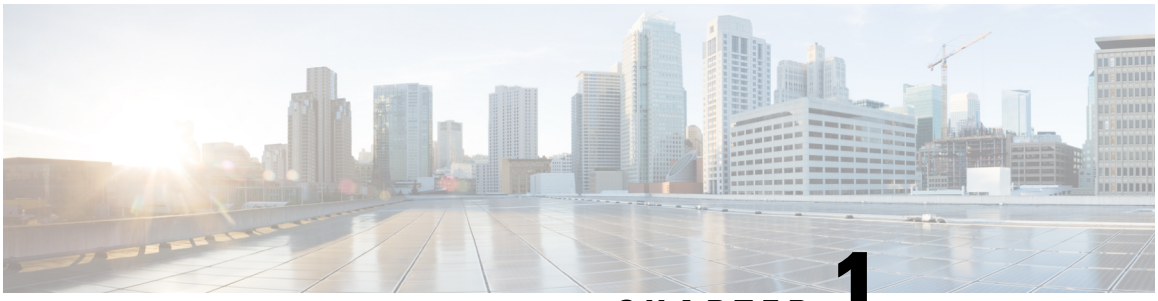
# IM および Presence サービス ドメイン内フェデレーション ガイド、リリース 15

**初版**：2024 年 2 月 29 日

**シスコシステムズ合同会社**
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

# 目 次



CHAPTER 1

# 新機能および変更された機能に関する情報



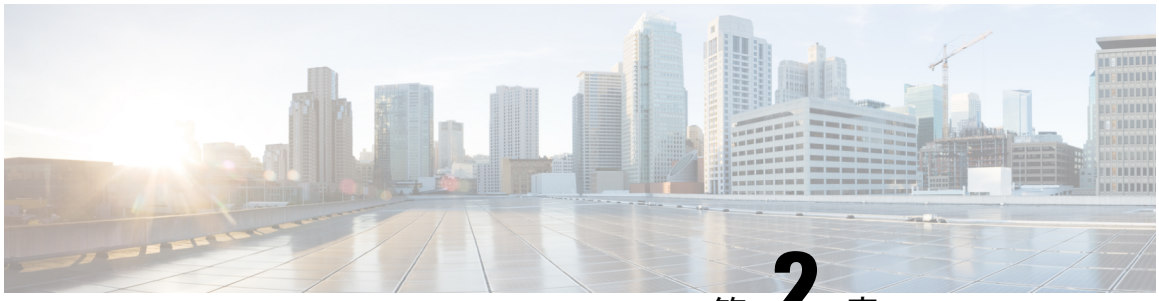
## 新機能および変更された機能に関する情報

次の表は、この最新リリースまでのガイドでの機能の主な変更点の概要を示したものです。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

***Table 1: Unified Communications Manager* と *IM and Presence* サービスの新機能と変更された動作**

| 機能または変更 | 説明 | 参照先 | 日付 |
|---|---|---|---|
| リリース 14 のマニュアルの初回リリース | — | — | 2021 年 3 月 31 日 |
| リリース 14SU1 のマニュアルの初回リリース | — | — | 2021 年 10 月 27 日 |
| リリース 14SU2 のマニュアルの初回リリース | — | — | 2022 年 6 月 16 日 |

新機能および変更された機能に関する情報



第 2 章

# この統合の概要

このセクションでは、統合の概要を示します。



## 基本的なフェデレーテッド ネットワーク

この統合により IM および Presence サービスが管理する任意のドメイン内のIM および Presence サービスユーザーが、外部ドメインユーザとーアベイラビリティ情報およびインスタントメッセージング（IM）を交換することができます。IM および Presence サービスは、さまざまなプロトコルを使用してさまざまな外部ドメインとフェデレーションします。

IM および Presence サービスは、標準の Session Initiation Protocol（SIP RFC 3261）を使用して、次のものとフェデレーションします。

- Microsoft Office 365（ビジネス ツー ビジネス）
- Microsoft Skype for Business 2015、Standard Edition および Enterprise Edition（ビジネス ツー ビジネス）
- Microsoft Lync 2010 および 2013、Standard Edition および Enterprise Edition

（注） IM および Presence サービス は、Microsoft Lync とのドメイン間フェデレーションをサポートしています。IM および Presence サービスでは、特に明記されていない限り、Microsoft S4B/Lync とのドメイン間フェデレーションへの言及には Microsoft Office 365 も含まれます。

IM および Presence サービスでは、以下のフェデレーションのため Extensible Messaging and Presence Protocol（XMPP）を使用します。

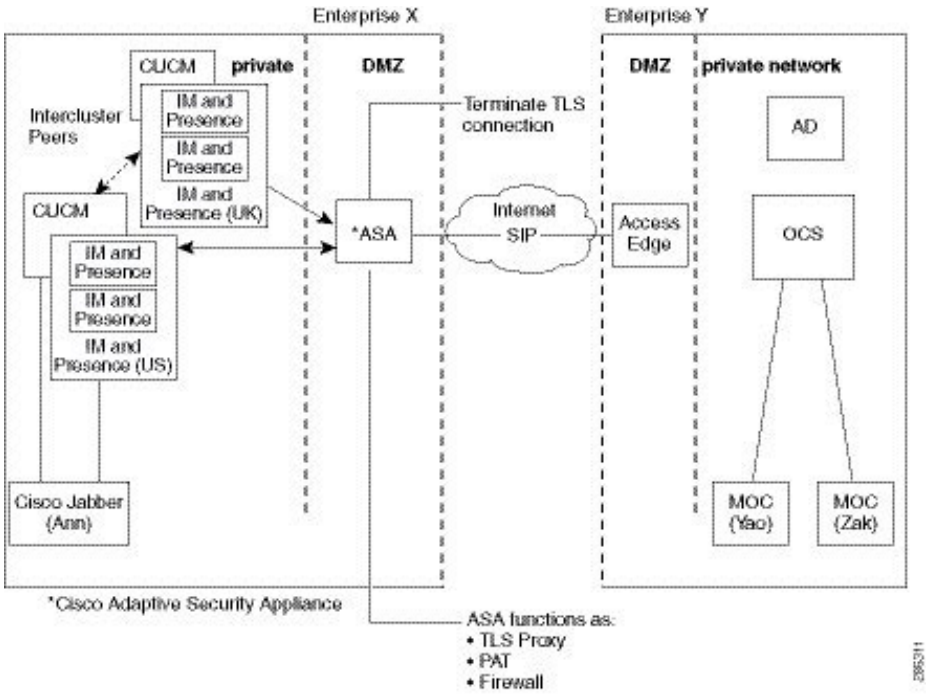
- IBM Sametime サーバ 8.2 および 8.5
- Cisco Webex Messenger
- IM および Presence サービス 9.x 以降
- XMPP 標準に準拠しているその他のサーバ

（注） 外部ドメインとの XMPP フェデレーションを有効にする場合は、外部ドメインが以前に IM および Presence サービスで SIP フェデレーション ドメインとして構成されていないことを確認します。

**例**： example.com を使用した IM および Presence の展開は、これまで SIP ベースのフェデレーションとして設定されていました。ただし、example.com では XMPP サポートが追加されているため、ローカル管理者は代わりに XMPP ベースのフェデレーションを有効にする必要があります。これを許可するには、ローカル管理者は最初に、IM および Presence サービスで SIP フェデレーテッド ドメインとして example.com を削除する必要があります。

次の図に、IM および Presence サービス エンタープライズ展開と Microsoft S4B/Lync エンタープライズ展開間の SIP フェデレーテッド ネットワークの例を示します。

図 *1 : IM* および *Presence* サービスと *Microsoft S4B/Lync* 間の基本的な *SIP* フェデレーション ネットワーク

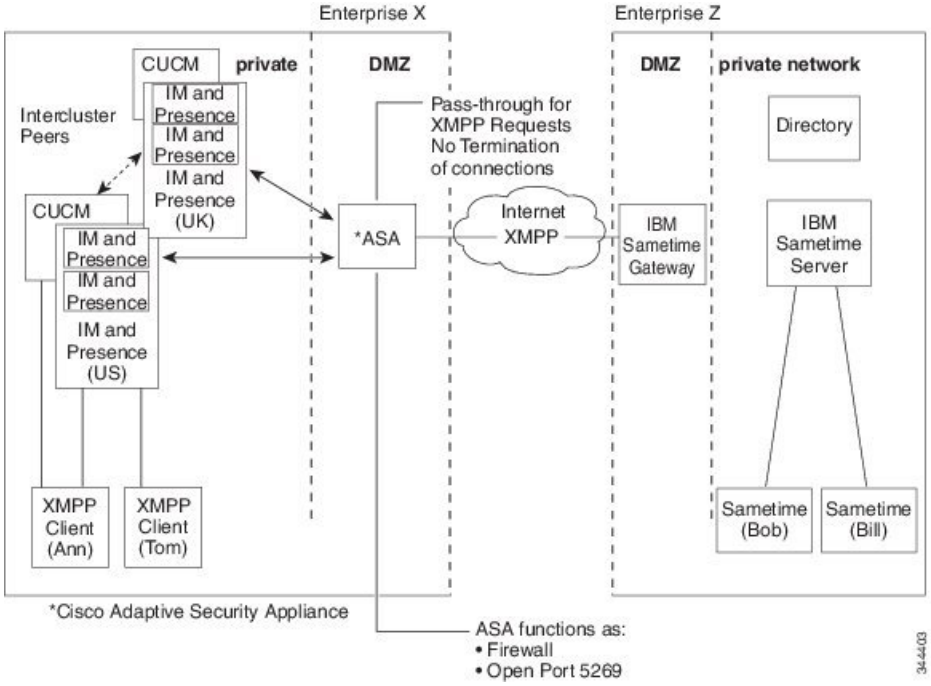



この例は、SIP フェデレーションが 1 つのクラスタでのみ有効になっているマルチクラスタ IM および Presence サービス展開のメッセージング フローを示しています。単一のルーティング ノードが Expressway-C からすべての着信 IM を受信し、IM をいずれかのクラスタ内の正しいノードに再ルーティングします。発信 IM は、いずれかのクラスタ内の任意のノードから Expressway-C に送信できます。

この図では、各内部エンタープライズ ドメインは、セキュアな TLS 接続を使用して DMZ エッジ サーバを使用してパブリック インターネット経由で相互接続しています。内部 IM および Presence サービス企業展開内で、Cisco 適応型セキュリティ アプライアンスは、ファイアウォール、ポート アドレス変換（PAT）、および TLS プロキシ機能を提供します。Cisco Expressway-C は、外部ドメインから開始されたすべての着信トラフィックを、指定された IM および Presence サービス ノードにルーティングします。

次の図は、IM および Presence サービス エンタープライズ展開と IBM Sametime エンタープライズ展開間のマルチクラスタ XMPP フェデレーテッドネットワークの例を示しています。TLS は、XMPP フェデレーションではオプションです。Cisco 適応型セキュリティ アプライアンスは、XMPP フェデレーションのファイアウォールとしてのみ機能します。 XMPP フェデレーション用の TLS プロキシ機能または PAT は提供しません。IM は、フェデレーションが有効になっている任意のノードから送受信できます。ただし、フェデレーションは両方のクラスタで並行して構成する必要があります。

図 *2 : IM* および *Presence* サービスと *IBM Sametime* 間の基本的な *XMPP* フェデレーテッド ネットワーク




内部 IM および Presence サービス エンタープライズ展開内に 2 つの DNS サーバがあります。1 台の DNS サーバが IM および Presence サービスのプライベート アドレスをホストします。もう一方の DNS サーバーは、SIP フェデレーション（_sipfederationtls）および IM および Presence サービスとの XMPP フェデレーション（_xmpp-server）の IM および Presence サービスパブリック アドレスと DNS SRV レコードをホストします。IM および Presence サービスのパブリック アドレスをホストする DNS サーバーは、ローカル DMZ にあります。

# クラスタ間展開とマルチノードの展開

（注） クラスタ間 IM and Presence Service の展開に関連するこのドキュメントの構成手順は、マルチノード IM and Presence Service の展開にも適用できます。

## SIP フェデレーションの展開

クラスタ間およびマルチノード クラスタ IM and Presence Service 展開では、外部ドメインが新しいセッションを開始すると、Cisco Expressway-C は、ルーティング用に指定された IM and Presence Service ノードにすべてのメッセージをルーティングします。 IM and Presence Service ルーティング ノードが受信者ユーザーをホストしていない場合、クラスタ間通信を介してメッセージをクラスタ内の適切な IM and Presence Service ノードにルーティングします。システム

は、この要求に関連付けられているすべての応答を、ルーティング IM and Presence Service ノードを介してルーティングします。

IM and Presence Service ノードは、Cisco Expressway-Cを介して外部ドメインへのメッセージを開始できます。Microsoft S4B/Lync では、外部ドメインがこれらのメッセージに応答すると、応答は Cisco Expressway-C を介してメッセージを開始した IM and Presence Service ノードに直接送信されます。Cisco Expressway-C で Port Address Translation (PAT) を構成するときにこの動作を有効にします。200 OK 応答メッセージには PAT が必要であるため、Cisco Expressway-C で PAT を構成することを推奨します。

関連情報： この統合向けのポート アドレス変換

# XMPP フェデレーションの展開

単一クラスタの場合、クラスタ内の1つのノードでXMPPフェデレーションのみを有効にする必要があります。パブリック DNS で企業の単一の DNS SRV レコードが公開されます。この DNS SRV レコードは、XMPP フェデレーションが有効になっている IM and Presence Service ノードにマッピングされます。外部ドメインからのすべての着信要求は、パブリッシュされた SRV レコードに基づいて、XMPP フェデレーションを実行しているノードにルーティングされます。内部的には、 IM and Presence Service が要求をユーザーの正しいノードに再ルーティングします。また、 IM and Presence Service は、XMPP フェデレーションを実行しているノードを介してすべての発信要求をルーティングします。

また、たとえば、拡張目的で、または複数の IM and Presence Service クラスタがあり、クラスタごとに少なくとも1回XMPPフェデレーションを有効にする必要がある場合に、複数のDNS SRV レコードを公開することもできます。SIP フェデレーションとは異なり、XMPP フェデレーションでは、 IM and Presence Service エンタープライズ ドメインの単一のエントリ ポイントは必要ありません。その結果、 IM and Presence Service は、XMPP フェデレーションを有効にした公開ノードのいずれかに着信要求をルーティングできます。

クラスタ間およびマルチノード クラスタ IM and Presence Service 展開では、外部 XMPP フェデレーテッド ドメインが新しいセッションを開始すると、DNS SRV ルックアップを実行して要求のルーティング先を決定します。複数の DNS SRV レコードをパブリッシュすると、DNS ルックアップは複数の結果を返します。 IM and Presence Service は、DNS が発行する任意のサーバに要求をルーティングできます。内部的には、 IM and Presence Service が要求をユーザーの正しいノードに再ルーティングします。 IM and Presence Service は、クラスタ内の XMPP フェデレーションを実行しているノードのいずれかに発信要求をルーティングします。

XMPP フェデレーションを実行している複数のノードがある場合でも、パブリック DNS で 1 つのノードのみを発行することを選択できます。この設定では、 IM and Presence Service は、XMPP フェデレーションを実行しているノード間で着信要求をロードバランシングするのではなく、すべての着信要求を単一のノードを介してルーティングします。 IM and Presence Service は発信要求をロード バランシングし、クラスタ内の XMPP フェデレーションを実行しているノードのいずれかに発信要求を送信します。

# 高可用性およびフェデレーション

このセクションでは、高可用性とフェデレーションの概念について説明します。

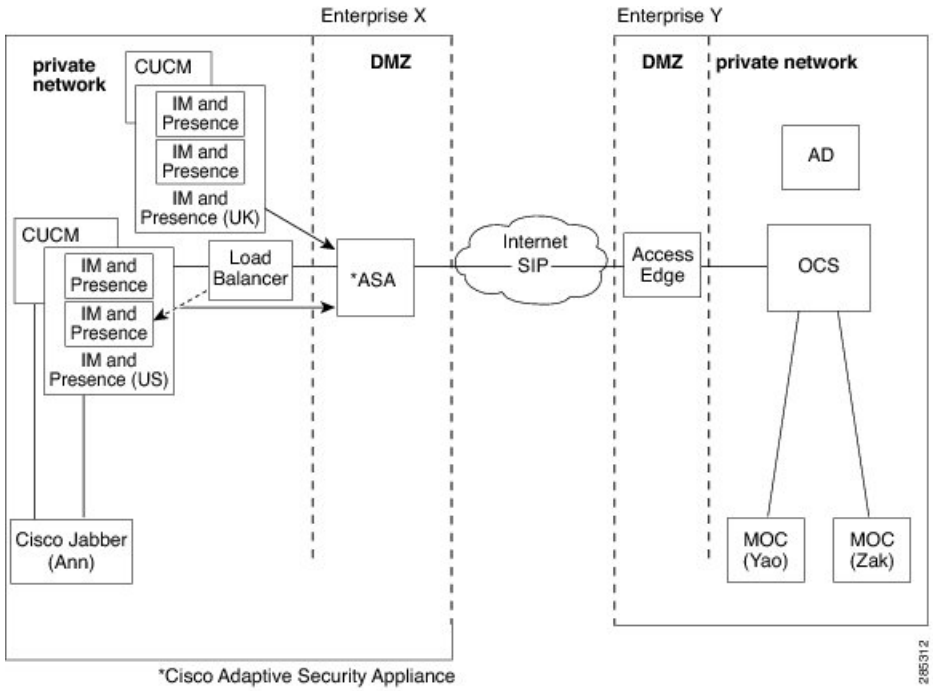
## SIP フェデレーションの高可用性

（注） IM and Presence Service リリース 8.5 以降でのみ高可用性がサポートされます。

Microsoft S4B/Lync とフェデレーションしている場合、Microsoft Access Edge サーバーは、DNS SRV ルックアップで単一のホスト名とサーバーアドレスの戻りのみをサポートします。また、Microsoft Access Edge サーバーは、単一の IP アドレスの手動プロビジョニングのみをサポートします。

したがって、Microsoft S4B/Lync とのフェデレーション時に高可用性を実現するには、次の図に示すように、 IM and Presence Service ノードと Cisco Expressway-C の間にロード バランサを組み込む必要があります。ロードバランサは、Cisco Expressway-C からの着信 TLS 接続を終了し、新しい TLS 接続を開始して、コンテンツを適切なバックエンド IM and Presence Service にルーティングします。

図 *3 :* 高可用性を備えた *IM and Presence Service* と *Microsoft S4B/Lync* 間のフェデレーテッド ネットワーク




**関連情報 -**

SIP フェデレーションの冗長性のためのロード バランサの構成

# XMPP フェデレーションのハイ アベイラビリティ

XMPP フェデレーションのハイ アベイラビリティは、2 ノード サブクラスタ モデルに関連付けられていないため、他の IM and Presence Service 機能のハイ アベイラビリティ モデルとは異なります。

XMPP フェデレーションの高可用性を実現するには、XMPP フェデレーション用にクラスタ内の 2 つ以上の IM and Presence Service ノードを有効にする必要があります。 XMPP フェデレーションに対して複数のノードを有効にすると、スケールが追加されるだけでなく、いずれかのノードに障害が発生した場合の冗長性も提供されます。

## アウトバウンド要求ルーティングのためのハイ アベイラビリティ

IM and Presence Service は、クラスタ内のすべての XMPP フェデレーション対応ノード間で、そのクラスタ内のユーザーからのアウトバウンド要求を均等にロードバランシングします。いずれかのノードに障害が発生した場合、 IM and Presence Service は、クラスタ内の残りのアクティブ ノードにアウトバウンド トラフィックを動的に分散します。

## インバウンド要求ルーティングのためのハイ アベイラビリティ

インバウンド要求ルーティングの高可用性を提供するには、追加の手順が必要です。外部ドメインがローカル IM and Presence Service 展開を検出できるようにするには、DNS SRV レコードをパブリック DNS サーバで公開する必要があります。このレコードは、XMPP フェデレーション対応ノードに解決されます。その後、外部ドメインは解決されたアドレスに接続します。

このモデルで高可用性を提供するには、ローカル IM and Presence Service 展開用に複数の DNS SRV レコードを発行する必要があります。これらの各レコードは、ローカル IM and Presence Service 展開内の XMPP フェデレーション対応ノードの 1 つに解決されます。

これらのレコードは、ローカル展開の DNS SRV レコードの選択肢を提供します。XMPP フェデレーション対応ノードに障害が発生した場合、外部システムには、ローカル IM and Presence Service 展開に接続するための他のオプションがあります。

（注）

- パブリッシュされた各DNS SRV レコードの優先順位と重みは同じである必要があります。これにより、パブリッシュされたすべてのレコードに負荷を分散でき、障害発生時に外部システムが DNS SRV レコードを使用して他のノードの 1 つに正しく再接続できるようになります。
- DNS SRV レコードは、XMPP フェデレーション対応ノードのすべてまたはサブセットに対してパブリッシュできます。パブリッシュされたレコードの数が多いほど、インバウンド要求処理に関するシステムの冗長性が高くなります。
- XMPP フェデレーション展開の IM and Presence Service ノードでチャット機能を構成する場合は、チャット ノード エイリアスの複数の DNS SRV レコードもパブリッシュできます。これにより、XMPPフェデレーション対応ノードで障害が発生した場合、外部システムは別の XMPP フェデレーション ノードを介してその特定のチャット ノードへの別のインバウンド ルートを見つけることができます。これはチャット機能自体のハイ アベイラビリティではなく、チャット ノード エイリアス宛てのインバウンド要求に対する XMPP フェデレーションのハイ アベイラビリティ機能の拡張であることに注意してください。

### IBM SameTime のフェデレーション

IM and Presence Service リリース 9.0 は、 IM and Presence Service エンタープライズと IBM Sametime エンタープライズおよびIBM Sametime エンタープライズ間のドメイン間フェデレーションの高可用性をサポートしていません。これは、IBM Sametime が DNS SRV ルックアップで返された他のレコードを再試行しないためです。見つかった最初の DNS SRV レコードのみを試行し、接続試行が失敗した場合は、重みの低いノードに再試行しません。

（注） IBM Sametime フェデレーション展開の IM and Presence Service で、XMMP フェデレーションの高可用性が発生しているように見える状況が 1 つあります。重要なサービスの障害が原因でユーザーがバックアップ ノードにフェールオーバしたが、Cisco XCP XMPP Federation Connection Managerはプライマリ ノードで実行されたままになります。この場合、着信トラフィックは引き続きプライマリ ノードに転送され、ルータ間接続を使用してバックアップ ノードにリダイレクトされます。ただし、このシナリオでは、XMPPフェデレーションは失敗しておらず、通常どおりに動作し続けることができます。

**関連情報 -**

XMPP フェデレーションの DNS 構成

ノードでの XMPP フェデレーションの有効化

# Cisco適応型セキュリティアプライアンス展開オプション

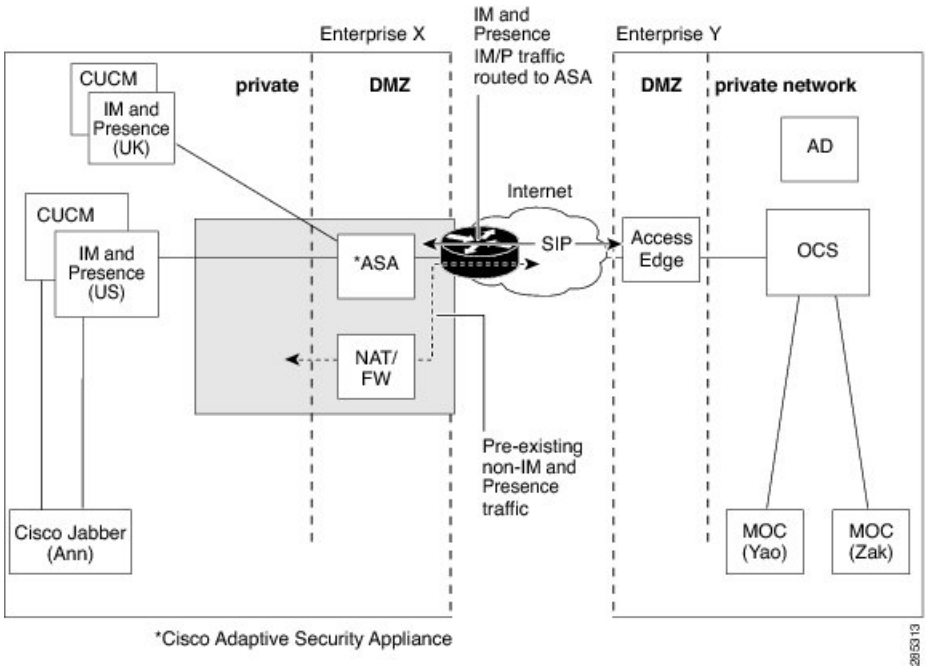
内部 IM and Presence Service 企業展開内で、Cisco 適応型セキュリティ アプライアンス は、パブリック インターネットからの着信接続を終端し、特定のフェデレーション ドメインからのトラフィックを許可するために、DMZ でファイアウォール、ポート アドレス変換（PAT）、および TLS プロキシ機能を提供します。

（注） XMPP フェデレーション展開では、Cisco適応型セキュリティアプライアンスはファイアウォール機能のみを提供します。すでにファイアウォールを展開している場合は、XMPP フェデレーション用の追加の Cisco 適応型セキュリティアプライアンス は必要ありません。

Cisco適応型セキュリティ アプライアンス は、既存のネットワークと展開するファイアウォール機能のタイプに応じて、さまざまな方法で展開できます。このセクションには、推奨される展開モデルの概要のみが含まれています。詳細については、Cisco 適応型セキュリティアプライアンス のマニュアルの展開ガイドラインを参照してください。ここで説明する Cisco適応型セキュリティアプライアンス の導入オプションは、SIP フェデレーションにのみ適用されます。

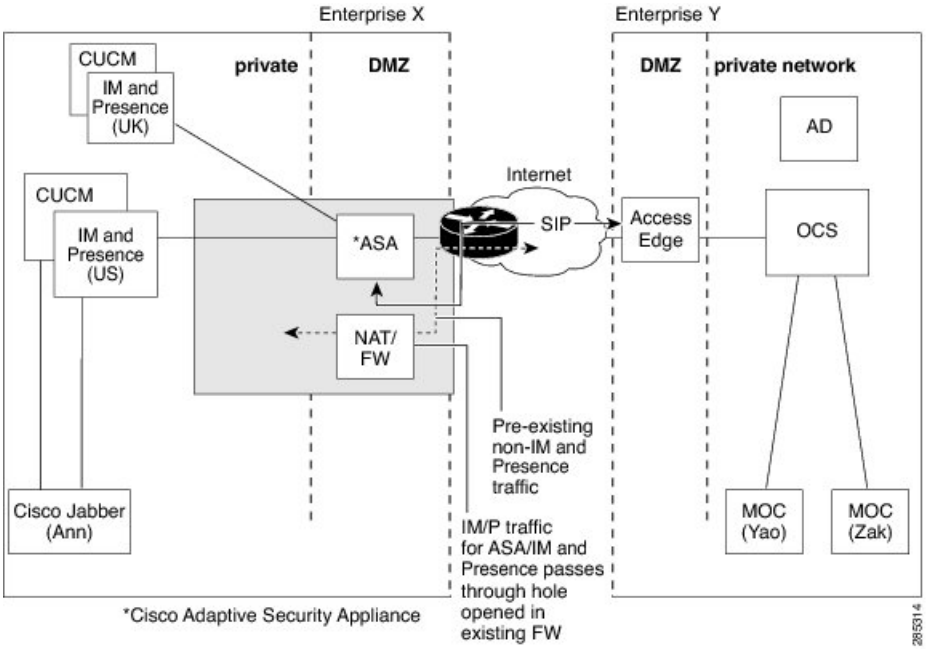
Cisco 適応型セキュリティ アプライアンス は、次の図に示すように、インスタント メッセージング（IM）トラフィック、可用性トラフィック、およびその他のトラフィックを保護するエンタープライズ ファイアウォールとして展開できます。これは最もコスト効率の高い展開であり、新規および既存のネットワークに推奨される展開です。次の図に示すように、既存のファイアウォールと並行して Cisco 適応型セキュリティアプライアンス を展開することもできます。この展開では、Cisco 適応型セキュリティアプライアンス は、IM and Presence Service とパブリックインターネット間の IM and Presence Service トラフィックを処理し、既存のトラフィックは引き続き既存のファイアウォールを使用します。次の図では、Cisco 適応型セキュリティアプライアンス も IM and Presence Service ノードのゲートウェイとして展開されています。つまり、Cisco 適応型セキュリティアプライアンスにトラフィックを転送するために別のルータは必要ありません。

図 *4 :* 既存の *NAT/*ファイアウォールと並行して導入された *Cisco ASA 5500*




また、既存のファイアウォールの背後に Cisco 適応型セキュリティ アプライアンス を展開することもできます。この場合、次の図に示すように、 IM and Presence Service 宛てのトラフィックが Cisco 適応型セキュリティアプライアンスに到達できるように既存のファイアウォールを設定します。このタイプの展開では、Cisco適応型セキュリティ アプライアンス が IM and Presence Service ノードのゲートウェイとして機能します。

図 *5 :* 既存の *NAT/*ファイアウォールの背後に展開された *Cisco ASA 5500*



# Presence サブスクリプションとブロッキング レベル

次の図に示すように、x@externaldomain.comからuser@local.comへのすべての新しいpresenceサブスクリプションは、Cisco Expressway-Cによって送信されます。Cisco Expressway-Cは、許可された外部ドメインのリストに対して着信 SIP サブスクリプションをチェックします。ドメインが許可されていない場合、Cisco Expressway-C は presence サブスクリプションを拒否します。

（注） XMPP フェデレーション展開では、Cisco Expressway-C はドメイン チェックを実行しません。

IM および Presence サービスは、インバウンド サブスクリプションを受信すると、外部ドメインが IM および Presence サービス ノードの管理レベルで定義した許可されたフェデレーション ドメインの 1 つであることを確認します。SIP フェデレーションの場合は、フェデレーション ドメインを構成します。XMPP フェデレーションの場合は、XMPP フェデレーションの管理者ポリシーを定義します。サブスクリプションが許可されたドメインからのものでない場合、IM および Presence サービスはサブスクリプションを拒否します（ローカル ユーザーに連絡することはありません）。

サブスクリプションが許可されたドメインからのものである場合、 IM および Presence サービスはローカルユーザーの許可ポリシーをチェックして、ローカルユーザーが以前にフェデレーテッド ドメインまたは Presence サブスクリプションを送信しているユーザーをブロックまたは許可していないことを確認します。 IM および Presence サービスは、着信サブスクリプションを受け入れ、保留状態にします。

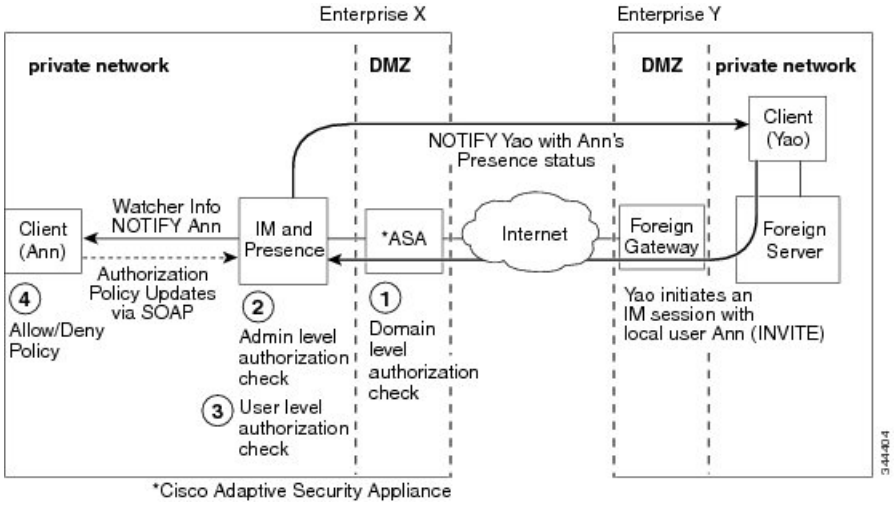
IM および Presence サービスは、クライアント アプリケーションにサブスクリプションの通知メッセージを送信することで、x@externaldomain.comがプレゼンスを監視することをローカル ユーザに通知します。これにより、ローカル ユーザーがサブスクリプションを許可または拒否できるようにするダイアログ ボックスがクライアント アプリケーションに表示されます。ユーザーが承認の決定を行うと、クライアント アプリケーションはその決定を IM および Presence サービスに通知します。許可の決定は、IM および Presence サービスに保存されているユーザーのポリシー リストに追加されます。

（注） サードパーティの XMPP クライアントは、ユーザーのポリシー リストを更新せず、サブスクリプションを受け入れるだけです。ユーザーは、 IM および Presence サービスのユーザー オプション インターフェイスでプライバシー リストを手動で更新できます。

拒否の決定は、ポライトブロッキングを使用して処理されます。これは、ユーザーの presence 状態が外部クライアントでオフラインに表示されることを意味します。ローカルユーザーがサブスクリプションを許可すると、 IM および Presence サービスは presence の更新を外部ウォッチャに送信します。

ユーザーは、ユーザー単位およびドメイン単位でサブスクリプションをブロックすることもできます。これは、Cisco Jabber クライアントで構成可能です。

**図 *6 :* 着信 *SIP Presence* メッセージ フロー**

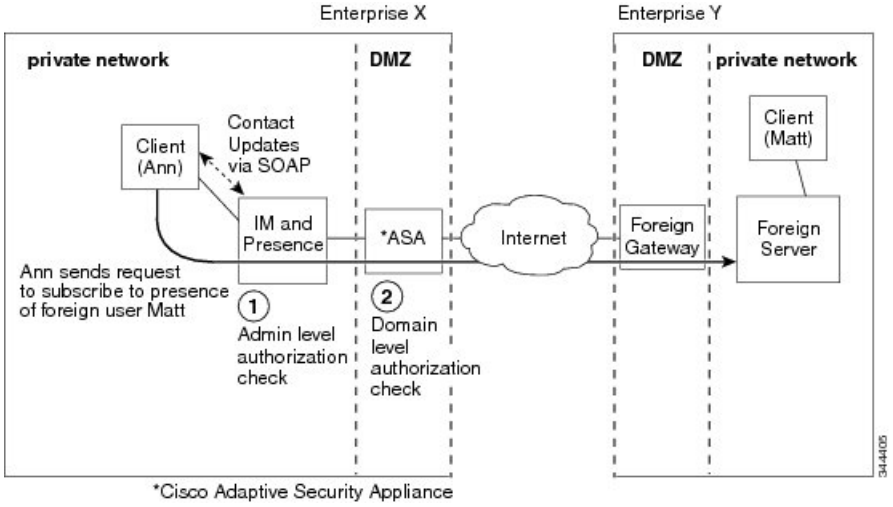



IM および Presence サービスは、Cisco Expressway-C を介してすべての発信サブスクリプションを送信し、Cisco Expressway-C はこれらのサブスクリプションを外部ドメインに転送します。IM および Presence サービスは、異なるローカル ユーザーから同じ外部ドメイン内の同じ外部ユーザーにアクティブなサブスクリプションがすでに存在する場合でも、発信サブスクリプションを送信します。次の図は、発信 presence サブスクリプション フローを示しています。

外部ユーザーは、クライアント アプリケーションおよび **IM および Presence サービスのユーザー オプション** インターフェイスの連絡先リストに `user@externaldomain.com`として追加されます。

（注） ドメイン レベルの認証チェックは、XMPP フェデレーション用の Cisco Expressway-C には適用されません。

図 *7:* アウトバウンド *Presence* 要求フロー




（注）

- Microsoft S4B/Lync は、1 時間 45 分ごとに更新サブスクライブを実行します。したがって、IM および Presence サービス ノードが再起動した場合、Microsoft S4B/Lync クライアントで IM および Presence サービス コンタクトの Presence ステータスがない最大時間は約 2 時間です。
- Microsoft S4B/Lync が再起動した場合、IM および Presence サービス クライアントで Microsoft S4B/Lync 連絡先の Presence ステータスがない最大時間は約 2 時間です。

**関連情報 -**

可用性状態マッピング

インスタント メッセージ

# 可用性状態マッピング

このセクションでは、可用性状態マッピングのさまざまな概念について説明します。

## Microsoft OCS の可用性状態マッピング

次の表に、Microsoft Office Communicator から IM and Presence Service、サードパーティの XMPP クライアント、および Cisco Jabberへの可用性マッピングの状態を示します。

表 *2 : Microsoft Office Communicator* からの可用性マッピングの状態

| Microsoft Office Communicator 設定 | サードパーティ XMPP クライアント設定（IM and Presence Service に接続） | Cisco Jabber リリース 8.x の設定 |
|---|---|---|
| 利用可能 | 利用可能 | 利用可能 |
| 取り込み中 | 退席中 | ビジー |
| サイレント | 退席中 | ビジー |
| すぐに戻る | 退席中 | 退席中 |
| 退席中 | 退席中 | 退席中 |
| Offline | Offline | Offline |

この表では、Microsoft Office Communicator の「ビジー」状態と「応答不可」状態は、サードパーティの XMPP クライアントで「ビジー」というステータステキストとともに「退席中」にマッピングされます。XMPP クライアントは、この「退席中」ステータスのレンダリング方法が異なります。たとえば、特定の XMPP クライアントには、テキストなしで「退席中」アイコンが表示されます。他の XMPP クライアントは、横に「ビジー」テキスト注釈付きの「退席中」アイコンをレンダリングします。

次の表に、 Cisco Jabber リリース 8.x から Microsoft Office Communicator への可用性マッピングの状態を示します。

表 *3 : Cisco Jabber* リリース *8.x* からの可用性マッピング状態

| Cisco Jabber リリース 8.x の設定 | Microsoft Office Communicator 設定 |
|---|---|
| 利用可能 | 利用可能 |
| ビジー（Busy） | ビジー |
| サイレント | ビジー |
| Offline | Offline |

次の表に、 IM and Presence Service に接続されているサードパーティ製 XMPP クライアントから Microsoft Office Communicator への可用性マッピングの状態を示します。

表 *4 :* サードパーティ製 *XMPP* クライアントからの可用性マッピングの状態

| サードパーティ XMPP クライアント設定（IM and Presence Serviceに接続） | Microsoft Office Communicator 設定 |
|---|---|
| 応答可能 | 応答可能 |
| 退席中 | 退席中 |
| 退席中（Extended Away） | 退席中 |
| サイレント | ビジー |
| Offline | オフライン |

### 関連情報

Presence サブスクリプションとブロッキング レベル

# Microsoft Lync の可用性状態マッピング

次の表に、Microsoft Lync から IM and Presence Service、サードパーティの XMPP クライアント、および Cisco Jabberへの可用性マッピングの状態を示します。

表 *5 : Microsoft Lync* からの可用性マッピングの状態

| Microsoft Lync[MicrosoftLync] 設定 | サードパーティ XMPP クライアント設定（IM and Presence Service に接続） | Cisco Jabber リリース 8.x 設定 |
|---|---|---|
| 利用可能 | 利用可能 | 利用可能 |
| 取り込み中 | 退席中 | ビジー |
| サイレント | 退席中 | ビジー |
| すぐに戻ります | 退席中 | 退席中 |
| 退席中 | 退席中 | 退席中 |
| Offline | Offline | Offline |

この表では、Lync クライアントの「ビジー」状態と「応答不可」状態は、サードパーティ製 XMPP クライアントのステータステキストが「ビジー」の状態で「退席中」にマッピングされます。XMPP クライアントは、この「退席中」ステータスの表示方法が異なります。たとえば、あるXMPPクライアントは、テキストなしで「退席中」アイコンを表示します。他のXMPPクライアントは、「ビジー」テキスト注釈の横に 「退席中」アイコンを表示する。

次の表に、 Cisco Jabber リリース 8.x から Lync クライアントへの可用性マッピングの状態を示します。

**表 *6 : Cisco Jabber* リリース *8.x* からの可用性マッピング状態**

| **Cisco Jabber**<br>**リリース 8.x 設定** | **Microsoft Lync[MicrosoftLync]**<br>**設定** |
|---|---|
| 利用可能 | 利用可能 |
| ビジー（Busy） | ビジー |
| サイレント | ビジー |
| Offline | Offline |

次の表に、 IM and Presence Serviceに接続されているサードパーティ製 XMPP クライアントから Lync クライアントへの可用性マッピングの状態を示します。

**表 *7 :* サードパーティ製 *XMPP* クライアントからのアベイラビリティ マッピングの状態**

| **サードパーティ XMPP クライアント設定（ IM and Presence Serviceに接続）** | **Microsoft Lync[MicrosoftLync]**<br>**設定** |
|---|---|
| 利用可能 | 使用可能 |
| 退席中 | 退席中 |
| Extended Away | 退席中 |
| サイレント | ビジー |
| Offline | オフライン |

**関連情報 -**

Presence サブスクリプションとブロッキング レベル

# XMPP フェデレーションの可用性状態マッピング

次の表に、IBM Sametime 8.2 から IM and Presence Service上のサードパーティ XMPP クライアントおよび Cisco Jabberへの可用性マッピング状態を示します。

表 *8 : IBM Sametime 8.2* クライアントからの可用性マッピングの状態

| IBM Sametime クライアント設定 | サードパーティ XMPP クライアント設定（IM and Presence Service に接続） | Cisco Jabber<br>リリース 8.x の設定 |
|---|---|---|
| 利用可能 | 利用可能 | ステータス メッセージで使用可能 |
| サイレント | 応答不可（Do Not Disturb） | 応答不可（ステータス メッセージあり） |
| ステータスが「[ミーティング中（In a meeting）]」で使用可能 | ステータスが「[ミーティング中（In a meeting）]」で使用可能 | ステータス メッセージで使用可能 |
| 退席中 | 退席中 | 退席中（ステータス メッセージあり） |
| Offline | Offline | オフライン |

次の表に、webex Connect から IM and Presence Service 上のサードパーティ XMPP クライアントおよび Cisco Jabberへの可用性マッピングの状態を示します。

表 *9 : Webex Connect* からの可用性マッピングの状態

| Webex Connect の設定 | サードパーティ XMPP クライアント設定（IM and Presence Service に接続） | Cisco Jabber<br>リリース 8.x の設定 |
|---|---|---|
| 利用可能 | 利用可能 | 利用可能 |
| サイレント | サイレント | 応答不可（Do Not Disturb） |
| 退席中（ステータスは「ミーティング中」） | 在席（ステータスが「ミーティング中」] | 退席中（ステータス「は会議中）」 |
| 退席中 | 退席中 | 退席中 |
| Offline | Offline | Offline |

次の表に、 Cisco Jabber リリース 8.x から他のフェデレーテッド クライアントへの可用性マッピング状態を示します。

表 *10 : Cisco Jabber* リリース *8.x* からの可用性マッピング状態

| Cisco Jabber リリース 8.x の設定 | フェデレーテッド Cisco Jabber リリース 8.x の設定 | フェデレーテッド サードパーティ XMPP クライアント設定（IM and Presence Service に接続） | Webex Connect クライアント設定 | IBM Sametime クライアント サーバー |
|---|---|---|---|---|
| 利用可能 | 利用可能 | 利用可能 | 利用可能 | 利用可能 |
| サイレント | サイレント | サイレント | サイレント | 応答不可（Do Not Disturb） |
| ビジー（Busy） | ビジー | 退席中 | アイドル（Idle） | 退席中 |
| アイドル | アイドル | アイドル | アイドル | アイドル |
| Offline | Offline | Offline | Offline | Offline |

次の表に、IM and Presence Service 上のサードパーティ XMPP クライアントから他のフェデレーテッド クライアントへの可用性マッピング状態を示します。

表 *11 : IM and Presence Service*に接続された *XMPP* クライアントからのアベイラビリティ マッピングの状態

| サードパーティ XMPP クライアント設定（IM and Presence Service に接続） | フェデレーテッド Cisco Jabber リリース 8.x の設定 | フェデレーテッド XMPP クライアント設定（IM and Presence Service に接続） | Webex Connect クライアント設定 | IBM Sametime クライアント サーバー |
|---|---|---|---|---|
| 利用可能 | 利用可能 | 利用可能 | 利用可能 | 利用可能 |
| サイレント | サイレント | サイレント | サイレント | 応答不可（Do Not Disturb） |
| 退席中 | 退席中 | 退席中 | 退席中 | 退席中 |
| 退席中（Extended Away） | 退席中 | 退席中（Extended Away） | 退席中（Extended Away） | 退席中 |
| 退席中（ステータスが 「アイドル」） | アイドル（Idle） | 退席中（ステータスが 「アイドル」） | 退席中（ステータスが 「アイドル」） | 退席中（ステータスが 「アイドル」） |
| Offline | Offline | Offline | Offline | Offline |

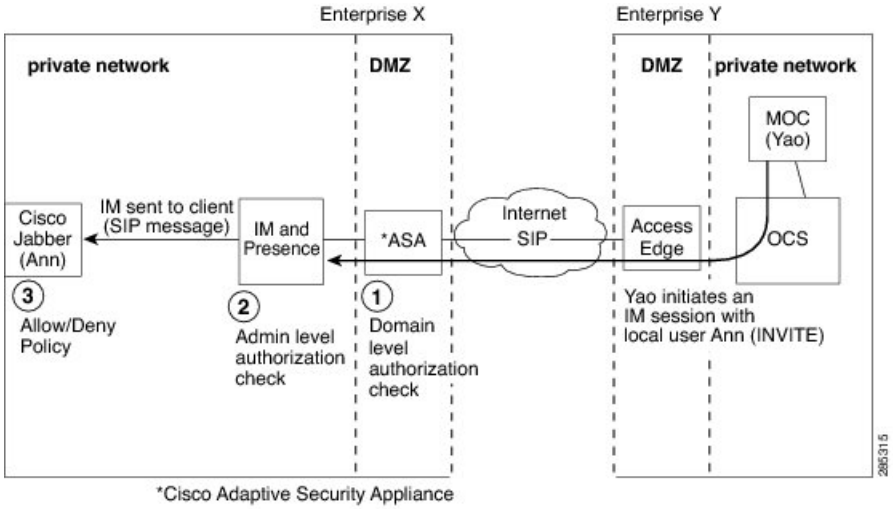
# インスタント メッセージ

このセクションでは、次の点について説明します。

## SIP フェデレーションのインスタント メッセージ フロー

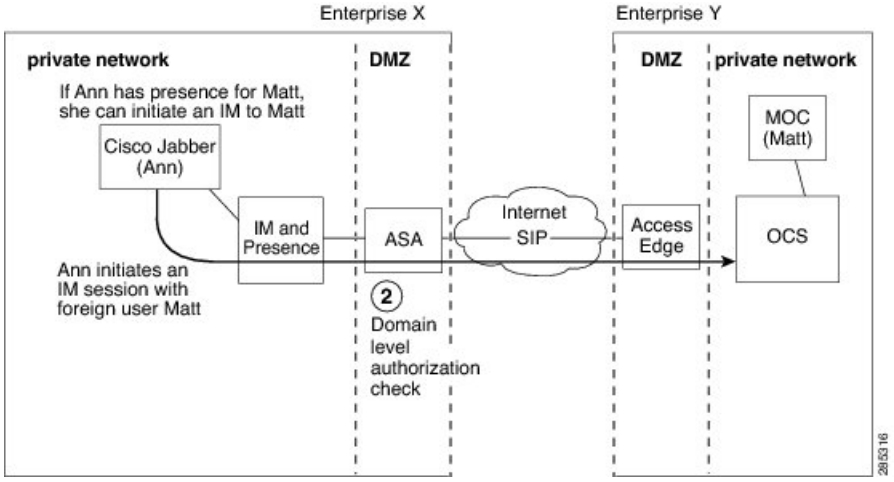
2 つのエンタープライズ展開間で送信されるインスタント メッセージ（IM）は、セッション モードを使用します。外部ドメインのユーザーが IM and Presence Service ドメインのローカル ユーザーに IM を送信すると、次の図に示すように、外部サーバーは INVITE メッセージを送信します。 Expressway-C は INVITE メッセージを IM and Presence Serviceに転送します。IM and Presence Service は外部サーバーに 200 OK メッセージで応答し、外部サーバーはテキスト データを含む SIP MESSAGE を送信します。 IM and Presence Service は、適切なプロトコルを使用して、ローカル ユーザーのクライアント アプリケーションにテキスト データを転送します。

**図 *8:* インバウンド インスタント メッセージング フロー**




IM and Presence Service ドメインのローカル ユーザが外部ドメインのユーザーに IM を送信すると、IM は IM and Presence Service ノードに送信されます。これら 2 人のユーザー間に既存の IM セッションが確立されていない場合、IM and Presence Service は INVITE メッセージを外部ドメインに送信して新しいセッションを確立します。次の図は、このフローを示しています。IM and Presence Service は、これら 2 人のユーザのいずれかからの後続の MESSAGE トラフィックにこのセッションを使用します。Cisco Jabber およびサードパーティ製の XMPP クライアントのユーザは、対応可能でない場合でも IM を開始できます。

