話 URI（Phone URI）] チェックボックスがオフになっていることを確認します。

ステップ 7 ネクスト ホップ トランスポート、ポート、IP アドレス/FQDN 値を設定します。

- TCP の場合は、[ネクスト ホップ トランスポート（Next Hop Transport）] 値に [TCP] を選択し、[ネクスト ホップ ポート（Next Hop Port）] 値に **5060** を入力します。ネクスト ホップ IP アドレスとして IM and Presence サービス ノードの IP アドレスを入力します。
- TLS の場合は、[ネクスト ホップ トランスポート（Next Hop Transport）] 値に [TLS] を選択し、[ネクスト ホップ ポート（Next Hop Port）] 値に **5061** を入力します。FQDN として IM and Presence サービス ノードの IP アドレスを入力します。

（注）
- TLS のスタティック ルートに使用するポートは、IM and Presence サービス ノードで設定されたピア認証のリスナー ポートに一致する必要があります。
- FQDN は OCS サーバで解決可能である必要があります。FQDN が IM and 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。

ステップ 8 [要求 URI のホストを置換（Replace host in request URI）] チェックボックスがオフになっていることを確認します。

ステップ 9 [OK] をクリックして、[静的ルートの追加（Add Static Route）] ウィンドウを閉じます。新しいスタティック ルートがルーティング リストに表示されるはずです。

ステップ 10 [OK] を再度選択して、[フロント エンド サーバ プロパティ（Front End Server Properties）] ウィンドウを閉じます。

次の作業

『Interdomain Federation for IM and Presence Service on Cisco Unified Communcations Manager guide』の「Verify Peer Authentication Listener」を参照してください。

ピア認証リスナーの確認

IM and Presence サービスでピア認証リスナー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 Cisco Unified CM IM and Presence Administration で、[システム（System）] > [アプリケーションリスナー（Application Listener）] を選択します。

ステップ 2 [検索（Find）] をクリックします。
設定済みのアプリケーションリスナーポートの一覧が表示されます。デフォルトのピア認証リスナー ポートとサーバ認証リスナー ポートも表示されます。

ステップ 3 [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）] ポートが 5061 になっていることを確認します。

ステップ 4 [デフォルトCisco SIPプロキシTLSリスナー-サーバ認証（Default Cisco SIP Proxy TLS Listener - Server Auth）] ポートが 5061 になっていないことを確認します。このポートが 5061 として設定されている場合は、別の値に変更する必要があります。たとえば 5063 と入力します。

次の作業

OCS での IM and Presence サービス ノード用ホスト認証エントリの追加, （7 ページ）

OCS での IM and Presence サービス ノード用ホスト認証エントリの追加

認証を求められずに OCS が IM and Presence サービス から SIP 要求を承認できるようにするには、IM and Presence サービス ノードごとに OCS でホスト認証エントリを設定する必要があります。

OCS とIM and Presence サービス間の TLS 暗号化を設定する場合、次のように各 IM and Presence サービス ノードに 2 つのホスト認証エントリを追加する必要があります。

- 最初のエントリには、IM and Presence サービス ノードの FQDN を含める必要があります。
- 2 つ目のエントリには、IM and Presence サービス ノードの IP アドレスを含める必要があります。

TLS 暗号化を設定しない場合は、IM and Presence サービス ノードに 1 つのホスト認証エントリのみを追加します。このホスト認証エントリには、IM and Presence サービス ノードの IP アドレスが含まれている必要があります。

次の手順では、必要なホスト認証エントリを追加する方法について説明します。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのプールでこの手順を実行する必要があります。

手順

ステップ 1 OCS の [ホスト認証（Host Authorization）] タブを選択します。

ステップ 2 次のいずれかの手順を実行します。

a) OCS で IP アドレスによって次ホップ（ネクストホップ）のコンピュータを指定するスタティック ルートを設定している場合は、承認されたホストの IP アドレスを入力します。

b) OCS で FQDN によって次ホップ（ネクスト ホップ）のコンピュータを指定するスタティック ルートを設定している場合は、承認されたホストの FQDN を入力します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [IP] を選択します。

ステップ 5 IM and Presence サービス ノードの IP アドレスを入力します。

ステップ 6 [サーバとしてのスロットル（Throttle as Server）] チェックボックスをオンにします。

ステップ 7 [認証付きとして処理（Treat as Authenticated）] チェックボックスをオンにします。

（注） [発信のみ（Outbound Only）] チェックボックスをオンにしないでください。

ステップ 8 [OK] をクリックします。

次の作業

ドメイン間フェデレーション用の OCS 上の証明書の設定, （8 ページ）

ドメイン間フェデレーション用の OCS 上の証明書の設定

OCS と IM and Presence サービスの間で TLS が設定されている場合は、OCS 上で IM and Presence サービスとのドメイン間フェデレーション用の証明書を設定します。