図 *9:* アウトバウンド インスタント メッセージ フロー




（注） IM and Presence Service は、Microsoft S4B/Lync 連絡先との三者間 IM セッション（グループ チャット）をサポートしていません。

**関連情報 -**

Presence サブスクリプションとブロッキング レベル

# XMPP フェデレーションの可用性とインスタント メッセージ フロー

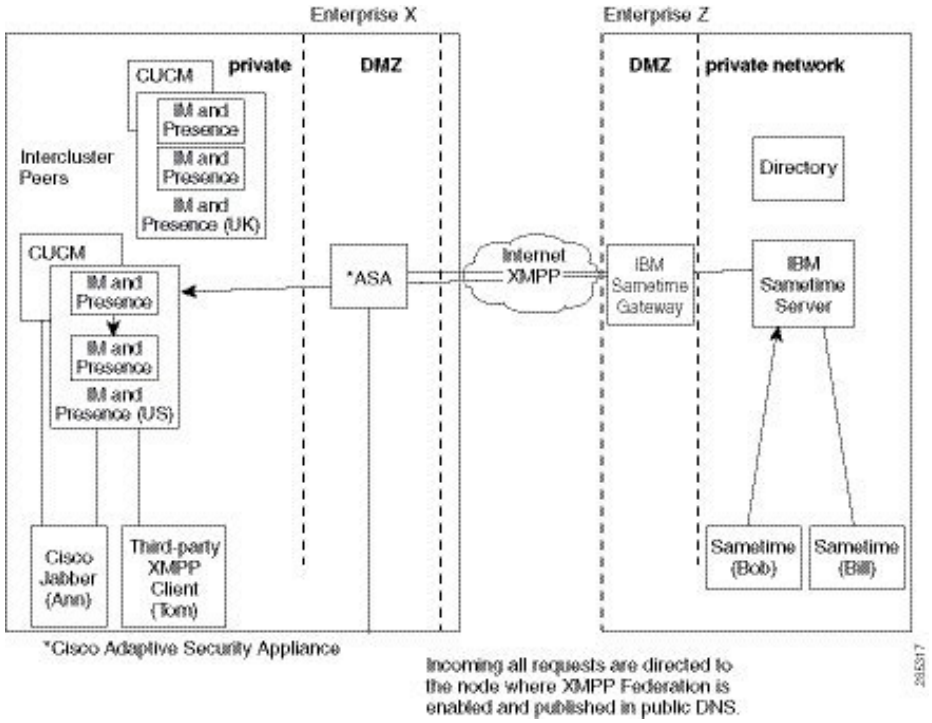
XMPP フェデレーションの着信および発信の可用性と IM 要求のフローは、マルチノード IM and Presence Service の展開によって異なる場合があります。

マルチノード展開では、クラスタ内の各ノードで XMPP フェデレーションを有効にすることも、クラスタ内の単一ノードでのみ有効にすることもできます。さらに、単一の DNS SRV レコードのみを公開するか、複数の DNS SRV レコード（XMPP フェデレーションを有効にするノードごとに 1 つのレコード）を公開するかを決定できます。

単一の DNS SRV レコードのみをパブリッシュする場合、システムはすべてのインバウンド要求をその単一ノードにルーティングし、 IM and Presence Service は、次の図に示すように、クラスタ間ルーティングを使用してトラフィックを内部的に正しいノードにルーティングします。複数の DNS SRV レコードをパブリッシュする場合、SRV レコードの構成方法に応じて、システムは各ノード間でインバウンド要求をロードバランシングする可能性があります。

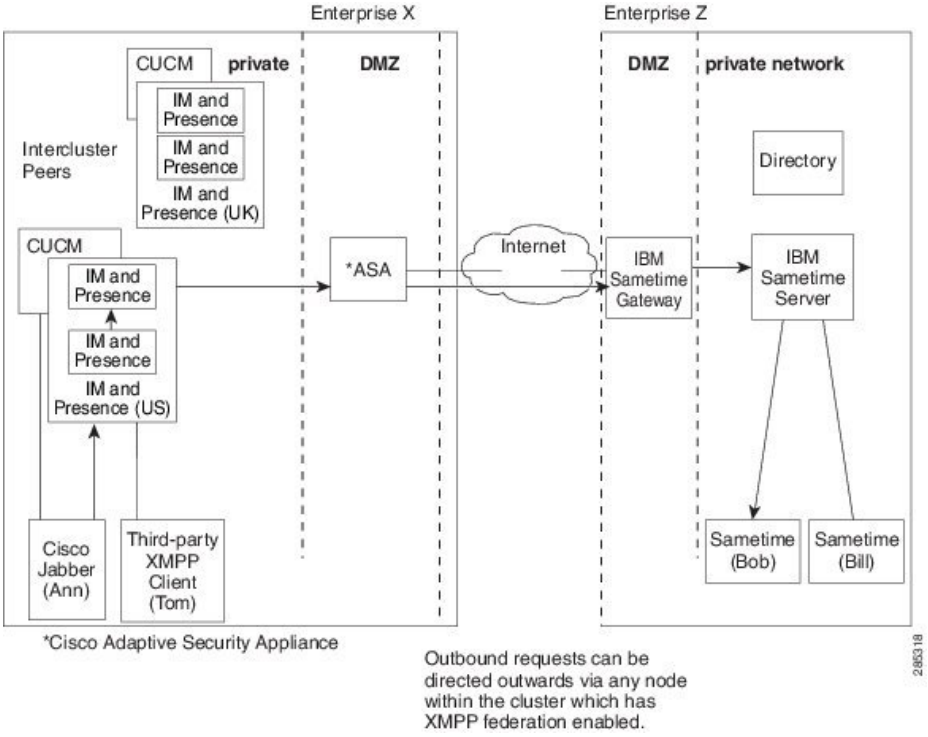
マルチクラスタ XMPP フェデレーション ネットワークのインバウンド メッセージ フローを示すこの図では、両方のクラスタでフェデレーションが有効になっています。着信メッセージは、宛先クラスタ内のフェデレーション対応ノードに直接送信されます。フェデレーション対応ノードは、メッセージを適切なクラスタ ノードに再ルーティングします。

図 *10 : XMPP* インバウンド要求フロー




IM and Presence Service は、次の図に示すように、XMPP フェデレーションを有効にしたクラスタ内の任意のノードに発信要求をルーティングします。この図では、フェデレーションは両方のピア クラスタで有効になっていますが、アウトバウンド フローはピア クラスタにヒットしません。

図 *11 : XMPP* アウトバウンド要求フロー




**関連情報 -**

XMPP フェデレーションのハイ アベイラビリティ

# 複数のドメインを含む展開でのフェデレーション

フェデレーションは、リモート ドメインがローカル IM and Presence Service 展開によって管理されていない場合、複数のドメインを含む IM and Presence Service 展開で完全にサポートされます。

ローカル クラスタ内のすべてのユーザーに対してフェデレーションを有効にするには、すべてのローカル ドメインの DNS レコードを作成する必要があります。

XMPP フェデレーションの場合、 cup-xmpp セキュリティ証明書には、すべてのローカル ドメインがサブジェクト代替名として含まれている必要があります。

# フェデレーションとサブドメイン

次のサブドメインが IM and Presence Service でサポートされています。

- IM and Presence Service が外部ドメインのサブドメインに属しています。たとえば、IM and Presence Service はサブドメイン「imp.cisco.com」に属します。IM and Presence Service は、ドメイン「cisco.com」に属する外部企業とフェデレーションします。この場合、 IM and

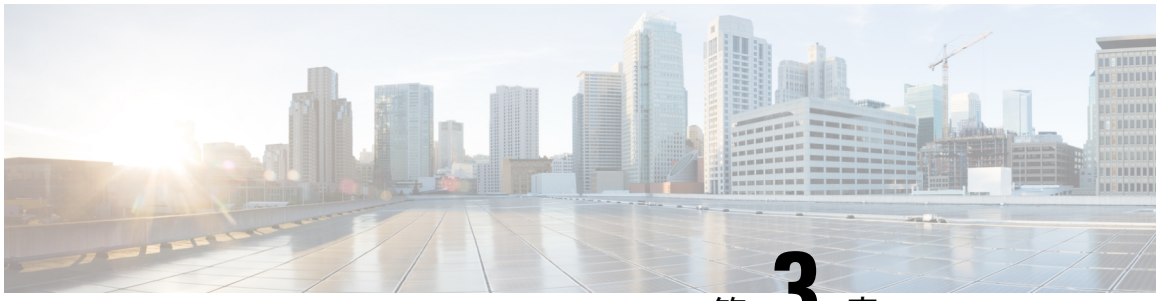
Presence Service ユーザーには「impuser@imp.cisco.com」という URI が割り当てられ、外部ユーザーには「foreignuser@cisco.com」という URI が割り当てられます。

- IM and Presence Service は親ドメインに属し、外部エンタープライズはその親ドメインのサブドメインに属します。たとえば、 IM and Presence Service はドメイン「cisco.com」に属します。 IM and Presence Service は、サブドメイン「foreign.cisco.com」に属する外部企業とフェデレーションします。この場合、 IM and Presence Service ユーザーには URI「impuser@cisco.com」が割り当てられ、外部ユーザーには URI「foreignuser@foreign.cisco.com」が割り当てられます。
- IM and Presence Service と外部エンタープライズはそれぞれ異なるサブドメインに属していますが、これらのサブドメインは両方とも同じ親ドメインに属しています。たとえば、IM and Presence Service はサブドメイン「cup.cisco.com」に属し、外部企業はサブドメイン「foreign.cisco.com」に属します。これらのサブドメインは両方とも、親ドメイン「cisco.com」に属します。この場合、 IM and Presence Service ユーザには URI「impuser@cup.cisco.com」が割り当てられ、外部ユーザーには URI「foreignuser@foreign.cisco.com」が割り当てられます。

サブドメインとフェデレーションする場合は、個別の DNS ドメインを設定するだけで済みます。 Active Directory を分割する必要はありません。企業内でフェデレーションを設定する場合、 IM and Presence Service ユーザーまたは外部ユーザーは同じ Active Directory ドメインに属することができます。たとえば、上記の 3 番目のシナリオでは、Active Directory は親ドメイン「cisco.com」に属することができます。ユーザーがサブドメイン「imp.cisco.com」または「foreign.cisco.com」に属し、URI が「impuser@」である場合でも、Active Directory の「cisco.com」ドメインの下にすべてのユーザーを設定できます。「imp.cisco.com」または「foreignuser@foreign.cisco.com」。

Cisco Jabber からの LDAP 検索で他のドメインまたはサブドメインのユーザーが返される場合がありますが、 Cisco Jabber ユーザーは CiscoJabber の LDAP ルックアップからこれらのフェデレーション ユーザーを追加できないことに注意してください。Cisco Jabber ユーザは、 IM and Presence Service がローカル ドメインではなく正しいドメインを適用するように、これらのユーザを外部（フェデレーション）連絡先として追加する必要があります。

（注） 2 つの IM and Presence Service エンタープライズ展開間でフェデレーションを設定する場合、IM and Presence Service は上記のシナリオもサポートします。



第 3 章

# この統合の準備

このセクションでは、この統合の準備について説明します。



## サポートされているドメイン間フェデレーション統合

このドキュメントでは、 IM and Presence Service ノードと外部ドメイン間のフェデレーテッション ネットワークを設定するための設定手順について説明します。

IM and Presence Service ノードがフェデレーションできるサポート対象の外部ドメインは次のとおりです。

- SIP を介した Microsoft Office 365（ビジネス間）
- SIP を介した Microsoft Skype for Business 2015（ビジネス間）
- SIP を介した Microsoft Lync 2010 および 2013

（注） IM and Presence Service は、Microsoft Lync/S4B とのドメイン間フェデレーションをサポートします。Microsoft Lync/S4B とのドメイン間フェデレーションへの言及には、特に明記されていない限り、Microsoft Office 365 も含まれます。

- XMPP を介した Cisco Webex Messenger
- XMPP を介した IBM Sametime サーバー リリース 8.2、8.5
- XMPP を介した IM and Presence Service リリース 9.x 以降

（注） IM and Presence Service エンタープライズ間でフェデレーションを行う場合は、XMPP フェデレーションの設定方法を説明する手順に従います。

**関連情報 -**

Hardware Requirements

ソフトウェア要件

# Presence Web Service API のサポート

Presence Web Service は、クライアント アプリケーションが IM and Presence Service とユーザー プレゼンス情報を共有できるようにするオープンインターフェイスです。サードパーティの開発者は、このインターフェイスを使用して、ユーザーのプレゼンス状態に関する更新を送信および取得できるクライアント アプリケーションを構築します。Presence Web Service API のサポートに関する次の制限事項に注意してください。

- SIP を介したドメイン間フェデレーションの場合、Presence Web Service API を使用して、Cisco以外のクライアントから豊富なプレゼンス情報を取得できますが、Cisco以外のクライアントの基本的なプレゼンスはサポートされていません。
- XMPP を介したドメイン間フェデレーションの場合、Presence Web Service API を使用してシスコ以外のクライアントからプレゼンス情報を取得することはできません。

Presence Web Service の詳細については、https://developer.cisco.com/site/collaboration/call-control/unified-presence/documentation/index.gsp にある 『*IM and Presence Service Developer Guide*』 を参照してください。

# Hardware Requirements

### Cisco Hardware

- IM and Presence Service node. For IM and Presence Service hardware support, refer to the IM and Presence Service compatibility matrix
- Cisco Unified Communications Manager node. For Cisco Unified Communications Manager hardware support, refer to the Cisco Unified Communications Manager compatibility matrix
- Two DNS servers within the IM and Presence Service enterprise
- Cisco Expressway-C 5500 Series
- We only recommend the Cisco Expressway-C for SIP federation as it provides the TLS proxy functionality. For XMPP federation, any firewall is sufficient.
- When selecting a Cisco Expressway-C model, go to: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_models_home.html. The TLS proxy component is available on all 5500 models.

- Make sure you use the correct version of Cisco Expressway-C software for your deployment. If you are configuring a new interdomain federation deployment, refer to the IM and Presence Service compatibility matrix for the correct version of Cisco Expressway-C software.

**Related Information -**

Compatibility Information

ソフトウェア要件

# ソフトウェア要件

### シスコソフトウェア

- IM and Presence Service
- Cisco Unified Communications Manager
- Cisco 適応型セキュリティ アプライアンス v8.3(1) 以降
- Cisco Adaptive Security Device Manager（ASDM）v6.3 以降
- サポートされる XMPP クライアント：
  - Cisco Unified Personal Communicator リリース8.5
  - Cisco Jabber for Mac
  - Windows 版 Cisco Jabber
  - Cisco Jabber IM for Mobile（iPhone、Android、Blackberry）
  - Cisco Jabber for iPad
  - Cisco Jabber for Cius

### SIP フェデレーション用 Microsoft ソフトウェア

- Microsoft Office 365（business to business）
- Microsoft Skype for Business Server 2015、Standard Edition または Enterprise Edition
- Microsoft Lync 2013 または 2010、Standard Edition または Enterprise Edition

### XMPP フェデレーション用ソフトウェア

- Cisco Webex Messenger
- IBM Sametime サーバ リリース 8.2

### 関連項目 -

Hardware Requirements

# 統合の準備

この統合を慎重に計画することが不可欠です。この統合の構成を開始する前に、このセクションの項目をお読みください。

## ルーティング設定

フェデレーテッドネットワークでルーティングを設定する方法を検討してください。外部ドメイン アドレス宛てのメッセージを IM and Presence Service から Cisco Expressway-C を介して外部ドメインにルーティングする方法を検討してください。IM and Presence Service エンタープライズ展開と Cisco Expressway-Cの間にルーティング エンティティ（ルータ、スイッチ、またはゲートウェイ）を展開することを検討できます。ルーティングエンティティはメッセージを Cisco Expressway-C にルーティングし、Cisco Expressway-C はこれらのメッセージを外部ドメインにルーティングします。

また、 IM and Presence Service と外部ドメイン間のゲートウェイとして Cisco Expressway-C を展開することもできます。Cisco Expressway-C を IM and Presence Serviceのゲートウェイとして使用する場合は、ローカルエンタープライズ展開内で、 Cisco Unified Communications Manager および IM and Presence Service クライアントが IM and Presence Service ノードにアクセスする方法を考慮する必要があります。Cisco Unified Communications Manager と IM and Presence Service クライアントが IM and Presence Service とは異なるサブネットにある場合は、Cisco Expressway-C を使用して IM and Presence Service にアクセスする必要があります。

ネットワーク内の既存のファイアウォールの背後に Cisco Expressway-C を展開する場合は、Cisco Expressway-C および IM and Presence Serviceにトラフィックをルーティングする方法を検討してください。既存のファイアウォールで、パブリック IM and Presence Service アドレスにトラフィックをルーティングするようにルートとアクセスリストを設定します。また、既存のファイアウォールを使用して外部ドメインへのルートを設定する必要があります。

### 関連情報

Cisco 適応型セキュリティアプライアンス展開オプション

## パブリック IP アドレス

SIP フェデレーションの場合、パブリック IM and Presence Service アドレスのパブリックにアクセス可能な IP アドレスが必要です。割り当て可能な IP アドレスがない場合は、Cisco Expressway-C の外部インターフェイスをパブリック IM and Presence Service アドレスとして使用します（Cisco Expressway-C を可用性と IM トラフィックにのみ使用する場合）。

XMPP フェデレーションの場合、XMPP フェデレーションを有効にする各 IM and Presence Service ノードのパブリック IP アドレスを公開するか、単一のパブリック IP アドレスを公開するかを選択できます。

- 複数の IP アドレスを公開する場合は、Cisco Expressway-C で NAT を使用してパブリック アドレスをプライベート アドレスに変換します。たとえば、NAT を使用して、パブリッ

クアドレス xxxx:5269 と yyyy:5269 をそれぞれプライベートアドレス aaaa:5269 と bbbb:5269 に変換できます。

- 単一の IP アドレスを公開する場合は、Cisco Expressway-C で PAT を使用して正しい IM and Presence Service ノードにマッピングします。たとえば、展開内のパブリック IP アドレスは x.x.x.x であり、_xmpp-server には複数の DNS SRV レコードがあります。各レコードには異なるポートがありますが、すべてのレコードは x.x.x.x に解決されます外部サーバーは、Cisco Expressway-Cを介して x.x.x.x:5269、x.x.x.x:15269、x.x.x.x:25269 に要求を送信します。Cisco Expressway-C は IP アドレスに対して PAT を実行し、各 IM and Presence Service ノードの対応する内部 IP アドレスに各アドレスをマッピングします。

  たとえば、パブリック IP アドレス x.x.x.x:5269 はプライベート IP アドレス a.a.a.a:5269 にマッピングされ、パブリック IP アドレス x.x.x.x:15269 はプライベート IP アドレス b.b.b.b.b:5269 にマッピングされ、パブリック IP アドレス x.x.x.x:25269 はプライベート IP address c.c.c.c:5269 などにマッピングされます。すべての IP アドレスは、 IM and Presence Serviceの同じポート（5269）に内部的にマッピングされます。

**関連情報 -**

外部および内部インターフェイスの構成

DNS の設定

# パブリック FQDN

SIP フェデレーションの場合、要求メッセージは FQDN に基づいてルーティングされます。したがって、ルーティング IM and Presence Service ノード（パブリッシャ）の FQDN は、パブリックに解決可能である必要があります。

# AOL SIP アクセス ゲートウェイ

AOL SIP（ソリューション インセンティブ プログラム）アクセス ゲートウェイは、企業の SIP/SIMPLE ベースのインスタント メッセージング サーバーがネットワーク上の他のインスタント メッセージング ユーザーと通信できるようにするフェデレーテッド サービスを提供します。AOL SIP アクセスゲートウェイを使用すると、企業の SIP/SIMPLE ベースのメッセージングサーバーのユーザーは、AIM または AOL サービスのパブリックユーザーの可用性情報を取得し、会話を行うことができます。また、AOL SIP アクセスゲートウェイを使用すると、AIM または AOL システムのユーザーは、インスタントメッセージを送信したり、社内の SIP/SIMPLE ベースのシステムのユーザーに対応可否情報を表示したりできます。

AOL SIP アクセスゲートウェイは、内部 AOL プロトコルのトランスレータへのフロントエンドとして機能します。会社のサーバーと AOL 間のすべての通信は SIP を使用します。AOL SIP アクセス ゲートウェイは、内部 AOL システムに必要なプロトコルへの変換を処理します。外部サーバーに変換機能を追加する必要はありません。その観点から、AOL プロトコルは非表示になります。会社のサーバーが SIP/SIMPLE を使用して通信する場合は、AOL SIP アクセスゲートウェイを介して AOL に接続できます。

AOL SIP アクセス ゲートウェイは、TCP を介した TLS による接続のみをサポートします。AOL SIP アクセス ゲートウェイ サーバーは、次のアドレスを使用して、インスタント メッセージング サーバーまたはプロキシ内で定義する必要があります。

サーバー名： `sip.oscar.aol.com`

サーバー ポート：5061

サーバー名 `sip.oscar.aol.com` は、205.188.153.55 および 64.12.162.248 に解決されます。

（注）
- これらの IP アドレスをネットワーク内の任意の場所で静的に設定する場合は、これらのアドレスが変更されていないか定期的に AOL に確認することを推奨します。
- IP アドレスは変更される可能性があるため、AOL SIP アクセスゲートウェイ（sip.oscar.aol.com）の FQDN に ping を実行して IP アドレスを確認することをお勧めします（例： **`ping sip.oscar.aol.com`** ）。

# 冗長性/ハイ アベイラビリティ

フェデレーテッドネットワークで冗長性をどのように設定するかを検討する必要があります。Cisco Expressway-C は、アクティブ/スタンバイ（A/S）展開モデルを提供することで冗長性をサポートします。

IM and Presence Service フェデレーション機能の可用性を高くする場合は、指定された（フェデレーション） IM and Presence Service クラスタの前にロード バランサを展開できます。

# DNS の設定

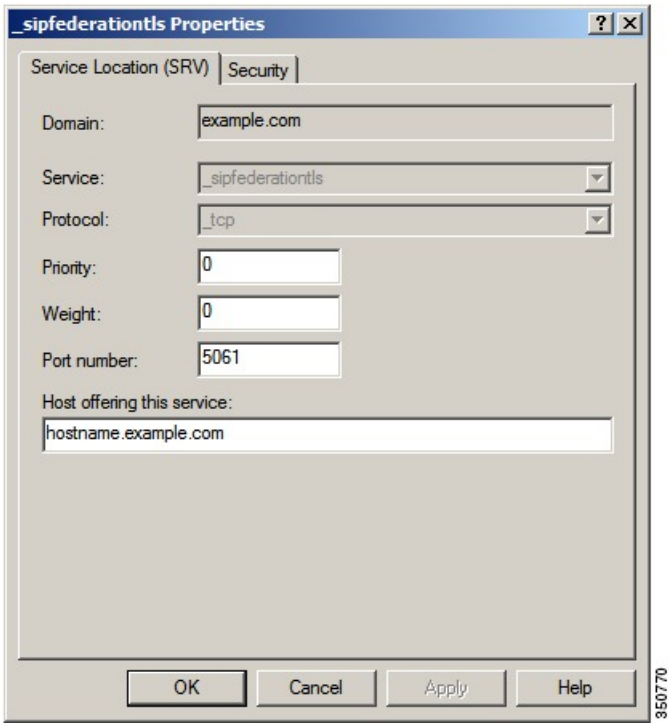
ローカル IM and Presence Service 企業展開では、 IM and Presence Service は IM and Presence Service ドメインの DNS SRV レコードを公開し、他のドメインが DNS SRV を介して IM and Presence Service ノードを検出できるようにする必要があります。DNS SRV レコードは、エンタープライズ DMZ 内の DNS サーバに存在します。

ローカル IM and Presence Service 展開で複数のドメインを管理している場合は、ローカル ドメインごとに DNS SRV レコードを公開する必要があります。各ローカルドメインに公開する DNS SRV レコードは、同じパブリック FQDN IP アドレスに解決する必要があります。

Microsoft S4B/Lync との SIP フェデレーションの場合、DNS SRV レコード「_sipfederationtls」を公開する必要があります。Microsoft エンタープライズ展開では、アクセス エッジ サーバーで IM and Presence Service をパブリック IM プロバイダーとして構成するため、このレコードが必要です。外部エンタープライズ展開では、 IM and Presence Service が Microsoft ドメインを検出するために、この外部ドメインを指す DNS SRV レコードが存在する必要があります。 IM and Presence Service ノードが DNS SRV を使用して Microsoft ドメインを検出できない場合は、この外部ドメインのパブリック インターフェイスを指すスタティック ルートを IM and Presence Service に構成する必要があります。

DNS SRV レコード "_sipfederationtls_tcp.example.com" のサンプル DNS 構成については、次の図を参照してください。

**図 *12*：「*_sipfederationtls*」の *DNS SRV***

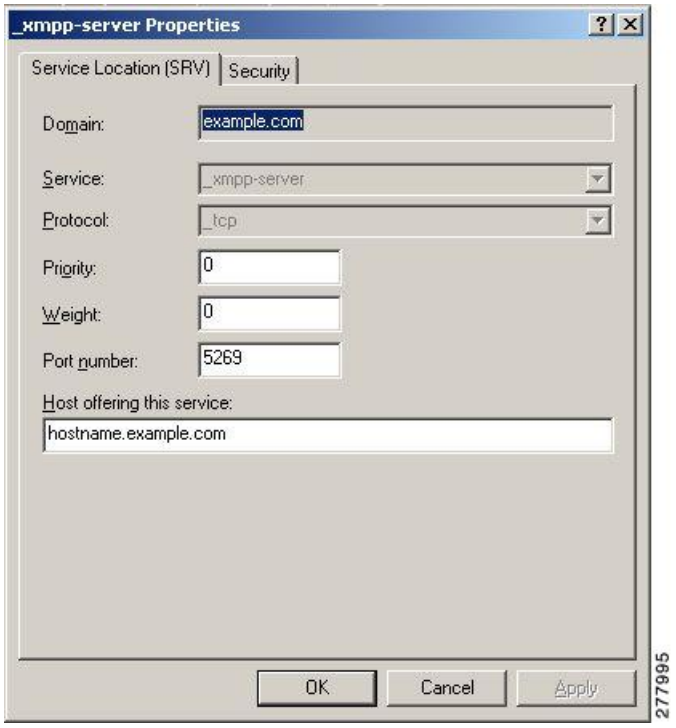



DNS SRV レコードはパブリックに解決可能であるため、ローカル エンタープライズで DNS 転送をオンにすると、DNS クエリはローカル エンタープライズ外のパブリック ドメインに関する情報を取得します。DNS クエリがローカル企業内の DNS 情報に完全に依存している場合（ローカル企業で DNS 転送をオンにしない場合）、外部ドメインを指す DNS SRV レコード/FQDN/IP アドレスを公開する必要があります。または、スタティック ルートを構成できます。

XMPP フェデレーションの場合は、DNS SRV レコード「_xmpp-server」を公開する必要があります。このレコードにより、フェデレーテッド XMPP ドメインは IM and Presence Service ドメインを検出できるため、両方のドメインのユーザーは XMPP を介して IM および可用性情報を交換できます。同様に、外部ドメインは、IM and Presence Service が外部ドメインを検出できるように、パブリック DNS サーバで _xmpp-server レコードを公開する必要があります。

DNS SRV レコード「_xmpp-server」の DNS 構成例については、次の図を参照してください。

図 *13*：「*_xmpp-server*」の *DNS SRV*




# 認証権限サーバー

SIP フェデレーションの場合、 IM and Presence Service エンタープライズ展開内の Cisco 適応型セキュリティ アプライアンス と外部エンタープライズ展開は、セキュアな SSL/TLS 接続を介して IM と可用性を共有します。

各エンタープライズ展開では、外部認証局（CA）によって署名された証明書を提示する必要がありますが、各エンタープライズ展開では異なる CA を使用できます。したがって、各エンタープライズ展開は、2 つのエンタープライズ展開間の相互信頼を実現するために、他のエンタープライズ展開の外部 CA からルート証明書をダウンロードする必要があります。

XMPP フェデレーションの場合、セキュアな TLS 接続を構成するかどうかを選択できます。TLS を構成する場合は、 IM and Presence Service で、外部企業の証明書に署名する認証局（CA）のルート証明書をアップロードする必要があります。Cisco Expressway-C は XMPP フェデレーションの TLS 接続を終了しないため、この証明書は IM and Presence Service の証明書信頼ストアに存在する必要があります。 Cisco Expressway-C は、XMPP フェデレーションのファイアウォールとして機能します。

# この統合の事前前提構成タスク

この章では、この準備のために実行するさまざまな前提条件の設定タスクについて説明します。

# 統合向け IM and Presence サービスの構成

（注） これらの前提条件タスクは、SIP フェデレーションと XMPP フェデレーションの両方に適用されます。

**ステップ 1** IM and Presence Service をインストールして構成します。

この時点で、次のチェックを実行して、 IM and Presence Service が正常に動作していることを確認します。

- IM and Presence Service システム構成のトラブルシュータを実行します。
- IM and Presence Serviceにローカル連絡先を追加できることを確認します。
- クライアントが IM and Presence Service ノードから可用性状態を受信していることを確認します。

**ステップ 2** Cisco Unified Communications Manager で IM and Presence Service の構成および管理で説明されているように、*Cisco Unified Communications Manager* ノードを持つ *IM and Presence Service* ノードを構成します。 IM and Presence Service ノードが動作しており、問題がないことを確認します。

**関連情報 -**

統合用の Cisco 適応型セキュリティ アプライアンスの構成

# 統合用の Cisco 適応型セキュリティ アプライアンスの構成

（注）
- SIP フェデレーションの場合は、Cisco 適応型セキュリティ アプライアンスが必要です。
- XMPP フェデレーションの場合は、ファイアウォールが必要です。基本的なファイアウォール/NAT/PAT 機能には、Cisco 適応型セキュリティ アプライアンス を含む任意のファイアウォールを使用できます。XMPP フェデレーションでは、TLS プロキシ機能に Cisco 適応型セキュリティ アプライアンス を使用しません。

統合用の Cisco 適応型セキュリティ アプライアンスのインストールおよび構成Cisco 適応型セキュリティ アプライアンスで、次の基本設定チェックを実行します。

**ステップ 1** コンソール、ハイパーターミナル、または Web ベースの Adaptive Security Device Manager（ASDM）を使用して、Cisco 適応型セキュリティ アプライアンス にアクセスします。

**ステップ 2** Cisco 適応型セキュリティ アプライアンスの適切なライセンスを取得します。Cisco 適応型セキュリティ アプライアンスの TLS プロキシにはライセンスが必要であることに注意してください。ライセンス情報については、Cisco の担当者にお問い合わせください。

**ステップ 3** ソフトウェアをアップグレードします（必要な場合）。

**ステップ 4** コマンドを使用してホスト名を構成します。

```
(config)# hostname name
```

**ステップ 5** **[デバイスのセットアップ（Device Setup）]** > **[システム時間（System Time）]** > **[時計（Clock）]** を選択するか、CLI から **clock set** コマンドを使用して、ASDM でタイムゾーン、日付、時刻を設定します。次の点に注意してください。

- TLS プロキシを構成する前に、Cisco 適応型セキュリティ アプライアンス 5500 のクロックを設定します。
- Cisco 適応型セキュリティ アプライアンス では、 IM and Presence Service クラスタと同じ NTP サーバを使用することを推奨します。Cisco 適応型セキュリティ アプライアンス と IM and Presence Service ノードの間でクロックが同期していない場合、証明書の検証の失敗が原因で TLS 接続が失敗する可能性があります。
- NTP サーバのアドレスを表示するには、 **ntp server** *server_address*コマンドと **show ntp associat |** コマンドを使用します。 ステータスをクリックして、NTP サーバのステータスを表示します。

**ステップ 6** Cisco 適応型セキュリティ アプライアンス 5500 のモードを確認します。Cisco 適応型セキュリティ アプライアンス 5500 は、デフォルトでシングル モードとルーテッド モードを使用するように構成されています。

- 現在のモードを確認します。このデフォルト値は、デフォルトでシングル モードです。

  ```
  (config)# show mode
  ```

- 現在のファイアウォール モードを確認します。これは、デフォルトではルーテッド モードです。

  ```
  (config)# show firewall
  ```

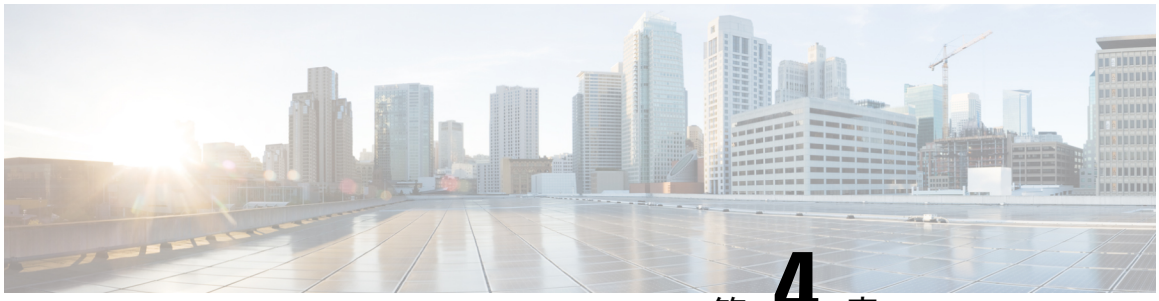
- 外部および内部インターフェイスをセットアップします。
- 基本的な IP ルートを設定します。

**関連情報 -**

外部および内部インターフェイスの構成

スタティック IP ルートの構成

統合向け IM and Presence サービスの構成



第 4 章

# ドメイン間フェデレーションの構成ワークフロー

ここでは、ドメイン間フェデレーションの構成ワークフローについて説明します。



# Office 365 Workflow (Business to Business via Expressway)

The IM and Presence Service supports interdomain SIP federation with Office 365 via Cisco Expressway session classification in a business to business configuration. With this integration, Office 365 hosts the Skype for Business deployment.

**Note** For interdomain federation with Skype for Business without Office 365, see Skype for Business Workflow, on page 38.

### IM and Presence Service Configuration

1. Start Federation services. See フェデレーション サービスのオン , on page 103.
2. Configure a public DNS SRV record for the IM and Presence domain. The SRV should resolve to the Expressway-E IP address. See IM および Presence サービスの DNS SRV レコードの追加, on page 103.

3. In the IM and Presence Service, add the Office 365 domain entry. See IM and Presence サービスへの Office 365 ドメインの追加 , on page 104.
4. In the IM and Presence Service, configure a TLS static route to Expressway-C. See Office 365 へのスタティック ルートの構成, on page 104.
5. In the IM and Presence Service, assign Expressway-C as a TLS peer. See TLS ピアとしての Expressway の追加, on page 105.
6. In the IM and Presence Service, add the Expressway-E server to the inbound access control list. See アクセス制御リストへの Expressway の追加, on page 106.
7. Restart the Cisco XCP Router on all IM and Presence Service nodes. See Cisco XCP ルータの再起動, on page 106.
8. Exchange certificates between the servers in your deployment. For the IM and Presence Service, you will need to upload the Expressway-C certificate chain to the **cup-trust** store. See Exchange Certificates, on page 107.

### Cisco Expressway Configuration

After interdomain federation is configured on the IM and Presence Service, set up Cisco Expressway for interdomain federation with Office 365. For Expressway configuration details, see *Chat and Presence XMPP Federation and Microsoft SIP Federation using IM and Presence or Expressway* at:

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

# Skype for Business Workflow

The IM and Presence Service supports SIP federation with Skype for Business via Expressway in the following integrations:

- Business to Business via Expressway—Federation with a remote Skype for Business server that is located in another company's network.
- Single Enterprise Network—Federation with an on-premise Skype for Business server that is located in the same enterprise network as the IM and Presence Service, but which is in a different domain.

**Note** Skype for Business can also be hosted by Office 365. For Office 365 deployments, see Office 365 Workflow (Business to Business via Expressway), on page 37.

Following is an overview of the configuration process. For a detailed task flow, see Skype for Business フェデレーションのタスク フロー, on page 110.

### IM and Presence Service Configuration

1. Turn on Federation Services. See フェデレーション サービスのオン , on page 112.

2. Configure a DNS SRV record for the IM and Presence domain. See IM および Presence の DNS SRV の割り当て, on page 113.
   - In business to business federations, it should be a public DNS SRV that points to Expressway-E.
   - For interdomain federation within a single enterprise, it can be an internal DNS SRV that points to Expressway-C.

**Note** You can still configure interdomain federation without the DNS SRV record, but you will have to add the route manually on the Skype for Business server.

3. In the IM and Presence Service, add the Skype for Business domain entry. See IM および Presence へのフェデレーテッド ドメインの追加, on page 113.
4. In the IM and Presence Service, configure a TLS static route to Expressway. See IM and Presence のスタティック ルートの構成, on page 114.
5. In the IM and Presence Service, assign Expressway-C as a TLS peer. See TLS ピアとしての Expressway の追加, on page 114.
6. In the IM and Presence Service, add the Expressway-C server to the inbound access control list. See アクセス制御リストへの Expressway の追加, on page 115.
7. Restart the Cisco XCP Router service on all IM and Presence nodes. See Cisco XCP ルータの再起動, on page 116.
8. Exchange certificates between the servers in your deployment. See Exchange Certificates, on page 120.

### Expressway Configuration

Configure Expressway for interdomain federation with Skype for Business. For Expressway configuration details, see the *Chat and Presence XMPP Federation and Microsoft SIP Federation using IM and Presence or Expressway* at:

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

### Additional Configuration Details

**Note** For a more detailed view of the configuration tasks for Skype for Business, see Skype for Business フェデレーションのタスク フロー, on page 110.

# Microsoft Lync ワークフロー（Expressway 経由の社内）

社内シナリオで Expressway を介して IM and Presence Service と Microsoft Lync 間のドメイン間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。

### IM and Presence Service の設定

1. 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。「企業内での Microsoft Lync ドメインの追加 （125 ページ）」を参照してください。
2. 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。「IM and Presenceから Lync へのスタティック ルートの構築 （126 ページ）」を参照してください。

（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。

3. 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 サブジェクトを設定します。「Set up Certificates on IM and Presence for Federation with Lync （133 ページ）」を参照してください。

### Expressway の設定

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。Expressway を構成するには、Configure Expressway Gateway for Microsoft Lync Federation （126 ページ） に進みます。

（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。

Expressway ゲートウェイの SIP ブローカを使用するチャット+コール展開の場合、サポートは社内シナリオのみに限定されます。ビジネスツービジネスはサポートされていません。

### Lync の構成

1. 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。

1. チャット + コール展開の場合は、Lync から IM および Presence へのスタティック ルートの構成 （128 ページ）
2. チャットのみの展開の場合は、Lync から Expressway ゲートウェイへの静的ルートの構成 （127 ページ）

2. 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 サーバー プールに追加します。「Lync Server での信頼できるアプリケーションの構成 （131 ページ）」を参照してください。
3. Lync サーバーで、トポロジをコミットします。「トポロジの公開 （133 ページ）」を参照してください。

# Microsoft Lync Workflow (Business to Business via Expressway)

**Note** This deployment is supported for intracompany deployments only. Federation via Expressway Gateway SIP broker is not supported for business to business federation.

Complete the following tasks to set up interdomain federation between IM and Presence Service and Microsoft Lync in a business to business deployment via Expressway's session classification method.

This configuration supports both chat-only and chat+calling deployments.

**Note** The minimum IM and Presence Service release for this configuration is 11.5(1)SU2.

### IM and Presence Service Configuration

1. In the IM and Presence Service, add a federated domain entry for the Microsoft Lync domain. The IM and Presence Service automatically adds the incoming ACL for the federated domain entry. See 企業内での Microsoft Lync ドメインの追加, on page 125.
2. In the IM and Presence Service, configure an individual TLS static route for each Microsoft Lync server domain. Each route should point to a specific Microsoft front end server. See IM and Presence から Lync へのスタティック ルートの構築, on page 126.

**Note** You must configure TLS static routes. TCP is not supported for federation with Microsoft Lync.

3. In the IM and Presence Service, upload the root certificate for the CA that signs the Lync server certificates to IM and Presence Service. Also, set up TLS Peer subjects. See Set up Certificates on IM and Presence for Federation with Lync, on page 133.

### Expressway Configuration

Configure Cisco Expressway session classification. Refer to your Cisco Expressway configuration documentation at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html. For Release X8.9.2, refer to *Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure*.

# Microsoft Lync Workflow (Business to Business via ASA)

- Configure a federated domain on the IM and Presence Service for Microsoft Lync federation, see SIP フェデレーテッド ドメインの追加, on page 47.
- Configure the DNS SRV records, see SIP フェデレーションの DNS 構成, on page 48.
- Configure the routing on the IM and Presence Service for Microsoft Lync federation, see IM および Presence サービスのルーティング構成, on page 48
- (Optional) Configure the email address for federation feature, see フェデレーション用の電子メールをオンにする, on page 193
- Configure the TLS security settings on the IM and Presence Service, see IM および Presence サービスでセキュリティ設定の構成, on page 51
- Configure the Cisco Adaptive Security Appliance for Microsoft Lync federation, see SIP フェデレーション向け Cisco 適応型セキュリティ アプライアンスのワークフロー and TLS プロキシ.
- Configure certificate exchange for Microsoft Lync federation, see Security Certificate Configuration on Lync Edge Server for TLS Federation, on page 75.
- Configuration of Lync Server 2010 and Edge servers for interdomain federation differs from that outlined within this guide for OCS. For information on configuring the Lync enterprise for interdomain federation with the IM and Presence Service, see Microsoft documentation.

# Microsoft OCS ワークフロー（直接フェデレーション）

IM and Presence Service と Microsoft OCS 間のドメイン間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、企業内で ASA ファイアウォールを使用しない SIP フェデレーション用です。

### IM and Presence Service の設定

1. IM and Presence Service で、Microsoft OCS 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。「企業内での Microsoft OCS ドメインの追加 （137 ページ）」を参照してください。

2. IM and Presence Service 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 サーバーを指す必要があります。「Microsoft サーバの IM および Presence サービスのスタティック ルートの構成（138 ページ）」を参照してください。

（注） OCS の場合、プロトコル タイプとして TCP または TLS を選択できます。

### Microsoft OCS の構成

1. OCS サーバーで、IM and Presence Service ドメインを指す 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 Service ノードを指している必要があります。「OCS で IM および Presence サービスに向かうスタティック ルートの構成（139 ページ）」を参照してください。
2. IM and Presence Service で、ピア認証リスナーがポート 5061 として設定され、サーバー認証リスナーがポート 5061 ではないことを確認します。「ピア認証リスナーの確認 （140 ページ）」を参照してください。
3. OCS サーバーで、各 IM and Presence Service ノードの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、各 IM and Presence ノードに 2 つのエントリを追加する必要があります。1 つはノード IP アドレスを含むエントリ、もう 1 つは FQDN を含むエントリです。「OCS での IM and Presence サービス ノードのホスト認証エントリの追加 （141 ページ）」を参照してください。
4. OCS と IM and Presence Service の間に TLS が設定されている場合は、IM and Presence Service とのドメイン間フェデレーション用に OCS で証明書を設定します。TLS を使用していない場合は、この手順をスキップできます。「ドメイン間フェデレーション用の OCS での証明書の構成 （142 ページ）」を参照してください。
5. OCS サーバーで、TLS（トランスポートは MTLS または TLS のいずれか）または TCP のリスナーポートが設定されていることを確認します。TLS の場合は、ポート 5061 を使用します。TCP の場合は、ポート 5060 を使用します。「OCS サーバーでポート 5060/5061 を有効にする （142 ページ）」を参照してください。
6. TLS を使用している場合は、FIPS を使用するように OCS を設定します。「FIPS を使用するための OCS の構成 （143 ページ）」を参照してください。
7. TLS を使用している場合は、OCS サーバー証明書に署名する CA のルート証明書を IM and Presence Service にアップロードします。「Set Up Certificates on the IM and Presence Service Node for Federation with Microsoft Server over TLS （144 ページ）」を参照してください。

# Microsoft OCS ワークフロー（ASA を介した Business to Business）

- Microsoft OCS フェデレーション用の IM and Presence Service でフェデレーテッド ドメインを設定します。「SIP フェデレーテッド ドメインの追加 （47 ページ）」を参照してください。
- DNS SRV レコードの構成は、「SIP フェデレーションの DNS 構成 （48 ページ）」を参照してください。
- Microsoft OCS フェデレーションの IM and Presence Service でルーティングを構成します。「IM および Presence サービスのルーティング構成 （48 ページ）」を参照してください。
- （オプション）フェデレーション機能の電子メールアドレスを設定します。「フェデレーション用の電子メールをオンにする （193 ページ）」を参照してください。
- IM and Presence サービスでのセキュリティを設定します。IM および Presence サービスでセキュリティ設定の構成 （51 ページ） を参照してください。
- Microsoft OCS フェデレーション用の Cisco 適応型セキュリティア プライアンスを構成します。SIP フェデレーション向け Cisco 適応型セキュリティ アプライアンスのワークフローと TLS プロキシ を参照してください。
- Microsoft OCS フェデレーションの証明書交換を設定します。「IM および Presence サービスと Cisco 適応型セキュリティ アプライアンス間のセキュリティ証明書の交換」を参照してください。
- Microsoft OCS サーバーを設定します。 「SIP フェデレーションの外部サーバー コンポーネントの構成 （147 ページ）」を参照してください。
- （オプション）冗長性のためにロードバランサを設定します。「SIP フェデレーションの冗長性のためのロード バランサの構成 （153 ページ）」を参照してください。
- Microsoft OCS フェデレーションのトラブルシューティング情報については、「SIP フェデレーション統合のトラブルシューティング （205 ページ）」 を参照してください。

# SIP フェデレーション向け Cisco 適応型セキュリティ アプライアンスのワークフロー

- Cisco 適応型セキュリティ アプライアンス と IM and Presence Service （内部インターフェイス）間の証明書を構成します。 「IM および Presence サービスと Cisco 適応型セキュリティ アプライアンス間のセキュリティ証明書の交換 （61 ページ）」を参照してください。

- Cisco 適応型セキュリティ アプライアンス とフェデレーション ドメイン（外部インターフェイス）間の証明書を構成します。「Microsoft CA を使用した Cisco 適応型セキュリティ アプライアンスと Microsoft Access Edge（外部インターフェイス）間のセキュリティ証明書の交換 （66 ページ）」を参照してください。
- プライベートからパブリックへのメッセージングの PAT ルールを設定します。 「ポート アドレス変換（PAT） （82 ページ）」を参照してください。
- パブリックからプライベートへのメッセージング用のスタティック PAT を設定します。「スタティック PAT コマンドの例 （87 ページ）」を参照してください。
- 必要なアクセスリストを構成します。 「アクセス リストの構成要件 （94 ページ）」を参照してください。
- TLS プロキシ インスタンスを構成します。「TLS プロキシ インスタンスの構成 （96 ページ）」を参照してください。
- アクセスリストを TLS プロキシに関連付けます。 「クラスマップを使用したアクセスリストと TLS プロキシ インスタンスの関連付け （97 ページ）」を参照してください。

# AOL を使用した SIP フェデレーションの構成ワークフロー

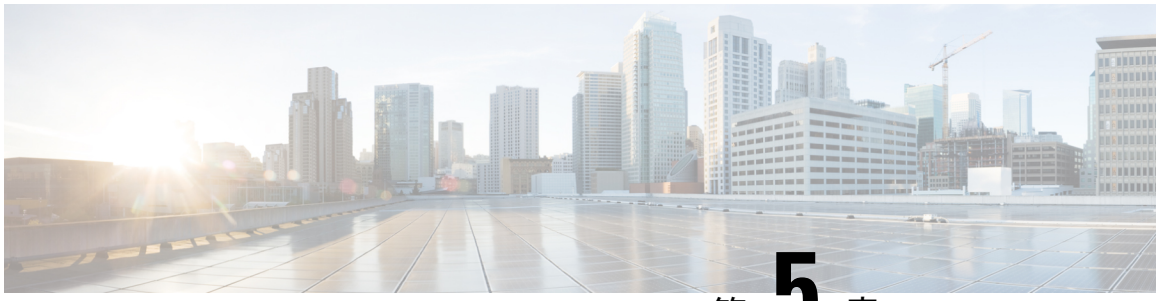
- AOL フェデレーションを有効にするには、AOL ライセンスを確立します。 「AOL フェデレーションのライセンス要件 （150 ページ）」 、 「AOL ルーティング情報の要件 （151 ページ）」 、および 「AOL プロビジョニング情報の要件 （151 ページ）」を参照してください。
- AOL フェデレーション用に IM and Presence Service でフェデレーテッド ドメインを構成します。 SIP フェデレーテッド ドメインの追加 （47 ページ） 「」を参照してください。
- DNS SRV レコードの構成は、「SIP フェデレーションの DNS 構成 （48 ページ）」を参照してください。DNS を使用していない場合は、次の手順を参照してください）。
- AOL フェデレーションのルーティングを構成します。 「TLS を使用したスタティック ルートの構成 （50 ページ）」を参照してください。
- （オプション）AOL でホストされているドメインのデフォルト フェデレーション ルーティング ドメインを確認して構成します。
- （オプション）フェデレーション機能の電子メールアドレスを設定します。「フェデレーション用の電子メールをオンにする （193 ページ）」を参照してください。
- IM and Presence Serviceで TLS セキュリティ設定と証明書を構成します。 「IM および Presence サービスでセキュリティ設定の構成 （51 ページ）」および「Cisco 適応型セキュリティ アプライアンスと AOL SIP アクセス ゲートウェイ間のセキュリティ証明書の交換 （75 ページ）」を参照してください。

- AOL の Cisco 適応型セキュリティ アプライアンス for AOL を構成します。AOL FQDN、サーバ ポート、およびパブリック IP アドレスの詳細については、AOL SIP アクセス ゲートウェイ （31 ページ） を参照してください。
- （オプション）冗長性のためにロードバランサを設定します。「SIP フェデレーションの冗長性のためのロード バランサの構成 （153 ページ）」を参照してください。

# XMPP フェデレーションのワークフロー

（注） Webex、 IM and Presence Service、および IBM Sametime については、このワークフローに従います。

- XMPP フェデレーション用に IM and Presence Service を設定します。「XMPP フェデレーションの IM および Presence サービス構成 （161 ページ）」を参照してください。
- XMPP フェデレーションのセキュリティを設定します。「XMPP フェデレーションのセキュリティ証明書の構成 （181 ページ）」を参照してください。
- （オプション）フェデレーション機能の電子メールアドレスを設定します。「フェデレーション用の電子メールをオンにする （193 ページ）」を参照してください。
- XMPP フェデレーションサービスをオンにします。「XMPP フェデレーションサービスをオンにする （179 ページ）」を参照してください。
- XMPP フェデレーション用に Cisco 適応型セキュリティアプライアンス を設定します。「XMPP フェデレーション用の Cisco 適応型セキュリティ アプライアンスの構成 （177 ページ）」を参照してください。
- XMPP フェデレーションのトラブルシューティング情報については、「XMPP フェデレーション統合のトラブルシューティング （217 ページ）」を参照してください。



第 5 章

# SIP フェデレーション用の IM および Presence サービスの構成

このセクションでは、SIP フェデレーション用の IM and Presence サービスの構成について説明します。



## SIP フェデレーテッド ドメインの追加

（注） SIP フェデレーションとリモート コール制御（RCC）は、同じ IM and Presence Service クラスタ上で連携しません。これは、SIP フェデレーションの場合、ユーザーは Cisco IM and Presence サービスと Microsoft Lync/S4B の両方のライセンスを取得できないためですが、RCC の場合、ユーザーは Cisco IM and Presence サービスと Microsoft Lync/S4b のライセンスを同時に取得する必要があります。

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 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、**Cisco Unified CM IM and Presence Administration** のユーザー インターフェイスで確認できますが、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。このテキスト文字列は、[ドメインの管理（Manage Domains）] タブから使用可能な Cisco Jabber リリース 8.x のプライバシー設定でユーザーに表示されます。したがって、ユーザーが簡単に認識できるドメイン名を入力してください。

**ステップ 5** **Lync/S4B**へのドメイン間を選択します

**ステップ 6** Microsoft とのフェデレーションを設定している場合は、**[直接フェデレーション（Direct Federation）]** の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** [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** のユーザ 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 センター - ネットワーク サービス（Control Center - Network Services）]** を選択して、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。

# IM および Presence サービスのルーティング構成

このセクションでは、IM and Presence Service でのルーティング設定の概念について説明します。

## SIP フェデレーションの DNS 構成

ローカル IM and Presence Service エンタープライズでは、IM and Presence Service は、他のドメインが DNS SRV を介して IM and Presence Service ノードを検出できるように、各ローカル IM and Presence Service ドメインの DNS SRV レコードをパブリッシュする必要があります。各 DNS SRV レコードは、同じパブリック IP アドレスに解決される必要があります。

Microsoft 企業展開では、 IM and Presence Service が IM and Presence Service ドメインの DNS SRV レコードをパブリッシュする必要があります。これは、IM and Presence Service を Access Edge サーバでパブリック IM プロバイダとして構成するためです。

IM and Presence Service 企業展開では、ポート 5061 を介して _sipfederationtls.*_tcp.imp_domain* を指す DNS SRV レコードを構成する必要があります（*imp_domain* は IM and Presence Service ドメインの名前）。この DNS SRV は、ルーティング IM and Presence Serviceのパブリック FQDN を指す必要があります。この FQDN は一般に解決可能である必要があります。

IM and Presence Service が外部ドメインを検出するには、外部ドメインの外部インターフェイスの FQDN を指す DNS SRV レコードが外部ドメインの DNS サーバに存在する必要があります。

ヒント　DNS SRV ルックアップを実行するには、次の一連のコマンドを使用します。

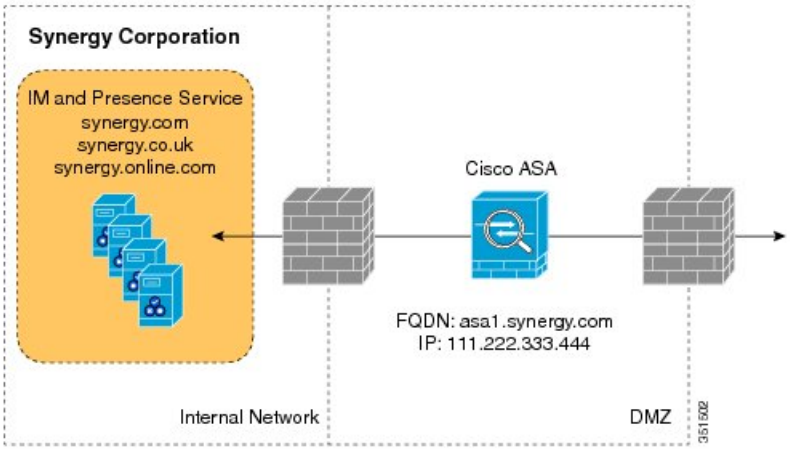
```
nslookupset type=srv _sipfederationtls._tcp.domain
```

IM and Presence Service がパブリック DNS ルックアップを介して外部エンタープライズを解決できない場合は、展開でスタティック ルートを構成する必要があります。

### ドメイン間フェデレーション展開での SIP DNS SRV

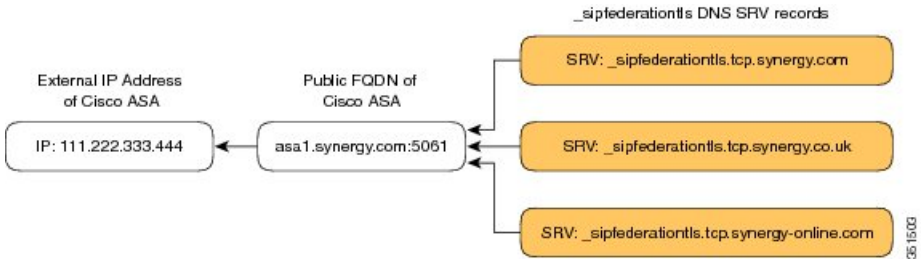
次の例では、複数のローカル ドメインをすべて同じパブリック FQDN に解決する必要があり、 IM and Presence Service 展開でホストされているドメインごとに DNS SRV レコードを公開する必要があります。次の図は、3 つのローカルドメインを使用したドメイン間フェデレーション展開の例を示しています。ドメインごとに _sipfederationtls DNS SRV レコードを公開する必要があります。

**図 *14 : SIP* ベースのフェデレーション ドメイン間展開での複数のドメイン**




次の図に示すように、各 DNS SRV レコードは、DMZ（ポート 5061）に展開されている Cisco Expressway-C の外部（パブリック）IP アドレスの FQDN に対して解決される必要があります。

**図 *15 : Cisco Expressway-C*の *FQDN* に解決する *SIP DNS SRV***




### 関連項目

TLS を使用したスタティック ルートの構成 （50 ページ）

# TLS を使用したスタティック ルートの構成

（注） スタティック ルートの設定は、SIP フェデレーションにのみ適用されます。

IM and Presence Service ノードが DNS SRV を使用して外部ドメインを検出できない場合は、外部ドメインの外部インターフェイスを指すスタティック ルートを IM and Presence Service に設定する必要があります。

**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）] > [ルーティング（Routing）] > [静的ルート（Static Routes）]** を選択します。

**ステップ 2** スタティック ルート パラメータを次のように構成します。

- 接続先パターン値は、外部エンタープライズ ドメインが逆になるように構成する必要があります。たとえば、ドメインが「domaina.com」の場合、接続先パターンの値は「.com.domaina.*」である必要があります。
- Next Hop 値は、Microsoft サーバーとのフェデレーション用の 外部 Access Edge の FQDN または IP アドレスです。
- Next Hop ポート番号は **5061**です。
- [ルート タイプ（Route Type）] の値は **domain**です。
- [プロトコル タイプ（Protocol Type）] は **TLS** です。

**ステップ 3** [保存（Save）] をクリックします。

# フェデレーション ルーティング パラメータの構成

### 始める前に

フェデレーション ルーティング パラメータをリセットする必要がある場合は、この手順を使用します。デフォルトでは、このパラメータはインストール時にパブリッシャ ノードの FQDN に自動的に設定されます。 IM and Presence Service は、この値を各サブスクライバ ノードに渡します。

**ステップ 1** **Cisco Unified CM IM and Presence Administration** のユーザーインターフェイスにログインします。**[システム（System）] > [サービスパラメータ（Service Parameters）]** を選択します。

**ステップ 2** [サーバ（Server）] ドロップダウン リストから [IM and Presence Service] ノードを選択します。

**ステップ 3** **[サービス（Service）]** ドロップダウン リストから、**[Cisco SIP プロキシ（Cisco SIP Proxy）]** を選択します。

**ステップ 4** **[フェデレーション ルーティング パラメータ（クラスタ全体）（Federation Routing Parameters (Clusterwide)）]** セクションで、**[フェデレーション ルーティング IM およびプレゼンス FQDN（Federation Routing IM and Presence FQDN）]** のパブリック FQDN 値を入力し、**[保存（Save）]** をクリックします。

（注）
- この FQDN 値は、その IM and Presence Service ドメインのパブリック DNS の `_sipfederationtls` エントリに対応している必要があります。例：
  - プレゼンス サーバの FQDN が `impl.cisco.com` で、DNS SRV が *_sipinternaltls* です。_tcp.cisco.com（FQDN`impl-public.cisco.com`を指す）の場合、フェデレーション ルーティング FQDN は、 `impl-public.cisco.com`になります。
  - プレゼンス サーバの FQDN が `impl.cisco.com` で、DNS SRV が *_sipinternaltls* です。_tcp.extcisco.com（`impl-public.ciscoext.com`）の場合、フェデレーション ルーティング FQDN は、 `impl-public.ciscoext.com`になります。

（注） このパラメータは、プレゼンス サーバと Lync Server の間に TLS プロキシを使用したファイアウォール（ASA）があり、**[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）]** で **[直接フェデレーション（Direct Federation）]** チェックボックスがオンになっているフェデレーションには適用されません。

- ルーティング IM and Presence Service ノードにユーザーを割り当てる場合、この FQDN 値をルーティング IM and Presence Service ノードの実際の FQDN と同じにすることはできません。

### 次のタスク

IM and Presence Service のフェデレーション ルーティング FQDN パラメータを変更した場合は、Cisco XCP ルータを再起動します。Cisco Unified Serviceability のユーザー インターフェイスにログインし、 **Cisco Unified Serviceability** で **[ツール（ Tools）]** > **[コントロール センター（Control Center）] - [ネットワーク サービス（Network Services）]**を選択します。

Cisco XCP ルータを再起動すると、 IM and Presence Service上のすべての XCP サービスが再起動されます。

# IM および Presence サービスでセキュリティ設定の構成

（注） この手順は、企業内でフェデレーションを展開し、セキュアな TLS 接続が必要な場合など、フェデレーション展開に Cisco Expressway-C がない場合にのみ適用されます。

（注） Microsoft Lync は EC 暗号をサポートしていません。EC 暗号を選択する場合は、非 EC 暗号のみを選択するか、EC 暗号と非 EC 暗号を組み合わせて選択する必要があります。EC 暗号を単独で選択することはできません。

（注） `Default_Cisco_SIP_Proxy_Peer_Auth_TLS_Context` は、追加の強力な暗号の選択をサポートします。必要な設定に基づいて適切な暗号方式を選択できます。ドメイン間フェデレーションを設定する前に、選択した暗号リストがピアでサポートされている暗号と一致していることを確認する必要があります。

## 新しい TLS ピア サブジェクトの作成

Cisco Expressway-C セキュリティ証明書を IM and Presence Serviceにインポートすると、IM and Presence Service は Cisco Expressway-C を TLS ピア サブジェクトとして自動的に追加します。したがって、 IM and Presence Service で TLS ピア サブジェクトとして Cisco Expressway-C を手動で追加する必要はありません。

**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。**[システム（System）] > [セキュリティ（Security）] > [TLSピアサブジェクト（TLS Peer Subjects）]**

**ステップ 2** [新規追加（Add New）] をクリックします。

**ステップ 3** 次のいずれかの値を入力します。

a) Microsoft サーバーとの SIP フェデレーションを設定する場合は、[ピア サブジェクト名（Peer Subject Name）] フィールドにアクセス エッジ サーバーの外部 FQDN を入力します。この値は、Microsoft Access Edge サーバーが提示する証明書のサブジェクト CN と一致する必要があります。

**ステップ 4** [説明（Description）] フィールドに外部サーバーの名前を入力します。

**ステップ 5** [保存（Save）] をクリックします。

# IM および Presence サービスでセキュリティ設定の構成

（注） この手順は、企業内でフェデレーションを展開し、セキュアな TLS 接続が必要な場合など、フェデレーション展開に Cisco Expressway-C がない場合にのみ適用されます。

（注） Microsoft Lync は EC 暗号をサポートしていません。EC 暗号を選択する場合は、非 EC 暗号のみを選択するか、EC 暗号と非 EC 暗号を組み合わせて選択する必要があります。EC 暗号を単独で選択することはできません。

（注） `Default_Cisco_SIP_Proxy_Peer_Auth_TLS_Context` は、追加の強力な暗号の選択をサポートします。必要な設定に基づいて適切な暗号方式を選択できます。ドメイン間フェデレーションを設定する前に、選択した暗号リストがピアでサポートされている暗号と一致していることを確認する必要があります。

# AOL を使用した SIP フェデレーションの構成ワークフロー

- AOL フェデレーションを有効にするには、AOL ライセンスを確立します。「AOL フェデレーションのライセンス要件 （150 ページ）」 、「AOL ルーティング情報の要件 （151 ページ）」 、および「AOL プロビジョニング情報の要件 （151 ページ）」を参照してください。
- AOL フェデレーション用に IM and Presence Service でフェデレーテッド ドメインを構成します。 SIP フェデレーテッド ドメインの追加 （47 ページ）「」を参照してください。
- DNS SRV レコードの構成は、「SIP フェデレーションの DNS 構成 （48 ページ）」を参照してください。DNS を使用していない場合は、次の手順を参照してください）。
- AOL フェデレーションのルーティングを構成します。 「TLS を使用したスタティック ルートの構成 （50 ページ）」を参照してください。
- （オプション）AOL でホストされているドメインのデフォルト フェデレーション ルーティング ドメインを確認して構成します。
- （オプション）フェデレーション機能の電子メールアドレスを設定します。「フェデレーション用の電子メールをオンにする （193 ページ）」を参照してください。
- IM and Presence Serviceで TLS セキュリティ設定と証明書を構成します。 「IM および Presence サービスでセキュリティ設定の構成 （51 ページ）」および「Cisco 適応型セキュリティ アプライアンスと AOL SIP アクセス ゲートウェイ間のセキュリティ証明書の交換 （75 ページ）」を参照してください。
- AOL の Cisco 適応型セキュリティ アプライアンス for AOL を構成します。AOL FQDN、サーバ ポート、およびパブリック IP アドレスの詳細については、 AOL SIP アクセス ゲートウェイ （31 ページ） を参照してください。
- （オプション）冗長性のためにロードバランサを設定します。「SIP フェデレーションの冗長性のためのロード バランサの構成 （153 ページ）」を参照してください。

# AOL を使用した SIP フェデレーションの SIP 要求のルーティング

（注） IM and Presence Service リリース 9.0 は、AOL との SIP フェデレーションをサポートします。

AOL を使用した SIP フェデレーションにより、IM and Presence Service ユーザは次のユーザーとフェデレーションできます。

- AOL パブリックコミュニティのユーザー（例：aiim.com、 aol.com）。
- ドメインが AOL によってホストされている企業のユーザー。
- AOL とフェデレートする外部企業のユーザー。IM and Presence Service は、これらの外部企業とフェデレーションするためのクリアリング ハウスとして AOL を使用できます。

たとえば、AOL は「hosteddomain.com」というドメインを持つ企業をホストし、「acompany.com」というドメインを持つ AOL とフェデレーションしている企業があるとします。IM and Presence Service でこれらのドメインごとに SIP フェデレーション ドメイン エントリを追加して、IM and Presence Service ユーザーが users@hosteddomain.com および users@acompany.com とフェデレーションできるようにすることができます。

IM and Presence Service のルーティング ロジックは、AOL を介してフェデレーションするドメインへのルーティングをサポートするように拡張されています。SIP フェデレーションと AOL を設定すると、IM and Presence Service はデフォルトのフェデレーション ルーティング ドメインに基づいてメッセージをルーティングします。このドメインのデフォルト値は「aol.com」です。

（注） ここで説明するルーティングは、「Inter-domain to AOL」タイプのフェデレーションドメインを設定する場合にのみ適用されます。

フェデレーテッドユーザーが AOL のホステッドドメインの 1 つに属している場合（aol.com 以外のドメイン）、IM and Presence Service は次の手順を実行します。

**ステップ 1** ホステッド ドメインのスタティック ルートのルックアップ。スタティック ルートが存在しない場合、IM and Presence Service は次を実行します。

**ステップ 2** ホストされたドメインの DNS SRV ルックアップ。ルックアップで何も返されない場合、IM and Presence Service は次を実行します。

**ステップ 3** デフォルトのフェデレーション ルーティング ドメイン（デフォルトでは aol.com）のスタティック ルートのルックアップ。スタティック ルートが存在しない場合、IM and Presence Service は次を実行します。

**ステップ 4** デフォルトのフェデレーション ルーティング ドメイン（デフォルトでは aol.com ）の DNS SRV ルックアップ。

フェデレーテッドユーザがデフォルトの AOL ドメイン（user@aol.com）にある場合、IM and Presence Service は次の手順を実行します。

**ステップ 5** デフォルト AOL ドメイン（デフォルトではaol.com）のスタティック ルートのルックアップ。スタティック ルートが IM and Presence Service に存在しない場合、

**ステップ 6** デフォルトのフェデレーション ルーティング ドメイン（デフォルトでは aol.com）の DNS SRV ルックアップします。

**関連トピック**

AOL を使用した SIP フェデレーションのデフォルト フェデレーション ルーティング ドメインの変更

# SIP フェデレーションサービスをオンにする

Cisco XCP SIP Federation Connection Manager サービスをオンにします。これにより、プロビジョニングする各ユーザーの SIP フェデレーション機能がオンになります。このタスクは、クラスタ内の各ノードで実行する必要があります。

**ステップ 1** **Cisco Unified IM and Presence Serviceability** のユーザーインターフェイスにログインします。**[Tools（ツール）] > [Service Activation（サービス アクティベーション）]** を選択します。

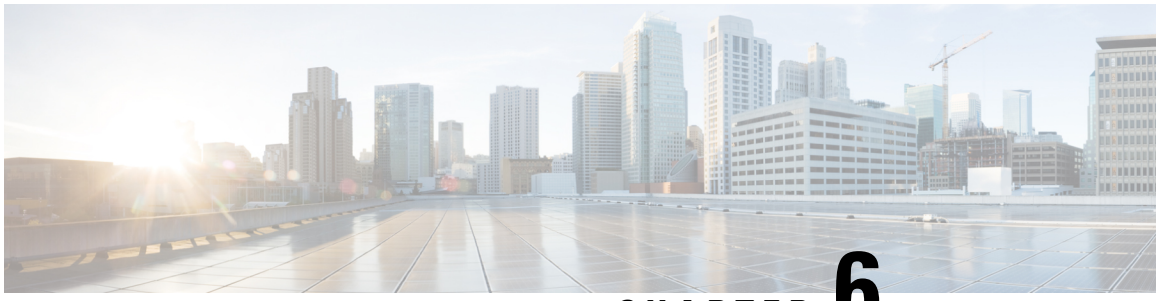
**ステップ 2** [サーバー（Server）] ドロップダウン リストからサーバーを選択します。

**ステップ 3** [移動（Go）] をクリックします。

**ステップ 4** [IM and Presence Service ] エリアで、 **Cisco XCP XMPP Federation Connection Manager** サービスの横にあるボタンをクリックします。

**ステップ 5** [保存（Save）] をクリックします。

**ステップ 6** SIP フェデレーションが機能するには、Cisco SIP プロキシ サービスが実行されている必要があります。**Cisco Unified IM and Presence Serviceability** のユーザ インターフェイスにログインします。**[ツール（Tools）] > [機能サービス（Feature Services）]** を選択し、Cisco SIP プロキシ サービスが実行されていることを確認します。



CHAPTER 6

# SIP オープン フェデレーションの IM and Presence Service 構成



# SIP オープン フェデレーションの IM および Presence サービス構成

Cisco IM and Presence サービスは、Cisco Jabber クライアントで SIP オープンフェデレーションをサポートします。

管理者は SIP オープンフェデレーションを設定して、Cisco Jabber ユーザが、利用可能なすべてのドメインのユーザとのシームレスなフェデレーションを行えるようにすることができます。

この機能は、IM and Presence サーバの SIP クライアントと XMPP クライアントの両方のオープン IM フェデレーションの共存を確立します。各フェデレーテッド ドメインを個別に構成する必要がある SIP フェデレーション用の IM および Presence サービスの構成とは異なり、事前構成された単一のスタティック ルートを使用して、すべてのドメインに対してオープン フェデレーションを構成できます。スタティックルートにより、Cisco Jabber は任意の外部ドメインとフェデレーションを行うことができます。さらに重要な点として、個々のドメインに対して SIP フェデレーションを設定および管理する場合にかかる時間が大幅に削減されます。

SIP オープン フェデレーションは、IM および Presence サービスではデフォルトで一部構成されています。これを機能させるために必要なのは、デフォルトのスタティックルート（**.***）を有効にしてアクティブにすることだけです。詳細については、「Configure Default Static Routes for SIP Open Federation on IM and Presence Service （60 ページ）」を参照してください。

SIP オープンフェデレーションを有効にするスタティック ルートはデフォルトで追加されますが、次の条件では無効になります。

- IM および Presence を初めてインストールする場合、または

- SIP オープン フェデレーションをサポートしていない古いバージョン（たとえば、IM および Presence リリース 12.5(1)SU2 以前）から新しいバージョンの IM and Presence へのアップグレード中

### SIP オープン フェデレーションの仕組み

SIP 要求が外部ドメインから送信されると、Cisco XCP SIP Federation Connection Manager（SIP CM）は、ドメインがシステムに構成またはキャッシュされているかどうかを確認します。ドメインが存在しない場合、SIP CM はそのパケットを Cisco XCP ルータに送信してキャッシュを確認します。キャッシュ内にドメインが見つからない場合は、XMPP Federation Connection Manager（XMPP CM）にパケットを送信します。XMPP CM がエラーを返した場合、XCP ルータは SIP CM に要求を送信し、最終的に事前定義されたオープン フェデレーション ルートを使用してそのパケットをルーティングします。

SIP ドメインは、最初の通信が成功した後にキャッシュに追加され、SIP CM とのルーティングは、ドメインが管理者によって追加されたかのように続行されます。その後、XMPP CM へのルーティングはなく、特定のエラーを待機します。

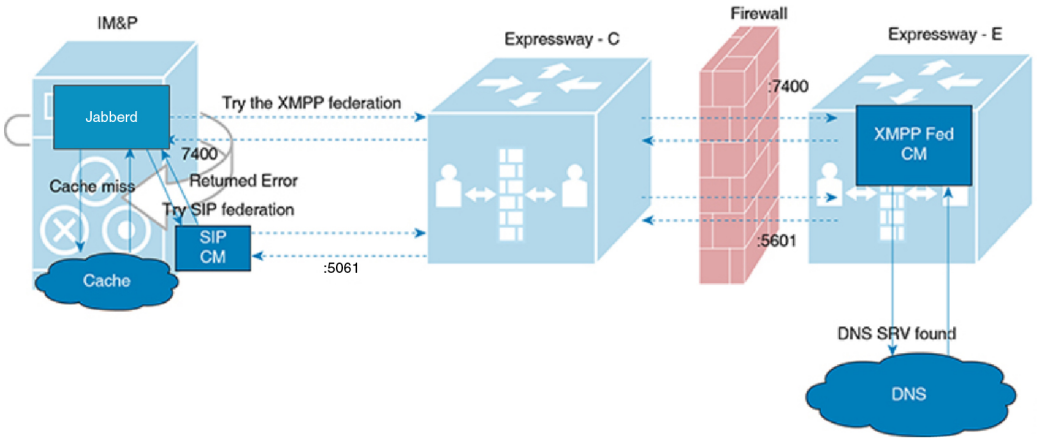
スタティック ルートが構成され、ブロック解除されると、IM および Presence ノードから SIP ドメイン（新規またはキャッシュ）をブロックできなくなります。ただし、展開に Expressway を含めると、Expressway 自体で特定の SIP ドメインをブロックできます。

[スタティック ルート（Static Route）] ページの [ルートのブロック（Block Route）] チェックボックスをオンにしてデフォルトのスタティック ルートをブロックすることで、いつでも SIP オープン フェデレーションを完全に無効にできます。

SIP オープン フェデレーションを無効にすると、新しいドメインが追加されなくなりますが、既存のドメインとのトラフィックは引き続き機能します。管理者は、SIP フェデレーテッド ドメイン UI ページからドメインを手動で削除して、そのドメイン内のトラフィックをブロックできます。

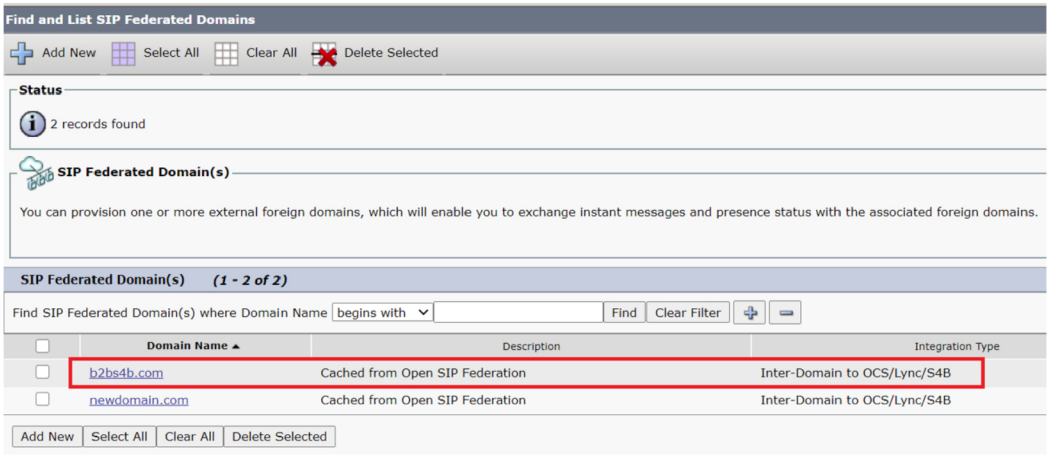
（注） SIP オープン フェデレーションを有効にすると、定義済みのデフォルト ルートよりもスタティック ルートが優先されます。

図 *16 : IM* および *Presence SIP* オープン フェデレーションのワークフロー




不明なドメインがSIPオープンフェデレーションを介してフェデレーションされると、ドメインはサーバに自動的にキャッシュされ、[SIP オープン フェデレーション ドメイン（SIP Open Federation Domains）] ページ（**[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）]**）にリストされます。

図 *17 :* キャッシュされたドメイン




その結果、キャッシュされたドメインから要求がヒットすると、前述のようにルート全体の新しいドメイン検出プロセスをバイパスして、ドメインと直接フェデレーションします。これは、キャッシュされたドメインを IM および Presence サーバのリストから削除する（または Expressway サーバで明示的にブロックする）まで続きます。

# Configure Default Static Routes for SIP Open Federation on IM and Presence Service

SIP Open Federation is partially configured by default on the IM and Presence Service. All you need to make it work is to unblock the static route and configure **Next Hop**, **Next Hop Port**, and **Protocol Type**.

Use this procedure to set up your static routes for SIP Open Federation:

**ステップ 1** Enable XMPP federation either on the IM and Presence node or Expressway-E (if included in the deployment) for the static pre-defined route to work.

For more information on how to enable XMPP federation, see *Chat and Presence XMPP Federation and Microsoft SIP Federation using IM and Presence or Expressway* at:

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

**ステップ 2** In Cisco Unified CM IM and Presence Administration, choose **Presence** > **Routing** > **Static Routes**.

**ステップ 3** Click **Find**. The pre-defined static route (*.) is displayed.

**ステップ 4** Click on the pre-defined static route (*.).

The **Static Route Configuration** page appears.

**Note** For SIP open federation, fields such as **Destination Pattern**, **Route Type**, **Priority**, **Weight**, and **Allow Specific Route** are prepopulated with default values.

**ステップ 5** In the **Next Hop** field, enter the IP Address, FQDN or hostname of the next hop server.

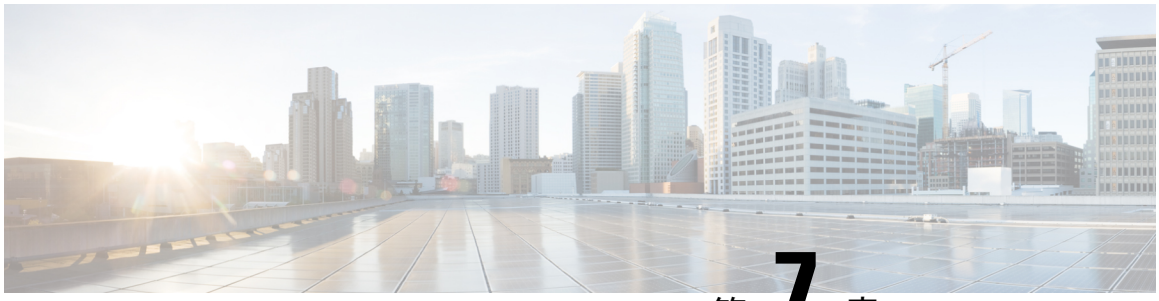
**ステップ 6** In the **Next Hop Port** field, enter the destination port on the Next Hop server.

**ステップ 7** From the **Protocol Type** dropdown, select the protocol for the static route, such as, TCP, UDP, or TLS.

**ステップ 8** Set the **Service** field to On if you want to be able to take a static route out of service without having to remove it completely from the system and add it again.

**ステップ 9** Uncheck the **Block Route** check box.

**ステップ 10** Click **Save**.



第 7 章

# Cisco 適応型セキュリティ アプライアンスを使用した SIP フェデレーション セキュリティ証明書の構成

ここでは、Cisco 適応型セキュリティ アプライアンスを使用した SIP フェデレーション セキュリティ証明書の構成について説明します。



# IM および Presence サービスと Cisco 適応型セキュリティ アプライアンス間のセキュリティ証明書の交換

ここでは、IM and Presence Service と Cisco 適応型セキュリティ アプライアンス間のセキュリティ証明書交換について説明します。

## Cisco 適応型セキュリティ アプライアンスでのキー ペアとトラストポイントの生成

この証明書のキー ペア（例 **imp_proxy_key**）を生成し、Cisco 適応型セキュリティ アプライアンス から IM and Presence Service への自己署名証明書を識別するトラストポイントを構成する必要があります（例 **imp_proxy**）。Cisco 適応型セキュリティ アプライアンス で自己署名証明書を生成していることを示すには、登録タイプを 「self」として指定し、内部インターフェイスの IP アドレスとして証明書のサブジェクト名を指定する必要があります。

### 始める前に

次の章で説明されている構成タスクが実行されていることを確認します。

- IM および Presence サービスでセキュリティ設定の構成
- SIP フェデレーション向け Cisco 適応型セキュリティ アプライアンスのワークフロー

---

**ステップ 1** Cisco 適応型セキュリティ アプライアンスで次のモードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** この証明書のキーペアを生成するには、次のコマンドを入力します。

```
crypto key generate rsa label imp_proxy_key modulus 1024
```

**ステップ 3** 次の一連のコマンドを入力して、 IM and Presence Serviceのトラストポイントを作成します。

```
crypto ca trustpoint trustpoint_name (for example, imp_proxy)
(config-ca-trustpoint)# enrollment self
(config-ca-trustpoint)# fqdn none
(config-ca-trustpoint)# subject-name cn=ASA_inside_interface_ip_address
(config-ca-trustpoint)# keypair imp_proxy_key
```

### トラブルシューティングのヒント

**show crypto key mypubkey rsa** コマンドを入力して、キー ペアが生成されたことを確認します。

---

### 次のタスク

Cisco 適応型セキュリティ アプライアンスで自己署名証明書の生成 （62 ページ）

# Cisco 適応型セキュリティ アプライアンスで自己署名証明書の生成

### 始める前に

- Cisco 適応型セキュリティ アプライアンスでのキー ペアとトラストポイントの生成 （61 ページ）の手順を完了します。
- この手順を実行するには、UNIX をサポートするテキスト エディタが必要です。Microsoft ワードパッド バージョン 5.1 または Microsoft メモ帳バージョン 5.1 サービス パック 2 を推奨します。

**ステップ 1** このコマンドを実行すると自己署名認証が生成されます。

```
(config-ca-trustpoint)# crypto ca enroll trustpoint_name (for example, imp_proxy)
```

**ステップ 2** サブジェクト名にデバイスのシリアル番号を含めるように求められたら、 **no** と入力します。

**ステップ 3** 自己署名証明書を生成するように求められたら、**[はい（yes）]** と入力します。

**ステップ 4** 次のコマンドを入力して、 IM and Presence Serviceにエクスポートする証明書を準備します。

```
crypto ca export imp_proxy identity-certificate
```

PEM エンコード ID 証明書が画面に表示されます。次に例を示します。

```
-----BEGIN CERTIFICATE-----MIIBnDCCAQWgAwIBAgIBMTANBgkqhkiG9w0BAQQFADAUMRIwEAYDVQQDEwlDVVAt……..
-----END CERTIFICATE-----
```

**ステップ 5** Cisco 適応型セキュリティ アプライアンス の証明書の内容全体をコピーして、拡張子 .pem を付けてワードパッドまたはメモ帳に貼り付けます。

**ステップ 6** .pem ファイルをローカル マシンに保存します。

### 次のタスク

IM and Presence Service への自己署名証明書のインポート （63 ページ）

# IM and Presence Service への自己署名証明書のインポート

### 始める前に

Cisco 適応型セキュリティ アプライアンスで自己署名証明書の生成 （62 ページ） の手順を実行します

**ステップ 1** **Cisco Unified IM and Presence Operating System Administration** ユーザー インターフェイスにログインします。**[Security（セキュリティ）]** > **[Certificate Management（証明書管理）]** を選択します。

**ステップ 2** **[証明書のアップロード]**をクリックします。

**ステップ 3** [証明書の用途（Certificate Purpose）] で **[cup-trust]** を選択します。

（注） [ルート名（Root Name）] フィールドはブランクのままにします。

**ステップ 4** **[参照（Browse）]** をクリックし、ローカル コンピュータで Cisco 適応型セキュリティ アプライアンス の .pem 証明書ファイル（前の手順で作成した）を見つけます。

**ステップ 5** **[ファイルのアップロード（Upload File）]** をクリックして、IM and Presence Service ノードに証明書をアップロードします。

### トラブルシューティングのヒント

証明書リストで検索を実行します。<asa ip address> .pem と <asa ip address>.der は証明書リストにあります。

### 次のタスク

IM および Presence サービスの新規証明書の生成 （64 ページ）

# IM および Presence サービスの新規証明書の生成

（注） Cisco ASA ファイアウォール証明書には、サーバー認証属性とクライアント認証属性が内部、外部に設定されている必要があります。これは、証明書の拡張キー使用法（EKU）パラメータまたはオブジェクト識別子（OID）値を確認することで確認できます。

1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2

### 始める前に

IM and Presence Service への自己署名証明書のインポート （63 ページ） の手順を実行します

**ステップ 1** **Cisco Unified IM and Presence Operating System Administration** ユーザー インターフェイスにログインします。**[Security（セキュリティ）]** > **[Certificate Management（証明書管理）]** を選択します。

**ステップ 2** [新規作成（Generate New）] をクリックします。

**ステップ 3** [証明書の目的（Certificate Purpose）]ドロップダウン リストから **cup** を選択します。

**ステップ 4** [生成（Generate）] をクリックします。

### 次のタスク

Cisco 適応型セキュリティ アプライアンスへの IM and Presence サービス証明書のインポート （64 ページ）

# Cisco 適応型セキュリティ アプライアンスへの IM and Presence サービス証明書のインポート

IM and Presence Service 証明書を Cisco 適応型セキュリティアプライアンス にインポートするには、トラストポイントを作成して IM and Presence Service からインポートされた証明書（**cert_from_imp など**）を識別し、登録タイプを 「terminal」 として指定する必要があります。そうすることで、IM and Presence Service から受信した証明書が端末に貼り付けられます。

（注） IM and Presence サービス と Cisco Unified Communications Manager ノード、および Cisco 適応型セキュリティ アプライアンス が同じ NTP ソースから同期されていることが重要です。

### 始める前に

- IM および Presence サービスの新規証明書の生成 （64 ページ）の手順を完了します。
- この手順を実行するには、UNIX をサポートするテキスト エディタが必要です。Microsoft ワードパッド バージョン 5.1 または Microsoft メモ帳バージョン 5.1 サービス パック 2 を推奨します。

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次の一連のコマンドを入力して、インポートされた IM and Presence Service 証明書のトラストポイントを作成します。

```
crypto ca trustpoint cert_from_imp enrollment terminal
```

**ステップ 3** IM and Presence Serviceから証明書をインポートするには、次のコマンドを入力します。

```
crypto ca authenticate cert_from_imp
```

**ステップ 4** **Cisco Unified IM and Presence Operating System Administration** ユーザー インターフェイスにログインします。IM and Presence Service の **[セキュリティ（Security）] > [証明書管理（Certificate Management）]** を選択します。.

**ステップ 5** [検索（Find）] をクリックします。

**ステップ 6** 前の手順で作成した IM and Presence Service 証明書を見つけます。

**ステップ 7** [ダウンロード（Download）] をクリックします。

**ステップ 8** 推奨されるテキスト エディタのいずれかを使用して、imp.pem ファイルを開きます。

**ステップ 9** Cisco 適応型セキュリティ アプライアンス の端末に、imp.pem の内容をカット アンド ペーストします。

**ステップ 10** **[終了（quit）]** を入力します。

**ステップ 11** 証明書を受け入れるように求められたら、**yes** を入力します。

**ステップ 12** 証明書を表示するには、 **show crypto ca certificate** コマンドを実行します。

**次に行う作業**：

Microsoft CA を使用した Cisco 適応型セキュリティアプライアンスと Microsoft Access Edge（外部インターフェイス）間のセキュリティ証明書の交換 （66 ページ）

# Microsoft CA を使用した Cisco 適応型セキュリティアプライアンスと Microsoft Access Edge（外部インターフェイス）間のセキュリティ証明書の交換

これらの手順は例であり、Microsoft CA を使用して証明書を構成する方法を示しています。

（注） VeriSign CA を使用したこの手順の例は、このガイドの付録に記載されています。

## CA トラストポイント

トラストポイントを生成する場合は、トラストポイントで使用する登録方式を指定する必要があります。登録方式として Simple Certificate Enrollment Process（SCEP）を使用できます（Microsoft CA を使用している場合）。この場合、 **enrollment url** コマンドを使用して、宣言したトラストポイントで SCEP 登録に使用する URL を定義します。定義する URL は CA の URL である必要があります。

登録方法として手動登録を使用することもできます。この場合、 **enrollment terminal** コマンドを使用して、CA から受信した証明書を端末に貼り付けます。このセクションでは、両方の登録方法の手順について説明します。登録方法の詳細については、『*Cisco* セキュリティ アプライアンス コマンド ライン構成ガイド』 を参照してください。

SCEP を使用するには、次の URL から Microsoft SCEP アドオンをダウンロードする必要があります。

http://www.microsoft.com/Downloads/details.aspx?familyid=9F306763-D036-41D8-8860-1636411B2D01&displaylang=en

SCEP アドオンは、証明書を構成する Microsoft CA にインストールする必要があります。

次のように SCEP アドオンをダウンロードします。

- **scepsetup.exe** をダウンロードして実行します。
- **ローカル システム アカウント**を選択します。
- **[登録する SCEP チャレンジ フレーズ（SCEP challenge phrase to enroll）]** を選択解除します。
- CA の詳細を入力します。

**[完了（Finish）]** をクリックしたら、SCEP URL を取得します。この URL は、Cisco 適応型セキュリティ アプライアンスでのトラストポイント登録時に使用します。

# SCEPを使用したCisco適応型セキュリティアプライアンスでの証明書の構成

**ステップ 1** このコマンドを入力して、CA のキー ペアを生成します。

**crypto key generate rsa label** *public_key_for_ca* **modulus 1024**

**ステップ 2** CA を識別するトラストポイントを生成するには、このコマンドを入力します。

**crypto ca trustpoint** *trustpoint_name*

**ステップ 3** **client-types** コマンドを使用して、ユーザー接続に関連付けられている証明書を検証するために使用可能なトラストポイントの、クライアント接続タイプを指定します。このトラストポイントを使用してSSL クライアント接続を検証できることを示す **client-types ssl** 構成を指定するには、次のコマンドを入力します。

```
(config-ca-trustpoint)# client-types ssl
```

**ステップ 4** 次のコマンドを入力して、 IM and Presence Service のパブリック アドレスの FQDN を構成します。

**fqdn** *fqdn_public_imp_address*

（注） ここで、VPN 認証に関する警告が表示される場合があります。

**ステップ 5** トラストポイントのキーペアを構成するには、次のコマンドを入力します。

**keypair** *public_key_for_ca*

**ステップ 6** このコマンドを入力して、トラストポイントの登録方法を構成します。

**enrollment url http://***ca_ip_address***/certsrv/mscep/mscep.dll**

**ステップ 7** このコマンドを入力して、構成したトラストポイントの CA 証明書を取得します。

**crypto ca authenticate** *trustpoint_name*

情報: 証明書に次の属性があります：フィンガープリント：cc966ba6 90dfe235 6fe632fc 2e521e48

**ステップ 8** CA からの証明書を受け入れるように求められたら、 **[はい（yes）]** と入力します。

```
Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

**ステップ 9** **crypto ca Enroll** コマンドを実行します。

**crypto ca enroll** *trustpoint_name*

次の警告が表示されます。

%警告：証明書の登録は、システム fqdn とは異なる fqdn で設定されています。この証明書が VPN 認証に使用される場合、接続の問題が発生する可能性があります。

**ステップ 10** 証明書の登録を続行するように求められたら、 **yes** と入力します。

この登録を続行しますか。[yes/no]: **yes**

```
% 証明書の登録開始..
```

**ステップ 11** チャレンジ パスワードの作成を求められたら、パスワードを入力します。

```
% Create a challenge password. 証明書を失効させるには、このパスワードを CA 管理者に口頭で伝える必要があります。For security reasons your password will not be saved in the configuration. Please make a note of it.