（注） TLS を使用しない場合は、この手順を省略できます。

手順

ステップ 1 CA ルート証明書と OCS 署名付き証明書を取得するには、以下の手順を実行します。

a) CA 証明書チェーンをダウンロードおよびインストールします。

b) CA サーバに証明書を要求します。
c) CA サーバから証明書をダウンロードします。

ステップ 2 [OCSフロントエンドサーバのプロパティ（OCS Front End Server Properties）] で、[証明書（Certificates）] タブを選択し、[証明書の選択（Select Certificate）] をクリックして、OCS 署名付き証明書を選択します。

次の作業

OCS サーバでのポート 5060/5061 の有効化, （9 ページ）

OCS サーバでのポート 5060/5061 の有効化

OCS サーバへの TCP スタティック ルートの場合は、ポート 5060 を使用します。

OCS サーバへの TLS スタティック ルートの場合は、ポート 5061 を使用します。

手順

ステップ 1 OCS で、[スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Microsoft Office Communicator Server 2007] を選択します。

ステップ 2 フロント エンド サーバの FQDN を右クリックします。

ステップ 3 [プロパティ（Properties）] > [フロント エンドのプロパティ（Front End Properties）] を選択し、[全般（General）] タブを選択します。

ステップ 4 [接続（Connections）] にポート 5060 または 5061 が記載されていない場合は、[追加（Add）] を選択します。

ステップ 5 次のように、ポート値を設定します。

a) [IP アドレス値（IP Address Value）] に [すべて（All）] を選択します。
b) ポート値を選択します。

- TCP の場合、ポート値として [5060] を選択します。
- TLS の場合、ポート値として [5061] を選択します。

c) 輸送値を選択します。

- TCP の場合は、[トランスポート（Transport）] の値として [TCP] を選択します。
- TLS で、[トランスポート（Transport）] の値として [TLS] を選択します。

ステップ 6 [OK] をクリックします。

次の作業

FIPS を使用するための OCS の設定, （10 ページ）

FIPS を使用するための OCS の設定

OCS サーバで FIPS を設定します。この手順は、TLS のみ（SSLv3 ではなく TLSv1）を使用している場合にのみ実行します。

手順

ステップ 1 OCS の [ローカルセキュリティ設定（Local Security Settings）] を開きます。

ステップ 2 コンソール ツリーで、[ローカルポリシー（Local Policies）] を選択します。

ステップ 3 [セキュリティ オプション（Security Options）] を選択します。

ステップ 4 暗号化、ハッシュ、および署名用の System Cryptography:Use FIPS Compliant アルゴリズムをダブルクリックします。

ステップ 5 セキュリティ設定を有効にします。

ステップ 6 [OK] をクリックします。

（注） 有効にするには、OCS を再起動する必要があります。

ステップ 7 IM and Presence サービスの証明書に署名する CA の CA ルート証明書をインポートします。証明書スナップインを使用して OCS の信頼ストアに CA ルート証明書をインポートします。

次の作業

Microsoft サーバとの TLS 経由のフェデレーションに関連する IM and Presence サービス ノード上の証明書の設定, （10 ページ）

Microsoft サーバとの TLS 経由のフェデレーションに関連する IM and Presence サービス ノード上の証明書の設定

この手順は、IM and Presence サービスと Microsoft サーバ間の TLS スタティック ルートをセットアップした場合にのみ適用されます。

手順

ステップ 1 IM and Presence サービスで、Microsoft サーバの証明書に署名する CA のルート証明書をアップロードします。

- CUP 信頼証明書として証明書をアップロードします。

- [ルート証明書（Root Certificate）] フィールドは空白のままにします。
- IM and Presence サービスに自己署名証明書をインポートします。

ステップ 2 CA が IM and Presence サービスの証明書に署名できるよう、IM and Presence サービスに対する CSR を作成します。証明書に署名する CA に CSR をアップロードします。

重要
- CA は、「サーバ認証」と「クライアント認証」の両方で「強化キー」を保有していることについて署名する必要があります。
- Microsoft Windows Server CA の場合は、「サーバ認証」と「クライアント認証」を持つ証明書テンプレートを使用する必要があります。

ステップ 3 CA 署名付き証明書と CA ルート証明書を取得する場合は、IM and Presence サービスに CA 署名付き証明書と CA ルート証明書をアップロードします。

- CUP 信頼証明書としてルート証明書アップロードします。
- CUP CA 署名付き証明書をアップロードします。ルート証明書としてルート証明書 .pem ファイルを指定します。

ステップ 4 OCS サーバの IM and Presence サービスに TLS ピア サブジェクトを追加します。Microsoft サーバの FQDN を使用します。

ステップ 5 [選択された TLS ピア サブジェクト（Selected TLS Peer Subjects）] リストに TLS ピアを追加します。

- [TLS コンテキスト設定（TLS Context Configuration）] で TLS_RSA_WITH_3DES_EDE_CBC_SHA 暗号が選択されていることを確認します。
- 空の TLS フラグメントが無効化されていることを確認します。

次の作業

Microsoft Lync サーバで、「サーバ認証」と「クライアント認証」の値に「拡張キー使用法」が設定されている証明書を設定します。参照先：

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