パスワード：<password>

********** パスワードの再入力： **********
```

**ステップ 12** サブジェクト名にデバイスのシリアル番号を含めるように求められたら、 **no** と入力します。

**ステップ 13** CA から証明書を要求するように求められたら、 **[はい（yes）]** と入力します。

```
CA サーバからの証明書を要求しますか？[yes/no]: yes

% 証明機関に証明書要求を送信します
```

**ステップ 14** CA に移動し、保留中の証明書を発行します（証明書が自動的に発行されなかった場合）。

### 次のタスク

外部 Access Edge インターフェイスの証明書構成 （70 ページ）

# 手動登録を使用した Cisco 適応型セキュリティ アプライアンスでの証明書の構成

CA 証明書のアップロードによるトラストポイントの登録：

**ステップ 1** 次のコマンドを入力して、CA のキー ペアを生成します。

**crypto key generate rsa label** *public_key_for_ca* **modulus 1024**

**ステップ 2** 次の一連のコマンドを入力して、CA を識別するトラストポイントを生成します。

**crypto ca trustpoint** *trustpoint_name* **fqdn** *fqdn_public_imp_address* **client-types ssl keypair** *public_key_for_ca*

（注）
- FQDN 値は、パブリック IM and Presence Service アドレスの FQDN である必要があります。
- キーペアの値は、CA 用に作成されたキーペアである必要があります。

**ステップ 3** 次のコマンドを入力して、トラストポイントの登録方式を設定します。

**enrollment terminal**

**ステップ 4** 次のコマンドを入力して、証明書を認証します。

**crypto ca authenticate** *trustpoint_name*

**ステップ 5** CA のルート証明書を取得します。

a) CA Web ページに移動します（例 ：`http(s)://ca_ip_address/certsrv` ）。
b) [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）] をクリックします。
c) **[Base 64 エンコード（Base 64 encoded）]** を選択します。
d) CA 証明書をダウンロードします。
e) 証明書を `CARoot.cer` として保存します。

**ステップ 6** ルート証明書（.cer）をテキストエディタで開きます。

**ステップ 7** 証明書の内容をコピーして、Cisco 適応型セキュリティ アプライアンス の端末に貼り付けます。

**ステップ 8** 証明書を受け入れるように求められたら、**yes** を入力します。

Cisco 適応型セキュリティアプライアンス 公開証明書の CSR の生成。

**ステップ 9** CA に登録要求を送信するには、次のコマンドを入力します。

```
crypto ca enroll trustpoint_name
```

**ステップ 10** サブジェクト名にデバイスのシリアル番号を含めるかどうかを尋ねられたら、 **no** と入力します。

**ステップ 11** 証明書要求を端末に表示するよう求められたら、 **yes** と入力します。

**ステップ 12** この Base-64 証明書をコピーしてテキスト エディタに貼り付けます（後の手順で使用します）。

**ステップ 13** 登録要求を再表示するように求められたら、 **no** と入力します。

**ステップ 14** （ステップ 4 でコピーした）base-64 証明書を CA の証明書要求ページに貼り付けます。

a) CA Web ページに移動します（例：`http(s)://ca_ip_address/certsrv`）。
b) [証明書を要求する（Request a certificate）] をクリックします。
c) **[詳細な証明書要求（Advanced certificate request）]** をクリックします。
d) **[Base 64エンコード形式のCMSまたはPKCS 10ファイルを使用して証明書要求を送信...（Submit a certificate request by using the base-64-encoded CMS or PKCS 10 file...）]** を選択します。
e) Base-64 証明書（手順 4 でコピーしたもの）を貼り付けます。
f) 要求を送信し、CA から証明書を発行します。
g) 証明書をダウンロードし、*.cer ファイルとして保存します。
h) テキスト エディタで証明書を開き、内容をコピーして端末に貼り付けます。別の行に単語「**quit**」で終了します。

**ステップ 15** 次のコマンドを入力して、CA から受信した証明書をインポートします。

```
crypto ca import trustpoint_name certificate
```

**ステップ 16** 登録を続行するかどうかを尋ねられたら、 **yes** と入力します。

**次の作業**：

外部 Access Edge インターフェイスの証明書構成 （70 ページ）

# 外部 Access Edge インターフェイスの証明書構成

この手順では、スタンドアロン CA を使用して Access Edge サーバーで証明書を設定する方法について説明します。

## CA 証明書チェーンのダウンロード

**ステップ 1** Access Edge サーバで、**[開始（Start）]**、> **[実行（Run）]** の順に選択します。

**ステップ 2** **`http://<name of your Issuing CA Server>/certsrv`** を選択し、**[OK]** をクリックします。

**ステップ 3** [タスクの選択（Select a task）] メニューから、**[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）]** をクリックします。

**ステップ 4** [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）] メニューから **[CA 証明書チェーンのダウンロード（Download CA certificate chain）]** をクリックします。

**ステップ 5** [File Download] ダイアログボックスで、[Save] をクリックします。

**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。このファイルの拡張子は .p7 です。この .p7b ファイルを開くと、チェーンに次の 2 つの証明書が表示されます。

a) スタンドアロン ルート CA 証明書の名前

b) スタンドアロン下位 CA 証明書の名前（存在する場合）

### 次のタスク

CA 証明書チェーンのインストール （70 ページ）

## CA 証明書チェーンのインストール

### 始める前に

CA 証明書チェーンのダウンロード （70 ページ） の手順を実行します

**ステップ 1** **[Start]** > **[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）] メニューで **[スナップインの追加または削除（Add/Remove Snap-in）]** を選択します。

**ステップ 4** [スナップインの追加または削除（Add/Remove Snap-in）] ダイアログ ボックスで、**[追加（Add）]** をクリックします。

**ステップ 5** [利用可能なスタンドアロン スナップイン（Available Standalone Snap-ins）] のリストで、**[証明書（Certificates）]** を選択します。

**ステップ 6** [Add] をクリックします。

**ステップ 7** **[コンピュータ アカウント（Computer account）]** を選択します。

**ステップ 8** [次へ（Next)] をクリックします。

**ステップ 9** [コンピュータの選択（Select Computer）] ダイアログ ボックスで、次のタスクを実行します。

a) 次のことを確認します。<Local Computer> **（このコンソールを実行しているコンピュータ）** が選択されていることを確認します。

b) **[終了]** をクリックします。

**ステップ 10** [閉じる（Close）] をクリックします。

**ステップ 11** [OK] をクリックします。

**ステップ 12** [証明書（Certificates）] コンソールの左側のペインで、**[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 13** 信頼できるルート認証局を拡張します。

**ステップ 14** **[証明書（Certificates）]** を右クリックし、[すべてのタスク（All Tasks）] をポイントします。

**ステップ 15** [インポート（Import）] をクリックします。

**ステップ 16** [インポート（Import）] ウィザードで、**[次へ（Next）]** をクリックします。

**ステップ 17** **[参照（Browse）]** をクリックし、証明書チェーンを保存した場所に移動します。

**ステップ 18** ファイルを選択し、**[開く（Open）]** をクリックします。

**ステップ 19** [次へ（Next)] をクリックします。

**ステップ 20** デフォルト値 **[すべての証明書をストアに配置（Place all certificates in the store）]** のままにし、[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）] が表示されるようにします。

**ステップ 21** [次へ（Next）] をクリックします。

**ステップ 22** **[完了（Finish）]** をクリックします。

### 次のタスク

CA サーバーからの証明書の要求 （71 ページ）

## CA サーバーからの証明書の要求

### 始める前に

CA 証明書チェーンのインストール （70 ページ） の手順を実行します

**ステップ 1** Access Edge サーバーにログインし、Web ブラウザを開きます。

**ステップ 2** 次の URL を開きます。**http://***certificate_authority_server_IP_address***/certsrv**

**ステップ 3** [証明書を要求する（Request a Certificate）] をクリックします。

**ステップ 4** **[詳細な証明書要求（Advanced certificate request）]** をクリックします。

**ステップ 5** **[この CA に要求を作成して送信する（Create and submit a request to this CA）]** をクリックします。

**ステップ 6** [必要な証明書のタイプ（Type of Certificate Needed）] リストで、**[その他（ Other）]** をクリックします。

**ステップ 7** サブジェクト共通名のアクセス エッジ外部インターフェイスの FQDN を入力します。

**ステップ 8** [オブジェクト識別子（OID）（Object Identifier (OID)）] フィールドに、次の値を入力します。

1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2

（注） OID の中央にある 2 つの 1 はカンマで区切ります。

**ステップ 9** 次のいずれかの手順を実行します。

a) Windows Certificate Authority 2003 を使用している場合は、[キー オプション（Key Options）] で、**[ローカル コンピュータの証明書ストアに証明書を保存する（Store certificate in the local computer certificate store）]** チェックボックスをオンにします。

b) Windows Certificate Authority 2008 を使用している場合は、このセクションのトラブルシューティングのヒントで説明されている回避策を参照してください。

**ステップ 10** わかりやすい名前を入力します。

**ステップ 11** [Submit] をクリックします。

---

**次のタスク**

CA サーバーからの証明書のダウンロード （72 ページ）

## CA サーバーからの証明書のダウンロード

**始める前に**

CA サーバーからの証明書の要求 （71 ページ） の手順を実行します

---

**ステップ 1** **[開始（Start）] > [管理ツール（Administrative Tools）] > [証明書権限（Certificate Authority）]** の順に選択して、CA コンソールを起動します。

**ステップ 2** 左側のペインで、**[保留中の要求（Pending Requests）]** をクリックします。

**ステップ 3** 右側のペインで、送信した証明書要求を右クリックします。

**ステップ 4** **[すべてのタスク（All Tasks）] > [問題（Issue）]** を選択します。

**ステップ 5** CA が実行されている Access Edge サーバーで `http://local_server/certsrv` を開きます。

**ステップ 6** **[保留中の証明書要求のステータスを表示する（View the status of a pending certificate request）]** をクリックします。

**ステップ 7** **[この証明書をインストールする（Install this certificate）]** をクリックします。

---

**次のタスク**

Access Edge への証明書のアップロード （72 ページ）

## Access Edge への証明書のアップロード

この手順では、証明書ウィザードを使用して Access Edge サーバーに証明書をアップロードする方法について説明します。**[Microsoft Office Communications Server 2007 > [プロパティ >**

**[Edge Interfaces]** を選択して、Access Edge サーバーに証明書を手動でインポートすることもできます。

**始める前に**

CA サーバーからの証明書のダウンロード （72 ページ） の手順を実行します

**ステップ 1** Access Edge サーバーで、**[開始（Start）]** > **[管理ツール（Administrative Tools）]** > **[コンピュータ管理（Computer Management）]** を選択します。

**ステップ 2** 左側のペインで、**[Microsoft Office Communications Server 2007]** を右クリックします。

**ステップ 3** [Certificates] をクリックします。

**ステップ 4** [次へ（Next)] をクリックします。

**ステップ 5** **[既存の証明書タスクの割り当て（Assign an existing certificate task）]** オプションをクリックします。

**ステップ 6** [次へ（Next)] をクリックします。

**ステップ 7** 外部 Access Edge インターフェイスに使用する証明書を選択し、**[次へ（Next）]** をクリックします。

**ステップ 8** [次へ（Next)] をクリックします。

**ステップ 9** **[Edge サーバー パブリック インターフェイス（Edge Server Public Interface）]** チェックボックスをオンにし、**[次へ（Next）]** をクリックします。

**ステップ 10** [次へ（Next）] をクリックします。

**ステップ 11** **[完了（Finish）]** をクリックします。

**次の作業：**

TLS プロキシ

# Create Custom Certificate for Access Edge Using Enterprise Certificate Authority

Refer to these instructions if you are using a Microsoft Enterprise CA to issue a client/server role certificate to the external interface of Access Edge or to the public interface of the Cisco Adaptive Security Appliance.

### Before you begin

These steps require that the Certificate Authority (CA) is an Enterprise CA and is installed on the Enterprise Edition of either Windows Server 2003 or 2008.

For additional details about these steps, refer to the Microsoft instructions:
http://technet.microsoft.com/en-us/library/bb694035.aspx

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| ステップ 1 | Perform the steps as mentioned above. | |

## Create and Issue a Custom Certificate Template

ステップ 1 Follow Steps 1- 6 from the Microsoft site: Creating and Issuing the Site Server Signing Certificate Template on the Certification Authority.

http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver1

**Tip** For Step 5, use a more appropriate name for this specific template, such as Mutual Authentication Certificate.

ステップ 2 Follow these steps in place of Steps 7-12 from the Microsoft site:

a) Choose the **Extensions** tab. Make sure that under **Application Policies** that both **Client Authentication** and **Server Authentication** are present and that no other Policies are present. If these policies are not available, then you must add them before proceeding.

- In the **Edit Application Policies Extension** dialog box, click **Add**.
- In the **Add Application Policy** dialog box, choose **Client Authentication**, press Shift and choose **Server Authentication**, and then click **Add**.
- In the **Edit Application Policies Extension** dialog box, choose any other policy that may be present and then click **Remove**.

In the **Properties of New Template** dialog box, you should now see listed as the description of Application Policies: Client Authentication, Server Authentication.

b) Choose the **Issuance Requirement** tab. If you do not want the Certificate to be automatically issued, then choose **CA certificate manager approval**. Otherwise, leave this option blank.
c) Choose the **Security** tab and ensure that all required users and groups have both read and enroll permission.
d) Choose the **Request Handling** tab and click the **CSP** button.
e) On the **CSP Selection** dialog box choose **Requests must use one of the following CSP's**.
f) From the list of CSP's choose **Microsoft Basic Cryptographic Provider v1.0 and Microsoft Enhanced Cryptographic Provider v1.0**, and click **OK**.

ステップ 3 Continue with Steps 13-15 from the Microsoft site: Creating and Issuing the Site Server Signing Certificate Template on the Certification Authority.

http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver1

### What to do next

Request Site Server Signing Certificate, on page 74

## Request Site Server Signing Certificate

ステップ 1 Follow Steps 1-6 from the Microsoft site: Site Server Signing Certificate for the Server That Will Run the Configuration Manager 2007 Site Server.

http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver2

**Tip** For Step 5, select the name of the certificate template you created previously, such as Mutual Authentication Certificate and enter the external FQDN of the access edge in the **Name** field.

**ステップ 2** Follow these steps in place of Steps 7-8 from the Microsoft site:

a) If the certificate request is automatically issued then you are presented with an option to install the signed certificate. Select **Install this Certificate**.

b) If the certificate request is not automatically issued then you must wait for the administrator to issue the certificate. Once issued:

- On the member server, load Internet Explorer and connect to the Web enrollment service with the address `http://<server>/certsrv` where `<server>` is the name or IP address of the Enterprise CA.
- On the Welcome page, choose **View the status of a pending certificate request**.

c) Choose the issued certificate and click **Install this Certificate**.

# Security Certificate Configuration on Lync Edge Server for TLS Federation

The following guide from Microsoft's TechNet Library (http://technet.microsoft.com/en-us/library/gg398409.aspx) explains how to configure certificates on Access Edge for TLS federation with Microsoft Lync. The IM and Presence Service requires Mutual TLS authentication for federated connections, therefore you must configure Microsoft Lync certificates to support both Server and Client Authentication. You can use this guide to configure Lync Server to federate directly with the IM and Presence Service over TLS.

For information about how to configure static routes on Lync server for direct federation, see Lync から IM および Presence へのスタティック ルートの構成, on page 128.

# Cisco 適応型セキュリティ アプライアンスと AOL SIP アクセス ゲートウェイ間のセキュリティ証明書の交換

AOL では、Cisco 適応型セキュリティ アプライアンス の証明書が信頼できる認証局（CA）によって署名されている必要があります。AOL には、Windows で一般的に使用されている CA や、主要なブラウザで配布されるライブラリ内の CA など、確立された信頼リストがあります。AOL 信頼リストにない CA を使用する場合は、Cisco の担当者と協力して、この情報を AOL に提供してください。

このガイドの付録には、Verisign CA を使用して Cisco 適応型セキュリティ アプライアンス と外部ドメイン（Microsoft Access Edge）との間の証明書交換を構成する方法を詳細に説明する構成ワークフローの例が記載されています。この手順は、Verisign CA を使用して Cisco 適応型セキュリティ アプライアンス と AOL SIP アクセス ゲートウェイ間の証明書交換を構成するための参考資料として使用します。手順の概要を以下に示します。

Verisign CA を使用して Cisco 適応型セキュリティアプライアンス と AOL SIP アクセスゲートウェイ間の証明書交換を構成するには、次の手順を実行します。

**AOL ルート証明書と中間証明書を ASA にアップロードします。**

- AOL ルート証明書を http://www.entrust.com/root-certificates/entrust_2048_ca.cer からダウンロードします。
- AOL リーフ証明書を http://www.entrust.com/root-certificates/entrust_l1c.cer からダウンロードします。
- 古い中間証明書と署名付き証明書、および Cisco 適応型セキュリティ アプライアンスのルート証明書のトラストポイントを削除します。
- Cisco 適応型セキュリティ アプライアンス で AOL ルート証明書用の新しいトラストポイントを作成します。セクション Cisco 適応型セキュリティ アプライアンスへの IM and Presence サービス証明書のインポート （64 ページ） を参照してください（ステップ 1 ～ 3）。
- Cisco 適応型セキュリティ アプライアンス で、AOL リーフ証明書用の新しいトラストポイントを作成します。

**公開認証局（Verisign）を使用して ASA 証明書に署名します。**

- Cisco 適応型セキュリティ アプライアンスで Verisign CA の新しいトラストポイントを作成します。
- Cisco 適応型セキュリティ アプライアンスで、ルート証明書をインポートし、証明書署名要求（CSR）を生成します。同様の手順については、セクション 手動登録を使用した Cisco 適応型セキュリティ アプライアンスでの証明書の構成 （68 ページ） を参照してください。

（注） IM および Presence サービス ノード証明書のサブジェクト CN は、 IM および Presence サービス ノードの FQDN と一致する必要があります。 IM および Presence サービス および CN 用の Cisco適応型セキュリティアプライアンス のパブリック証明書は、 **フェデレーション ルーティング IM および Presence FQDN** サービス パラメータ値と同じである必要があります。

- CSR を Verisign CA に送信します。
- Verisign CA は、次の証明書を提供します。
  - Verisign 署名付き証明書
  - Verisign 下位中間ルート証明書
  - Verisign root CA 証明書
- Cisco適応型セキュリティアプライアンスで、証明書署名要求の生成に使用された一時ルート証明書を削除します。

- Verisign の下位中間ルート証明書を Cisco 適応型セキュリティ アプライアンスにインポートします。
- Cisco 適応型セキュリティ アプライアンスで Verisign ルート CA 証明書のトラストポイントを作成します。
- Verisign ルート CA 証明書を Cisco 適応型セキュリティ アプライアンスにインポートしてから、Verisign 署名付き証明書を Cisco 適応型セキュリティ アプライアンスにインポートします。
- AOL に VeriSign ルート証明書と中間証明書を提供します。

（注） CA が AOL 信頼リストに含まれていない場合は、AOL にルート CA を提供する必要があります。

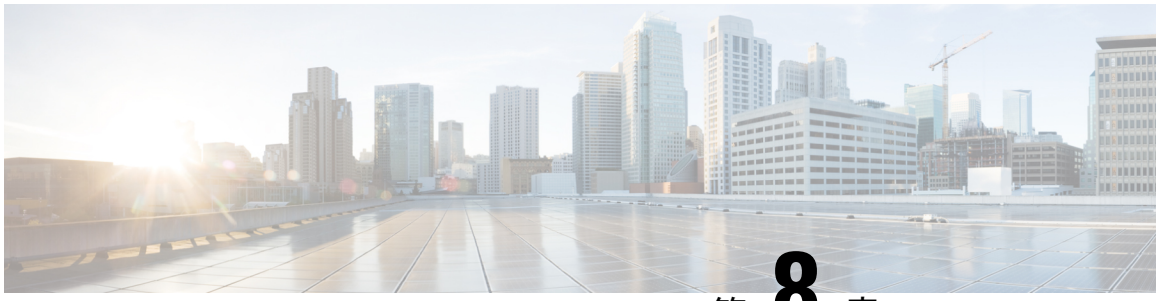
**関連情報**：

Cisco 適応型セキュリティ アプライアンスへの IM and Presence サービス証明書のインポート

手動登録を使用した Cisco 適応型セキュリティ アプライアンスでの証明書の構成

VeriSign を使用した Cisco 適応型セキュリティアプライアンスと Microsoft Access Edge 間のセキュリティ証明書の交換

AOL ルーティング情報の要件



第 8 章

# SIP フェデレーションのための Cisco 適応型セキュリティ アプライアンスの構成

ここでは、SIP フェデレーション用の Cisco 適応型セキュリティ アプライアンスの設定について説明します。



## Cisco 適応型セキュリティ アプライアンス ユニファイド コミュニケーション ウィザード

ドメイン間フェデレーション展開に単一の IM and Presence Service を展開する場合は、Cisco 適応型セキュリティアプライアンス の Unified Communication ウィザードを使用して、Cisco 適応型セキュリティアプライアンス と IM and Presence Service間のプレゼンス フェデレーション プロキシを構成できます。

Unified Communication ウィザードを示す構成例は、 適応型セキュリティ アプライアンス のドキュメント Wiki で提供されています。次の URL を参照してください。

### 関連情報

Cisco Unified Presence リリース 8.x

# 外部および内部インターフェイスの構成

Cisco 適応型セキュリティ アプライアンス では、次のように 2 つのインターフェイスを構成する必要があります。

- 1 つのインターフェイスを外部インターフェイスまたは外部インターフェイスとして使用します。これは、インターネットおよび外部ドメイン サーバ（Microsoft Access Edge/Access Proxy など）へのインターフェイスです。
- 2 番目のインターフェイスを内部インターフェイスまたは内部インターフェイスとして使用します。これは、展開に応じて、 IM and Presence Service またはロード バランサへのインターフェイスです。
- インターフェイスを構成する場合は、インターフェイス タイプ（イーサネットやギガビット イーサネットなど）とインターフェイス スロットを指定する必要があります。Cisco 適応型セキュリティ アプライアンス には、スロット 0 に 4 つの組み込みイーサネットまたはギガビット イーサネット ポートがあります。オプションで、スロット 1 に SSM-4GE モジュールを追加して、スロット 1 に 4 つのギガビット イーサネット ポートを追加できます。
- トラフィックをルーティングするインターフェイスごとに、インターフェイス名と IP アドレスを構成する必要があります。内部インターフェイスと外部インターフェイスの IP アドレスは、異なるサブネットに存在する必要があります。つまり、異なるサブマスクが必要です。
- 各インターフェイスには、0 ～ 100（最低から最高）までのセキュリティ レベル範囲が必要です。セキュリティ レベル値 100 は、最もセキュアなインターフェイス（内部インターフェイス）です。セキュリティ レベル値 0 は、最も安全性の低いインターフェイスです。内部インターフェイスまたは外部インターフェイスのセキュリティ レベルを明示的に設定しない場合、Cisco 適応型セキュリティ アプライアンス はセキュリティ レベルをデフォルトで 100 に設定します。
- CLI を使用した外部および内部インターフェイスの設定の詳細については、『*Cisco* セキュリティ アプライアンス コマンド ライン構成ガイド』を参照してください。

（注） ASDM スタートアップ ウィザードを使用して、内部インターフェイスと外部インターフェイスを構成できます。**[構成（Configuration）]** > **[デバイス設定（Device Setup）]** > **[インターフェイス（Interfaces）]** を選択して、ASDM でインターフェイスを表示または編集することもできます。

# スタティック IP ルートの構成

Cisco 適応型セキュリティ アプライアンス は、スタティック ルートと、OSPF、RIP、EIGRP などのダイナミック ルーティング プロトコルの両方をサポートします。この統合では、Cisco 適応型セキュリティ アプライアンスの内部インターフェイスにルーティングされる IP トラフィックと外部インターフェイスにルーティングされるトラフィックのネクスト ホップ アドレスを定義するスタティック ルートを構成する必要があります。次の手順では、dest_ip mask は接続先ネットワークの IP アドレスであり、gateway_ip 値はネクストホップ ルータまたはゲートウェイのアドレスです。

Cisco 適応型セキュリティ アプライアンスでのデフォルトルートおよびスタティック ルートの設定の詳細については、『*Cisco* セキュリティ アプライアンス コマンド ライン構成ガイド』を参照してください。

### 始める前に

外部および内部インターフェイスの構成 （80 ページ） の手順を実行します

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 内部インターフェイスのスタティック ルートを追加するには、次のコマンドを入力します。

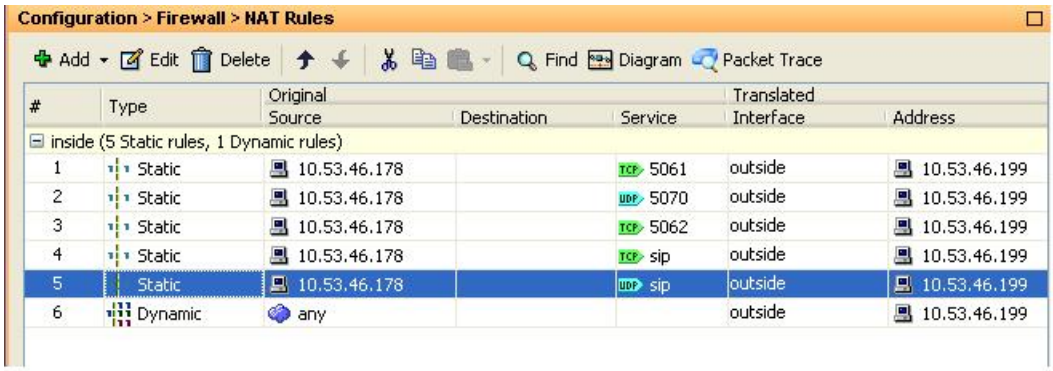
```
hostname(config)# route inside dest_ip mask gateway_ip
```

**ステップ 3** 次のコマンドを入力して、外部インターフェイスのスタティック ルートを追加します。

```
hostname(config)# route outside dest_ip mask gateway_ip
```

（注） また、**[構成（Configuration）] > [デバイス セットアップ（Device Setup）] > [ルーティング（Routing）] > [スタティック ルート（Static routes）]** を選択して、ASDM からスタティック ルートを表示および構成することもできます。

図 *18 : ASDM* を介したスタティック ルートの表示




次のタスク

ポート アドレス変換（PAT） （82 ページ）

# ポート アドレス変換（PAT）

ここでは、ポート アドレス変換の概念について説明します。

## この統合向けのポート アドレス変換

（注） 外部ドメイン内の別の IM および Presence サービス エンタープライズ展開とフェデレーションする場合も、ポート アドレス変換を使用します。

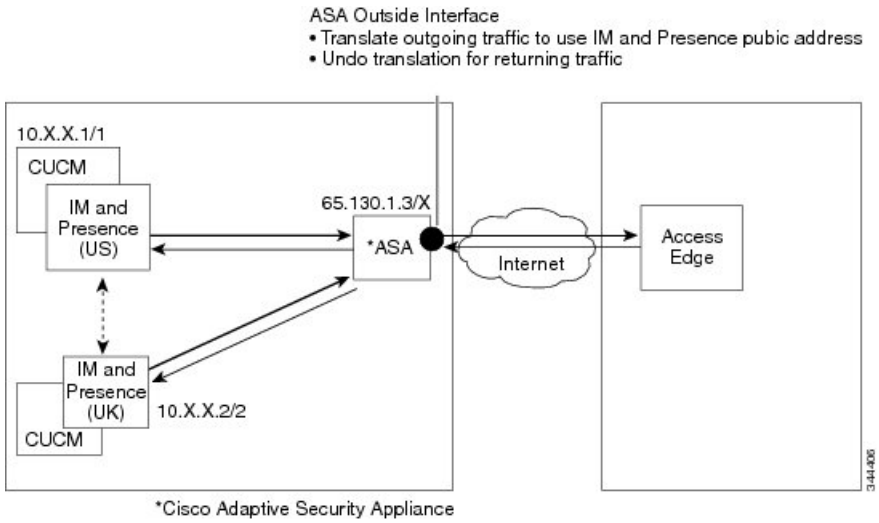
この統合のために、Cisco 適応型セキュリティ アプライアンス はポート アドレス変換（PAT）とスタティック PAT を使用してメッセージ アドレスを変換します。Cisco 適応型セキュリティ アプライアンス は、この統合にネットワークアドレス変換（NAT）を使用しません。

この統合では、PAT を使用して、 IM および Presence サービス から外部ドメインに送信されたメッセージを変換します（プライベート メッセージからパブリック メッセージへ）。ポート アドレス変換（PAT）は、パケット内の実際のアドレスを、宛先ネットワーク上でルーティング可能な、マッピングされた固有のポートと置き換えることを意味します。この変換方式では、実際の IP アドレスとポートをマッピング IP アドレスとポートに変換する 2 段階のプロセスを使用します。その後、変換はリターン トラフィックに対して「取り消されます」。

Cisco 適応型セキュリティ アプライアンスは、IM および Presence サービスのプライベート IP アドレスとポートを、パブリック IP アドレスと 1 つ以上のパブリック ポートに変更することで、IM および Presence サービスから外部ドメイン（プライベート メッセージからパブリック メッセージ）に送信されたメッセージを変換します。したがって、ローカル IM および Presence

サービス ドメインは 1 つのパブリック IP アドレスのみを使用します。Cisco IM および Presence サービスは、次の図に示すように、NAT コマンドを外部インターフェイスに割り当て、そのインターフェイスで受信したメッセージの IP アドレスとポートを変換します。

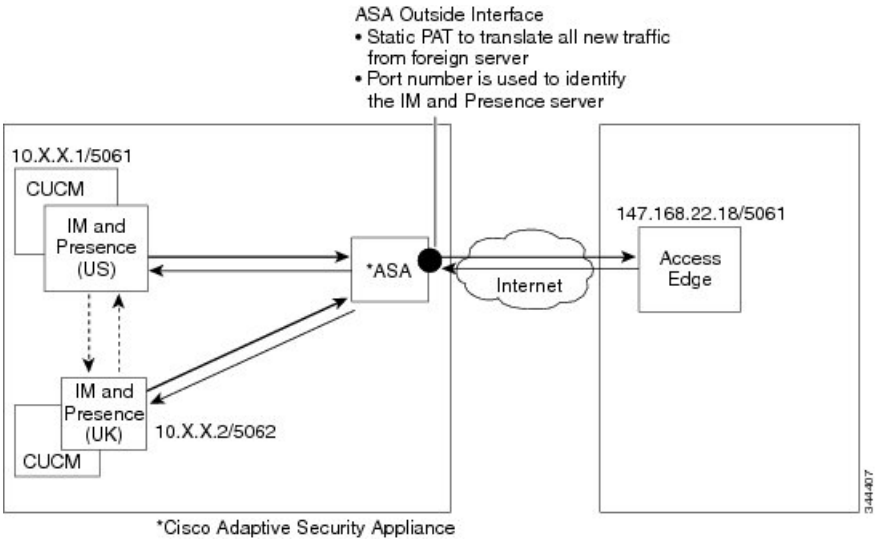
**図 *19 : IM* および *Presence* サービスから外部ドメインに発信されるメッセージの *PAT* の例**




外部ドメインから IM および Presence サービスに送信された新しいメッセージの場合、Cisco 適応型セキュリティ アプライアンス はスタティック PAT を使用して、IM および Presence サービスのパブリック IP アドレスとポートに送信されたメッセージを、指定された IM および Presence サービス ノードにマッピングします。スタティック PAT を使用すると、実際の IP アドレスをマッピング IP アドレスに変換し、実際のポート番号をマッピング ポート番号に変換できます。実際のポート番号を同じポート番号または別のポート番号に変換できます。この場合、次の図に示すように、ポート番号はメッセージ要求を処理する正しい IM および Presence サービス ノードを識別します。

（注） ユーザーが IM および Presence サービス ノードに存在しない場合、 IM および Presence サービス ルーティング ノードはクラスタ間ルーティングを使用してメッセージをリダイレクトします。すべての応答は、 IM および Presence サービス ルーティング ノードから Cisco 適応型セキュリティ アプライアンス に送信されます。

図 *20 :* 外部ドメインから発信されたメッセージのスタティック *PAT*




# プライベートからパブリックへの要求の PAT

この統合では、プライベート メッセージからパブリック メッセージへのアドレス変換に次の構成が含まれます。

- 変換する実際の IP アドレスとポート番号を識別する NAT ルールを定義します。この場合、Cisco 適応型セキュリティ アプライアンスが内部インターフェイスで受信したすべてのメッセージに NAT アクションを適用する必要があることを示す NAT ルールを構成します。
- グローバル NAT アクションを設定して、外部（外部）インターフェイスを通過するメッセージに使用するマッピング アドレスを指定します。この統合では、アドレスを 1 つだけ指定します（PAT を使用するため）。NAT アクションは、（内部インターフェイスで受信したメッセージの）IP アドレスを IM および Presence サービスのパブリック アドレスにマッピングします。

次の表に、Cisco 適応型セキュリティ アプライアンス リリース 8.2 および 8.3 のグローバル アドレス変換コマンドの例を示します。最初の行は、単一の IM および Presence サービス展開と複数の IM および Presence サービス展開の両方に必須です。2 番目の行は、単一の IM および Presence サービス展開専用です。3 番目の行は、複数の IM および Presence サービス展開用です。

表 *12 :* グローバル アドレス変換コマンドの例

| 構成サンプル | Cisco 適応型セキュリティ アプライアンス リリース 8.2 グローバル コマンド | Cisco 適応型セキュリティ アプライアンス リリース 8.3 グローバル コマンド |
|---|---|---|
| この NAT 設定例は、内部インターフェイスに 1 つ以上の IM および Presence サービス ノードがあり、他のファイア ウォール トラフィックがない展開で使用できます。 | **global (outside) 1** *public_imp_address* **nat (inside) 1 0 0** | **object network obj_any host 0.0.0.0 nat (inside,outside) dynamic** *public_imp_address* |
| この NAT 設定例は、内部インターフェイスに 1 つの IM および Presence サービス ノードがあり、他のファイアウォール トラフィックがある展開で使用できます。 | **global (outside) 1** *public_imp_address* **nat (inside) 1** *private_imp_address* **255.255.255.255 global (outside) 2 interface nat (inside) 2 0 0** | **host** *private_imp_address* **nat (inside,outside) dynamic** *public_imp_address*<br>**object network** *my_inside* **subnet 0.0.0.0 0.0.0.0 nat**（内部、外部）動的インターフェイス |
| この NAT 構成例は、内部インターフェイスに複数の IM および Presence サービス ノードがあり、他のファイアウォール トラフィックがある展開で使用できます。 | **global (outside) 1** *public_imp_ip* **nat (inside) 1** *private_imp_net private_imp_netmask*<br>**global**（**outside**）**2 interface nat**（**inside**）**2 0 0** | **object network** *obj_private_subnet.0_255.255.255.0* **subnet** *private_subnet* **255.255.255.0 nat (inside,outside) dynamic** *public_imp_address*<br>**object network** *my_inside* **subnet 0.0.0.0 0.0.0.0 nat (inside,outside) dynamic interface** |

（注） 表の最後の行に示されている構成例は、Cisco 適応型セキュリティ アプライアンス の背後に複数の IM および Presence サービスノードがあり、これらの IM および Presence サービス ノードがすべて同じサブネット上にあることを前提としています。具体的には、すべての内部 IM および Presence サービス ノードが 2.2.2.x/24 ネットワーク上にある場合、NAT コマンドは **nat (inside) 1 2.2.2.0 255.255.255.0** です。

# 新しい要求のスタティック PAT

この統合では、プライベート メッセージからパブリック メッセージへのアドレス変換に次の構成が含まれます。

- 次のポートの TCP でスタティック PAT コマンドを構成します。5060、5061、5062、および 5080。

- ポート 5080 の UDP で別のスタティック PAT コマンドを構成します。

この統合では、次のポートを使用します。

- 5060：Cisco 適応型セキュリティ アプライアンス は、このポートを汎用 SIP インスペクションに使用します。
- 5061：SIP 要求がこのポートに送信され、TLS ハンドシェイクがトリガされます。
- 5062、5080： IM and Presence Service は、SIP VIA/CONTACT ヘッダーでこれらのポートを使用します。

（注） IM and Presence Service のピア認証リスナー ポートを確認するには、 **Cisco Unified CM IM and Presence Administration** 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）]** を選択します。

**関連情報 -**

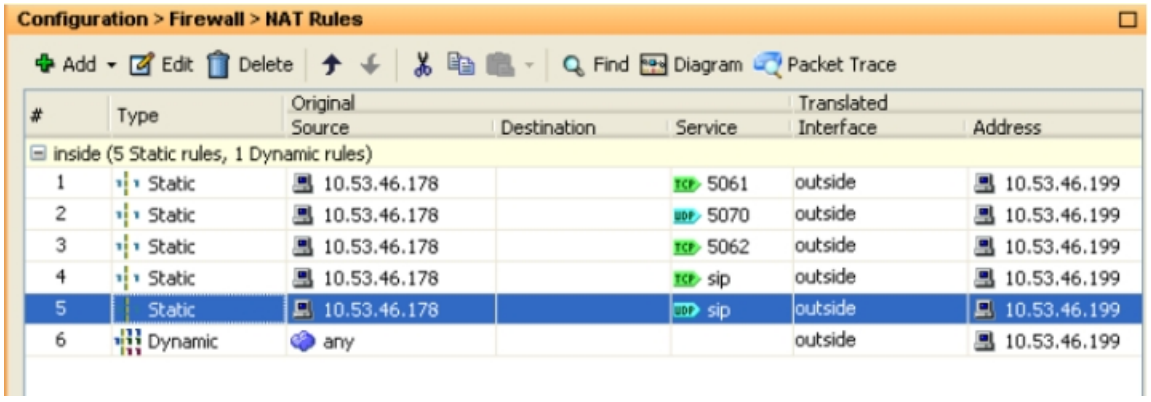
スタティック PAT コマンドの例

Cisco 適応型セキュリティ アプライアンス の構成例

# ASDM の NAT ルール

ASDM で NAT ルールを表示するには、**[Configuration（構成）] > [Firewall（ファイアウォール）] > [NAT Rules（NAT ルール）]** を選択します。次の図に示す最初の 5 つの NAT ルールはスタティック PAT エントリで、最後のダイナミック エントリは発信トラフィックをパブリック IM and Presence Service の IP アドレスとポートにマッピングする発信 PAT 構成です。

**図 *21 : ASDM* での *NAT* ルールの表示**




**関連情報**

スタティック PAT コマンドの例

Cisco 適応型セキュリティ アプライアンス の構成例

# スタティック PAT コマンドの例

（注） ここでは、Cisco 適応型セキュリティ アプライアンス リリース 8.3 およびリリース 8.2 のコマンド例を示します。フェデレーション用に Cisco 適応型セキュリティアプライアンス の新しい設定を行う場合は、これらのコマンドを実行する必要があります。

## IM and Presence サービス ノードをルーティングするための PAT 構成

次の表に、ピア認証リスナーポートが 5062 である IM and Presence Service ノードをルーティングするための PAT コマンドを示します。

（注） Cisco 適応型セキュリティ アプライアンス8.3 の設定では、オブジェクトを 1 回定義するだけで、複数のコマンドでそのオブジェクトを参照できます。同じオブジェクトを繰り返し定義する必要はありません。

表 *13 : IM and Presence* サービス ノードをルーティングするための *PAT* コマンド

| Cisco 適応型セキュリティ アプライアンス リリース 8.2 のスタティック コマンド | Cisco 適応型セキュリティ アプライアンス |
|---|---|
| **static (inside,outside) tcp** *public_imp_ip_address* **5061** *routing_imp_private_address* **5062 netmask 255.255.255.255**<br><br>ルーティング IM and Presence Service ピア認証リスニング ポートが 5061 の場合は、次のコマンドを使用します。<br><br>**static (inside,outside) tcp** *public_imp_ip_address* **5061** *routing_imp_private_address* **5061 netmask 255.255.255.255**<br><br>**static (inside,outside) tcp** *public_imp_ip_address* **5080** *routing_imp_private_address* **5080 netmask 255.255.255.255**<br><br>**static (inside,outside) tcp** *public_imp_ip_address* **5060** *routing_imp_private_address* **5060 netmask 255.255.255.255** | **object network** *obj_host_public_imp_ip_*<br>**network** *obj_host_10.10.10.10*) **#host** *pu*<br><br>**object network** *obj_host_routing_imp_pr*<br>*routing_imp_private_address*<br><br>**object service** *obj_tcp_source_eq_5061*<br><br>**object service** *obj_tcp_source_eq_5062*<br><br>**nat (inside,outside) source static**<br>*obj_host_routing_imp_private_address ob*<br>**service** *obj_tcp_source_eq_5062 obj_tcp*<br><br>ルーティング IM and Presence Service ピア認<br>の場合は、次のコマンドを使用します。<br><br>**nat (inside,outside) source static**<br>*obj_host_routing_imp_private_address ob*<br>**service** *obj_tcp_source_eq_5061 obj_tcp* |
| -- | **object service** *obj_tcp_source_eq_5080*<br>**nat (inside,outside) source static**<br>*obj_host_routing_imp_private_address ob*<br>**service** *obj_tcp_source_eq_5080 obj_tcp* |

| Cisco 適応型セキュリティ アプライアンス リリース 8.2 のスタティック コマンド | Cisco 適応型セキュリティ アプライアンス リード |
|---|---|
| -- | **object service** *obj_tcp_source_eq_5060* **ser**<br>（注） 5060 は、サービス オブジェクトで「<br>**nat (inside,outside) source static**<br>*obj_host_routing_imp_private_addres*<br>*obj_host_public_imp_ip_address* **serv**<br>*obj_tcp_source_eq_5060 obj_tcp_sou* |
| **static (inside,outside) tcp** *public_imp_ip_address* **5062** *routing_imp_private_address* **5062 netmask 255.255.255.255** | **nat (inside,outside) source static**<br>*obj_host_routing_imp_private_address obj_h*<br>**service obj_tcp_source_eq_5062 obj_tcp_so** |

# クラスタ間またはクラスタ内 IM および Presence サービス ノードの PAT 構成

マルチノードまたはクラスタ間 IM and Presence Service 展開で、 IM and Presence Service クラスタの非ルーティング ノードが Cisco 適応型セキュリティ アプライアンスと直接通信する場合は、これらのノードごとに一連のスタティック PAT コマンドを構成する必要があります。次に示すコマンドは、単一ノードに設定する必要がある一連のスタティック PAT コマンドの例です。

未使用の任意のポートを使用する必要があります。対応する番号を選択することを推奨します（例：5080 は未使用の任意のポート X5080 を使用）。X は、IM and Presence Service クラスタ間またはクラスタ内サーバに一意にマッピングされる番号に対応します。たとえば、45080 は 1 つのノードに一意にマッピングされ、55080 は別のノードに一意にマッピングされます。

次の表に、非ルーティング IM and Presence Service ノードの NAT コマンドを示します。それぞれの非ルーティング IM and Presence Service ノードのコマンドを繰り返します。

（注） Cisco 適応型セキュリティ アプライアンス8.3 の設定では、オブジェクトを 1 回定義するだけで、複数のコマンドでそのオブジェクトを参照できます。同じオブジェクトを繰り返し定義する必要はありません。

表 *14* : 非ルーティング *IM and Presence Service* ノードの *NAT* コマンド

| Cisco 適応型セキュリティ アプライアンス リリース 8.2 のスタティック コマンド | Cisco 適応型セキュリティ アプライアンス |
|---|---|
| **static (inside,outside) tcp** *public_imp_address* **45062** *intercluster_imp_private_address* **5062 netmask 255.255.255.255**<br><br>クラスタ間 IM and Presence Service ピア認証リスニング ポートが 5061 の場合は、 コマンドを使用します。<br><br>**static (inside,outside) tcp** *public_imp_address* **45061** *intercluster_imp_private_address* **5061 netmask 255.255.255.255** | **object network** *obj_host_intercluster_imp intercluster_imp_private_address*<br><br>**object service** *obj_tcp_source_eq_45062* **s**<br><br>**nat (inside,outside) source static** *obj_host_intercluster_imp_private_addre obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_45062*<br><br>クラスタ間 IM and Presence Service ピア認証 の場合は、 コマンドを使用します。<br><br>**object service** *obj_tcp_source_eq_45061* **s nat (inside,outside) source static** *obj_host_intercluster_imp_private_addre obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_45061* |
| **static (inside,outside) tcp** *public_imp_ip_address* **45080** *intercluster_imp_private_address* **5080 netmask 255.255.255.255** | **object service** *obj_tcp_source_eq_45080* **s nat (inside,outside) source static** *obj_host_intercluster_imp_private_addre obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_45080* |
| **static (inside,outside) tcp** *public_imp_ip_address* **45060** *intercluster_imp_private_address* **5060 netmask 255.255.255.255** | **object service** *obj_tcp_source_eq_45060* **s nat (inside,outside) source static** *obj_host_intercluster_imp_private_addre obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_45060* |

**関連情報 -**

新しい要求のスタティック PAT

IM and Presence サービス ノードをルーティングするための PAT 構成

# 既存の展開での Cisco 適応型セキュリティアプライアンスのアップグレード オプション

Cisco 適応型セキュリティ アプライアンス リリース 8.2 からリリース 8.3 にアップグレードする場合、Cisco 適応型セキュリティ アプライアンス はアップグレード中に既存のコマンドをシームレスに移行します。

（注） IM and Presence Service リリース 9.0 にアップグレードしたら、Cisco 適応型セキュリティ アプライアンスの背後にある IM and Presence Service 9.0 ノードごとに、Cisco >適応型セキュリティ アプライアンスのポート 5080 を開く必要があります。これは、Cisco 適応型セキュリティ アプライアンス もアップグレードしたかどうかには関係ありません。

既存のフェデレーション展開で IM and Presence Service と Cisco 適応型セキュリティ アプライアンス の両方をアップグレードする場合は、次のいずれかのアップグレード手順を使用します。

**アップグレード手順オプション 1**：

1. IM and Presence Service をリリース 9.0 にアップグレードします。
2. Cisco 適応型セキュリティ アプライアンスでポート 5080 の NAT ルールを構成します。
3. IM and Presence Service のアップグレード後に、展開でフェデレーションが機能していることを確認します。
4. Cisco 適応型セキュリティ アプライアンス をリリース 8.3 にアップグレードします。
5. Cisco 適応型セキュリティ アプライアンス のアップグレード後に、展開環境でフェデレーションが機能していることを確認します。

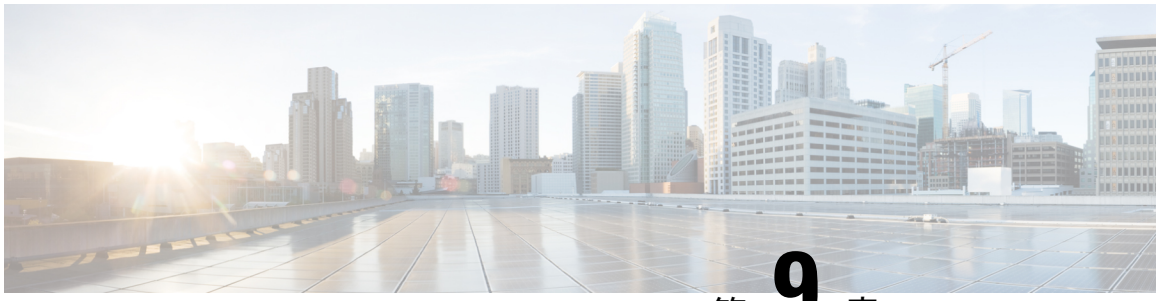
**アップグレード手順オプション 2**：

1. IM and Presence Service ノードをリリース 9.0 に、Cisco 適応型セキュリティ アプライアンス をリリース 8.3 にアップグレードします。
2. 両方のアップグレード後に、Cisco 適応型セキュリティ アプライアンスでポート 5080 の NAT ルールを構成します。
3. 展開環境でフェデレーションが機能していることを確認します。

これらは、Cisco 適応型セキュリティ アプライアンス の背後にある IM and Presence Serviceリリース 9.0 ノードごとにポート 5080 を開くために必要なコマンドです。

表 *15 :* ポート *5080* を開く *Cisco ASA* コマンド

| Cisco 適応型セキュリティ アプライアンス リリース 8.2 のスタティック コマンド | Cisco 適応型セキ |
|---|---|
| **static (inside,outside) tcp** *public_imp_ip_address* **5080** *routing_imp_private_address* **5080 netmask 255.255.255.255**<br><br>**static (inside,outside) tcp** *public_imp_ip_address* **45080** *intercluster_imp_private_address* **5080 netmask 255.255.255.255**<br><br>（注） クラスタ間 IM and Presence Service 9.0 ノードごとにこれらのコマンドを構成し、それぞれに異なる任意のポートを使用します。 | **object service**<br><br>**nat (inside,outs** *obj_host_public*<br><br>**object service**<br><br>**nat (inside,outs** *obj_host_public*<br><br>（注） クラスタ間<br>れに異なる |



第 9 章

# Cisco 適応型セキュリティ アプライアンスでの TLS プロキシ構成

ここでは、Cisco 適応型セキュリティ アプライアンスでの TLS プロキシ構成について説明します。



## TLS プロキシ

Cisco 適用型セキュリティ アプライアンス は、 IM and Presence サービス と外部サーバー間の TLS プロキシとして機能します。これにより、Cisco 適用型セキュリティ アプライアンス は（TLS 接続を開始する）サーバーに代わって TLS メッセージをプロキシし、プロキシからクライアントに TLS メッセージをルーティングできます。TLS プロキシは、着信レッグで必要に応じて TLS メッセージを復号、検査、および変更してから、リターン レッグでトラフィックを再暗号化します。

（注） TLS プロキシを設定する前に、Cisco 適用型セキュリティ アプライアンス と IM and Presence Serivce の間、および Cisco 適用型セキュリティ アプライアンスと外部サーバーの間で Cisco 適用型セキュリティ アプライアンス セキュリティ証明書を設定する必要があります。これを行うには、次の項の手順を実行します。

- IM および Presence サービスと Cisco 適応型セキュリティ アプライアンス間のセキュリティ証明書の交換 （61 ページ）
- Microsoft CA を使用した Cisco 適応型セキュリティアプライアンスと Microsoft Access Edge（外部インターフェイス）間のセキュリティ証明書の交換 （66 ページ）

### 関連情報

Cisco 適応型セキュリティ アプライアンスの一般的な問題と推奨されるアクション

# アクセス リストの構成要件

このセクションでは、単一の IM および Presence サービス展開のアクセス リスト構成要件を一覧表示します。

（注）
- アクセス リストごとに、対応するクラス マップを構成し、ポリシー マップ グローバル ポリシーにエントリを構成する必要があります。
- IM および Presence サービスのピア認証リスナー ポートを確認するには、 **Cisco Unified Communications Manager IM および Presence 管理**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）]** を選択します。

表 *16* : 単一の *IM* および *Presence* サービス アクセス リストの構成要件

| 項目 | 説明 |
|---|---|
| 展開シナリオ：IM および Presence サービス ノードと 1 つ以上の外部ドメインのフェデレーション | |

| 項目 | 説明 |
|---|---|
| 構成の要件： | IM および Presence サービスがフェデレーションする外部ドメインごとに、次の 2 つのアクセス リストを構成します。<br>• IM および Presence サービスがポート 5061 で外部ドメインにメッセージを送信できるように、アクセス リストを構成します。<br>• IM および Presence サービスがポート 5061 で外部ドメインからメッセージを受信できるように、アクセス リストを構成します。Cisco 適応型セキュリティ アプライアンス リリース 8.3 を使用する場合は、 IM および Presence サービスが SIP フェデレーションをリッスンする実際のポートを使用します（IM および Presence サービスのピア認証リスナー ポートを確認します）。 |
| 設定例： | **access-list** *ent_imp_to_external_server* **extended permit tcp host** *routing_imp_private_address* **host** *external_public_address* **eq 5061**<br>（Cisco 適応型セキュリティ アプライアンス リリース 8.2:）<br>**access-list** *ent_external_server_to_imp* **extended permit tcp host** *external_public_address* **host** *imp_public_address* **eq 5061**<br>（Cisco 適応型セキュリティ アプライアンス リリース 8.3:）<br>**access-list** *ent_external_server_to_imp* **extended permit tcp host** *external_public_address* **host** *imp_private_address* **eq 5061**<br>（注） 上記のアクセス リストで、5061 は IM および Presence サービスが SIP メッセージングをリッスンするポートです。IM および Presence サービスがポート 5062 でリッスンする場合は、アクセス リストで 5062 を指定します。 |
| 展開シナリオ：クラスタ間展開。これは、マルチノード展開にも適用されます。 | |
| 構成の要件： | クラスタ間 IM および Presence サービス ノードごとに、次の 2 つのアクセス リストを構成します。<br>• IM および Presence サービスがポート 5061 で外部ドメインにメッセージを送信できるように、アクセス リストを構成します。<br>• IM および Presence サービスが任意のポート 5061 で外部ドメインからメッセージを受信できるように、アクセス リストを構成します。Cisco 適応型セキュリティ アプライアンス リリース 8.3 を使用する場合は、 IM および Presence サービスが SIP フェデレーションをリッスンする実際のポートを使用します（IM および Presence サービスのピア認証リスナー ポートを確認します）。 |

| 項目 | 説明 |
|---|---|
| 設定例： | **access-list** *ent_intercluster_imp_to_external_server* **extended permit tcp host** *intercluster_imp_private_address* **host external public address eq 5061**<br>（Cisco 適応型セキュリティ アプライアンス リリース 8.2:）<br>**access-list** *ent_external_server_to_intercluster_imp* **extended permit tcp host** *external_public_address* **host** *imp* **public address eq** *arbitrary_port*<br>（Cisco 適応型セキュリティ アプライアンス リリース 8.3:）<br>*ent_external_server_to_intercluster_imp* **extended permit tcp host** *external_public_address* **host** *imp_private_address* **eq** *5061*<br>上記のアクセス リストで、5061 は IM および Presence サービスが SIP メッセージングをリッスンするポートです。IM および Presence サービスがポート 5062 でリッスンする場合は、アクセス リストで 5062 を指定します。 |

**関連情報**

Cisco 適応型セキュリティ アプライアンス の構成例

TLS プロキシ インスタンスの構成

クラスマップを使用したアクセスリストと TLS プロキシ インスタンスの関連付け

TLS プロキシの有効化

# TLS プロキシ インスタンスの構成

この統合では、2 つの TLS プロキシ インスタンスを作成する必要があります。最初の TLS プロキシは、IM and Presence Service によって開始された TLS 接続を処理します。IM and Presence Service はクライアントであり、外部ドメインはサーバです。この場合、Cisco 適応型セキュリティアプライアンス は、 IM and Presence Service である「クライアント」に面する TLS サーバとして機能します。2 番目の TLS プロキシは、外部ドメインによって開始された TLS 接続を処理します。外部ドメインはクライアントであり、 IM and Presence Service はサーバです。

TLS プロキシ インスタンスは、サーバとクライアントの両方の 「トラストポイント」 を定義します。TLS ハンドシェイクが開始される方向によって、サーバおよびクライアント コマンドで定義されるトラストポイントが決まります。

- IM and Presence Service から外部ドメインへの TLS ハンドシェイクが開始される場合、server コマンドは、Cisco 適応型セキュリティアプライアンス の自己署名証明書を含むトラストポイントを指定します。client コマンドは、Cisco 適応 型セキュリティ アプライアンス と外部ドメイン間の TLS ハンドシェイクで使用される Cisco 適応型セキュリティ アプライアンス 証明書を含むトラストポイントを指定します。
- 外部ドメインから IM and Presence Serviceへのハンドシェイクが開始される場合、server コマンドは、TLS ハンドシェイクが Cisco 適応型セキュリティ アプライアンス と外部ドメイン間で使用する Cisco 適応型セキュリティ アプライアンス 証明書を含むトラストポイン

トを指定します。client コマンドは、Cisco 適応型セキュリティ アプライアンスの自己署名証明書を含むトラストポイントを指定します。

### 始める前に

- アクセス リストの構成要件 （94 ページ）の手順を完了します。

---

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** IM and Presence Serviceによって開始された TLS 接続用の TLS プロキシ インスタンスを作成します。次に、imp_to_external という TLS プロキシ インスタンスを作成する例を示します。

```
tls-proxy ent_imp_to_external
server trust-point imp_proxy
client trust-point trustpoint_name
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
```

**ステップ 3** 外部ドメインによって開始された TLS 接続用の TLS プロキシ インスタンスを作成します。この例では、external_to_imp という名前の TLS プロキシ インスタンスを作成します。

```
tls-proxy ent_external_to_imp
server trust-point trustpoint_name
client trust-point imp_proxy
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
```

---

### 次のタスク

クラスマップを使用したアクセスリストと TLS プロキシ インスタンスの関連付け （97 ページ）

# クラスマップを使用したアクセスリストと TLS プロキシ インスタンスの関連付け

class map コマンドを使用して、以前に定義した各外部ドメイン アクセス リストに TLS プロキシ インスタンスを関連付ける必要があります。

### 始める前に

TLS プロキシ インスタンスの構成の手順を完了します。

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 各アクセス リストを、クラス マップが使用する TLS プロキシ インスタンスに関連付けます。選択する TLS プロキシは、クラスマップが IM and Presence Service から外部ドメインへのメッセージ用であるか、または外部ドメインから IM and Presence Serviceへのメッセージ用であるかによって異なります。

次の例では、 IM and Presence Service から外部ドメインに送信されたメッセージのアクセス リストは、IM and Presence Service によって開始された TLS 接続の TLS プロキシ インスタンス（「ent_imp_to_external」）に関連付けられます。

```
class-map ent_imp_to_external match access-list ent_imp_to_external
```

次の例では、外部ドメインから IM and Presence Service に送信されたメッセージのアクセス リストが、「ent_external_to_imp」と呼ばれる外部サーバーによって開始された TLS 接続の TLS プロキシ インスタンスに関連付けられます。

```
class-map ent_external_to_imp match access-list ent_external_to_imp
```

**ステップ 3** クラスタ間 IM and Presence Service を 導入している場合は、各 IM and Presence Service ノードのクラス マップを設定し、以前に定義したサーバーの適切なアクセス リストに関連付けます。次に例を示します。

```
class-map ent_second_imp_to_external match access-list ent_second_imp_to_external
class-map ent_external_to_second_imp match access-list ent_external_to_second_imp
```

### 次のタスク

TLS プロキシの有効化 （98 ページ）

# TLS プロキシの有効化

policy map コマンドを使用して、前のセクションで作成した各クラス マップの TLS プロキシを有効にする必要があります。

（注） 構成が失敗するため、フェデレーション展開の Cisco 適応型セキュリティ アプライアンス で高セキュリティ sip-inspect ポリシーマップを使用することはできません。低/中セキュリティ ポリシー マップを使用する必要があります。

### 始める前に

「クラスマップを使用したアクセスリストと TLS プロキシ インスタンスの関連付け」の手順を実行します。

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** sip-inspect ポリシー マップを定義します。次に例を示します。

```
policy-map type inspect sip sip_inspectParameters
```

**ステップ 3** グローバル ポリシー マップを定義します。次に例を示します。

```
policy-map global_policy class ent_cup_to_external inspect sip sip_inspect tls-proxy
ent_cup_to_external
```

# クラスタ間展開用の Cisco 適応型セキュリティ アプライアンスの構成

クラスタ間 IM and Presence Service 展開では、追加の IM and Presence Service ノードごとに Cisco 適応型セキュリティ アプライアンス で次の構成を実行する必要があります。

**ステップ 1** IM and Presence Serviceの追加のアクセス リストを作成します。

**ステップ 2** Cisco 適応型セキュリティ アプライアンス のセキュリティ証明書を生成し、 IM and Presence Service ノードにインポートします。

**ステップ 3** IM and Presence Service セキュリティ証明書を生成し、Cisco 適応型セキュリティ アプライアンスにインポートします。

**ステップ 4** 外部ドメインごとにクラス マップを構成します。

**ステップ 5** グローバル ポリシー マップにクラス マップを含めます。

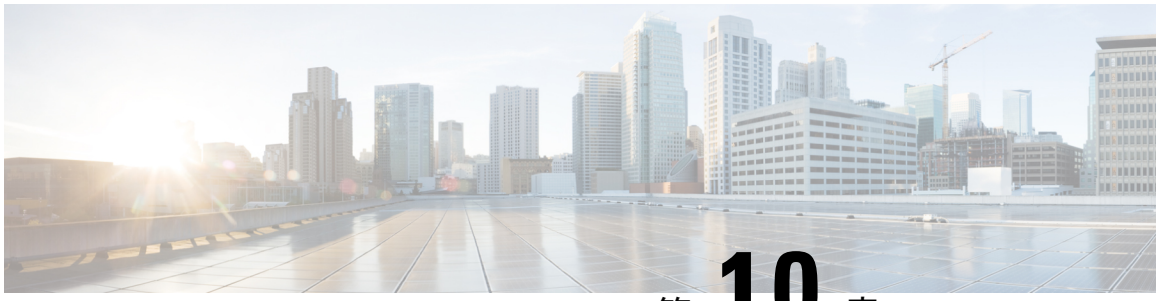
### 関連情報

IM および Presence サービスと Cisco 適応型セキュリティ アプライアンス間のセキュリティ証明書の交換

クラスマップを使用したアクセスリストと TLS プロキシ インスタンスの関連付け

TLS プロキシの有効化

クラスタ間展開とマルチノードの展開



第 10 章

# Office 365 とのドメイン間フェデレーション

このセクションでは、Office 365 とのドメイン間フェデレーションについて説明します。



## Office 365 ドメイン間フェデレーションの概要

IM and Presence Service は、Office 365 展開ネットワークを使用したビジネスツービジネス ドメイン間フェデレーションをサポートします。この統合により、Office 365 は Skype for Business サーバーをホストし、Office 365 ユーザーのインスタント メッセージングとプレゼンスを処理します。

（注） この統合により、Office 365 はクラウド内で Skype for Business サーバーをホストします。また、以下とフェデレーションすることもできます。

- 別の会社のネットワーク内のリモート Skype for Business サーバー（ビジネス ツー ビジネス）
- 別のドメインにあるが、IM and Presence Service と同じエンタープライズネットワーク（単一のエンタープライズネットワーク）にあるオンプレミスの Skype for Business サーバー

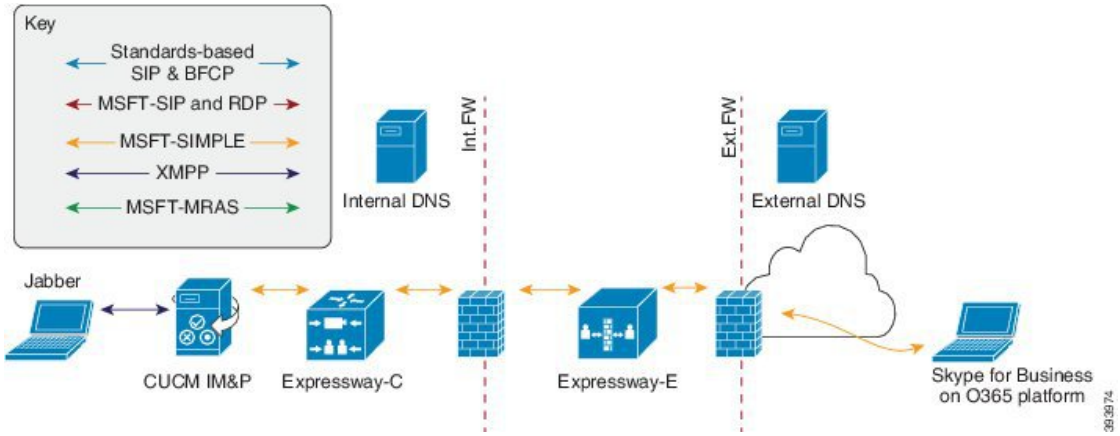
これらの Skype for Buisness フェデレーションについては、「Skype for Business とのドメイン間フェデレーション （109 ページ）」を参照してください。

### Office 365 フェデレーションの例

次の図は、Office 365 でホストされている Skype for Business サーバーとのビジネス ツー ビジネス フェデレーションを示しています。IM and Presence Service と Office 365 間の通信は、企業のファイアウォールを越えてクラウドに移動する必要があります。企業ネットワークに出入

りするトラフィックを保護するには、内部ネットワークにExpressway-Cを展開し、企業のファイアウォールの DMZ に Expressway-E を展開する必要があります。

図 *22 : Office 365* フェデレーションの例




# Office 365 ドメイン間フェデレーションのタスク フロー

IM and Presence Service で次のタスクを実行して、Office 365 展開でビジネス ツー ビジネス ドメイン間フェデレーションを構成します。

## 始める前に

デフォルトでは、フェデレーション ルーティング パラメータは、インストール時にデータベース パブリッシャ ノードの FQDN に設定されます。この値をリセットする場合は、フェデレーション ルーティング パラメータの構成 （50 ページ） に移動します。

## 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | フェデレーション サービスのオン （103 ページ） | Cisco XCP SIP Federation Connection Manager サービスをオンにします。 |
| ステップ 2 | IM および Presence サービスの DNS SRV レコードの追加 （103 ページ） | IM and Presence ドメインのパブリック DNS SRV レコードを構成します。SRV は Expressway-E の IP アドレスに解決する必要があります。 |
| ステップ 3 | IM and Presence サービスへの Office 365 ドメインの追加 （104 ページ） | IM and Presence Service で、Office 365 ドメイン エントリを追加します。 |
| ステップ 4 | Office 365 へのスタティック ルートの構成 （104 ページ） | IM and Presence Service で、Expressway-C への TLS スタティック ルートを設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | TLS ピアとしての Expressway の追加 （105 ページ） | IM and Presence Service で、Expressway-C を TLS ピアとして割り当てます。 |
| ステップ 6 | アクセス制御リストへの Expressway の追加 （106 ページ） | IM and Presence Service で、Expressway-E サーバーをインバウンド アクセス制御リストに追加します。 |
| ステップ 7 | Cisco XCP ルータの再起動 （106 ページ） | すべての IM and Presence Service のクラスタ ノード上で Cisco XCP ルータを再起動します。 |
| ステップ 8 | Exchange Certificates （107 ページ） | 展開内のサーバー間で証明書を交換します。IM and Presence Service の場合は、Expressway-C 証明書チェーンを cup-trust ストアにアップロードする必要があります。 |
| ステップ 9 | Configure Expressway for Federation with Office 365 （108 ページ） | Office 365 とのドメイン間フェデレーション用に Expressway を構成します。 |

# フェデレーション サービスのオン

**Cisco XCP SIP Federation Connection Manager** サービスをオンにします。プロビジョニングする各ユーザーの SIP フェデレーション機能がオンになります。クラスタの各ノードで、このタスクを完了する必要があります。

**ステップ 1** **Cisco Unified IM and Presence Serviceability** のユーザーインターフェイスにログインします。**[Tools（ツール）] > [Service Activation（サービス アクティベーション）]** を選択します。

**ステップ 2** **[サーバ（X8.9.2）]** ドロップダウンから、IM and Presence ノードを選択し、**[移動（Go）]**をクリックします。

**ステップ 3** **IM and Presence Services** で、**[Cisco XCP SIP Federation Connection Manager]** サービスの下にある隣接ラジオ ボタンをオンにしてください。

**ステップ 4** [保存（Save）] をクリックします。

**ステップ 5** Cisco SIP プロキシ サービスを動作させるには、Cisco SIP Proxyサービスが動作している必要があります。**Cisco Unified IM and Presence 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）] > [機能サービス（Feature Services）]** を選択し、Cisco SIP プロキシ サービスが実行されていることを確認します。

# IM および Presence サービスの DNS SRV レコードの追加

IM and Presence Service を指すパブリック DNS SRV レコードを設定します。Office 365 は、このレコードを使用してトラフィックを IM and Presence Service にルーティングします。レコードは、次の例のように Expressway-C サーバーを指す必要があります。`expwye` は Expressway-E ドメインを表します。

```
nslookup
set type=srv
_sipfederationtls._tcp.expwye
```

（注） DNS SRV レコードがなくてもドメイン間フェデレーションを設定できますが、Office 365 は IM and Presence Service へのルートを使用して手動で設定する必要があります。

### 次のタスク

IM and Presence サービスへの Office 365 ドメインの追加 （104 ページ）

# IM and Presence サービスへの Office 365 ドメインの追加

IM and Presence Service で、Office 365 ドメインをフェデレーテッド ドメインとして追加します。

**ステップ 1** Cisco Unified CM IM およびプレザンス管理から、**[プレザンス（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（Domain Name）]** フィールドに、Office 365 ドメイン名を入力します。

**ステップ 4** ドメインの**説明**を入力します。たとえば、 `Office 365 フェデレーテッド ドメイン`などです。

**ステップ 5** **[統合タイプ（Integration Type）]** ドロップダウンから、**[Inter-domain to OCS/Lync/S4B]** を選択します。

**ステップ 6** [保存（Save）] をクリックします。

### 次のタスク

Office 365 へのスタティック ルートの構成 （104 ページ）

# Office 365 へのスタティック ルートの構成

IM and Presence Service で、Expressway-C を介して Office 365 への TLS スタティック ルートを構成します。

**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** **[接続先パターン（Destination Pattern）]** フィールドに、逆の形式で Office 365 FQDN を入力します。たとえば、ドメインが `office365.com` の場合、 `.com.office365.*` と入力します。

**ステップ 4** **[次のホップ（Next Hop）]** フィールドに、Expressway-C 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。

### 次のタスク

TLS ピアとしての Expressway の追加 （105 ページ）

# TLS ピアとしての Expressway の追加

IM and Presence Service で次の手順を使用して、Expressway を TLS ピア サブジェクトとして追加します。

**ステップ 1** Expressway-C を TLS ピア サブジェクトとして追加します。

a) Cisco Unified CM IM and Presence 管理 で、**[システム（System）]** > **[セキュリティ（Security）]** > **[TLS ピア サブジェクト（TLS Peer Subject）]**を選択します。
b) [新規追加（Add New）] をクリックします。
c) [ピア サブジェクト名（ **Peer Subject Name** ）] フィールドに、Expressway-C の Expressway-C の完全修飾ドメイン名を入力します。
d) [説明（Description）] を入力します。
e) [保存（Save）] をクリックします。

**ステップ 2** 設定した Expressway TLS ピア サブジェクトを含む TLS コンテキストを作成します。

a) [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] から **[システム（System）]** > **[セキュリティ（Security）]** > **[TLS コンテキスト構成（TLS Context Configuration）]** の順に選択します。
b) [検索（Find）] をクリックします。
c) **[Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context]** をクリックします。
d) **[ TLS 暗号マッピング（TLS Cipher Mapping）]**で、矢印を使用して目的の TLS 暗号を **[選択した TLS 暗号（Selected TLS Ciphers）]** ボックスに移動します。ただし、ほとんどの場合、デフォルト設定のままで十分です。
e) **[TLS ピア サブジェクト マッピング（TLS Peer Subject Mapping）]** で、矢印を使用して、作成した TLS ピア サブジェクトを **[選択した TLS ピア サブジェクト（Selected TLS Peer Subjects）]** リスト ボックスに移動します。
f) [保存（Save）] をクリックします。

### 次のタスク

アクセス制御リストへの Expressway の追加 （106 ページ）

# アクセス制御リストへの Expressway の追加

IM and Presence Service で、Expressway-C サーバーのインバウンドアクセス制御リスト（ACL）エントリを追加して、Expressway-C が認証なしで IM and Presence Service にアクセスできるようにします。マルチクラスタ展開の場合は、各クラスタでこの手順を実行します。

（注） グローバル アクセスを提供する ACL（[すべての許可（`Allow from all`）]）、または Expressway-C サーバーが存在するドメインへのアクセスを提供する ACL（たとえば、`[company.com の許可（Allow from company.com）]`）がある場合は、Expressway-C サーバーの ACL エントリを追加する必要はありません。

**ステップ 1** IM and Presence Service のパブリッシャ ノードにログインします。

**ステップ 2** Cisco Unified CM IM and Presence 管理で、**[システム（System）]** > **[セキュリティ（Security）]** > **[受信 ACL（Incoming ACL）]** を選択します。

**ステップ 3** ACL エントリを作成します。

a) [新規追加（Add New）] をクリックします。
b) 新しい ACL エントリの **[説明（Description）]** を入力します。たとえば、`Expressway-C を介した Skype for Business フェデレーション`。
c) Expressway-C の IP アドレスまたは FQDN へのアクセスを提供する **[アドレス パターン（Address Pattern）]** を入力します。たとえば、`Allow from 10.10.10.1` または `Allow from expwyc.company.com` です。
d) [保存（Save）] をクリックします。
e) この一連の手順を繰り返して、別の ACL エントリを作成します。サーバー アクセスを提供するには、サーバー IP アドレスを含む ACL とサーバー FQDN を含む ACL の 2 つのエントリが必要です。

**ステップ 4** Cisco SIP Proxy サービスを再開します。

a) **[プレゼンス（Presence）]** > **[ルーティング（Routing）]** > **[設定（Settings）]** を選択します。
b) **[すべてのプロキシ サービスの再開（Restart All Proxy Services）]**をクリックします。

### 次のタスク

Cisco XCP ルータの再起動 （106 ページ）

# Cisco XCP ルータの再起動

構成が完了したら、 **Cisco XCP ルータ** を再起動します。

ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] から、**[ツール（Tools）] > [コントロールセンタ-ネットワークサービス（Control Center - Network Services）]** を選択します。

ステップ 2 **サーバ** ドロップダウン リスト ボックスで、IM and Presence データベース パブリッシャ ノードを選択して、**[移動（Go）]** をクリックします。

ステップ 3 **[IM and Presenceサービス（IM and Presence Services）]** の下で、**[Cisco XCP Router]** サービスを選択します。

ステップ 4 をクリックします。

ステップ 5 すべての IM and Presence サービスのクラスタ ノードでこの手順を繰り返します。

### 次のタスク

[Restart]

Office 365 へのスタティック ルートの構成 （104 ページ）

# Exchange Certificates

Exchange certificates among the servers in your deployment.

ステップ 1 Download certificates from each system in the deployment:

- IM and Presence Service (internal certificate can be self-signed)
- Expressway-C (internal certificate can be self-signed)
- Expressway-E (external certificate must be CA-signed)
- Office 365 server (external certificate must be CA-signed)

ステップ 2 On the IM and Presence Service, upload the Expressway-C certificate chain to the **cup-trust** store.

ステップ 3 On the Expressway-C, upload the IM and Presence Service certificate.

ステップ 4 On the Expressway-E, upload the Office 365 certificate.

**Note** For business to business Federation, the other company must upload the Expressway-E certificate to the Office 365 server.

### Certificate Notes

- For IM and Presence Service, you can download and upload certificates from the **Certificate Management** window in Cisco Unified IM OS Administration (choose **Security** > **Certificate Management**). For detailed procedures, see the "Security Configuration" chapter of the *Configuration and Administration Guide for IM and Presence Service* at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html.

- For Expressway certificate management, see the *Cisco Expressway Administrator Guide* at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html.

### What to do next

Configure Expressway for Federation with Office 365, on page 108

# Configure Expressway for Federation with Office 365

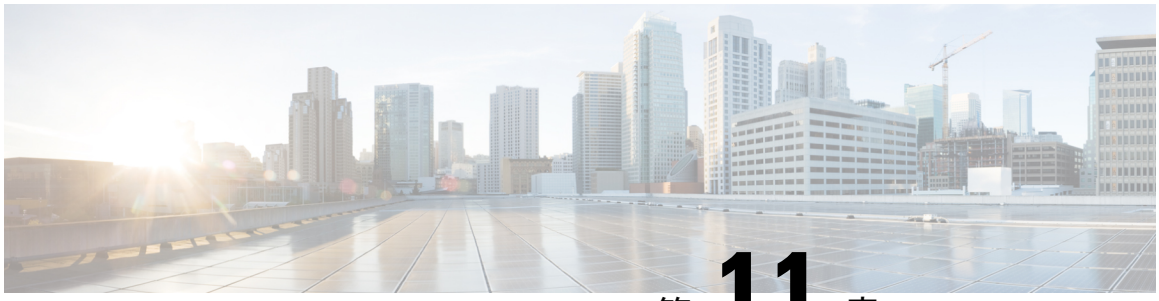
After interdomain federation is configured on the IM and Presence Service, set up Cisco Expressway for business to business interdomain federation with Office 365. For Expressway configuration details, see *Chat and Presence XMPP Federation and Microsoft SIP Federation using IM and Presence or Expressway* at:

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

**Note** Make sure that your Expressway-C zone configuration points to the port that is associated with TLS Peer Authentication on the IM and Presence Service. You can confirm the correct port on Cisco Unified CM IM and Presence Administration by going to **System** > **Application Listeners** and confirming the port associated to **Default Cisco SIP Proxy TLS Listener - Peer Auth**. The default is **5062**.

### What to do next

For business to business Federation to work, the other company must configure their Office 365 deployment to federate with the IM and Presence Service.



第 11 章

# Skype for Business とのドメイン間フェデレーション

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



## Skype for Business ドメイン間フェデレーション

IM and Presence Service は、Expressway を介した Skype for Business サーバーとのドメイン間フェデレーションをサポートします。次の統合がサポートされています。

- Business to Business：別の会社のネットワーク内のリモート Skype for Business サーバーとのフェデレーション
- 単一のエンタープライズ ネットワーク：同じエンタープライズ ネットワーク内にあるが、異なるドメインにあるオンプレミスの Skype for Business サーバーとのフェデレーション。

（注） また、Office365 展開でホストされている Skype for Business サーバーとのフェデレーションを構成することもできます。構成情報を含む詳細については、「Office 365 とのドメイン間フェデレーション （101 ページ）」を参照してください。

### Skype for Business フェデレーションの例

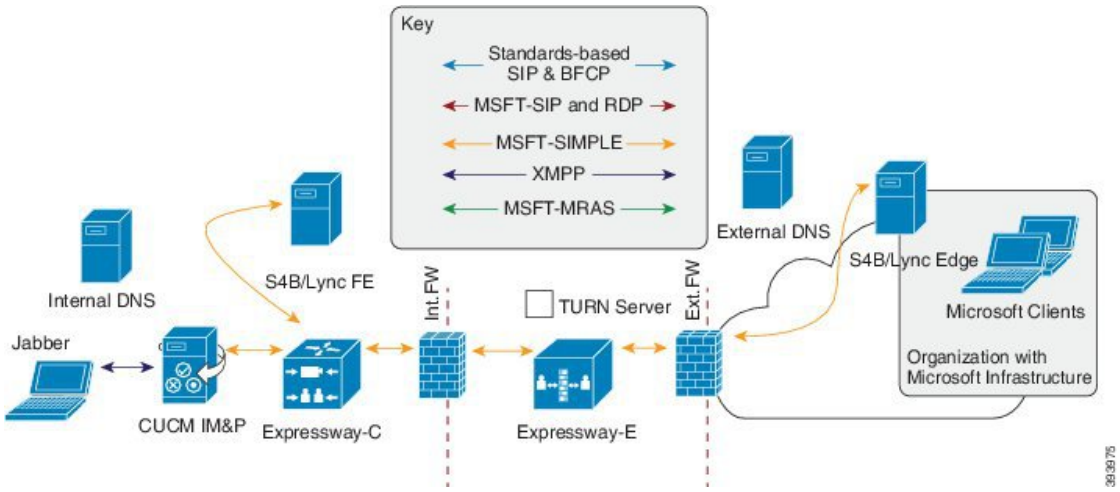
次の図は、Skype for Business サーバーのビジネス ツー ビジネス フェデレーションと単一エンタープライズ ネットワーク フェデレーションの両方を示しています。

- Business to Business フェデレーションでは、図の左側にある IM and Presence Service と、図の右側にある別の会社のネットワークにあるリモート Skype for Business サーバーの間で通信が行われます。この統合には、企業のファイアウォールを通過する通信が必要です。そ

のため、エンタープライズネットワーク内に展開されている Expressway-C に加えて、ファイアウォールの DMZ 内に Expressway-E を展開する必要があります。

- 単一エンタープライズネットワークでは、オンプレミスの Skype for Business サーバーは企業ネットワーク内にありますが、別のドメインにあります。この図では、Skype for Business サーバーは内部ファイアウォール内にあります。この統合には Expressway-C が必要ですが、通信がファイアウォールを通過する必要がないため、Expressway-E は必要ありません。

図 *23 : Skype for Business* とのフェデレーション




# Skype for Business フェデレーションのタスク フロー

オンプレミスまたはリモートの Skype for Business サーバーとのドメイン間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。この設定を使用して、次の展開のいずれかを設定できます。

- オンプレミスの Skype for Business サーバーを展開している別の企業との企業間統合。
- 単一の企業内では、IM and Presence Service とオンプレミスの Skype for Business サーバ間のドメイン間フェデレーションを設定できます。

（注） Office 365 でホストされている Skype for Business 展開とのフェデレーションについては、Office 365 とのドメイン間フェデレーション （101 ページ） を参照してください。

### はじめる前に

デフォルトでは、フェデレーションルーティングパラメータは、インストール時にデータベースパブリッシャノードの FQDN に設定されます。この値をリセットする場合は、フェデレーション ルーティング パラメータの構成 （50 ページ） に移動します。

| | IM and Presence Service の設定 | Expressway の設定 | Skype for Business の構成 | 説明 |
|---|---|---|---|---|
| ステップ 1 | フェデレーション サービスのオン （112 ページ） | | | フェデレーション サービスが実行中であることを確認します。 |
| ステップ 2 | IM および Presence の DNS SRV の割り当て （113 ページ） | | | Skype for Business が IM and Presence Service にトラフィックをルーティングできるように、DNS SRV レコードを構成します。 |
| ステップ 3 | IM および Presence へのフェデレーテッド ドメインの追加 （113 ページ） | | | すべての Skype for Business ドメインのドメインエントリを追加します。 |
| ステップ 4 | IM and Presence のスタティック ルートの構成 （114 ページ） | | | Expressway-C を指すスタティック ルートを設定します。 |
| ステップ 5 | TLS ピアとしての Expressway の追加 （114 ページ） | | | Expressway-C を TLS ピアとして設定します。 |
| ステップ 6 | アクセス制御リストへの Expressway の追加 （115 ページ） | | | すべての Expressway-C サーバーをアクセス制御リストに追加します。 |
| ステップ 7 | Cisco XCP ルータの再起動 （116 ページ） | | | 構成が完了したら、Cisco XCP ルータ サービスを再起動します。 |

| | IM and Presence Service の設定 | Expressway の設定 | Skype for Business の構成 | 説明 |
|---|---|---|---|---|
| ステップ 8 | | Configure Expressway for Federation with Skype for Business（116 ページ） | | ドメイン間フェデレーション用に Expressway を構成します。 |
| ステップ 9 | | | ユーザー信頼設定の構成 （117 ページ） | IM and Presence ユーザーの信頼設定を構成します。 |
| ステップ 10 | | | グローバル フェデレーション アクセス設定の構成 （118 ページ） | フェデレーションのグローバル アクセス エッジ設定を構成します。 |
| ステップ 11 | | | IM および Presence を許可ドメインとして追加 （118 ページ） | オプション。このタスクは、グローバル アクセス エッジ設定で IM and Presence ドメインが許可されていない場合にのみ実行します。 |
| ステップ 12 | | | IM および Presence の SIP フェデレーテッド プロバイダとして Expressway を追加 （119 ページ） | オプション。IM and Presence Service へのトラフィックのルーティングに DNS SRV を使用していない場合にのみ、このタスクを実行します。 |
| ステップ 13 | Exchange Certificates （120 ページ） | | | セットアップ内のサーバー間で証明書を交換します。 |

# フェデレーション サービスのオン

**Cisco XCP SIP Federation Connection Manager** サービスをオンにします。これにより、プロビジョニングする各ユーザーの SIP フェデレーション機能がオンになります。このタスクは、クラスタ内の各ノードで実行する必要があります。

**ステップ 1** **Cisco Unified IM and Presence Serviceability** のユーザーインターフェイスにログインします。**[Tools（ツール）] > [Service Activation（サービス アクティベーション）]** を選択します。

**ステップ 2** **[サーバー（X8.9.2）]** ドロップダウンから、IM and Presence ノードを選択し、**[移動（Go）]** をクリックします。

**ステップ 3** [ **IM and Presence Services**] で、 **Cisco XCP SIP Federation Connection Manager** サービスの横にあるオプション ボタンがオンになっていることを確認します。

**ステップ 4** [保存（Save）] をクリックします。

**ステップ 5** SIP フェデレーションが機能するには、Cisco SIP プロキシ サービスが実行されている必要があります。**Cisco Unified IM and Presence Serviceability** のユーザ インターフェイスにログインします。**[ツール（Tools）]** > **[機能サービス（Feature Services）]** を選択し、Cisco SIP プロキシ サービスが実行されていることを確認します。

# IM および Presence の DNS SRV の割り当て

IM and Presence Service の DNS SRV レコードを構成します。Skype for Business は、このレコードを使用して、Expressway 経由で IM and Presence Service にトラフィックをルーティングします。

- 企業間フェデレーションでは、レコードは Expressway-E の IP アドレスを指すパブリック DNS SRV である必要があります。
- 単一企業内のフェデレーションでは、Expressway-C の IP アドレスを指す内部 DNS を使用できます。フェデレーションは単一の企業内で行われるため、Expressway-E は必要ありません。

**例：**

```
nslookup
set type=srv
_sipfederationtls._tcp.expwye
```

ここで、`expwye` は Expressway-E のドメインです。

（注） DNS SRV レコードがなくてもドメイン間フェデレーションを構成できますが、この場合は、Skype for Business サーバにルートを手動で追加する必要があります。これを行うことを選択した場合は、このタスクをスキップできます。

**次のタスク**

IM および Presence へのフェデレーテッド ドメインの追加 （113 ページ）

# IM および Presence へのフェデレーテッド ドメインの追加

IM and Presence Service で、フェデレーションする Skype for Business ドメインごとにフェデレーション ドメイン エントリを追加します。

**ステップ 1** Cisco Unified CM IM およびプレザンス管理から、**[プレザンス（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、ドメイン名を入力します。

**ステップ 4** ドメインの**説明**を入力します。たとえば、 `Skype for Business フェデレーションドメイン`。

**ステップ 5** **[統合タイプ（Integration Type）]** ドロップダウンから、**[Inter-domain to OCS/Lync/S4B]** を選択します。

**ステップ 6** [保存（Save）] をクリックします。

### 次のタスク

Cisco XCP ルータの再起動 （116 ページ）

# IM and Presence のスタティック ルートの構成

IM and Presence Service で、Skype for Business ユーザーのスタティック ルートを構成します。スタティック ルートは TLS を使用し、Expressway-C を指している必要があります。

**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** **[接続先パターン（Destination Pattern）]** フィールドに、Skype for Business の FQDN を逆の形式で入力します。たとえば、ドメインが `s4b.com`の場合は、 `.com.s4b.*`と入力します。

**ステップ 4** **[次のホップ（Next Hop）]** フィールドに、Expressway-C 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。

### 次のタスク

TLS ピアとしての Expressway の追加 （114 ページ）

# TLS ピアとしての Expressway の追加

IM and Presence Service で次の手順を使用して、Expressway-C を TLS のピアとして設定します。

**ステップ 1** Expressway-C を TLS ピア サブジェクトとして追加します。

a) Cisco Unified CM IM and Presence 管理 で、**[システム（System）]** > **[セキュリティ（Security）]** > **[TLS ピア サブジェクト（TLS Peer Subject）]**を選択します。
b) [新規追加（Add New）] をクリックします。
c) [ピア サブジェクト名（ **Peer Subject Name** ）] フィールドに、Expressway-C の Expressway-C の完全修飾ドメイン名を入力します。
d) [説明（Description）] を入力します。
e) [保存（Save）] をクリックします。

**ステップ 2** 設定した Expressway TLS ピア サブジェクトを含む TLS コンテキストを作成します。

a) [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] から **[システム（System）]** > **[セキュリティ（Security）]** > **[TLS コンテキスト構成（TLS Context Configuration）]** の順に選択します。
b) [検索（Find）] をクリックします。
c) **[Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context]** をクリックします。
d) **[ TLS 暗号マッピング（TLS Cipher Mapping）]**で、矢印を使用して目的の TLS 暗号を **[選択した TLS 暗号（Selected TLS Ciphers）]** ボックスに移動します。ただし、ほとんどの場合、デフォルト設定のままで十分です。
e) **[TLS ピア サブジェクト マッピング（TLS Peer Subject Mapping）]** で、矢印を使用して、作成した TLS ピア サブジェクトを **[選択した TLS ピア サブジェクト（Selected TLS Peer Subjects）]** リスト ボックスに移動します。
f) [保存（Save）] をクリックします。

# アクセス制御リストへの Expressway の追加

IM and Presence Service で、Expressway-C が認証なしで IM and Presence Service にアクセスできるように、各 Expressway-C サーバのインバウンド アクセス制御リスト（ACL）エントリを追加します。マルチクラスタ展開の場合は、各クラスタでこの手順を実行します。

（注） グローバル アクセスを提供する ACL（[すべての許可（Allow from all）]）、または Expressway-C サーバーが存在するドメインへのアクセスを提供する ACL（たとえば、[company.com からの許可（Allow from company.com）]）がある場合は、Expressway-C サーバーの ACL エントリを追加する必要はありません。

**ステップ 1** IM and Presence Service のパブリッシャ ノードにログインします。

**ステップ 2** Cisco Unified CM IM and Presence 管理で、**[システム（System）]** > **[セキュリティ（Security）]** > **[受信 ACL（Incoming ACL）]** を選択します。

**ステップ 3** ACL エントリを作成します。

a) [新規追加（Add New）] をクリックします。

b) 新しい ACL エントリの **[説明（Description）]** を入力します。たとえば、`Expressway-C を介した Skype for Business フェデレーション`。
c) Expressway-C の IP アドレスまたは FQDN へのアクセスを提供する **[アドレス パターン（Address Pattern）]** を入力します。たとえば、`Allow from 10.10.10.1` または `Allow from expwyc.company.com` です。
d) [保存（Save）] をクリックします。
e) この一連の手順を繰り返して、別の ACL エントリを作成します。サーバー アクセスを提供するには、サーバー IP アドレスを含む ACL とサーバー FQDN を含む ACL の 2 つのエントリが必要です。

**ステップ 4** Cisco SIP Proxy サービスを再開します。
a) **[プレゼンス（Presence）]** > **[ルーティング（Routing）]** > **[設定（Settings）]** を選択します。
b) **[すべてのプロキシ サービスの再開（Restart All Proxy Services）]**をクリックします。

**次のタスク**

Cisco XCP ルータの再起動 （116 ページ）

# Cisco XCP ルータの再起動

設定が完了したら、 **Cisco XCP ルータ** を再起動します。

**ステップ 1** [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] から、**[ツール（Tools）]** > **[コントロールセンタ-ネットワークサービス（Control Center - Network Services）]** を選択します。
**ステップ 2** **サーバー** ドロップダウン リスト ボックスで、IM and Presence データベース パブリッシャ ノードを選択して、**[移動（Go）]** をクリックします。
**ステップ 3** **[IM and Presenceサービス（IM and Presence Services）]** の下で、**[Cisco XCP Router]** サービスを選択します。
**ステップ 4** **[再起動（Restart）]** をクリックします。
**ステップ 5** すべての IM and Presence サービスのクラスタ ノードでこの手順を繰り返します。

**次のタスク**

IM and Presence のスタティック ルートの構成 （114 ページ）

# Configure Expressway for Federation with Skype for Business

After interdomain federation is configured on the IM and Presence Service, set up Expressway for interdomain federation with Skype for Business.

- For business to business interdomain federation, you must deploy both Expressway-C and Expressway-E.

- For interdomain federation with a Skype for Business server that is located within your enterprise network, you can deploy an Expressway-C cluster only as the communication does not need to extend across the WAN.

For Expressway configuration details, see the *Chat and Presence XMPP Federation and Microsoft SIP Federation using IM and Presence or Expressway* at:

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

**Note** Make sure that your Expressway-C zone configuration points to the port that is associated with TLS Peer Authentication on the IM and Presence Service. You can confirm the correct port on Cisco Unified CM IM and Presence Administration by going to **System** > **Application Listeners** and confirming the port associated to **Default Cisco SIP Proxy TLS Listener - Peer Auth**. The default is **5062**.

### What to do next

After Expressway is configured, proceed with the Skype for Business setup:

ユーザー信頼設定の構成, on page 117

# ユーザー信頼設定の構成

Skype for Business サーバーで、Federated IM and Presence ユーザーのユーザー信頼設定を構成します。

**ステップ 1** Skype for Business サーバーにログインします。

**ステップ 2** 左側のナビゲーション バーで、**[フェデレーションと外部アクセス（Federation and External Access）]** をクリックします。

**ステップ 3** ヘッダー バーで、**[外部アクセス ポリシー（EXTERNAL ACCESS POLICY）]** をクリックします。

**ステップ 4** **[新規 （New）]** をクリックし、**[ユーザー ポリシー（User Policy）]** を選択します。

**ステップ 5** **[名前（Name）]** フィールドに、IM and Presence ドメインを入力します。

**ステップ 6** 次のいずれかのオプションを選択します。

- フェデレーテッド ユーザーとの通信を有効にする
- リモート ユーザーとの通信を有効にする
- パブリック ユーザーとの通信を有効にする

**ステップ 7** [確定する（Commit）] をクリックします。

### 次のタスク

グローバル フェデレーション アクセス設定の構成 （118 ページ）

# グローバル フェデレーション アクセス設定の構成

Skype for Business サーバーで、SIP フェデレーションのグローバル アクセス エッジ設定を構成します。

**ステップ 1** 左側のナビゲーション バーで、**[フェデレーションと外部アクセス（Federation and External Access）]** をクリックします。

**ステップ 2** ヘッダー バーで、**[アクセス エッジ構成（ACCESS EDGE CONFIGURATION）]** をクリックします。

**ステップ 3** **[グローバル（Global）]**を選択します。

**ステップ 4** すべてのドメインへのアクセスをグローバルに許可する場合は、次の各オプションを選択します。それ以外の場合は、許可するオプションを選択します。

- フェデレーションとパブリック IM 接続の有効化
- [パートナー ドメイン検出の有効化（Enable partner domain discovery）]：パブリック DNS SRV レコードを使用してトラフィックを IM and Presence Service にルーティングするには、このオプションを選択します。DNS SRV レコードを使用しない場合、または DNS SRV レコードがない場合は、このオプションをオフのままにします。
- リモート ユーザー アクセスの有効化
- 会議への匿名ユーザ アクセスの有効化

（注） アクセスをグローバルに許可しない場合は、IM and Presence を許可ドメインおよび SIP フェデレーテッド プロバイダーとして手動で追加する必要があります。

**ステップ 5** [確定する（Commit）] をクリックします。

### 次のタスク

制限付きアクセスを設定した場合（つまり、一部のグローバルオプションをオフのままにした場合）、IM および Presence を許可ドメインとして追加 （118 ページ）。

グローバルにアクセスを許可しているが、IM and Presence Service にルーティングするためのパブリック DNS SRV レコードがない場合は、IM および Presence の SIP フェデレーテッド プロバイダとして Expressway を追加 （119 ページ）。

それ以外の場合、グローバルにアクセスを許可し、IM and Presence Service にトラフィックをルーティングするパブリック DNS SRV レコードがある場合は、Exchange Certificates （120 ページ）。

# IM および Presence を許可ドメインとして追加

Skype for Business サーバのグローバル アクセス エッジ設定ですべてのドメインが許可されていない場合は、この手順を使用します。この場合、IM and Presence Service ドメインの特定のエントリを追加します。

**ステップ 1** 左側のナビゲーション バーで、**[フェデレーションと外部アクセス（Federation and External Access）]** をクリックします。

**ステップ 2** ヘッダー バーで、**[SIP フェデレーション ドメイン（SIP FEDERATED DOMAINS）]** をクリックします。

**ステップ 3** **[新規 （New）]** をクリックし、**[許可されたドメイン（ Allowed domain）]** を選択します。

**ステップ 4** **[ドメイン名（Domain name）]** フィールドに、IM and Presence ドメインを入力します。

**ステップ 5** **[アクセス エッジ サービス（FQDN）（Access Edge Service (FQDN)）]** フィールドで、Expressway-E 完全修飾ドメイン名を入力します。

**ステップ 6** [確定する（Commit）] をクリックします。

### 次のタスク

Skype for Business から IM and Presence Service にトラフィックをルーティングするためにパブリック DNS SRV レコードを使用しているかどうかを確認します。

- DNS SRV レコードを使用していない場合は、IM and Presence の SIP プロバイダーとして Expressway を手動で追加します。「IM および Presence の SIP フェデレーテッド プロバイダとして Expressway を追加 （119 ページ）」を参照してください。
- DNS SRV レコードを使用している場合は、Exchange Certificates （120 ページ） を選択します。

# IM および Presence の SIP フェデレーテッド プロバイダとして Expressway を追加

Skype for Business からのトラフィックをルーティングするために DNS SRV レコードを使用していない場合は、Skype for Business サーバーでこの手順を使用します。この場合、IM and Presence Service の SIP フェデレーション プロバイダとして Expressway を手動で追加する必要があります。

（注） IM and Presence Service の DNS SRV レコードがある場合は、このタスクをスキップできます。

**ステップ 1** Skype for Business サーバーで、**[フェデレーションおよび外部アクセス（ Federation and External Access）]** をクリックします。

**ステップ 2** **[SIP フェデレーション プロバイダ（SIP FEDERATED PROVIDERS）]**をクリックします。

**ステップ 3** **[新規 （New）]** をクリックし、**[ホステッド プロバイダ（Hosted provider）]** を選択します。

**ステップ 4** **[プロバイダ名（ Provider name）]** フィールドに、IM and Presence ドメインを入力します。

**ステップ 5** **[Access Edge service (FQDN)]** フィールドに、Expressway-E サーバの完全修飾ドメイン名を入力します。

ステップ 6 [確定する（Commit）] をクリックします。

### 次のタスク

Exchange Certificates （120 ページ）

# Exchange Certificates

Follow this process to exchange certificates among the servers in your Interdomain Federation with Skype for Business deployment.

**Note** External Edge certificates from the Skype for Business edge server must have the following OID values under Enhanced Key Usage:

- Server Authentication: (1.3.6.1.5.5.7.3.1)
- Client Authentication: (1.3.6.1.5.5.7.3.2)

ステップ 1 Download certificates from each system in the deployment:

- IM and Presence Service (internal certificate can be self-signed)
- Expressway-C (internal certificate can be self-signed)
- Expressway-E (external certificate must be CA-signed). Note that the Expressway-E is required for Business to Business federation only. Expressway-E is not used for single enterprise network.
- Skype for Business edge server (External Edge certificate must be CA-signed)

**Note** In this context, if any of the certificates, such as Expressway-E and Skype for Business, are signed by a Certificate Authority, it is the Root CA certificate that is actually added in the relevant far end trust store. Only in the scenario of self-signed certificates should themselves be added to the far end trust stores.

ステップ 2 On the IM and Presence Service, upload the Expressway-C certificate to **cup-trust**.

ステップ 3 On the Expressway-C, upload the IM and Presence Service certificate and, (for Single Enterprise Network federation only) the Skype for Business certificate.

ステップ 4 Upload the Skype for Business certificate as follows:

- (Single Enterprise Network). On the Expressway-C, upload the Skype for Business certificate
- (Business to Businss only) On the Expressway-E, upload the Skype for Business External Edge certificate.

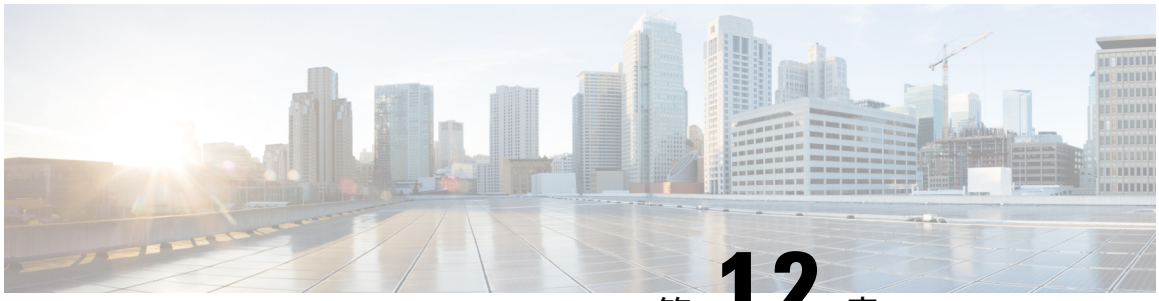
ステップ 5 On the Skype for Business edge server, upload the Expressway-E external certificate (for Business to Business) or the Expressway-C certificate (for federation within a single enterprise).

### Certificate Notes

- For IM and Presence Service, you can download and upload certificates from the **Certificate Management** window in Cisco Unified IM OS Administration (choose **Security** >

**Certificate Management**). For detailed procedures, see the "Security Configuration" chapter of the *Configuration and Administration Guide for IM and Presence Service* at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html.

- For Expressway certificate management, see the *Cisco Expressway Administrator Guide* at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html.
- For Skype for Business certificates, you can use the Skype for Business Deployment Wizard to install or download certificates. Run the wizard and select the **Request, Install or Assign Certificates** option. For details, see your Microsoft Skype for Business documentation.



第 12 章

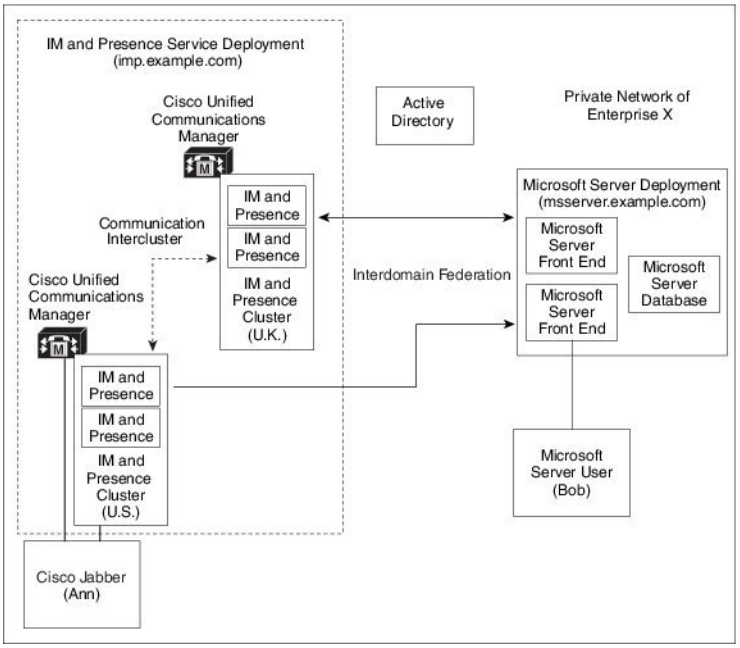
# Microsoft Lync へのドメイン間フェデレーション

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 *24* : 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 （125 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 （126 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。<br>（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 （126 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。<br>（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 （127 ページ）<br>• Lync から IM および Presence へのスタティック ルートの構成 （128 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 （131 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 （133 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 （133 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 （126 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 （126 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 （128 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 127

# 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 （131 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 *17 : 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）<br>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<br>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。<br>（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 （131 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`。<br>**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`。<br>**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。<br>**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`<br>• impserverPub = IM and Presence Service のホスト名。<br>• 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`<br>（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 （133 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 （133 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.

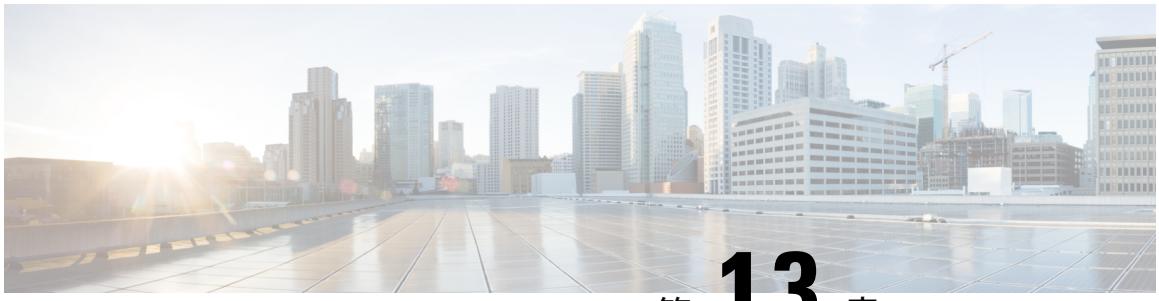
ステップ 5 Add the TLS Peer to the Selected TLS Peer Subjects list.

- 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, on page 71
- Microsoft TechNet Library, Windows Server — Implementing and Administering Certificate Templates at http://technet.microsoft.com/en-us/library/cc731256(v=ws.10).aspx.



第 13 章

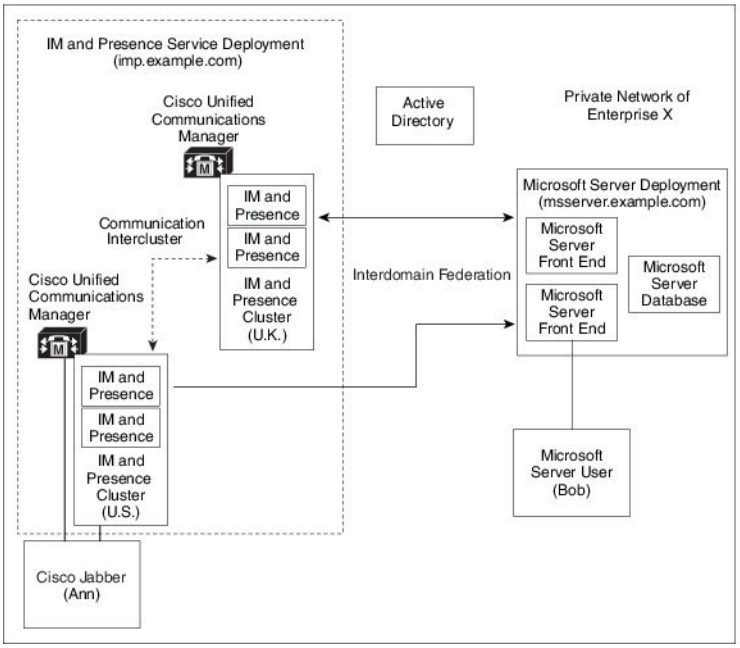
# Microsoft OCS へのドメイン間フェデレーション

ここでは、Microsoft OCS 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 OCS へのドメイン間フェデレーション

図 *25* : 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 OCS フェデレーションの構成タスク フロー

IM and Presence Service と Microsoft OCS 間のフェデレーテッド リンクを設定するには、次のタスクを実行します。

Access Edge サーバーまたは Cisco 適応型セキュリティ アプライアンスを使用せずに IM and Presence Service から OCS への直接フェデレーションを使用している場合は、OCS サーバーの各ドメインに TLS または TCP スタティック ルートを構成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 Service ノードを指します。Cisco 適応型セキュリティアプライアンスまたは Microsoft Access Edge は必要ありません。

- Standard Edition の場合は、すべての Standard Edition サーバーでスタティック ルートを設定します。
- Enterprise Edition の場合は、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** | 企業内での Microsoft OCS ドメインの追加 （137 ページ） | IM and Presence Service で、Microsoft OCS 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** | Microsoft サーバの IM および Presence サービスのスタティック ルートの構成 （138 ページ） | IM and Presence Service 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 サーバーを指す必要があります。<br>（注） OCS の場合、プロトコル タイプとして TCP または TLS を選択できます。 |
| **ステップ 3** | OCS で IM および Presence サービスに向かうスタティック ルートの構成 （139 ページ） | OCS サーバーで、IM and Presence Service ドメインを指す 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 Service ノードを指している必要があります。 |
| **ステップ 4** | ピア認証リスナーの確認 （140 ページ） | IM and Presence Service で、ピア認証リスナーがポート 5061 として設定され、サーバー認証リスナーがポート 5061 では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 ノードのホスト認証エントリの追加 （141 ページ） | OCS サーバーで、各 IM and Presence Service ノードのホスト認証エントリを設定します。TLS 暗号化で |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | は、IM and Presence ノードごとに 2 つのエントリを追加する必要があります。<br>• IM and Presence ノードの IP アドレスを含む 1 つのエントリ<br>• IM and Presence ノードの FQDN を含む 1 つのエントリ<br>TLS 暗号化を使用していない場合は、ノード IP アドレスを使用して、各 IM and Presence Service ノードに 1 つのホスト認証エントリを構成します。 |
| ステップ 6 | ドメイン間フェデレーション用の OCS での証明書の構成 （142 ページ） | OCS と IM and Presence Service の間に TLS が設定されている場合は、IM and Presence Service とのドメイン間フェデレーション用に OCS で証明書を構成します。<br>（注） TLS を使用していない場合は、この手順をスキップできます。 |
| ステップ 7 | OCS サーバーでポート 5060/5061 を有効にする （142 ページ） | OCS サーバーで、TLS（トランスポートは MTLS または TLS のいずれか）または TCP のリスナーポートが設定されていることを確認します。。<br>• OCS サーバーへの TLS スタティック ルートの場合は、ポート 5061 を使用します。<br>• OCS サーバーへの 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 の構成 （143 ページ） | TLS を使用している場合は、FIPS を使用するように OCS を設定します。 |
| ステップ 9 | Set Up Certificates on the IM and Presence Service Node for Federation with Microsoft Server over TLS （144 ページ） | TLS を使用している場合は、OCS サーバー証明書に署名する CA のルート証明書を IM and Presence Service にアップロードします。 |

# 企業内での Microsoft OCS ドメインの追加

OCS サーバのフェデレーション 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ション 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

Microsoft サーバの IM および Presence サービスのスタティック ルートの構成 （138 ページ）

# Microsoft サーバの IM および Presence サービスのスタティック ルートの構成

フェデレーション Microsoft サーバー ドメインと IM および可用性を交換するときに TLS を使用するように IM and Presence Serviceを 構成したり、OCS ドメインに TCP を使用したりするには、 Microsoft Access Edge の外部エッジではなく Microsoft サーバーを指す IM and Presence Service でスタティック ルートを構成する必要があります。

各 Microsoft サーバー ドメインに個別スタティック ルートを追加する必要があります。Microsoft サーバー ドメインのスタティック ルートは、特定の Microsoft サーバー Enterprise Edition フロントエンド サーバーまたは Standard Edition サーバーの IP アドレスを指す必要があります。

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 ルートは優先度が低く、プライマリ スタティック ルートのネクスト ホップ アドレスが到達不可能な場合にのみ使用されます。

**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）] > [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、接続先パターン値を入力します。例：

- ドメインが `domaina.com`の場合は、[接続先パターン（Destination Pattern）] 値として `.com.domaina.*` と入力します。

**ステップ 4** 次のように残りのパラメータを入力します。

a) [ネクスト ホップ（Next Hop）] を入力します。値は Microsoft サーバーの IP アドレスまたは FQDN です。

b) [ネクスト ホップ ポート（Next Hop Port）] の番号と [プロトコル タイプ（Protocol Type）] の値を選択します。

- TCP の場合：ドロップダウン リストから、[プロトコル タイプ（Protocol Type）] として **[TCP ]** を選択し、[ネクスト ホップ ポート（Next Hop Port）] 番号として **5060** を選択します。
- TLS の場合：ドロップダウン リストから、[プロトコル タイプ（Protocol Type）] として **[TLS]** を選択し、[ネクスト ホップ ポート（Next Hop Port）] 番号として **5061** を選択します。

（注） Microsoft OCS サーバーは、TCP または TLS を介した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。

### 次のタスク

OCS で IM および Presence サービスに向かうスタティック ルートの構成 （139 ページ）

# OCS で IM および Presence サービスに向かうスタティック ルートの構成

OCS が直接フェデレーションのために IM and Presence Service に要求をルーティングできるようにするには、各 IM and Presence Service ドメインの OCS サーバで TLS または TCP スタティック ルートを構成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 Service ノードを指します。

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

**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]]** の順に選択します。

**ステップ 2** 必要に応じて、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）]**の順に選択します。

**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** IM and Presence Service ノードのドメインを入力します（例：foo.com）。

**ステップ 6** **[電話 URI（Phone URI）]** のチェックボックスがオフになっていることを確認してください。

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

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

（注）
- TLS スタティック ルートに使用されるポートは、 IM and Presence Service ノードで構成されているピア認証リスナー ポートと一致する必要があります。
- FQDN は、OCS サーバによって解決可能である必要があります。FQDN が IM and Presence Service 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 のホストを置換する（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]** をクリックすると、**[スタティック 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（Routing）] リストに表示されます。

**ステップ 10** もう一度 **[OK]** をクリックして、**[フロント エンド サーバーのプロパティ（ Front End Server Properties）]** ウィンドウを閉じます。

### 次のタスク

『Cisco Unified Communcations Manager ガイド』で IM and Presence Service のドメイン間フェデレーションの「ピア認証リスナーの確認」を参照してください。

# ピア認証リスナーの確認

IM and Presence Service 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。

**ステップ 1** Cisco Unified CM IM and Presence Administration から、**[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。
設定されたアプリケーション リスナー ポートのリストが表示されます。デフォルトのピア認証リスナー ポートとサーバー認証リスナー ポートも表示されます。

**ステップ 3** **[デフォルトの Cisco SIP プロキシ TLS リスナー - ピア認証ポート（Default Cisco SIP Proxy TLS Listener - Peer Auth port）]** が 5061 であることを確認します。

**ステップ 4** **[デフォルトの Cisco SIP プロキシ TLS リスナー - サーバー認証ポート（Default Cisco SIP Proxy TLS Listener - Server Auth port）]** が 5061 では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 です。

### 次のタスク

OCS での IM and Presence サービス ノードのホスト認証エントリの追加 （141 ページ）

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

OCS が認証を求められることなく IM and Presence Service からの SIP 要求を受け入れることができるようにするには、各 IM and Presence Service ノードの OCS でホスト認証エントリを構成する必要があります。

OCS と IM and Presence Service間の TLS 暗号化を構成する場合は、次のように各 IM and Presence Service 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 Service ノードの FQDN が含まれている必要があります。
- 2 番目のエントリには、 IM and Presence Service ノードの IP アドレスが含まれている必要があります。

TLS 暗号化を構成しない場合は、各IM and Presence Service ノードにホスト認証エントリを 1 つだけ追加します。このホスト許可エントリには、 IM and Presence Service 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、必要なホスト許可エントリを追加する方法について説明します。

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

**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) IP アドレスでネクストホップ コンピュータを指定するスタティック ルートを OCS で構成した場合は、承認済みホストの IP アドレスを入力します。

b) FQDN でネクスト ホップ コンピュータを指定するスタティック ルートを OCS で構成した場合は、承認済みホストの FQDN を入力します。

**ステップ 3** [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 Service ノードの IP アドレスを入力します。

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

**ステップ 7** **[認証済みとして扱う（Treat as Authenticated）]** チェックボックスをオンにします。

（注） **[アウトバウンドのみ（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。

### 次のタスク

ドメイン間フェデレーション用の OCS での証明書の構成 （142 ページ）

# ドメイン間フェデレーション用の OCS での証明書の構成

OCS と IM and Presence Service の間に TLS が設定されている場合は、IM and Presence Service とのドメイン間フェデレーション用に OCS で証明書を構成します。

（注） TLS を使用していない場合は、この手順をスキップできます。

**ステップ 1** 次の手順を実行して、CA ルート証明書と OCS 署名付き証明書を取得します。

a) CA 証明書チェーンをダウンロードしてインストールします。

b) CA サーバーから証明書を要求します。

c) CA サーバーからの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ーのプロパティから、**[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。

### 次のタスク

OCS サーバーでポート 5060/5061 を有効にする （142 ページ）

# OCS サーバーでポート 5060/5061 を有効にする

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

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

**ステップ 2** フロントエンド サーバーの FQDN を右クリックします。

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

**ステップ 4** ポート 5060 または 5061 が [接続（Connections）] の下に表示されていない場合は、**[追加（Add）]** をクリックします。

**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）] として **[すべて（All）]** を選択します。

b) [ポート値（Port Value）] 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 の場合は、[ポート値（Port Value）] として **5061** を選択します。

c) トランスポート値 を選択します。

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

**ステップ 6** **[OK]** をクリックします。

### 次のタスク

FIPS を使用するための OCS の構成 （143 ページ）

# FIPS を使用するための OCS の構成

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

**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）]** のいずれかを選択します。

**ステップ 4** **[システム暗号化：暗号化、ハッシュ、署名のためのFIPS準拠アルゴリズムを使う（System Cryptography: Use FIPS Compliant algorithms for encryption, hashing and signing）]** をダブルクリップします。

**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） これを有効にするには、OCS を再起動する必要がある場合があります。

ステップ 7 IM and Presence Service 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 の信頼ストアへ CA ルート証明書をインポートします。

### 次のタスク

Set Up Certificates on the IM and Presence Service Node for Federation with Microsoft Server over TLS（144 ページ）

# Set Up Certificates on the IM and Presence Service Node for Federation with Microsoft Server over TLS

This procedure applies only if you have set up TLS static routes between IM and Presence Service and Microsoft servers.

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.

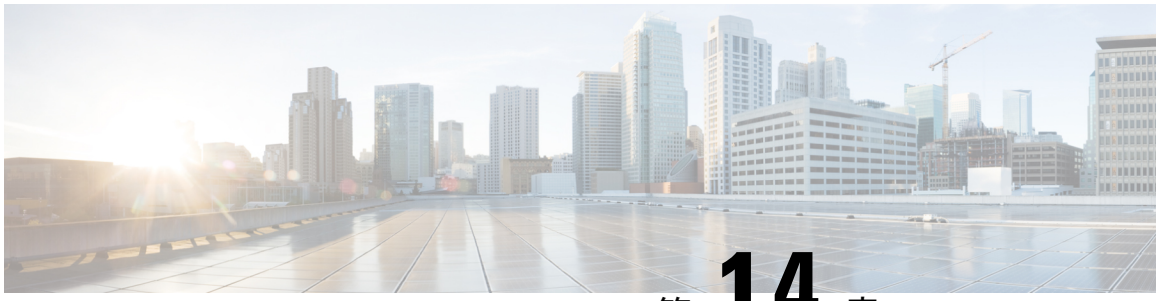
ステップ 5 Add the TLS Peer to the Selected TLS Peer Subjects list.

- 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. See:

- CA サーバーからの証明書の要求, on page 71
- Microsoft TechNet Library, Windows Server — Implementing and Administering Certificate Templates at http://technet.microsoft.com/en-us/library/cc731256(v=ws.10).aspx



第 14 章

# SIP フェデレーションの外部サーバー コンポーネントの構成

このセクションでは、SIP フェデレーションの外部サーバー コンポーネントの設定について説明します。



# Microsoft Component Configuration for SIP Federation

The following tables provide a brief checklist to configure federation on the Microsoft OCS and Access Edge servers. For detailed instructions on setting up and deploying the OCS server and the Access Edge server, refer to the Microsoft documentation.

***Table 18: Configuration Tasks for Microsoft Components - OCS Server***

| Task | Procedure |
|---|---|
| Enable Global Federation Setting | **1.** In the global forest branch in the left pane, choose **Properties** > **Global Properties** > **Federation**.<br>**2.** Check the **Enable Federation and Public IM Connectivity** check box.<br>**3.** Enter the FQDN and the port number for the internal interface of the Access Edge server. |
| Configure the Access Edge server address | **1.** In the global forest branch in the left pane, choose **Properties** > **Global Properties** > **Edge Servers**.<br>**2.** In the **Access Edge and Web Conferencing Edge Servers** window, click **Add** .<br>**3.** Enter the FQDN for the internal interface of the Access Edge server. |

| Task | Procedure |
|---|---|
| Enable Each Front End Federation Setting | You need to enable the federation setting for each front-end server that is federating:<br>1. In the front-end server branch in the left pane, choose **Properties** > **Front End Properties** > **Federation**.<br>2. Check the **Enable Federation and Public IM Connectivity** check box. |
| Check your users are enabled for MOC and for Federation | • Choose the **Users** tab and check that your users are enabled for MOC.<br>• If your user is not present in this list, you need to enable the user for MOC in Microsoft Active Directory.<br>• You also need to enable the user for **Public IM Connectivity** in Microsoft Active Directory.<br>Refer to the Microsoft Active Directory documentation at the following URL: http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx |
| Configure the security certificates | • You need to configure security certificates between the OCS server and the Access Edge server.<br>• A CA server is required to perform this procedure.<br>• Please refer to the Microsoft documentation for details on configuring security certificates between these servers. |

*Table 19: Configuration Tasks for Microsoft Components - Access Edge Server*

| Task | Procedure |
|---|---|
| Configure DNS | In the Microsoft enterprise deployment, you need to configure an external SRV record for all Access Edge Servers that points to _sipfederationtls._tcp.*domain*, over port 5061, where *domain* is the name of the SIP domain of your organization. This SRV should point to the external FQDN of the Access Edge server. |

| Task | Procedure |
|---|---|
| Configure IM and Presence Service as an IM Provider | **1.** On the external Access Edge server, choose **Start** > **Administrative Tools** > **Computer Management**.<br>**2.** In the left pane, right-click **Microsoft Office Communications Server 2007**.<br>**3.** Choose the **IM Provider** tab.<br>**4.** Click **Add**.<br>**5.** Check the **Allow the IM service provider** check box.<br>**6.** Define the IM service provider name, for example, the IM and Presence Service node.<br>**7.** Define the network address of the IM service provider, in this case the public FQDN of the IM and Presence Service node.<br>**8.** Ensure that the IM service provider is not marked as “public”.<br>**9.** Click the filtering option **Allow all communications from this provider** option.<br>**10.** Click **OK**.<br>In the IM and Presence Service enterprise deployment, you need to configure a DNS SRV record for each IM and Presence Service domain. The DNS SRV record should point to _sipfederationtls._tcp.*IM and Presence_domain* over port 5061, where *IM and Presence _domain* is the name of the IM and Presence Service domain. This DNS SRV should point to the public FQDN of the IM and Presence Service node. |
| Check the Access Method Settings | **1.** Iin the console tree, right-click on Microsoft Office Communications Server 2007.<br>**2.** Choose **Properties** > **Access Methods**.<br>**3.** Check the **Federation** check box.<br>**4.** Check the**Allow discovery** check box if you are using DNS SRV. |

| Task | Procedure |
|---|---|
| Configure Access Edge to use TLSv1 | 1. To open the Local Security Policy, choose **Start** > **Administrative Tools** > **Local Security Policy**.<br>**Note** If you are configuring this on a domain controller, the path is **Start** > **Administrative Tools** > **Domain Controller Security Policy**.<br>2. In the console tree, choose **Security Settings** > **Local Policies** > **Security Options**.<br>3. Double-click the FIPS security setting in the details pane.<br>4. Enable the FIPS security setting.<br>5. Click **OK**.<br>**Note** There is a known issue with remote desktop to the Access Edge server with FIPS enabled on Windows XP. Refer to リモートデスクトップから Edge にアクセスできない, on page 215 for a resolution to this issue. |
| Configure the security certificates | • You need to configure security certificates between the OCS server and the Access Edge server.<br>• A CA server is required to perform this procedure.<br>• Please refer to the Microsoft documentation for details on configuring security certificates between these servers. |

# AOL との SIP フェデレーションの要件

## AOL フェデレーションのライセンス要件

IM and Presence Service と AOL 間のドメイン間フェデレーションを有効にするには、Cisco から AOL-FEDERATION SKU ライセンスを注文する必要があります。このライセンス要求を送信すると、Ciscoは、このトピックの後のセクションで説明されている AOL 顧客のルーティング情報と連絡先情報を要求します。Cisco が AOL の顧客ルーティング情報と連絡先情報を受信すると、 IM and Presence Service と AOL 間の AOL フェデレーションがオンになります。

**関連情報 -**

AOL ルーティング情報の要件

AOL プロビジョニング情報の要件

**関連トピック**

AOL ルーティング情報の要件 （151 ページ）

AOL プロビジョニング情報の要件 （151 ページ）

# AOL ルーティング情報の要件

IM and Presence Service と AOL SIP（ソリューション インセンティブ プログラム）アクセス ゲートウェイ間のドメイン間フェデレーションを構成する場合は、AOL に次の情報を提供する必要があります。

| 展開タイプ | 提供（ドメインごと） | 注記 |
|---|---|---|
| ロード バランサなし | • フェデレーション ルーティング IM and Presence Service ノードのパブリック FQDN：<sip.domain.com><br>• IM and Presence Service ノードのドメイン名：@<domain.com> | • IM and Presence Service サーバ証明書のサブジェクト CN は、IM and Presence Service ノードの FQDN と一致する必要があります<br>• IM and Presence Service サーバー証明書に署名する CA は、AOL サーバーによって信頼されている必要があります。 |
| ロード バランサ | • ロード バランサの FQDN：<lb.domain.com><br>• ロードバランサのドメイン名：@<domain.com> | • IM and Presence Service サーバー証明書のサブジェクト CN は、ロードバランサの FQDN と一致する必要があります。<br>• IM and Presence Service サーバー証明書に署名する CA は、AOL サーバーによって信頼されている必要があります。 |
| | ドメインに使用される IM and Presence Service ノードのセキュア SIP フェデレーション ポート | AOL SIP アクセス ゲートウェイは、このポートの nslookup によって返される IP アドレスに（SSL 経由で）接続します。デフォルト値は5061です。 |

Cisco のサポート担当者と協力して、この情報を AOL に提供することを推奨します。

# AOL プロビジョニング情報の要件

Cisco のサポート担当者と協力して、次のコンタクトとプロビジョニング情報を AOL に提供することをお勧めします。

- 企業、会社などの名前。

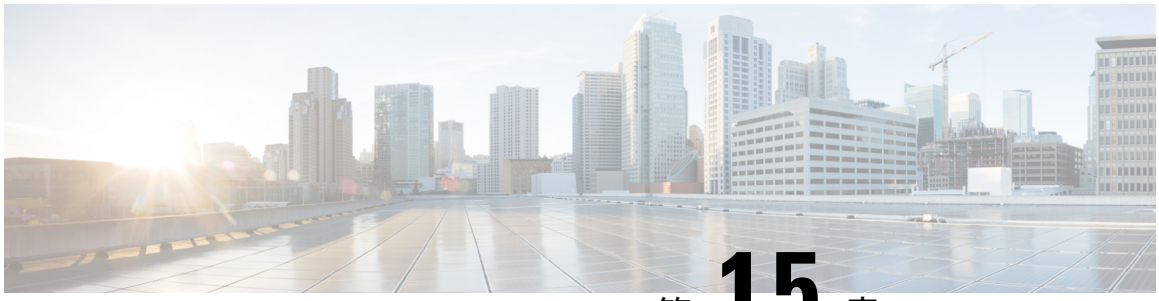
- フェデレーションに使用される、IM and Presence Service によってホストされるすべてのローカル ドメイン名（companyabc.com、sales-companyabc.com など）。リリース 10.5(1) 以降では、**[Cisco Unified CM IM and Presence Administration]の** > **[プレゼンス ドメイン（Presence Domains）]** ウィンドウでこれらの名前の完全なリストを確認できます。
- フェデレーションに使用されている IM and Presence Service ノードのパブリックに解決可能な FQDN。
- 顧客のコンタクトの詳細：名前、電子メール アドレス、電話番号。
- 証明書のコピー：

（注） 必要な証明書の詳細については、「AOL ルーティング情報の要件」を参照してください。

  - 証明書認証局によって署名されている場合、証明書認証局Yの証明書のチェーン全体を含むルート証明書を提供する必要があります。
  - 証明書の Base 64 エンコーディングが必要です。次に例を示します。

BEGIN CERTIFICATE-----
MIIGKDCCBRCgAwIBAgIKH5c9LAAIAAGTvjANBgkqhkiG9w0BAQUFADCBizETMBEG
CgmSJomT8ixkARkWA2NvbTEZMBcGCgmSJomT8ixkARkWCW1pY3Jvc29mdDEUMBIG.....
6HKfdML7AkWOV0Wiwc8HUb/0iFmfB24jWOnjj3NW15k0tDJXmbSMuAxjZ/2dZ4dA
4zd4FeZvoCzyVglPkoLvA0Z+AJyOkO7/tie4EF3n/kEedaPWimv2TpRrlAP5lBXn
tbM82NpEDaSqzg0d4Dswqe7W30CKGgUBYS1fO7xJHSRju719D+H7XivmjvU= -----END
CERTIFICATE-----

（注） このプロセスの詳細については、「AOL フェデレーションのライセンス要件」を参照してください。



第 15 章

# SIP フェデレーションの冗長性のためのロード バランサの構成

このセクションでは、SIP フェデレーションの冗長性のためのロードバランサの構成について説明します。



## ロード バランサについて

冗長性と高可用性を実現するために、ロード バランサをフェデレーション ネットワークに組み込むことができます。ロード バランサは、 IM and Presence Service ノードと Cisco 適応型セキュリティ アプライアンス の間に配置されます（SIP フェデレーションの高可用性 （8 ページ） を参照）。

ロードバランサは、Cisco適応型セキュリティアプライアンスからの着信TLS接続を終了し、新しい TLS 接続を開始して、コンテンツを適切なバックエンド IM and Presence Service ノードにルーティングします。

## IM and Presence Service ノードの更新

冗長性のためにロード バランサを使用する場合は、 IM and Presence Service のパブリッシャ ノードとサブスクライバ ノードの設定を更新する必要があります。

**手順**

| タスク | 手順 |
| --- | --- |
| フェデレーション ルーティング パラメータの更新 | **Cisco Unified IM and Presence Administration**にログインし（Service）] メニューから**[システム（System）]** > **[サービス（ServiceParameters）]** > **[Cisco SIP プロキシ（Cisco SIP Pr**し、次の値を入力します。<br>• **仮想IPアドレス（Virtual IP Address）**：ロード バランれている仮想 IP アドレス セットを入力します<br>1. **サーバー名（Server Name）**：ロード バランサの Fトします<br>2. **Federation Routing IM and Presence Service FQDN**ランサの FQDN にセットします。 |
| 新しい TLS ピア サブジェクトの作成 | 1. **Cisco Unified CM IM and Presence 管理** で、**[システム [セキュリティ（Security）]** > **[TLS ピア サブジェクト Subjects）]**を選択します。<br>2. **[新規の追加（Add New）]** をクリックして次の値を入力<br>• **ピアのサブジェクト名（Peer Subject Name）**：ロサの外部 FQDN を入力します。<br>• **説明（Description）**：ロードバランサーの名前を入 |
| TLS ピア サブジェクト リストへの TLS ピアの追加 | 1. **[Cisco Unified CM IM and Presence の管理（Cisco Unifi and Presence Administration）] [システム（System）]** > ティ（Security）]** > **[TLS コンテキスト構成（TLS Con Configuration）]**の順に選択します。<br>2. [検索（Find）] をクリックします。<br>3. **[Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Conte**クします。<br>4. ロードバランサのロード バランサフェデレーション T ジェクトを TLS ピア サブジェクト リストに移動します |

# Cisco 適応型セキュリティ アプライアンスの更新

ロード バランサを使用する場合、外部ドメインはパブリック IM and Presence Service アドレスにメッセージを送信しますが、Cisco 適応型セキュリティ アプライアンス はそのアドレスをロード バランサの仮想 IP アドレスにマッピングします。したがって、Cisco 適応型セキュリティ アプライアンス は、外部ドメインからメッセージを受信すると、そのメッセージをロー

ドバランサに転送します。ロード バランサは、適切な IM and Presence Service ノードにそれを渡します。

この設定をサポートするには、Cisco 適応型セキュリティ アプライアンスにいくつかの変更を加える必要があります。

# スタティック PAT メッセージの更新

ロード バランサの詳細を含めるには、スタティック PAT メッセージを更新する必要があります。

**手順**

| タスク | Cisco 適応型セキュリティ アプライアンス リリース 8.2 コマンド | Cisco 適応型セキュ |
|---|---|---|
| IM and Presence Service Publisher に必要な変更 | | |
| パブリック IM and Presence Service アドレスに任意の未使用ポートを使用するようにスタティック PAT を変更します。 | 変化：<br>**static (inside,outside) tcp** *public_imp_ip_address 5061 routing_imp_private_ip_address 5062* **netmask** *255.255.255.255*<br>：<br>**static (inside,outside) tcp** *public_imp_ip_address 55061 routing_imp_publisher_ private_ip_address 5062* **netmask** *255.255.255.255* | 変化：<br>**object service** *obj 5061*<br>**nat (inside,outsid** *obj_host_routing_i obj_host_public_im obj_tcp_source_eq_*<br>宛先<br>**object service** *obj 55061*<br>**nat (inside,outsid** *obj_host_routing_i obj_host_public_im obj_tcp_source_eq_* |
| 新しいスタティック PAT を追加して、パブリック IM and Presence Service アドレスに送信されたメッセージを仮想ポート アドレス（ロード バランサが TLS メッセージをリッスンしているポート）に転送できるようにします。 | **static (inside,outside) tcp** *public_imp_address 5061 load_balancer_vip 5062* **netmask** *255.255.255.255* | **object network** *obj routing_imp_privat*<br>**object service** *obj 5061*<br>**nat (inside,outsid** *obj_host_public_im obj_tcp_source_eq_* |
| IM and Presence Service Subscriber に必要な変更 | | |

| タスク | Cisco 適応型セキュリティ アプライアンス リリース 8.2 コマンド | Cisco 適応型セキュリ |
|---|---|---|
| ロード バランサの仮想 IP アドレスの新しいアクセス リストを追加します。IM and Presence Service でアクセスする必要がある各外部ドメインのアクセス リストを追加する必要があります。 | **access-list** *ent_lber_to_external_ocs* **extended permit tcp host** *external_domain_public_ip_address 5061*<br>**access-list** *ent_lcs_to_lber_routg_imp* **extended permit tcp hos** *imp_public_ip_address 65061* | |
| ロード バランサの仮想 IP アドレスが設定されている場合に、 IM and Presence Serviceサーバへのメッセージを開始するための **extended permit tcp hos** 外部ドメインの新しいアクセス リストを追加します。IM and Presence Service にアクセスする必要がある各外部ドメインのアクセス リストを追加する必要があります。 | | |

**関連トピック**

スタティック IP ルートの構成 （81 ページ）
ポート アドレス変換（PAT） （82 ページ）

# アクセス リストの更新

ロード バランサをサポートするには、導入シナリオに固有の Cisco 適応型セキュリティ アプライアンス のアクセス リストも更新する必要があります。

（注） IM and Presence サービス のパブリック IP アドレスは、Cisco 適応型セキュリティ アプライアンス で設定され、DNS レコードに表示される IM and Presence サービスドメインのパブリック IPアドレスを指します。このレコードは、Cisco適応型セキュリティアプライアンスのパブリック IP を含むロードバランサの FQDN を示します。

**手順**

展開シナリオ：1 つ以上の外部ドメインとフェデレーションする IM and Presence Service ノード

| タスク | 設定例 |
|---|---|
| 新しいロードバランサの仮想 IP アドレスの新しいアクセス リストを追加します。IM and Presence Service がアクセスする必要がある外部ドメインごとにアクセス リストを追加する必要があります。 | Publisher：<br>Cisco 適応型セキュリティ アプライアンス リリース 8.2<br>**access-list** *ent_lber_to_external_ocs* **extended permi** **host** *external_domain_public_ip_address* **eq 5061** |

| タスク | 設定例 |
|---|---|
| ロードバランサの仮想 IP アドレスが設定されている場合に IM and Presence Service ノードへのメッセージを開始するには、外部ドメインの新しいアクセス リストを追加します。IM and Presence Serviceにアクセスする必要がある外部ドメインごとにアクセス リストを追加する必要があります。 | Publisher：<br>Cisco 適応型セキュリティ アプライアンス リリース<br>**access-list** *ent_lcs_to_lber_routgimp* **extended pe**<br>*external_domain_public_ip_address* **host** *imp_publi*<br>Cisco 適応型セキュリティ アプライアンス リリース<br>**access-list** *ent_external_server_to_lb* **extended p**<br>*external_public_address* **host** *loadbalancer_virtua* |
| アクセス リストごとに、新しいクラスを追加して新しいアクセス リストを組み込みます。 | **class** *ent_lber_to_external_ocs* **match access-list** |
| クラスごとに、 IM and Presence Serviceによって開始されたメッセージのポリシーマップ global_policy にエントリを作成します。 | **policy-map global_policy class** *ent_lber_to_exter*<br>**tls-proxy** *ent_imp_to_external* |
| クラスごとに、外部ドメインで開始されたメッセージのポリシーマップ global_policy にエントリを作成します。 | **policy-map global_policy class** *ent_lcs_to_lber_r*<br>**tls-proxy** *ent_external_to_imp* |

展開シナリオ：外部ドメインが 1 つ以上のクラスタ間 IM and Presence Service ノードを追加した IM and Presence Service から IM and Presence Service へのフェデレーション

| タスク | 設定例 |
|---|---|
| 外部ドメインの 適応型セキュリティ アプライアンス は、ローカル ドメインのパブリッシャおよびサブスクライバ用に選択された任意のポートへのアクセスを許可する必要があります。 | **access-list** *ent_imp_to_externalPubimpwlber* **exten**<br>*external_domain_private_imp_address* **host** *public_*<br>**access-list** *ent_imp_to_externalSubimpwlber* **exten**<br>*external_domain_private_imp_address* **host** *public_* |
| アクセス リストごとに、新しいクラスを追加して新しいアクセス リストを組み込みます。 | -- |
| クラスごとに、ポリシーマップ global_policy にエントリを作成します。 | -- |

**関連情報 -**

アクセス リストの構成要件

# TLS プロキシ インスタンスの更新

Cisco 適応型セキュリティ アプライアンスの TLS プロキシ インスタンスを更新します。

**手順**

変化：

```
tls-proxy ent_external_to_imp server trust-point msoft_public_fqdn
client trust-point imp_proxy
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
tls-proxy ent_imp_to_external
server trust-point imp_proxy
client trust-point msoft_public_fqdn
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
:
tls-proxy ent_external_to_imp server trust-point msoft_public_fqdn
client trust-point msoft_public_fqdn
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
tls-proxy ent_imp_to_external
server trust-point msoft_public_fqdn
client trust-point msoft_public_fqdn
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
```

**関連トピック**

TLS プロキシ インスタンスの構成 （96 ページ）

# CA 署名付きセキュリティ証明書の更新

ロード バランサを構成に追加する場合は、次のセクションで説明するように、ロード バランサ、Cisco 適応型セキュリティ アプライアンス、および IM and Presence Service ノード間で CA 署名付きセキュリティ証明書を生成する必要もあります。

## ロード バランサと Cisco 適応型セキュリティ アプライアンス間のセキュリティ証明書の構成

このトピックでは、ロードバランサと Cisco 適応型セキュリティ アプライアンスの間でセキュリティ証明書を構成するために必要な手順の概要を示します。

| タスク | 手順 |
|---|---|
| Cisco 適応型セキュリティアプライアンスでロード バランサの CA 署名付き証明書を生成します。 | **crypto ca Enroll** コマンドを使用して、ロード バします。 |
| Cisco 適応型セキュリティ アプライアンス からロード バランサに CA 署名付き証明書をインポートします。 | ロード バランサのマニュアルを参照してくださ |

| タスク | 手順 |
| --- | --- |
| ロードバランサでCisco適応型セキュリティ アプライアンス の CA 署名付き証明書を生成します。 | ロード バランサのマニュアルを参照してくだ |
| CA 署名付き証明書をロード バランサから Cisco 適応型セキュリティ アプライアンスにインポートします。 | `crypto ca trustpoint` コマンドを使用します。<br>証明書がインストールされていることを確認す `certificate` コマンドを使用します。 |

**関連情報 -**

SCEP を使用した Cisco 適応型セキュリティ アプライアンスでの証明書の構成

Cisco 適応型セキュリティ アプライアンスへの IM and Presence サービス証明書のインポート

Microsoft CA を使用した Cisco 適応型セキュリティアプライアンスと Microsoft Access Edge（外部インターフェイス）間のセキュリティ証明書の交換

# ロード バランサと IM and Presence Service ノード間のセキュリティ証明書の構成

このトピックでは、ロード バランサと IM and Presence Service ノード間のセキュリティ証明書を設定するために必要な手順の概要を示します。

| タスク | 手順 |
| --- | --- |
| パブリッシャ ノードとサブスクライバ ノードの両方で CA 署名付き証明書を生成します。 | 手順に従って、CA 署名付き証明書を使用して証明書を |
| CA 署名付き証明書を（パブリッシャ ノードとサブスクライバ ノードから）ロード バランサにインポートします。 | ロード バランサのマニュアルを参照してください。 |

# Microsoft コンポーネントの更新

ロード バランサの詳細を使用して、一部の Microsoft コンポーネントを更新する必要があります。

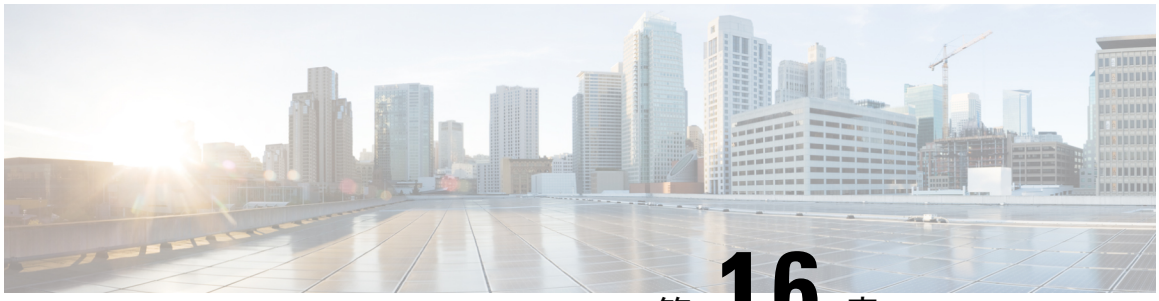
**手順**

| タスク | 手順 |
| --- | --- |
| ロード バランサの FQDN に対応するように FQDN のすべてのインスタンスを更新します。 | |

| タスク | 手順 |
| --- | --- |
| ロード バランサを使用して、IM プロバイダ リストのドメイン名を更新します。 | 1. 外部 Access Edge サーバーで、**[開始（Start）] > [管理（Administrative Tools）] > [コンピュータ管理（Comp Management）]** を選択します。<br>2. 左側のペインで、**[Microsoft Office Communications Ser** 右クリックします。<br>3. **[IM プロバイダ（IM Provider）]** タブをクリックしま<br>4. [Add] をクリックします。<br>5. **[IM サービス プロバイダを許可する（Allow the IM ser provider）]** チェックボックスをオンにします。<br><br>IM サービス プロバイダのネットワーク アドレスをロード パブリック FQDN として定義します。 |

関連トピック

SIP フェデレーションの外部サーバー コンポーネントの構成 （147 ページ）



第 16 章

# XMPP フェデレーションの IM および Presence サービス構成

このセクションでは、XMPP フェデレーションの IM and Presence サービスの設定について説明します。

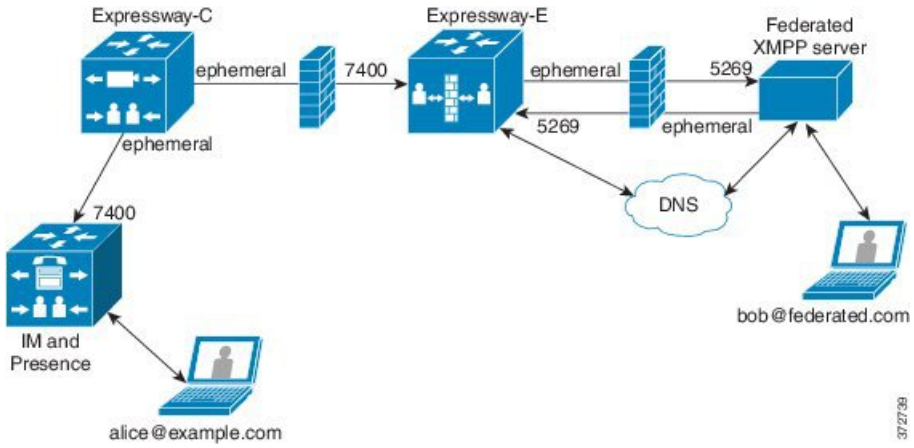


## External XMPP Federation through Cisco Expressway

The preferred method for deploying external XMPP federation is through Cisco Expressway. Cisco Expressway enables users registered to IM and Presence Service to communicate via the Expressway-E with users from a different XMPP deployment. The following diagram shows how XMPP messages are routed from an on-premises IM and Presence Service server via the Expressway-C and Expressway-E Collaboration Edge solution to the federated XMPP server. It also shows the ports and connections that are used as the messages traverse DMZ firewalls.

**Note** The Expressway-C and Expressway-E combination is shown here, however the same external XMPP federation functionality is also available when using a VCS Control and VCS Expressway combination. Refer to Cisco Expressway Administrator Guide (X8.2) for more information about the Expressway series option or Cisco TelePresence Video Communication Server Administrator Guide (X8.2) for more information about the VCS option.

*Figure 26: External XMPP Federation through Cisco Expressway*




**Note** SIP and XMPP federations are separate and do not impact each other. For example, it is possible to deploy SIP federation on IM and Presence Service and external XMPP federation on Cisco Expressway.

### Supported Federations

Expressway-E supports XMPP federation with the following enterprises:

- Cisco Unified Communications Manager IM and Presence Service Release 9.1 or later
- Cisco WebEx Connect Release 6.x
- XMPP standards-compliant servers

### Supported Deployment Configurations

The following XMPP federation deployment options are available:

- external XMPP federation only (terminated on Cisco Expressway)
- internal XMPP federation only (terminated on IM and Presence Service)
- internal and external XMPP federation (terminated on IM and Presence Service) but requires you to configure your firewall to allow inbound connections.

For more information about external XMPP federation through Cisco Expressway, see Cisco Expressway Administrator Guide (X8.2)

### Restrictions

- Simultaneous internal XMPP federation terminated on IM and Presence Service and external XMPP federation terminated on Cisco Expressway is not supported.

**Important** If you deploy external XMPP federation through Cisco Expressway, do not activate the Cisco XCP XMPP Federation Connection Manager feature service on IM and Presence Service.

- Expressway-E does not support XMPP address translation (of email addresses, for example). If you are using Expressway-E for XMPP federation, you must use native presence Jabber IDs from IM and Presence Service.

# XMPP フェデレーションの全般設定の構成

このセクションでは、XMPP フェデレーションの一般設定を行う方法について説明します。

## XMPP フェデレーションの概要

IM and Presence Service では、以下の企業の XMPP フェデレーションをサポートします。

- Cisco Webex Messenger リリース 7.x
- IBM Sametime リリース 8.2 および 8.5
- IM and Presence リリース 9.x 以降

IM and Presence Service が Webex Enterprise とフェデレートしている場合、Webex Connect クライアント ユーザーは、 IM and Presence Service ユーザーを一時的または永続的なチャットルームに招待することはできません。これは、WebEx Connect クライアントの設計上の制約によるものです。

IM and Presence Service が XMPP を介してフェデレーションできるようにするには、この章で説明する手順に従って、 IM and Presence Serviceで XMPP フェデレーションを有効にして構成する必要があります。

複数の IM and Presence Service クラスタがある場合は、クラスタごとに少なくとも 1 つのノードでXMPPフェデレーションを有効にして構成する必要があります。XMPPフェデレーション構成は、クラスタ間で同一である必要があります。**診断トラブルシューター**は、クラスタ間でXMPPフェデレーション構成を比較し、XMPPフェデレーション構成がクラスタ間で同一でない場合に報告します。

ファイアウォールの目的でCisco適応型セキュリティアプライアンスを展開する場合は、次の点に注意してください。

- ルーティング、スケール、パブリック IP アドレス、および CA 権限に関する考慮事項については、統合の準備に関連するトピックを参照してください。
- ホスト名、タイムゾーン、クロックなどの前提条件情報の構成については、Cisco 適応型セキュリティ アプライアンス を構成するタスクを参照してください。

# XMPP フェデレーションのサービスの再起動に関する重要事項

XMPP フェデレーションの設定を変更した場合は、Cisco XCP ルータと Cisco XCP XMPP Federation Connection Manager を再起動する必要があります。サービスを再起動するには、 **IM and Presence Serviceability** ユーザー インターフェイスにログインします。

- Cisco XCP ルータで、**[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 XMPP Federation Connection Manager で、[ツール（ **Tools**） > **] [コントロール センター（Control Center - Feature Services）]**を選択します。

。

Cisco XCP ルータ サービスを再起動すると、IM and Presence Service によりすべての XCP サービスが再起動されます。

ノードでXMPPフェデレーションを有効または無効にする場合は、XMPPフェデレーションが有効または無効になっているノードだけでなく、クラスタ内のすべてのノードで Cisco XCP ルータを再起動する必要があります。他のすべてのXMPPフェデレーション設定の場合、Cisco XCP ルータの再起動は、設定を変更するノードでのみ必要です。

# ノードでの XMPP フェデレーションの有効化

デフォルトでこの設定は無効です。

**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）] > [XMPPフェデレーション（XMPP Federation）] > [設定（Settings）]** を選択します。

[XMPP フェデレーション ノード ステータス（XMPP Federation Node Status）] ドロップダウン リストで、**[オン（On）]** を選択します。

**ステップ 2** [保存（Save）] をクリックします。

**トラブルシューティング項目**

ノードで XMPP フェデレーションをオンにしない限り、 IM and Presence Service ノードで XCP XMPP Federation Connection Manager サービスを開始できません。

**次の作業**：

XMPP フェデレーションのセキュリティ設定の構成

# XMPP フェデレーションのセキュリティ設定の構成

### 始める前に

- フェデレーションしている外部ドメインが TLS 接続をサポートしているかどうかを確認します。
- TLS および SASL 固有の設定は、SSL モードの 「[TLS オプション（ TLS Optional ）]」 または 「[TLS 必須（ TLS Required）」] を選択した場合にのみ構成できます。
- TLS を使用して IM and Presence Service と IBM 間のフェデレーションを構成する場合は、SSL モード 「TLS Required」を構成し、SASL を有効にする必要があります。

**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）] > [XMPPフェデレーション（XMPP Federation）] > [設定（Settings）]** を選択します。

**ステップ 2** ドロップダウン リストからセキュリティ モードを選択します。

a) [TLS なし（No TLS）] : IM and Presence Service は外部ドメインとの TLS 接続を確立しません。システムは、暗号化されていない接続を使用して外部 DOMIM and Presence Service ain とフェデレーションし、サーバー ダイヤルバック メカニズムを使用して他のサーバーの ID を確認します。

b) TLS オプション：外部ドメインとの TLS 接続の確立を試行します。 IM and Presence Service が TLS 接続の確立に失敗した場合、サーバー ダイヤルバックに戻り、他のサーバーの ID を確認します。

c) [必須の TLS（TLS Required）] : システムは、外部ドメインとのセキュアな（暗号化された）接続を保証します。

**ステップ 3** インストールされたルート CA 証明書に対して外部ドメイン サーバからの証明書を厳密に検証する場合は、**[クライアント側のセキュリティ証明書が必要（Require client-side security certificates）]** チェックボックスをオンにします。[TLS オプション（TLS Optional）] または [TLS 必須（TLS Required）] セキュリティ設定を選択した場合、この設定はデフォルトでオンになります。

（注） Webex で XMPP フェデレーションを構成する場合は、**[クライアント側のセキュリティ証明書を要求する（Require client-side security certificates）]** チェックボックスをオンにしないでください。

**ステップ 4** **[すべての着信接続で SASL EXTERNAL を有効にする（Enable SASL EXTERNAL on all incoming connections）]** チェックボックスをオンにして、 IM and Presence Service が着信接続試行で SASL EXTERNAL のサポートをアドバタイズし、SASL EXTERNAL 検証を実装するようにします。

**ステップ 5** **[発信接続で SASL を有効にする（Enabling SASL on outbound connections）]** チェックボックスをオンにして、外部サーバーが SASL EXTERNAL を要求した場合に IM and Presence Service が外部ドメインに SASL 認証 ID を送信するようにします。

**ステップ 6** IM and Presence Serviceに接続しようとしている外部サーバーの ID を確認するために DNS を使用する場合は、ダイヤルバック シークレットを入力します。 IM and Presence Service は、DNS が外部サーバの ID を検証するまで、外部サーバーからのパケットを受け入れません。

**ステップ 7** [保存（Save）] をクリックします。

ヒント
- セキュリティ設定に関する詳細は、オンライン ヘルプを参照してください。
- ノードがクラスタ間展開の一部である場合は、各クラスタに同じセキュリティ設定を構成する必要があります。システム トラブルシュータを実行して、構成がすべてのノードで一貫していることを確認します。

### 関連情報

ノードでの XMPP フェデレーションの有効化

# XMPP フェデレーションの DNS 構成

ここでは、XMPP フェデレーションの DNS 構成の概要について説明します。

## XMPP フェデレーションの DNS SRV レコード

IM and Presence Service が特定の XMPP フェデレーテッド ドメインを検出できるようにするには、フェデレーテッド エンタープライズがパブリック DNS サーバーで _xmpp-server DNS SRV レコードを発行する必要があります。同様に、IM and Presence Service は、そのドメインの DNS で同じ DNS SRV レコードを発行する必要があります。両方のエンタープライズがポート 5269 を発行する必要がある。発行された FQDN は、DNS の IP アドレスに解決できる必要もあります。

IM and Presence Service 展開内のドメインごとに、DNS SRV レコードを発行する必要があります。**Cisco Unified Communications Manager IM and Presence Administration** ユーザー インターフェイスを使用して、すべてのドメインのリストを表示できます。**[プレゼンス ドメイン（Presence Domains）]** ウィンドウに移動して、システム内のすべてのドメインのリストを表示します。**[Cisco Unified CM IM and Presence Administration]** にログインし、**[プレゼンス（Presence）] > [ドメイン（Domains）]** を選択します。

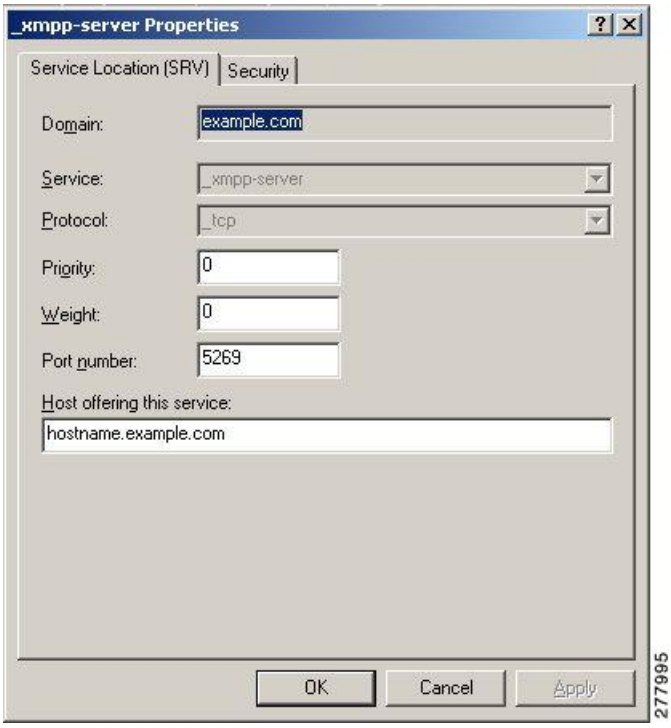
フェデレーション機能の電子メール アドレスが有効になっている場合は、**[フェデレーションの電子メール ドメイン（Email Domains for Federation）]** ウィンドウを使用して、システム内のすべての電子メール ドメインのリストを表示することもできます。**Cisco Unified CM IM and Presence Administration** のユーザー インターフェイスにログインします。**[プレゼンス（Presence）] > [ドメイン間フェデレーション（Inter-Domain Federation）] > [電子メール フェデレーテッド ドメイン（Email Federated Domains）]** を選択します。

必要な DNS レコードは次のとおりです。

_xmpp-server._tcp.*domain*

次の図に、ドメイン **example.com**の _xmpp-server DNS SRV レコードの DNS 設定の例を示します。

図 *27 : _xmpp-server* の *DNS SRV*




クラスタ内のサーバーごとに 2 つの DNS レコードが必要です。1 つは IPv4 用の DNS レコード、もう 1 つは IPv6 用の DNS レコードです。**[このサービスを提供するホスト（Host Offering this service）]** フィールドの ホスト名（*hostname*） の値を使用して、レコードが IPv4 または IPv6 バージョンであるかどうかを示します。例 :

- **hostname-v4.example.com** は、DNS レコードが IPv4 バージョンであることを示します。
- **hostname-v6.example.com** は、DNS レコードが IPv6 バージョンであることを示します。

IM and Presence Service へのリモート ルート アクセスがある場合は、 **nslookup** を実行して、フェデレーテッド ドメインが検出可能かどうかを確認できます。

ヒント DNS SRV ルックアップを実行するには、次の一連のコマンドを使用します。

**nslookup**

**set type=srv**

**_xmpp-server._tcp.***domain*

（*domain* はフェデレーテッド エンタープライズのドメインです。）

このコマンドにより、次の例のような出力が返されます。ここで、「example.com」はフェデレーテッド サーバーのドメインです。

```
_xmpp-server._tcp.example.com service = 0 0 5269 hostname.example.com
```

単一クラスタの場合、クラスタ内の1つのノードでXMPPフェデレーションのみを有効にする必要があります。パブリック DNS で企業の 1 つの DNS SRV レコードを発行します。IM and Presence Service は、外部ドメインからのすべての着信要求を、フェデレーションを実行しているノードにルーティングします。内部的には、IM and Presence Service が要求をユーザの正しいノードに再ルーティングします。また、 IM and Presence Service は、XMPP フェデレーションを実行しているノードにすべての発信要求をルーティングします。

また、複数の DNS SRV レコードを発行することもできます（スケール目的など）。または、複数の IM and Presence Service クラスタがあり、クラスタごとに少なくとも 1 回は XMPP フェデレーションを有効にする必要があります。SIP フェデレーションとは異なり、XMPP フェデレーションでは、 IM and Presence Service エンタープライズ ドメインの単一のエントリ ポイントは必要ありません。その結果、 IM and Presence Service は、XMPP フェデレーションを有効にしたクラスタ内で発行されたノードのいずれかに着信要求をルーティングできます。

クラスタ間およびマルチノード クラスタ IM and Presence Service 展開では、外部 XMPP フェデレーテッド ドメインが新しいセッションを開始すると、DNS SRV ルックアップを実行して要求のルーティング先を決定します。ドメインごとに複数の DNS SRV レコードを発行すると、DNS ルックアップは複数の結果を返します。 IM and Presence Service は、DNS が発行する任意のサーバに要求をルーティングできます。内部的には、 IM and Presence Service が要求をユーザの正しいノードに再ルーティングします。IM and Presence Service は、XMPP フェデレーションを実行しているノードのいずれかに発信要求をルーティングします。

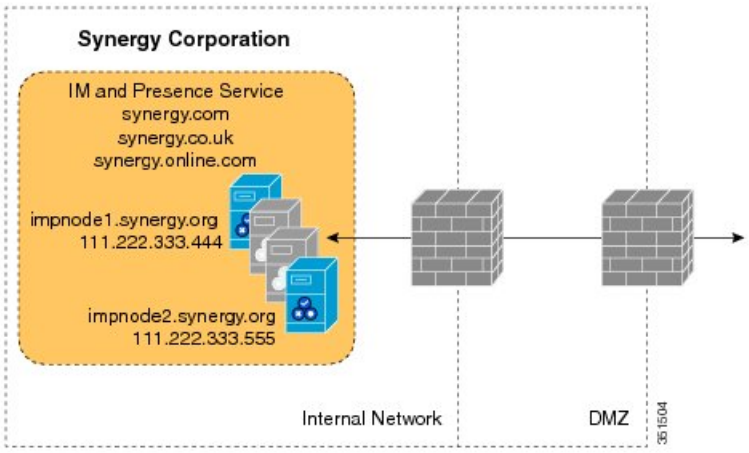
XMPP フェデレーションを実行している複数のノードがある場合でも、パブリック DNS で 1 つのノードのみを発行することを選択できます。この設定では、 IM and Presence Service は、XMPP フェデレーションを実行しているノード間で着信要求をロードバランシングするのではなく、すべての着信要求を単一のノードにルーティングします。IM and Presence Service は発信要求をロードバランシングし、XMPP フェデレーションを実行しているノードのいずれかから発信要求を送信します。

（注） 発行する DNS SRV レコードとともに、対応する DNS A および AAAA レコードも追加する必要があります。

### ドメイン間フェデレーション展開での XMPP DNS SRV

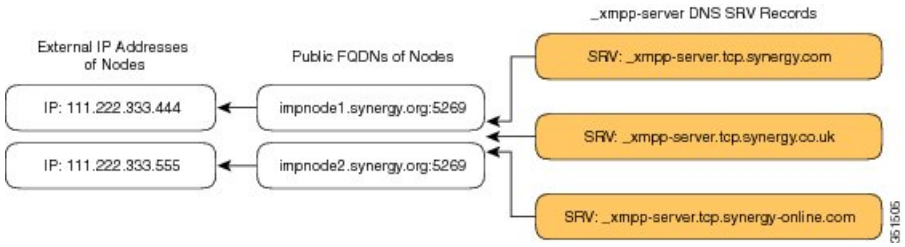
次のドメイン間フェデレーション展開の例では、2 つの IM and Presence Service ノードで XMPP フェデレーションが有効になっています。IM and Presence Service 展開でホストされているドメインごとに、DNS SRV レコードを発行する必要があります。次の図は、3 つのローカルドメインを使用したドメイン間フェデレーション展開の例を示しています。ドメインごとに_xmpp-server DNS SRV レコードを発行する必要があります。

図 *28 : XMPP* ベースのフェデレーテッド ドメイン間展開での複数のドメイン




各 DNS SRV レコードは、XMPP フェデレーテッド トラフィック用に指定された IM and Presence Service ノードの両方のパブリック FQDN に解決する必要があり、FQDN は IM and Presence Service ノードの外部 IP アドレスに解決する必要があります。

図 *29 : IM and Presence* サービス ノードのパブリック *FQDN* への *XMPP DNS SRV* の解決




（注） DMZ 内に展開されたファイアウォールは、IP アドレス（NAT）をノードの内部 IP アドレスに変換できます。ノードの FQDN は、パブリック IP アドレスにパブリックに解決可能である必要があります。

**関連情報 -**

XMPP フェデレーションのチャット機能の DNS SRV レコード

# XMPP フェデレーションのチャット機能の DNS SRV レコード

XMPP フェデレーション展開の IM and Presence Service ノードでチャット機能を構成する場合は、DNS でチャット ノード エイリアスを公開する必要があります。

チャットノードの DNS SRV レコードが解決するホスト名は、パブリック IP アドレスに解決されます。展開に応じて、ネットワーク内のチャットノードごとに単一のパブリック IP アドレスまたはパブリック IP アドレスを使用できます。

表 *20 :* チャット リクエスト ルーティング

| デプロイ | チャット リクエスト ルーティング |
|---|---|
| 単一のパブリック IP アドレス、内部に複数のノード | すべてのチャット要求を XMPP フェデレーション ノードにルーティングしてからチャット ノードにルーティングするには、次の手順を実行します。<br>1. チャット ノード エイリアスの DNS SRV がポート 5269 を指すように構成定します。<br>2. publicIPAddress:5269 を XMPPFederationNodePrivateIPAddress:5269 にマッピングする Cisco 適応型セキュリティ アプライアンス または firewall\NAT サーバで構成された NAT コマンドを構成します。 |
| 複数のパブリック IP アドレス、内部に複数のノード | 複数のパブリック IP アドレスがある場合は、チャット要求を適切なチャットノードに直接ルーティングすることを選択できます。<br>1. 5269 以外の任意のポート（25269 など）を使用するようにチャット ノードの DNS SRV を構成します。<br>2. Cisco 適応型セキュリティ アプライアンス または firewall\NAT サーバで、textChatServerPublicIPAddress:25269 を textChatServerPrivateIPAddress:5269 にマッピングする NAT コマンドを構成します。<br>（注） チャット ノードが着信フェデレーション テキスト要求を処理できるようにするには、チャット ノードで Cisco XCP XMPP Federation Connection Manager をオンにする必要があります。 |

IM and Presence Service のチャット機能構成に関する詳細は、『*Cisco Unified Communications Maanger*』記載の「*IM and Presence Service*」の構成および管理を参照してください。

**関連情報 -**

XMPP フェデレーションのチャット機能の DNS SRV レコード

# XMPP フェデレーションのチャット ノードの DNS SRV レコードの構成

**ステップ 1** チャット ノードのエイリアスを取得するには、次の手順を実行します。

a) **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。**[メッセージング（Messaging）] > [グループ チャット サーバ エイリアスのマッピング（Group Chat Server Alias Mapping）]** を選択します。

b) **[検索（Find）]** をクリックして、チャット ノード エイリアスのリストを表示します。

c) DNS で公開するチャット ノード エイリアスを選択します（例：`conference-2.StandAloneCluster.example.com`）

**ステップ 2** `example.com` ドメインのパブリック DNS サーバで、StandAloneCluster ドメインを作成します。

**ステップ 3** StandAloneClusterdomain で、conference-2 ドメインを作成します。

**ステップ 4** Conference-2 ドメインで、_tcp ドメインを作成します。

**ステップ 5** _tcp ドメインで、_xmpp-server 用に 2 つの新しい DNS SRV レコードを作成します。1 つは IPv4 用、もう 1 つは IPv6 用です。DNS 構成レコードの例については、次の図を参照してください。

（注） テキスト会議サーバのエイリアスが `Conference-2-StandAloneCluster.example.com` の場合、手順 2 のドメインは Conference-2-StandAloneCluster であるため、手順 3 をスキップします。手順 4 で、conference-2-StandAloneCluster の下に _tcp ドメインを作成します。

**図 *30 : チャット機能の _xmpp-server の IPv4 DNS SRV レコード***

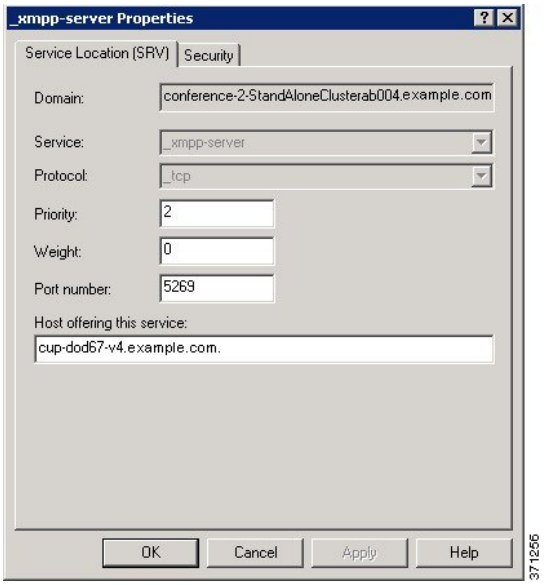


図 *31* : チャット機能の *_xmpp-server* の *IPv6 DNS SRV* レコード

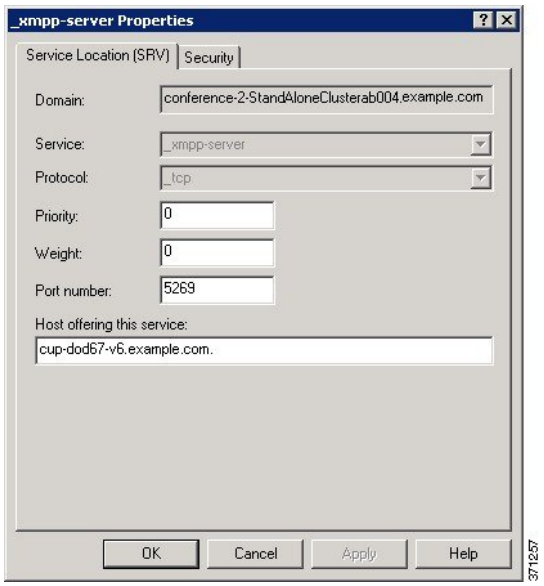
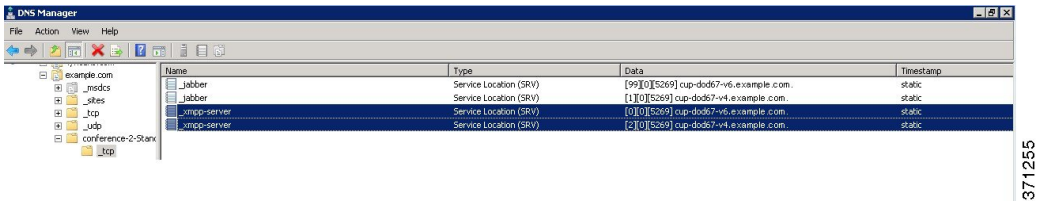



図 *32* : チャット機能の *DNS* 構成




# Configure MFT on XMPP Federation Without TLS

In this scenario, you must perform the following two extra steps for the MFT over XMPP Federation feature to work:

1. Extract file transfer aliases.
2. Create the DNS SRV records for file transfer aliases extracted in the previous step.

### Before you begin

- Configure DNS SRV records for XMPP Federation. For more information, see XMPP フェデレーションの DNS SRV レコード, on page 166.
- Configure the Managed File Tranfer (MFT) feature as described in the Configuration and Administration of the IM and Presence Service guide for your release of Unified CM.

ステップ 1 To extract the file transfer aliases:

a) On each IM and Presence Service node where MFT is configured, create a CLI session and run **file build log cisco_xcp_config_mgr**.
b) Download the newly created archive and open `cm-5.xml` file.
c) The file transfer alias is stored with other MFT parameters in a common section of the file. In this example, you can find the file transfer alias in the following line:

```
<host-filter xmlns="http://www.jabber.com/config/cm/aft">
filetransfer-4-StandAloneClusterd41e3.cow.com
</host-filter>
```

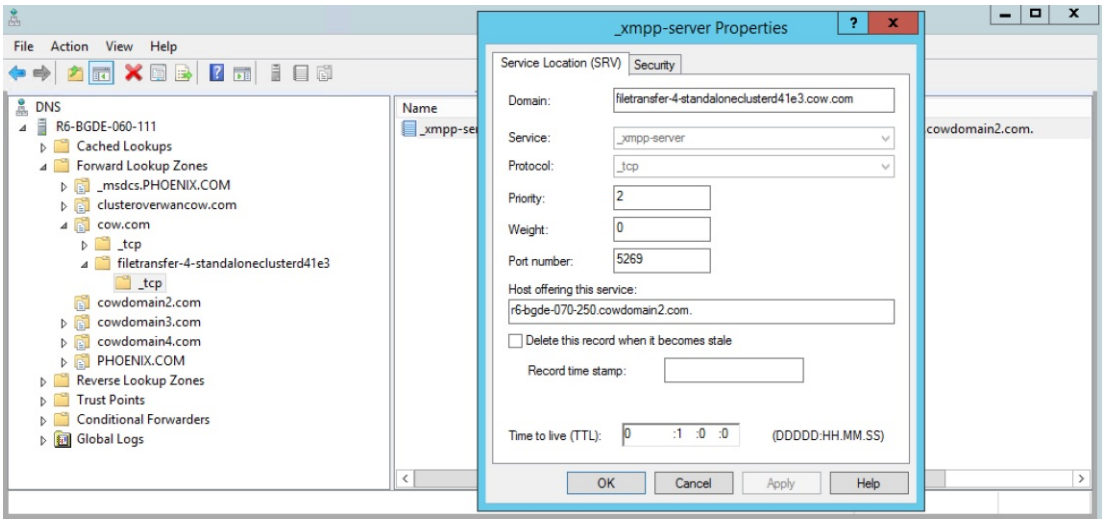
**Important** You must extract the file transfer aliases from each IM and Presence Service node which has MFT configured individually. Each node has its own unique alias that needs to be added to the DNS servers.

**ステップ 2** Add aliases to the DNS server.

The file transfer alias extracted in the previous step belongs to the IM and Presence Service Publisher node (**r6-bgde-070-250.cowdomain2.com**) on the local side. We will use this alias as an example of how DNS records should be added.

The domains need to be added to DNS servers in the same way as the chat node aliases as described in XMPP フェデレーションのチャット ノードの DNS SRV レコードの構成, on page 170.

In the following screenshot, you can view the DNS SRV record for the file transfer alias.




# Configure MFT on XMPP Federation with TLS

In this scenario, you must perform another step after extracting file transfer aliases and adding DNS SRV records as described in Configure MFT on XMPP Federation Without TLS, on page 172.

Perform the following steps on the local side:

### Before you begin

**Note**

- We recommend that you use this method to configure MFT on XMPP Federation.
- To manually add file transfer aliases to the certificate, you must generate a CSR for the Multi SAN certificate. This is not possible in single node deployments. This is a limitation of this method.
- Use the following settings on the XMPP federation page on both sides:
  - **Security mode** must be set to TLS required.
  - The **Require client-side security certificates** checkbox must be checked.

For MFT on XMPP TLS federation to work, the cup -xmpp-s2s certificate must contain file transfer aliases. On IM and Presence Service, these file transfer aliases are not added automatically to the Certificate Signing Request (CSR). This default behavior can be overcome on a multinode IM and Presence Service cluster by generating and signing a Multi SAN certificate. However, on a single node cluster, it is impossible to generate a Multi SAN certificate CSR.

- Configure DNS SRV records for XMPP Federation. For more information, see XMPP フェデレーションの DNS SRV レコード, on page 166.
- Configure the Managed File Transfer (MFT) feature as described in the Configuration and Administration of the IM and Presence Service guide for your release of Unified CM.

ステップ 1 After extracting the file transfer aliases from all the nodes of the local cluster, generate a CSR for the MultiSan certificate.

ステップ 2 Log in to the **Cisco Unified IM and Presence OS Administration** page and choose **Security** > **Certificate Management**.

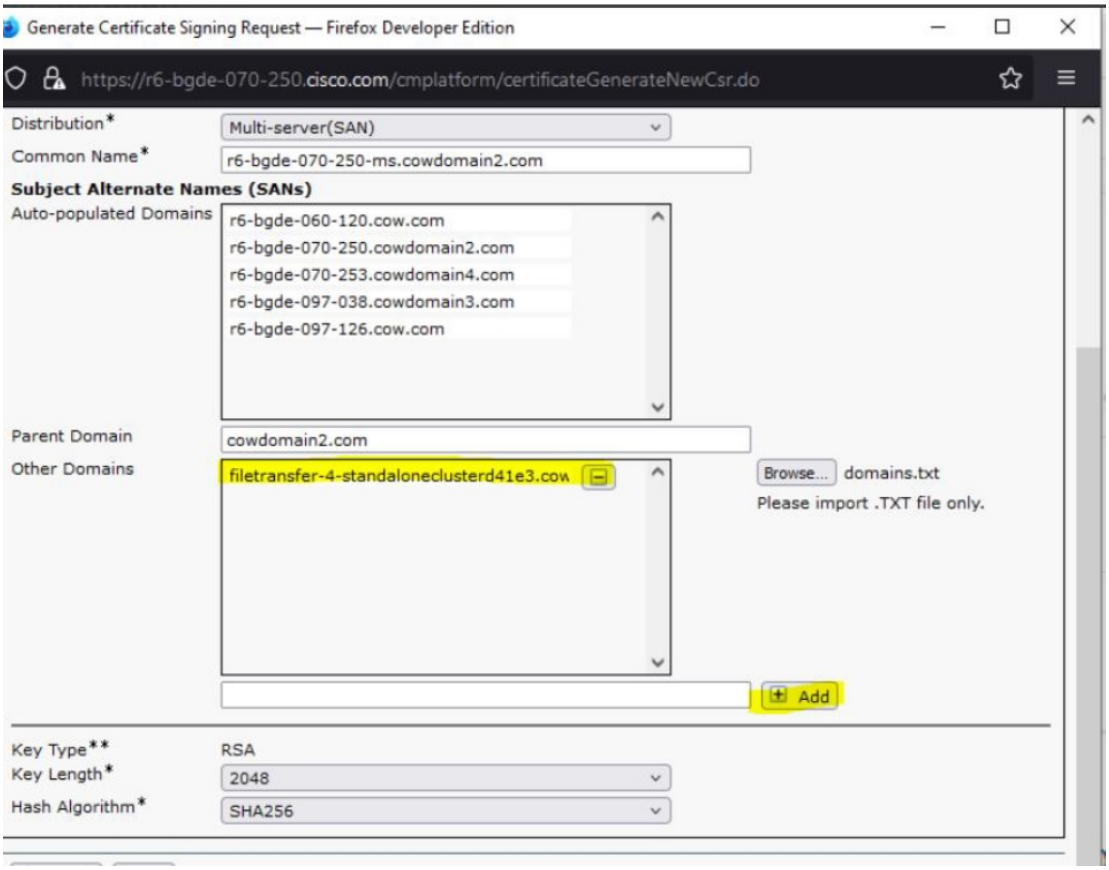
The **Certificate List** window appears.

ステップ 3 Click **Generate CSR**.

ステップ 4 From the **Certificate Purpose** drop-down list, choose **cup-xmpp-s2s**.

ステップ 5 From the **Distribution** drop-down list, choose **Multi-server(SAN)**.

ステップ 6 In the **Other Domains** section, add all file transfer aliases from the local cluster as shown in the following screenshot.




**ステップ 7** Sign the cup-xmpp-s2s certificate using Certificate Authority.

**ステップ 8** Upload the Root certificate and the newly signed Multi-SAN certificate according to the steps described in Upload a CA-Signed Certificate for XMPP Federation, on page 185.

**ステップ 9** Upload the Root certificate in the cup-xmpp-trust on the federated side.

**Note** Repeat all the above steps on the federated side.

# XMPP フェデレーションのポリシー構成の構成

このセクションでは、XMPP フェデレーションのさまざまなポリシー設定構成について説明します。

## ポリシー例外の構成

XMPP フェデレーションのデフォルトポリシーに対する例外を構成できます。例外では、例外を適用する外部ドメインと、例外の方向ルールを指定する必要があります。ポリシー例外のドメイン名を構成する場合は、次の点に注意してください。

- ユーザーの URI または JID が `user@example.com`の場合は、例外の外部ドメイン名を `example.com`として構成します。
- 外部企業がユーザーの URI または JID で hostname.domain を使用する場合（`user@hostname.example.com` など）、例外で外部ドメイン名を `hostname.example.com`として構成します。
- 例外の外部ドメイン名にワイルドカード（*）を使用できます。たとえば、値 `*.example.com`は、 `example.com`および example.com のサブドメイン（たとえば、どこか.example.com ）にポリシーを適用します。

また、 IM and Presence Service がポリシー例外を適用する方向も指定する必要があります。次の方向オプションを使用できます。

- **上記のドメイン/ホストとの間で送受信されるすべてのフェデレーション パケット** ： IM and Presence Service は、指定されたドメインで送受信されるすべてのトラフィックを許可または拒否します。
- **上記のドメイン/ホストからの着信フェデレーション パケットのみ**：IM and Presence Service は指定されたドメインからのインバウンド ブロードキャストを受信できますが、 IM and Presence Service は応答を送信しません。
- **[上記のドメイン/ホストへの発信フェデレーション パケットのみ（Onlyouting federated packets to the above domain/host ）]**： IM and Presence Service が指定されたドメインにアウトバウンド ブロードキャストを送信することを許可しますが、 IM and Presence Service は応答を受信しません。

**関連情報 -**

XMPP フェデレーションのポリシーの構成

# XMPP フェデレーションのポリシーの構成

⚠

**注意** XMPP フェデレーション設定のいずれかに変更を加えた場合は、 **Cisco Unified IM and Presence Serviceability** のユーザー インターフェイスで、Cisco XCP ルータ（**[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）、Cisco XCP XMPP フェデレーション接続マネージャ（**[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]**）のサービスを再起動する必要があります。Cisco XCP ルータ サービスを再起動すると、IM and Presence Service によりすべての XCP サービスが再起動されます。

**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）] > [XMPPフェデレーション（XMPP Federation）] > [ポリシー（Policy）]** を選択します。

**ステップ 2** ドロップダウン リストからポリシー設定を選択します。

- [許可（Allow）]： IM and Presence Service は、ポリシー例外リストで明示的に拒否したドメインを除き、XMPP フェデレーション ドメインからのすべてのフェデレーション トラフィックを許可します。
- [拒否（Deny）]： IM and Presence Service は、ポリシー例外リストで明示的に許可したドメインを除き、XMPP フェデレーテッド ドメインからのすべてのフェデレーション トラフィックを拒否します。

**ステップ 3** ポリシー例外リストにドメインを構成するには、次の手順を実行します。

a) [新規追加（Add New）] をクリックします。
b) 外部サーバのドメイン名またはホスト名を指定します。
c) ポリシー例外を適用する方向を指定します。
d) ポリシー例外ウィンドウで **[保存（Save）]** をクリックします。

**ステップ 4** ポリシー ウィンドウで **[保存（Save）]** をクリックします。

**ヒント**：

フェデレーション ポリシーの推奨事項については、オンライン ヘルプを参照してください。

**関連情報 -**

ポリシー例外の構成

# XMPP フェデレーション用の Cisco 適応型セキュリティ アプライアンスの構成

XMPP フェデレーションの場合、Cisco 適応型セキュリティ アプライアンス はファイアウォールとしてのみ機能します。Cisco 適応型セキュリティ アプライアンスでは、XMPP フェデレーション トラフィックの着信と発信の両方に対してポート 5269 を開く必要があります。

これらは、Cisco 適応型セキュリティ アプライアンスリリース 8.3 でポート 5269 を開くアクセス リストの例です。

ポート 5269 で任意のアドレスから任意のアドレスへのトラフィックを許可します。

```
access-list ALLOW-ALL extended permit tcp any any eq 5269
```

任意のアドレスから任意の単一ノードへのポート 5269 でのトラフィックを許可します。

```
access-list ALLOW-ALL extended permit tcp any host private_imp_ip_address eq 5269
```

上記のアクセスリストを構成せず、DNS で追加の XMPP フェデレーションノードを公開する場合は、これらの各ノードへのアクセスを設定する必要があります。次に例を示します。

```
object network obj_host_private_imp_ip_address

#host private_imp_ip_address

object network obj_host_private_imp2_ip_address
```

**#host** *private_imp2_ip_address*

**object network** *obj_host_public_imp_ip_address*

**#host** *public_imp_ip_address*

次の NAT コマンドを構成します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **nat (inside,outside) source static** *obj_host_private_imp1_ip obj_host_public_imp_ip* **service** | |
| ステップ 2 | *obj_udp_source_eq_5269 obj_udp_source_eq_5269* | |
| ステップ 3 | **nat (inside,outside) source static** *obj_host_private_imp1_ip obj_host_public_imp_ip* **service** | |
| ステップ 4 | *obj_tcp_source_eq_5269 obj_tcp_source_eq_5269* | DNS で単一のパブリック IP アドレスを公開し、任意のポートを使用する場合は、次のように構成します。<br>（この例は、2 つの追加の XMPP フェデレーション ノード用です） |
| ステップ 5 | **nat (inside,outside) source static** *obj_host_private_imp2_ip obj_host_public_imp_ip* **service** | |
| ステップ 6 | *obj_udp_source_eq_5269 obj_udp_source_eq_25269* | |
| ステップ 7 | **nat (inside,outside) source static** *obj_host_private_imp2_ip obj_host_public_imp_ip* **service** | |
| ステップ 8 | *obj_tcp_source_eq_5269 obj_tcp_source_eq_25269* | |
| ステップ 9 | **nat (inside,outside) source static** *obj_host_private_imp3_ip obj_host_public_imp_ip* **service** | |
| ステップ 10 | *obj_udp_source_eq_5269 obj_udp_source_eq_35269* | |
| ステップ 11 | **nat (inside,outside) source static** *obj_host_private_imp3_ip obj_host_public_imp_ip* **service** | |
| ステップ 12 | *obj_tcp_source_eq_5269 obj_tcp_source_eq_35269* | DNS で複数のパブリック IP アドレスをすべてポート 5269 を使用して公開する場合は、次のように構成します。<br>（この例は、2 つの追加の XMPP フェデレーション ノード用です） |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 13 | **nat (inside,outside) source static** *obj_host_private_imp2_ip obj_host_public_imp2_ip* **service** | |
| ステップ 14 | *obj_udp_source_eq_5269 obj_udp_source_eq_5269* | |
| ステップ 15 | **nat (inside,outside) source static** *obj_host_private_imp2_ip obj_host_public_imp2_ip* **service** | |
| ステップ 16 | *obj_tcp_source_eq_5269 obj_tcp_source_eq_5269* | |
| ステップ 17 | **nat (inside,outside) source static** *obj_host_private_imp3_ip obj_host_public_imp3_ip* **service** | |
| ステップ 18 | *obj_udp_source_eq_5269 obj_udp_source_eq_5269* | |
| ステップ 19 | **nat (inside,outside) source static** *obj_host_private_imp3_ip obj_host_public_imp_ip* **service** | |
| ステップ 20 | *obj_tcp_source_eq_5269 obj_tcp_source_eq_5269* | **関連情報 -**<br>SIP フェデレーション向け Cisco 適応型セキュリティ アプライアンスのワークフロー |

# XMPP フェデレーション サービスをオンにする

XMPP フェデレーションを実行する各 IM and Presence Service ノードで Cisco XCP XMPP Federation Connection Manager サービスをオンにする必要があります。**[サービスのアクティブ化（Service Activation）]**ウィンドウから Federation Connection Manager サービスをオンにすると、 IM and Presence Service が自動的にサービスを開始します。 **[コントロール センター - 機能サービス（Control Center - Feature Services）]** ウィンドウからサービスを手動で開始する必要はありません。

### 始める前に

Cisco Unified CM IM and Presence Administration からノードの XMPP フェデレーションをオンにします。 「ノードでの XMPP フェデレーションの有効化 （164 ページ）」を参照してください。

**ステップ 1** **Cisco Unified IM and Presence Serviceability** のユーザーインターフェイスにログインします。**[Tools（ツール）]** > **[Service Activation（サービス アクティベーション）]** を選択します。

**ステップ 2** [サーバ（Server）] ドロップダウン リストからサーバを選択します。

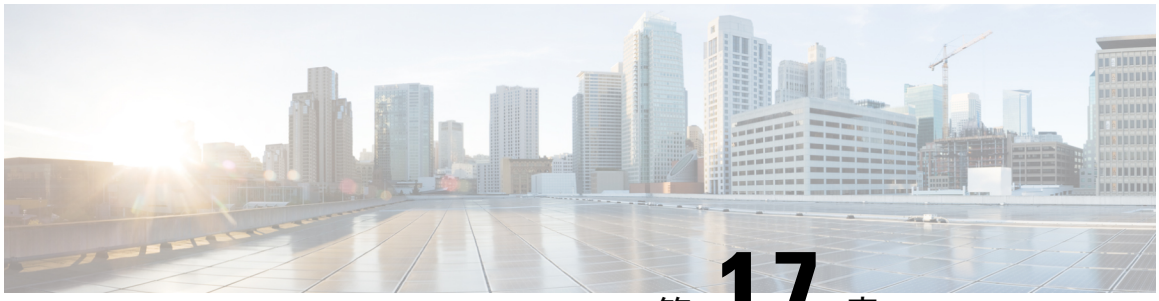
**ステップ 3** [移動（Go）] をクリックします。

**ステップ 4** [ IM and Presence Service ] エリアで、 **Cisco XCP XMPP Federation Connection Manager** サービスの横にある ボタンをクリックします。

**ステップ 5** [保存（Save）] をクリックします。

**関連情報 -**

フェデレーションの有用性の構成



第 17 章

# XMPP フェデレーションのセキュリティ証明書の構成

このセクションでは、XMPP フェデレーションのセキュリティ証明書の設定について説明します。



## XMPP フェデレーションのセキュリティ証明書の構成

XMPP フェデレーションのセキュリティを設定するには、次の手順を実行する必要があります。

1. cup-xmpp-s2s 証明書を生成する前に、すべてのローカル ドメインがシステムで作成および構成されていることを確認し、必要に応じて、欠落しているローカル ドメインを手動で作成します。
2. 次のいずれかのタイプの証明書を使用して証明書を 1 回作成します。
   - XMPP フェデレーション用の自己署名単一サーバー証明書
   - XMPP フェデレーション用の CA 署名付き単一サーバー証明書または複数サーバー証明書
3. ルート CA 証明書をインポートする

   まだ信頼していない CA を持つ新しいエンタープライズとフェデレーションするたびに、この手順を繰り返す必要があります。同様に、新しい企業が自己署名証明書を使用し、ルート CA 証明書の代わりに自己署名証明書がアップロードされる場合は、この手順に従う必要があります。

# XMPP フェデレーションのローカル ドメイン検証

すべてのローカルドメインが、生成された cup-xmpp-s2s 証明書に含まれている必要があります。cup-xmpp-s2s 証明書を生成する前に、すべてのローカル ドメインが設定され、[ドメイン（Domains）] ウィンドウに表示されていることを確認します。予定されているが、ローカル ドメインのリストにまだ表示されていないドメインを手動で追加します。たとえば、現在ユーザーが割り当てられていないドメインは、通常はドメインのリストに表示されません。

**Cisco Unified CM IM and Presence Administration** のユーザー インターフェイスにログインし、**[プレゼンス（Presence）] > [ドメイン（Domains）]** を選択します。

すべてのドメインがシステムに作成されていることを確認したら、XMPP フェデレーション用の自己署名証明書または CA 署名付き証明書を使用して cup-xmpp-s2s 証明書の作成に進むことができます。フェデレーションの電子メールアドレスが有効になっている場合は、すべての電子メールドメインも証明書に含まれている必要があります。

ローカルドメインを追加、更新、または削除し、 cup-xmpp-s2s 証明書を再生成する場合は、Cisco XCP XMPP Federation Connection Manager サービスを再起動する必要があります。このサービスを再開するには、**[Cisco Unified IM and Presence の有用性（Cisco Unified IM and Presence Serviceability）]**ユーザー インターフェイスにログインし、**[ツール（Tools）] > [コントロール センターの機能サービス（Control Center - Feature Services）]** を選択します。

**関連トピック**

電子メール ドメインの追加または更新 （194 ページ）
XMPP フェデレーションに自己署名証明書を使用する （182 ページ）
XMPP フェデレーションでの CA 署名付き証明書の使用 （183 ページ）
電子メール ドメインの表示 （193 ページ）

# マルチサーバ証明書の概要

IM and Presence Service は、tomcat、cup-xmpp および cup-xmpp-s2s の証明のための証明書に基づいて、マルチサーバ SAN をサポートします。単一サーバまたはマルチサーバの配布から選択し、適切な証明書署名要求（CSR）を生成できます。最終的な署名付きのマルチサーバ証明書と、署名を行う証明書の関連チェーンが、クラスタ内の個々のサーバのいずれかにマルチサーバ証明書をアップロードするときにクラスタ内の他のサーバに分配されます。マルチサーバ証明書の詳細については、『*Release Notes for Cisco Unified Communications Manager Release 10.5(1)*』の新機能と変更された機能に関する章を参照してください。

# XMPP フェデレーションに自己署名証明書を使用する

ここでは、XMPP フェデレーションの自己署名証明書を使用する方法を示します。CA 署名付き証明書の使用については、「XMPP フェデレーションでの CA 署名付き証明書の使用 （183 ページ）」を参照して ください。

ステップ 1 **Cisco Unified IM and Presence Operating System Administration** ユーザー インターフェイスにログインします。**[Security（セキュリティ）]** > **[Certificate Management（証明書管理）]** を選択します。

ステップ 2 **[Generate Self-signed（自己署名付きを生成）]** をクリックします。

ステップ 3 [証明書の目的（Certificate Purpose）]ドロップダウン リストで、証明書名に **cup-xmpp-s2s** を選択し、**[生成（Generate）]** をクリックします。

ステップ 4 Cisco XMPP Federation Connection Manager サービスを再起動します。**Cisco Unified IM and Presence Serviceability** のユーザ インターフェイスにログインします。**[Tools（ツール）]** > **[Control Center - Network Services（コントロール センタ - ネットワーク サービス）]** を選択して、このサービスを再起動します。

ステップ 5 証明書をダウンロードして別の企業に送信し、XMPP サーバーに信頼できる証明書として追加できるようにします。これは、 IM and Presence Service ノードまたは別の XMPP サーバーです。

### 次のタスク

XMPP フェデレーションでの CA 署名付き証明書の使用 （183 ページ）

# XMPP フェデレーションでの CA 署名付き証明書の使用

ここでは、CA 署名付き証明書の使用方法について説明します。自己署名証明書の作成の詳細については、XMPP フェデレーションに自己署名証明書を使用する （182 ページ） を参照してください。

## XMPP フェデレーションの証明書署名要求の生成

この手順では、Microsoft 証明書サービス CA の証明書署名要求（CSR）を生成する方法について説明します。

（注） この手順では、Microsoft 証明書サービス CA に署名するための CSR を生成しますが、CSR を生成する手順（手順 1 ～ 3）は、任意の認証局から証明書を要求する場合に適用されます。

### 始める前に

XMPP 証明書のドメインを構成します。

ステップ 1 **Cisco Unified IM and Presence Operating System Administration** ユーザー インターフェイスにログインします。**[Security（セキュリティ）]** > **[Certificate Management（証明書管理）]** を選択します。

ステップ 2 CSR を生成するには、次の手順を実行します。

a) [CSR の作成（Generate CSR）] をクリックします。

b) [証明書の用途（Certificate Purpose）]ドロップダウン リストで、証明書名に **cup-xmpp-s2s** を選択します。

c) ディストリビューションの場合、ローカル サーバーの FQDN を選択して単一署名証明書を生成するか、 **マルチサーバー（SAN）** を選択してマルチサーバー証明書を生成します。

（注） どちらの配信オプションでも、Cisco Unified IM and Presence Administration のユーザー インターフェイスで設定されたすべてのプレゼンス ドメイン、電子メール ドメイン、およびグループ チャット サーバー エイリアスは、生成される CSR に自動的に含まれます。[ **マルチサーバー（SAN）（Multi-server (SAN)）** ] オプションを選択すると、各 IM and Presence Service ノードのホスト名または FQDN も生成される CSR に追加されます。マルチサーバー証明書の詳細については、『*Release Notes for Cisco Unified Communications Manager Release 10.5(1)*』の新機能と変更された機能に関する章を参照してください。

d) [生成（Generate）] をクリックします。

（注） **[マルチサーバー（SAN）（Multi-server (SAN)）]** を選択した場合、CSR はクラスタ内の他のすべての IM and Presence サービス ノードのファイル システムにコピーされます。

e) **[閉じる（Close）]** をクリックし、メインの証明書ウィンドウに戻ります。

**ステップ 3** ローカル マシンに `.csr` ファイルをダウンロードします。

a) [CSR のダウンロード（Download CSR）] をクリックします。

b) [証明書の目的（Certificate Purpose）] ドロップダウン メニューから **cup-xmpp-s2s** を選択します。

c) **[CSR の ダウンロード（Download CSR）]** をクリックして、このファイルをローカル マシンにダウンロードします。

**ステップ 4** テキスト エディタを使用して、 `cup-xmpp-s2s.csr` ファイルを開きます。

**ステップ 5** ファイルの内容をコピーします。

9- BEGIN CERTIFICATE REQUESTCSR

の行から、

END CERTIFICATE REQUEST -

までの情報をすべてコピーします。

**ステップ 6** インターネット ブラウザで、CA サーバー（例： `http://<name of your Issuing CA Server>/certsrv`）を参照します。

**ステップ 7** [証明書を要求する（Request a certificate）] をクリックします。

**ステップ 8** **[詳細な証明書要求（Advanced certificate request）]** をクリックします。

**ステップ 9** **[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（Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file）]** をクリックするか、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します をクリックします。

**ステップ 10** CSR ファイルの内容（手順 5 でコピーしたもの）を [保存された要求（Saved Request）] フィールドに貼り付けます。

**ステップ 11** [送信（Submit）] をクリックします。

**ステップ 12** インターネット ブラウザで、URL：。`http://<name of your Issuing CA Server>/certsrv`に戻ります。

**ステップ 13** **[保留中の証明書要求のステータスを表示する（View the status of a pending certificate request）]** をクリックします。

**ステップ 14** 前のセクションで発行した証明書要求をクリックします。

**ステップ 15** **[Base 64 エンコード（Base 64 encoded）]** を選択します。

**ステップ 16** **[証明書をダウンロード（Download Certificate）]** をクリックします。

**ステップ 17** 証明書をローカル マシンに保存します。

a) 証明書ファイル名 `cup-xmpp-s2s.pem` を指定します。

b) 証明書をタイプ [セキュリティ証明書（ **Security Certificate**）] として保存します。

### 次のタスク

Upload a CA-Signed Certificate for XMPP Federation （185 ページ）

### トラブルシューティングのヒント

- IM and Presence Service でサポートされるドメインのリストが変更された場合は、新しいドメイン リストを反映するように cup-xmpp-s2s 証明書を再生成する必要があります。

# Upload a CA-Signed Certificate for XMPP Federation

### Before you begin

Complete the steps in XMPP フェデレーションの証明書署名要求の生成, on page 183.

**ステップ 1** Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security** > **Certificate Management**.

**ステップ 2** Click **Upload Certificate/Certificate chain.**.

**ステップ 3** Choose **cup-xmpp-s2s** for Certificate Name.

**ステップ 4** Browse to the location of the CA-signed certificate that you saved to your local machine.

**ステップ 5** Click **Upload File**.

**Note** If you have generated a multi-server SAN based certificate, you can upload this to any IM and Presence Service node in the cluster. When this is done the resulting signed multi-server certificate and its associated chain of signing certificates are automatically distributed to the other servers in the cluster on upload of the multi-server certificate to any of the individual servers in the cluster. If a self-signed certificate already exists on any of the nodes, it will be overwritten by the new multiple server certificate. For more information on multi-server certificates, see the New and Changed Features chapter of the *Release Notes for Cisco Unified Communications Manager, Release 10.5(1)*.

**ステップ 6** Restart the Cisco XMPP Federation Connection Manager service. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Control Center - Network Services** to restart this service.

**Note** If you upload a multi-server certificate you must restart the XCP Router service on **all** IM and Presence Service nodes in the cluster.

### What to do next

To support cross navigation for serviceability between nodes in the same cluster, the Cisco Tomcat service trust stores between IM and Presence Service and Cisco Unified Communications Manager are automatically synchronized.

When CA signed certificates are generated to replace the original self-signed trust certificates on either IM and Presence Service or Cisco Unified Communications Manager, the original certificates persist in the node's service trust store. Leaving the original self-signed certificates in the service trust store is not an issue because no service presents them. However, you can delete these certificates, but if you do, you must delete them on the IM and Presence Service and Cisco Unified Communications Manager,

See the section Delete Self-Signed Trust Certificates in Part II, Chapter 9 — Security Configuration on IM and Presence Service, in the appropriate release of the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

# XMPP フェデレーションのルート CA 証明書のインポート

（注） このセクションでは、cup-xmpp-s2s 信頼証明書を IM and Presence Service に手動でアップロードする方法について説明します。また、証明書インポート ツールを使用して cup-xmpp-s2s 信頼証明書を自動的にアップロードすることもできます。証明書インポート ツールにアクセスするには、**Cisco Unified CM IM and Presence Administration** のユーザー インターフェイスにログインします。**[システム（System）] > [セキュリティ（Security）] > [証明書インポート ツール（Certificate Import Tool）]** を選択し、このツールの使用方法についてはオンライン ヘルプを参照してください。

IM and Presence Service がエンタープライズとフェデレートし、一般的に信頼されている認証局（CA）がその企業の証明書に署名する場合は、CA から IM and Presence Service ノードにルート証明書をアップロードする必要があります。

IM and Presence Service が、一般的に信頼されている CA によって署名された証明書ではなく、自己署名証明書を使用する企業とフェデレーションする場合は、この手順を使用して自己署名証明書をアップロードできます。

### 始める前に

ルート CA 証明書をダウンロードし、ローカル マシンに保存します。

**ステップ 1** **Cisco Unified IM and Presence Operating System Administration** ユーザー インターフェイスにログインします。IM and Presence Service の **[セキュリティ（Security）]** > **[証明書管理（Certificate Management）]** を選択します。.

**ステップ 2** [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします。

**ステップ 3** [証明書名（Certificate Name）] に **cup-xmpp-trust** を選択します。

（注） [ルート名（Root Name）] フィールドはブランクのままにします。

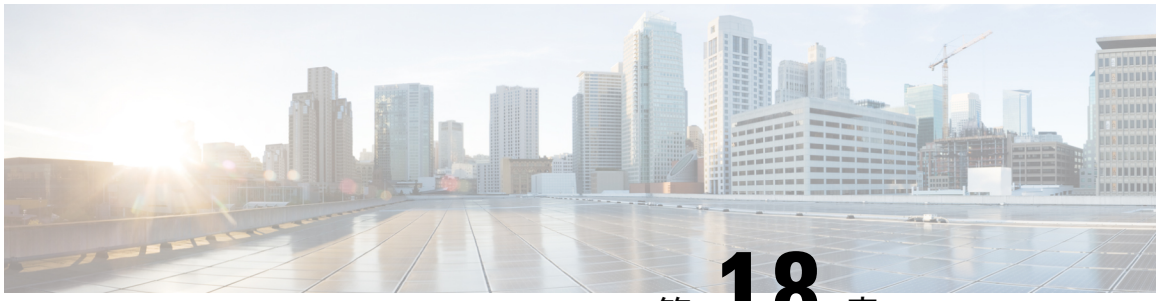
**ステップ 4** **[参照（Browse）]** をクリックし、以前にダウンロードしてローカル マシンに保存したルート CA 証明書の場所を参照します。

**ステップ 5** **[ファイルのアップロード（Upload File）]** をクリックして、IM and Presence Service ノードに証明書をアップロードします。

（注） まだ信頼していない CA を持つ新しいエンタープライズとフェデレーションするたびに、この手順を繰り返す必要があります。同様に、新しいエンタープライズが自己署名証明書を使用し、ルート CA 証明書の代わりに自己署名証明書がアップロードされる場合は、この手順に従う必要があります。

### トラブルシューティングのヒント

信頼証明書が自己署名されている場合、XMPP フェデレーション セキュリティ設定ウィンドウで **[クライアント側の証明書が必要（Require client side certificates ）]** パラメータをオンにすることはできません。



第 18 章

# フェデレーション構成用の電子メール アドレス

この章では、フェデレーションの電子メールアドレス機能と複数ドメインの構成について説明します。



## フェデレーション有効化用の電子メール

フェデレーション機能の電子メール アドレスをオンにすると、 IM and Presence Service はローカル ユーザーの JID を連絡先の電子メールアドレスに変更します。

クラスタ間展開の場合は、展開内のすべてのクラスタ間ノードでフェデレーションの電子メール アドレスをオンにする必要があります。フェデレーション機能の電子メールをオンにした後、Cisco XCP ルータ サービスを再起動する必要があります。

XMPP フェデレーション展開では、フェデレーション機能の電子メールアドレスは現在、マルチクラスタ IM and Presence Service 展開で一時的または永続的なチャットルームをサポートしていません。ローカル ドメインに複数の IM and Presence Service クラスタがある展開シナリオでは、ローカル ユーザーの実際の JID がフェデレーテッド ユーザーに送信される場合があります。チャット ルームへの唯一の影響は、フェデレーテッド ユーザーに表示される名前が、ローカル ユーザーの電子メール アドレスではなく、ローカル ユーザーのユーザー ID になることです。他のすべてのチャットルーム機能は通常どおりに動作します。これは、フェデレーテッド ユーザーとの一時的または永続的なチャットルームでのみ発生します。

SIP および XMPP フェデレーションのフェデレーション機能の電子メールアドレスの詳細と、機能をオンにする手順については、フェデレーション設定の電子メールアドレスに関連するトピックを参照してください。

# フェデレーションに関する考慮事項の電子メールアドレス

SIP または XMPP フェデレーションに電子メールアドレスを使用するように IM および Presence Service を設定すると、IM and Presence Service は、フェデレーテッド連絡先とのすべての通信で、ローカルユーザの IM アドレスをユーザの電子メールアドレスに交換します。

ドメイン間フェデレーションの電子メールアドレスを有効にする前に、次の点に注意してください。

- 外部ドメインとのフェデレーションをまだ試行しておらず、フェデレーション用の電子メールをオンにする場合は、ユーザーがフェデレーション連絡先の追加を開始する前に、この設定をオンにすることをお勧めします。
- フェデレーションの電子メール アドレスをオンにした場合、ユーザーの電子メール アドレスが Active Directory で構成されていない場合、IM および Presence サービスはフェデレーションにユーザーの JID を使用します。
- この機能の前提条件は、各ユーザーの Cisco Unified Communications Manager Mail ID がユーザーの完全な電子メール アドレスと一致している必要があることです。

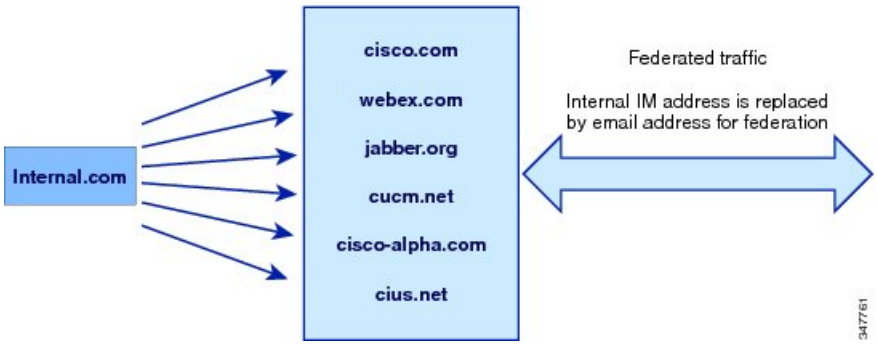
  ユーザーの [メール ID（Mail ID）] フィールドが空であるか、完全な電子メール アドレスが含まれていない場合、 IM および Presence サービスはデフォルトで、ユーザーの IM および Presence サービス JID をフェデレーションに使用します。
- フェデレーションの電子メールアドレスをオンにし、フェデレーテッドコンタクトが電子メールアドレスではなく IM および Presence サービス ユーザーの JID を使用する場合、IM および Presence サービスはこれらの要求をドロップします（ユーザーに対して有効な電子メール アドレスが構成されている場合でも）。
- IM および Presence サービスは、フェデレーション機能の電子メール アドレスの電子メール エイリアスをサポートしていません。

（注） この機能は、SIP と XMPP の両方のフェデレーションに適用されます。

## 複数ドメインのフェデレーション サポート用の電子メール アドレス

フェデレーションの電子メール アドレス機能は、複数のドメインをサポートします。次の図は、フェデレーテッド トラフィックに使用されている複数の電子メール ドメインの例を示しています。

図 *33* : 複数ドメインのフェデレーション サポートの電子メール アドレス




ローカル IM and Presence Service 展開で複数の電子メール ドメインを管理している場合は、ローカル電子 メール ドメインごとに必要な DNS SRV レコードを公開する必要があります。

XMPP フェデレーションの場合、cup-xmpp-s2s セキュリティ証明書には、すべてのローカル IM および電子メール ドメインがサブジェクト代替名として含まれている必要があります。

# 電子メール ドメイン構成概要

IM and Presence Service が各ユーザーの電子メール アドレスのすべての一意のドメインを自動的に読み取り、その情報を [フェデレーションの電子メール アドレス（Email Address for Federation）] 機能に使用するため、フェデレーションの電子メールアドレス機能で使用する電子メール ドメインを手動で追加および編集することはオプションです。

IM and Presence Service 用にまだ構成されていないユーザーがいるが、それらのユーザーを構成する予定のドメインがある場合は、 **Cisco Unified CM IM and Presence Administration** ユーザーインターフェイスを使用して、それらのドメインを IM and Presence Service に手動で追加できます。現在ユーザーが割り当てられていないドメインは、ユーザーインターフェイスにローカル電子メールドメインとして自動的に表示されません。

フェデレーションの電子メールアドレスに使用されるユーザー ドメインは、 **Cisco Unified CM IM and Presence 管理**ユーザーインターフェイスの **[電子メールドメイン（ Email Domain ）]** ウィンドウにシステム管理ドメインとして表示されます。これらは、ユーザーインターフェイスでは構成できません。

# 外部ドメインの管理者に提供する情報

フェデレーションの電子メールアドレスをオンにする前に、外部ドメインのシステム管理者に次のことを通知する必要があります。

- フェデレーションに電子メールアドレスを使用しており、外部ドメインのユーザーは、フェデレーション連絡先を連絡先リストに追加するときに電子メールアドレスを指定する必要がある。
- すでに外部ドメインとフェデレーションしていて、フェデレーション用の電子メールを有効にする場合、外部ドメインのユーザーは、連絡先リストから既存のフェデレーション連

絡先を削除し、電子メールアドレスを指定してこれらのフェデレーションの連絡先を再度追加する必要があります。

# IM and Presence Service ユーザーに提供する情報

フェデレーションの電子メール アドレスをオンにする場合は、すべての IM and Presence Service ユーザーに次のことを通知する必要があります。

- フェデレーテッド連絡先は、user_id@domain アドレスではなく、電子メール アドレスを使用するようになりました。
- 連絡先リストに新しい連絡先を追加する場合、フェデレーテッド連絡先は、user_id@domain ではなく、 IM and Presence Service ユーザーの電子メール アドレスを使用する必要があります。
- user_id@domain で追加された（フェデレーテッド ウォッチャの連絡先リストにある）既存の IM and Presence Service 連絡先を削除し、 IM and Presence Service ユーザの電子メール アドレスを使用して再度追加する必要があります。
- IM and Presence Service がフェデレーテッド連絡先から user_id@domain アドレス宛てに受信したメッセージはすべてドロップされます（Active Directory で構成された電子メール アドレスと同じであり、 IM and Presence Serviceのユーザー テーブルで構成されているアドレスである場合を除く）。
- IM and Presence Service ユーザーがすでに連絡先リストにフェデレーテッド連絡先を持っている場合、これらのユーザーがクライアントに再度サインインすると、フェデレーテッド連絡先に電子メール アドレスを含むポップアップが表示されることがあります。

（注） フェデレーションの電子メール アドレスをオンにすると、 IM and Presence Service ユーザーは IM and Presence Serviceに接続するときにクライアントで何も変更する必要はなく、 IM and Presence Service ノードとのやり取りも変わりません。

# 電子メール ドメイン管理の連携動作と制約事項

- ローカルクラスタに関連付けられている管理者が管理するドメインのみを追加または削除できます。
- システムが管理するドメインは編集できません。
- 他のクラスタに関連付けられている、システムが管理するかまたは管理者が管理するドメインは編集できません。
- 2 個のクラスタでドメインを設定することはできますが、ピア クラスタのみで使用されている場合に限ります。これは、ローカルクラスタのシステムが管理するドメインとして表示されますが、ピア クラスタで使用中であると識別されます。

- TLS による XMPP フェデレーションでは、IM アドレス ドメインを追加または削除する場合、TLS 証明書 cup-xmpp-s2s を再作成する必要があります。

# フェデレーション構成および電子メール ドメイン管理用の電子メールアドレス

## フェデレーション用の電子メールをオンにする

（注） クラスタ間展開の場合は、展開内のクラスタ間ノードでフェデレーションの電子メールアドレスをオンにする必要があります。

**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）] > [設定（Settings）]** を選択します。

**ステップ 2** **[ドメイン間フェデレーションに電子メール アドレスの使用を有効にする（Enable use of Email Address for Inter-domain Federation）]** チェックボックスをオンにします。

**ステップ 3** 警告メッセージの内容を確認し、**[OK]** をクリックします。

**ステップ 4** [保存（Save）] をクリックします。

**ステップ 5** フェデレーション用の電子メールをオンにした後、Cisco XCP ルータを再起動します。**Cisco Unified IM and Presence Serviceability** のユーザ 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 センター - ネットワーク サービス（Control Center - Network Services）]** を選択します。

（注） フェデレーションのルーティング パラメータを編集する場合は、フェデレーション ルーティング パラメータの構成 （50 ページ） に移動します。

## 電子メール ドメインの表示

システム管理ドメインと管理者管理ローカル ドメインは、 **Cisco Unified CM IM and Presence 管理**のユーザー インターフェイスを使用して、[電子メール ドメインの検索と一覧表示（Find and List Email Domains）] ウィンドウに表示されます。このウィンドウでは、管理者が管理する各ドメインがローカル クラスタ、ピア クラスタ、またはその両方で構成されたかどうかも示されます。

**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（Inter-Domain Federation）]** > **[電子メール フェデレーテッド ドメイン（Email Federated Domains）]** を選択します。**[電子メール ドメインの検索と一覧表示（Find and List Email Domains）]** ウィンドウが表示されます。

# 電子メール ドメインの追加または更新

**Cisco Unified CM IM Presence 管理**ユーザー インターフェイスを使用して、ローカル クラスタに手動で IM アドレス ドメインを追加し、ローカル クラスタにある既存の IM アドレスのドメインを更新できます。

最大 255 文字のドメイン名を入力でき、各ドメインはクラスタ全体で一意である必要があります。指定できる値は、すべての大文字または小文字（a-zA-Z）、すべての番号（0-9）、ハイフン（-）、またはドット（.）です。ドメイン ラベルの区切り文字はドットです。ドメイン ラベルの先頭文字をハイフンにすることはできません。最後のラベル（たとえば、.com）の先頭文字を数字にすることはできません。たとえば、Abc.1om は無効なドメインです。

システム管理ドメインと管理者管理ローカル ドメインは、[ドメインの検索と一覧表示（Find and List Domains）] ウィンドウに表示されます。このウィンドウでは、管理者が管理する各ドメインがローカル クラスタ、ピア クラスタ、またはその両方で構成されたかどうかも示されます。

システム管理ドメインが使用中であるため、編集できません。その IM アドレス ドメインのシステムにユーザーが存在しない場合（たとえば、ユーザーが削除された場合）、システム管理ドメインは自動的に管理者の管理ドメインになります。管理者の管理ドメインは編集または削除できます。

**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（Inter-Domain Federation）]** > **[電子メール フェデレーテッド ドメイン（Email Federated Domains）]** を選択します。

すべての管理者管理およびシステム管理電子メール ドメインを表示する **[電子メール ドメインの検索/一覧表示（Find and List Email Domains）]** ウィンドウが表示されます。

**ステップ 2** 次のいずれかの操作を実行します。

- [新規追加（Add New）] をクリックすることで、新しいドメインを追加します。**[電子メール ドメイン（Email Domains）]** ウィンドウが表示されます。
- ドメインのリストから編集するドメインを選択します。**[電子メール ドメイン（Email Domains）]** ウィンドウが表示されます。

**ステップ 3** **[ドメイン名（Domain Name）]** フィールドに、新しいドメイン名を入力し、**[保存（Save）]** を選択します。

最大 255 文字までのユニークなドメイン名を入力します。指定できる値は、すべての大文字または小文字（a-zA-Z）、すべての番号（0-9）、ハイフン（-）、またはドット（.）です。ドメイン ラベルはハイフンで始まらないようにして、最後のラベル（たとえば、.com）の先頭文字を数字にすることはできません。

**ヒント** 警告メッセージが表示されます。TLS XMPP フェデレーションを使用した場合、新しい TLS 証明書を生成する手順に進む必要があります。

# 電子メール ドメインの削除

**Cisco Unified CM IM and Presence** の管理用ユーザー インターフェイスを使用して、ローカル クラスタにある管理者の管理用電子メール アドレス ドメインを削除できます。

システム管理ドメインは使用中のため削除できません。その電子メール ドメインのシステムにユーザーが存在しない場合（たとえば、ユーザーが削除された場合）、システム管理ドメインは自動的に管理者の管理ドメインになります。管理者の管理ドメインは編集または削除できます。

（注） ローカル クラスタとピア クラスタの両方に設定された管理者の管理ドメインを削除すると、ドメインは管理者の管理ドメインのリストに保持されます。ただし、そのドメインはピア クラスタでのみ設定済みとマークされます。完全にエントリを削除するには、設定されたすべてのクラスタからドメインを削除する必要があります。

**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（Inter-Domain Federation）] > [電子メール フェデレーテッド ドメイン（Email Federated Domains）]** を選択します。

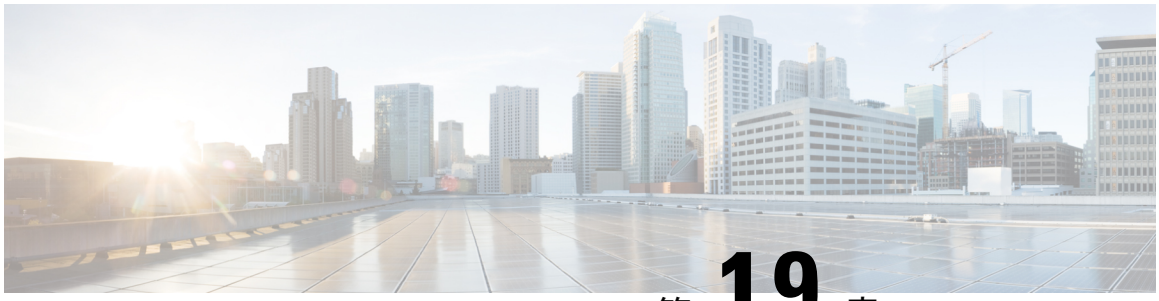
すべての管理者管理およびシステム管理電子メール ドメインを表示する **[電子メール ドメインの検索/一覧表示（Find and List Email Domains）]** ウィンドウが表示されます。

**ステップ 2** 次の方法の 1 つを使用して削除する管理者の管理ドメインを選択し、次に [選択項目の削除（Delete Selected）] をクリックします。

- 削除するドメインの横のチェックボックスをオンにします。
- 管理者の管理ドメインのリストのドメインをすべて選択するには、**[すべてを選択（Select All）]** をクリックします。

**ヒント** すべての選択をクリアするには、[すべてをクリア（Clear All）] をクリックします。

**ステップ 3** [OK] をクリックして削除を確定するか、[取消（Cancel）] をクリックします。



第 19 章

# フェデレーションの有用性の構成

このセクションでは、フェデレーションの有用性構成について説明します。



# フェデレーションのロギングの使用

このセクションでは、フェデレーションでのロギングの使用について説明します。

## SIP フェデレーションのログ ファイルの場所

SIP フェデレーションには、次のログ ファイルが適用されます。

- /var/log/active/epas/trace/xcp/log にあるsip-cm-3_0000000X.log
- /var/log/active/epas/trace/esp/sdi にある esp0000000X.log

これらのログは RTMT からキャプチャすることもできます。

## XMPP フェデレーションのログ ファイルの場所

次のログファイルが XMPP フェデレーションに適用されます。

- /var/log/active/epas/trace/xcp/log にあるxmpp-cm-4_0000000X.log

RTMT からログをキャプチャすることもできます。

## フェデレーションのロギングをオンにする

**ステップ 1** **Cisco Unified IM and Presence Serviceability** のユーザー インターフェイスにログインします。**[トレース（Trace）] > [設定（Configuration）]** を選択します。

**ステップ 2** [サーバー] ドロップダウン リスト ボックスから、IM and Presence サーバーを選択して、**[移動（Go）]** をクリックします

**ステップ 3** [サービス グループ] リスト ボックスで、**[IM and Presence Services]** を選択して、**[移動（Go）]** をクリックします。

**ステップ 4** 次のいずれかの手順を実行します。

a) SIP フェデレーションの場合は、[サービス（Service）] ドロップダウン リストから [Cisco XCP SIP Federation Connection Manager サービス] を選択し、**[移動（Go）]** をクリックします。

b) XMPP フェデレーションの場合は、[サービス（Service）] ドロップダウンリストから [Cisco XCP XMPP Federation Connection Manager サービス] を選択し、**[移動（Go）]** をクリックします。

**ステップ 5** **[トレースをオンにする（Trace On）]** をクリックします。

[トレース フィルタ設定（Trace Filter Settings）] で [デバッグ トレース レベル（Debug Trace Level）] を選択します。トレースでデバッグ レベルを有効にする場合は、[デバッグ トレース レベル（Debug Trace Level）] で [デバッグ（Debug）] を選択します。

# Cisco XCP ルータの再起動方法

ここでは、Cisco XCP ルータの再起動方法について説明します。

## Cisco XCP Router

SIP または XMPP フェデレーション設定の設定を変更した場合は、 IM and Presence Serviceで Cisco XCP ルータを再起動する必要があります。Cisco XCP ルータを再起動すると、IM and Presence Service によりすべてのアクティブな XCP サービスが自動的に再起動されます。

Cisco XCP ルータは、停止して再開するのではなく、再起動する必要があります。Cisco XCP Router を再起動するのではなくオフにした場合、IM and Presence Service により他のすべての XCP サービスが停止されます。その後で XCP ルータを起動しても、IM and Presence Service は他の XCP サービスを自動的には起動しません。手動で他の XCP サービスを起動する必要があります。

## Cisco XCP ルータの再起動

**ステップ 1** **Cisco Unified IM and Presence Serviceability** のユーザ 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 センター - ネットワーク サービス（Control Center - Network Services）]** を選択します。

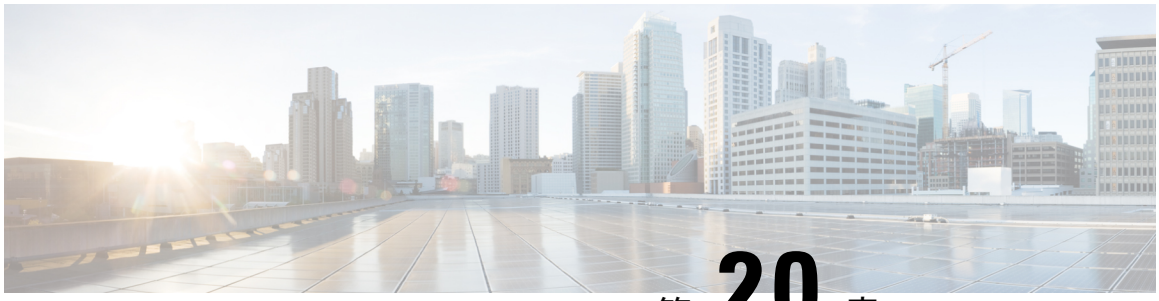
**ステップ 2** [サーバ（Server）] ドロップダウン リストからサーバを選択します。

**ステップ 3** [移動（Go）] をクリックします。

**ステップ 4** [IM and Presence サービス（IM and Presence Service）] エリアで、[Cisco XCP ルータ（Cisco XCP Router）] サービスの横にあるオプション ボタンをクリックします。

**ステップ 5** **[再起動（Restart）]** をクリックします。

**ステップ 6** リスタートに時間がかかることを示すメッセージが表示されたら、[OK] をクリックします。



第 20 章

# フェデレーション統合の検証

このセクションでは、フェデレーション統合の検証について説明します。



## SIP フェデレーション設定の確認

この手順では、 IM and Presence Service エンタープライズ展開と Microsoft OCS エンタープライズ展開の間のフェデレーテッドネットワークの設定を確認する方法について説明します。必要に応じて、他のタイプの統合を確認するためのガイドとしてこの手順を使用します。

（注） 複数のローカル IM and Presence Service ドメインがある場合は、各ローカル ドメインのユーザに対してこの手順を再実行します。

**ステップ 1** Cisco Jabber クライアントまたはサードパーティ製 XMPP クライアントにログオンします。

**ステップ 2** 2 つのフェデレーテッド Microsoft Office Communicator クライアントにログオンします。

**ステップ 3** 最初の Microsoft Office Communicator クライアントで次の手順を実行します。

a) IM and Presence Service ユーザーを連絡先として追加します。

b) Microsoft Office Communicator ユーザーのプレゼンス サブスクリプションを受け入れるか、ブロックするか、無視するかを要求するポップアップ メッセージが IM and Presence Service に表示されます。

c) IM and Presence Service ユーザーと Microsoft Office Communicator ユーザーが互いの対応可否を確認できることを確認します。

**ステップ 4** IM and Presence Service クライアントのクライアントで次の手順を実行します。

a) 2 番目の Microsoft Office Communicator ユーザーを連絡先として追加します。

b) Microsoft Office Communicator ユーザーの可用性を確認できることを確認します。

c) Microsoft Office Communicator ユーザーのユーザー クライアントに、 Cisco Jabber ユーザーが連絡先として追加されたことを通知するポップアップ メッセージが表示されます。

**ステップ 5** IM and Presence Service ユーザーのクライアントと Microsoft Office Communicator クライアントの両方の可用性状態を切り替えます。各クライアントの連絡先の可用性状態が変更されたことを確認します。

**ステップ 6** IM and Presence Service ユーザのクライアントから Microsoft Office Communicator ユーザーへの IM を開始します。

**ステップ 7** IM and Presence Service ユーザーからのメッセージを含む [IM] ウィンドウが Microsoft Office Communicator に表示されていることを確認します。

**ステップ 8** IM and Presence Service ユーザーのクライアントの IM ウィンドウと Microsoft Office Communicator クライアントの IM ウィンドウの両方を閉じます。

**ステップ 9** Microsoft Office Communicator ユーザーから IM and Presence Service ユーザーへの IM を開始します。

**ステップ 10** IM and Presence Service ユーザーのクライアントに IM ウィンドウが表示され、Microsoft Office Communicator ユーザーからのメッセージが表示されていることを確認します。

**ステップ 11** Cisco Jabber クライアントで、次の手順を実行します。

a) Microsoft Office Communicator ユーザーの 1 人をブロックします。

（注） XEP-0016 - プライバシー リストをサポートしていないサードパーティ製クライアントでは、サードパーティ製 XMPP クライアントからブロックすると、IM のみがブロックされます。ユーザーは引き続き可用性ステータスを交換できます。サーバー側の IM と可用性をブロックするには、ユーザーは [IM and Presence Users Options] インターフェイスから、または Cisco Jabberの [Privacy configuration] からプライバシー設定を行います。

b) この Microsoft Office Communicator ユーザーに、 IM and Presence Service ユーザーの可用性がオフラインとして表示されていることを確認します。2 番目の Microsoft Office Communicator ユーザーは、引き続き IM and Presence Service ユーザーの可用性ステータスを確認できます。

c) IM and Presence Service ユーザーのクライアントでは、ブロックされた Microsoft Office Communicator ユーザーは引き続きオンラインとして表示され、ブロックされた Microsoft Office Communicator ユーザーへの IM を開始できます。

**ステップ 12** Microsoft Office Communicator クライアントから IM and Presence Service ユーザーをブロックします。

**ステップ 13** Microsoft Office Communicator ユーザーのプレゼンスが、 IM and Presence Service ユーザーのクライアントで使用できなくなっていることを確認します。

# XMPP フェデレーション構成の確認

この手順では、IM および Presence サービス リリース 9.0 エンタープライズ展開と、Webex、IBM Sametime、または別の IM および Presence サービス リリース 9.0 エンタープライズ展開の間のフェデレーテッド ネットワークの構成を確認する方法について説明します。次の手順では、IM および Presence サービス リリース 9.0 および Webex 展開の手順について説明します。この手順をガイドとして使用して、他のタイプの XMPP フェデレーションを確認します。

（注） 複数のローカル IM および Presence サービス ドメインが存在する場合、各ローカル ドメインのユーザーにこの手順を再度実行します。

**ステップ 1** IM および Presence サービス リリース 9.0 サーバに接続されている Cisco Jabber クライアントまたはサードパーティ製 XMPP クライアントにログオンします。

**ステップ 2** 2 つのフェデレーテッド WebEx Connect クライアントにログオンします。

**ステップ 3** 最初の WebEx Connect クライアントで次の手順を実行します。

a) コンタクトとして IM および Presence サービス ユーザーを追加します。

b) IM および Presence サービス ユーザーのクライアントに、WebEx Connect ユーザーからの Presence サブスクリプションを受け入れるか、ブロックするか、無視するかを要求するポップアップ メッセージが表示されます。サブスクリプションを承認します。

c) IM および Presence サービス ユーザーと WebEx Connect ユーザーが互いの対応可否を確認できることを確認します。

**ステップ 4** IM および Presence サービス ユーザーのクライアントで次の手順を実行します。

a) 2 番目の WebEx Connect ユーザーを連絡先として追加します。

b) WebEx Connect クライアントにポップアップが表示されます。サブスクリプションを承認します。

c) WebEx Connect ユーザーの対応可否を確認できることを確認します。

**ステップ 5** IM および Presence サービス ユーザーのクライアントと WebEx Connect クライアントの両方の可用性状態を切り替えます。各クライアント上のコンタクトのアベイラビリティ状態の変更を確認します。

**ステップ 6** IM および Presence サービス ユーザーのクライアントから WebEx Connect 連絡先への IM を開始します。

**ステップ 7** IM および Presence サービス ユーザーからの IM を含む IM ウィンドウが WebEx Connect クライアントに表示されることを確認します。

**ステップ 8** 両方のクライアントで IM ウィンドウを閉じます。

**ステップ 9** WebEx Connect ユーザーから IM および Presence サービス ユーザーへの IM を開始します。

**ステップ 10** IM および Presence サービス ユーザーのクライアントに IM ウィンドウが表示され、WebEx Connect ユーザーからの IM が表示されることを確認します。

**ステップ 11** IM および Presence サービス ユーザーのクライアントで、次の手順を実行します。

a) WebEx Connect ユーザーの 1 人をブロックします。

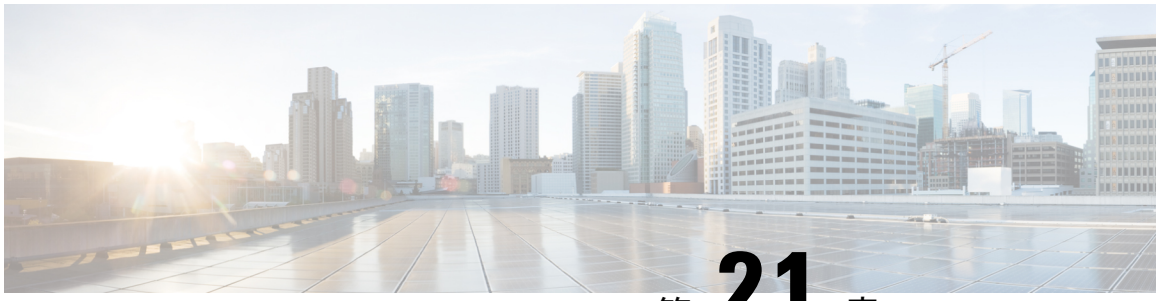
（注） サードパーティの XMPP クライアントからブロックする場合は、IM のみをブロックします。ユーザーは引き続き可用性ステータスを交換できます。サーバ側の IM およびアベイラビリティをブロックするため、ユーザーは IM および Presence ユーザー オプション インターフェイス、または Cisco Jabber のプライバシー構成からプライバシー設定を構成します。

b) この WebEx Connect ユーザーに、 IM および Presence サービス ユーザーの可用性がオフラインとして表示されていることを確認します。2 番目の Webex Connect ユーザーは、引き続き IM および Presence サービス ユーザーの対応可否ステータスを確認できます。

c) IM および Presence サービス ユーザーのクライアントでは、ブロックされた Webex Connect ユーザーは引き続きオンラインとして表示されますが、ブロックされた Webex Connect ユーザーに IM を送信することはできません。

**ステップ 12** WebEx Connect クライアントから IM および Presence サービス ユーザーをブロックします。

**ステップ 13** IM および Presence サービス ユーザーのクライアントで、WebEx Connect ユーザーの可用性が使用できなくなっていることを確認します。



第 21 章

# SIP フェデレーション統合のトラブルシューティング

このセクションでは、SIP フェデレーション統合のトラブルシューティング方法について説明します。

- Cisco 適応型セキュリティ アプライアンスの一般的な問題と推奨されるアクション （205 ページ）
- 統合に関する一般的な問題と推奨されるアクション （209 ページ）

# Cisco 適応型セキュリティ アプライアンスの一般的な問題と推奨されるアクション

ここでは、Cisco 適応型セキュリティアプライアンスの一般的な問題と推奨されるアクションについて説明します。

## 証明書構成の問題

### IM および Presence サービスと Cisco 適応型セキュリティ アプライアンス間の証明書の障害

IM and Presence Service と Cisco 適応型セキュリティ アプライアンス 間の証明書構成が失敗しています。

Cisco 適応型セキュリティ アプライアンス の時刻とタイムゾーンが正しく構成されていない可能性があります。

- Cisco 適応型セキュリティアプライアンスの時刻とタイムゾーンを設定します。
- IM and Presence Service と Cisco Unified Communications Managerで時刻とタイムゾーンが正しく構成されていることを確認します。

この統合の事前前提構成タスク （34 ページ）

# Cisco 適応型セキュリティアプライアンスと Microsoft Access Edge 間の証明書の障害

Cisco 適応型セキュリティアプライアンス と Microsoft Access Edge 間の証明書構成は、Cisco 適応型セキュリティ アプライアンスでの証明書の登録時に失敗します。

Cisco 適応型セキュリティアプライアンスで SCEP 登録を使用している場合、SCEP アドオンが正しくインストールおよび構成されていない可能性があります。SCEP アドオンをインストールして設定します。

### 関連情報

CA トラストポイント

# SSL ハンドシェイクの証明書エラー

SSL ハンドシェイクに証明書エラーが表示されます。

証明書に FQDN がありません。IM and Presence Service CLI でドメインを設定し、IM and Presence Service で証明書を再生成して FQDN を設定する必要があります。証明書を再生成する場合は、IM and Presence Service で SIP プロキシを再起動する必要があります。

# VeriSign に証明書署名要求を送信する際のエラー

証明書の登録に VeriSign を使用しています。証明書署名要求を VeriSign Web サイトに貼り付けると、エラー（通常は 9406 または 9442 エラー）が表示されます。

証明書署名要求のサブジェクト名に情報がありません。更新証明書署名要求（CSR）ファイルを VeriSign に送信する場合は、証明書署名要求のサブジェクト名に次の情報を含める必要があります。

- 国（2 文字の国コードのみ）
- 州（略語なし）
- 地域（略語なし）
- 組織名
- 組織単位
- 共通名（FQDN）

subject-name 行エントリの形式は次のとおりです。

```
(config-ca-trustpoint)# subject-name cn=fqdn、U=organizational_unit_name、C=country、St=state、L=locality、O=organization
```

### 関連トピック

VeriSign の新しいトラストポイントの生成 （228 ページ）

## IM および Presence Service のドメインまたはホスト名が変更された場合の SSL エラー

CLI から IM and Presence Service ドメインを変更すると、 IM and Presence Service と Cisco 適応型セキュリティアプライアンスの間で SSL 証明書エラーが発生します。

CLI から IM and Presence Service のドメイン名を変更すると、 IM and Presence Service の自己署名証明書 sipproxy.pem が再生成されます。そのため、sipproxy.pem 証明書を Cisco Cisco 適応型セキュリティアプライアンスに再インポートする必要があります。具体的には、Cisco Cisco 適応型セキュリティアプライアンスの現在の sipproxy.pem 証明書を削除し、（再生成された）Cisco 適応型セキュリティアプライアンス の sipproxy.pem 証明書を再インポートする必要があります。

# TLS プロキシ クラス マップ作成時のエラー

TLS プロキシ クラス マップを設定すると、次のエラーが表示されます。

```
ciscoasa(config)# class-map ent_imp_to_external

ciscoasa(config-cmap)# match access-list ent_imp_to_external

エラー：指定された ACL（ent_imp_to_external）が存在しないか、そのタイプが match コマンドでサポートされていません。

ciscoasa(config-cmap)# exit

ciscoasa(config)# class-map ent_external_to_imp

ciscoasa(config-cmap)# match access-list ent_external_to_imp

エラー: 指定された ACL（ent_external_to_imp）が存在しないか、そのタイプが match コマンドでサポートされていません。

ciscoasa(config-cmap)#
```

外部ドメインのアクセスリストが存在しません。上記の例では、ent_external_to_imp というアクセス リストは存在しません。**access list** を使用して、外部ドメインの拡張アクセス リストを作成します。

**関連情報 -**

アクセス リストの構成要件

TLS プロキシ デバッグ コマンド

# サブスクリプションが Access Edge に到達しない

Microsoft Office Communicator からのサブスクリプションが Access Edge に到達しない。OCS は、Access Edge をピアとして使用するネットワーク機能エラーを報告します。Access Edge サービスが開始されません。

Access Edge では、[許可（Allow）] タブと [IM プロバイダー（IM provider）] タブの両方で IM and Presence Service ドメインを構成できます。IM and Presence Service ドメインは、[IM プロバイダー（IM Provider）] タブでのみ構成する必要があります。Access Edge で、[許可（Allow）]

タブから IM and Presence Service ドメイン エントリを削除します。[IM プロバイダー（IM Provider）] タブに IM and Presence Service ドメインのエントリがあることを確認します。

（注） IM and Presence Service は複数のドメインをサポートします。各 IM and Presence ドメインを確認して、[許可（Allow）] タブに削除する必要がある誤ったエントリがあるかどうかを確認してください。

# アップグレード後の Cisco 適応型セキュリティ アプライアンスの問題

Cisco 適応型セキュリティ アプライアンスは、ソフトウェアのアップグレード後に起動しません。

TFTP サーバを使用し、Cisco 適応型セキュリティ アプライアンスの ROM モニタ（ROMMON）を使用して、新しいソフトウェア イメージを Cisco 適応型セキュリティ アプライアンスにダウンロードできます。ROMMON は、TFTP および関連する診断ユーティリティを介したイメージのロードと取得に使用されるコマンドライン インターフェイスです。

**ステップ 1** コンソール ケーブル（Cisco 適応型セキュリティ アプライアンス に付属している青色のケーブル）をコンソール ポートから近くの TFTP サーバのポートに接続します。

**ステップ 2** ハイパーターミナルまたは同等のものを開きます。

**ステップ 3** プロンプトが表示されたら、すべてのデフォルト値を受け入れます。

**ステップ 4** Cisco 適応型セキュリティ アプライアンスを再起動します。

**ステップ 5** ブートアップ中に ESC を押して ROMMON にアクセスします。

**ステップ 6** 次の一連のコマンドを入力して、Cisco 適応型セキュリティ アプライアンス が TFTP サーバからイメージをダウンロードできるようにします。

```
ip asa_inside_interface server tftp_server interface ethernet 0/1 file name_of_new_image
```

（注） 指定するイーサネット インターフェイスは、Cisco 適応型セキュリティ アプライアンス の内部インターフェイスと同等である必要があります。

**ステップ 7** TFTP サーバ上の推奨される場所（TFTP ソフトウェアによって異なる）にソフトウェア イメージを配置します。

**ステップ 8** 次のコマンドを入力して、ダウンロードを開始します。

```
tftp dnld
```

（注） TFTP サーバが別のサブネットにある場合は、ゲートウェイを定義する必要があります。

## Microsoft OCS 2008 に署名付き Microsoft CA サーバ クライアント認証証明書をインストールできない

Microsoft CA によって署名されたサーバ クライアント認証証明書を、Windows 2008 を実行している Microsoft Office Communications Server（OCS）のローカル コンピュータ ストアにインストールすることはできません。現在のユーザー ストアからローカル コンピュータ ストアに証明書をコピーしようとすると、秘密キーが見つからないというエラー メッセージが表示されて失敗します。

以下の手順を実行できます。

1. ローカル ユーザーとして OCS にログインします。
2. 証明書を作成します。
3. CA サーバーからの証明書を承認します。
4. OCS にログオンしている間に、証明書をファイルにエクスポートし、秘密キーがエクスポートされていることを確認します。
5. OCS（ローカル コンピュータ）からログオフします。
6. OCS に再度ログインしますが、今回は OCS ドメイン ユーザーとしてログインします。
7. 証明書ウィザードを使用して、証明書ファイルをインポートします。証明書がローカル コンピュータ ストアにインストールされます。[OCS 証明書（OCS certificate）] タブで証明書を選択できるようになりました。

# 統合に関する一般的な問題と推奨されるアクション

ここでは、統合に関する一般的な問題と推奨されるアクションについて説明します。

## 可用性交換を取得できません

**問題**　Cisco Jabber と Microsoft Office Communicator の間で可用性情報を交換できません。

**解決法**　OCS/アクセスエッジ、 IM and Presence Service 、および Cisco Jabber について記載されているトラブルシューティング手順を実行します。

OCS/Access Edge：

1. Access Edge のパブリック インターフェイスで証明書が正しく設定されていない可能性があります。Microsoft CA を使用している場合は、OID 値 1.3.6.1.5.5.7.3.1、1.3.6.1.5.5.7.3.2 を使用していることを確認します。証明書の [全般（General）] タブに誤った値が表示されます（正しい場合は表示されません）。また、 IM and Presence Service と Access Edge 間の TLS ハンドシェイクの ethereal トレースに誤った値が表示されることもあります。

証明書タイプが「その他」で、OID 値が 1.3.6.1.5.5.7.3.1、1.3.6.1.5.5.7.3.2 の Access Edge のパブリック インターフェイスの証明書を再生成します。

2. フロントエンド サーバーがOCSで実行されていない可能性があります。

   「Office Communications Server Front-End」サービスが実行されていることを確認します。このサービスを確認するには、**[スタート（Start）]**>**[プログラム（Administrative）]**>**[管理ツール（Administrative Tools）]**>**[コンピュータの管理（Computer Management）]**の順に選択します。**[サービスとアプリケーション（Services and Applications）]** で、**[サービス（Services）]** を選択し、「Office Communications Server Front-End」 サービスを見つけます。実行中の場合、このサービスのステータスは「開始」になります。

IM and Presence Service

1. IM and Presence Serviceで証明書が正しく設定されていない可能性があります

   IM and Presence Serviceの正しい sipproxy-trust 証明書を生成します。

2. スタティック ルートを使用している場合は、Access Edge のパブリック インターフェイスを指すスタティック ルートを設定します。スタティック ルートでは、ルート タイプを「domain」に設定し、逆の接続先パターンを設定する必要があります。たとえば、フェデレーション ドメインが abc.com の場合、接続先アドレスパターンは 「.com.abc.*」に設定する必要があります。スタティック ルートは、[Cisco Unified CM IM and Presence Administration] を使用して、**[プレゼンス（Presence）]** > **[ルーティング（Routing）]** > **[スタティック ルート（Static Routes）]** を選択して設定します。

3. DNS SRV のチェックを実行し、両側が影響を受けるユーザーのドメインを解決できることを確認します。

Cisco Jabber クライアント：

Cisco Jabber は、クライアント コンピュータから誤った DNS 設定を取得する可能性があります。次の手順を実行する必要があります。

1. クライアント コンピュータの DNS 構成を確認します。
2. DNS 設定を変更した場合は、Cisco Jabberを再起動します。

**関連トピック**

外部 Access Edge インターフェイスの証明書構成 （70 ページ）
IM および Presence サービスの新規証明書の生成 （64 ページ）
SIP フェデレーションの DNS 構成 （48 ページ）

# IM の送受信の問題

Microsoft Office Communicator ユーザーと Cisco Jabber 8.0 ユーザー間の IM の送受信に問題があります。

DNS 設定、Access Edge、Microsoft Office Communicator クライアント、および IM and Presence Serviceについてリストされているトラブルシューティング手順を実行します。

**DNS の設定**：

DNS SRV レコードが作成されていないか、正しく設定されていない可能性があります。DNS SRV レコードがすべてのドメインに対して正しく設定されているかどうかを確認します。IM and Presence Service と Access Edge の両方から type=srv の nslookup を実行します。

**Access Edge で**

1. Access Edge のコマンドプロンプトから、 **nslookup**と入力します。
2. **set type=srv** と入力します。
3. IM and Presence ドメインの SRV レコードを入力します。例：**_sipfederationtls._tcp.abc.com** ここで、**abc.com** はドメイン名です。SRV レコードが存在する場合は、 IM and Presence Service/Cisco 適応型セキュリティ アプライアンス の FQDN が返されます。

   IM and Presence Service で：

4. リモート アクセス アカウントを使用して、 IM and Presence Service ノードに ssh 接続します。
5. 上記の Access Edge と同じ手順を実行しますが、この場合は OCS ドメイン名を使用します。

**Microsoft Office Communicator クライアント**：

Microsoft Office Communicator 2007 ユーザーのプレゼンスが [応答不可（DND）] に設定されている場合があります。Microsoft Office Communicator 2007 が DND に設定されている場合、 は他のユーザーからの IM を受信しません。Microsoft Office Communicator ユーザーのプレゼンスを別の状態に設定します。

**IM and Presence Service**

1. DNS SRV の代わりにスタティック ルートを使用している場合は、スタティック ルートが正しく構成されていない可能性があります。Access Edge のパブリック インターフェイスを指すスタティック ルートを構成します。スタティック ルートでは、ルート タイプを「domain」に設定し、逆の接続先パターンを設定する必要があります。たとえば、フェデレーション ドメインが 「abc.com」 の場合、宛先アドレス パターンは 「.com.abc.*」に設定する必要があります。**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）]**を選択することで、スタティック ルートが構成されます。
2. フェデレーション IM コントローラ モジュールのステータスが無効になっている可能性があります。**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）]**で**[システム（System）] > [サービス パラメータ（Service Parameters）]** を選択し、[SIP プロキシ（SIP Proxy）] サービスを選択します。ウィンドウの下部で、**[IM ゲートウェイ ステータス（IM Gateway Status）]** パラメータが [オン（On）] に設定されていることを確認します。
3. フェデレーション ドメインが追加されていないか、正しく設定されていない可能性があります。**Cisco Unified CM IM and Presence Administration** で、**[プレゼンス（Presence）] >**

**[ドメイン間フェデレーション（Inter-Domain Federation）]** を選択し、正しいフェデレーション ドメインが追加されていることを確認します。

**関連情報 -**

SIP フェデレーションの DNS 構成

SIP フェデレーテッド ドメインの追加

# 短期間で可用性と IM 交換が失われる

ユーザーは Cisco Jabber と Microsoft Office Communicator の間で可用性と IM を共有できますが、しばらくすると互いの可用性が失われ、IM を交換できなくなります。

**OCS/Access Edge**：

1. Access Edge では、内部エッジと外部エッジの両方に同じ FQDN が設定されている場合があります。また、DNS には、その FQDN に 2 つの「A」レコードエントリが存在する場合があります。1 つは外部エッジの IP アドレスに解決し、もう 1 つは内部エッジの IP アドレスに解決します。

   Access Edge で、内部エッジの FQDN を変更し、更新されたレコードエントリを DNS に追加します。Access Edge の内部 IP に最初に解決された DNS エントリを削除します。また、Access Edge の内部エッジの証明書を再設定します。

2. OCS のグローバル設定とフロントエンドのプロパティで、Access Edge の FQDN が誤って入力されている可能性があります。OCS で、内部エッジの新しい FQDN を反映するようにサーバーを再設定します。

**DNSの設定**：

DNS SRV レコードが作成されていないか、正しく設定されていない可能性があります。必要な「A」レコードと SRV レコードを追加します。

**関連情報 -**

SIP フェデレーションの外部サーバー コンポーネントの構成

# 可用性状態の変更と IM 配信時間の遅延

Cisco Jabber と Microsoft Office Communicator の間で IM and Presence Service の状態変更の配信時間に遅延があります。

IM and Presence Service ノードでは、Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context に対して **[空の TLS フラグメントを無効にする（Disable Empty TLS Fragments）]** オプションが選択されていない場合があります。

**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。**[システム（System）] > [システム（System）] > [TLS コンテキスト設定（TLS Context Configuration）]** を選択します。

**ステップ 2** **[Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context]** をクリックします。

**ステップ 3** [TLS コンテキスト情報（TLS Context Information）] エリアで、**[空の TLS フラグメントを無効にする（Disable Empty TLS Fragments）]** チェックボックスをオンにします。

**ステップ 4** [保存（Save）] をクリックします。

# 可用性サブスクリプションの試行後に 403 FORBIDDEN が返される

IM and Presence Service は、Microsoft Office Communicator ユーザの可用性に登録しようとし、OCS サーバーから 403 FORBIDDEN メッセージを受信します。

Access Edge サーバーで、 IM and Presence Service ノードが IM サービス プロバイダ リストに追加されていない可能性があります。Access Edge サーバーで、 IM and Presence Service ノードのエントリを IM サービス プロバイダー リストに追加します。Access Edge の DNS サーバで、IM and Presence Service ノードのパブリック アドレスを指す IM and Presence Service ドメインの _sipfederationtls レコードがあることを確認します。

または

Access Edge サーバーで、 IM and Presence Service ノードが許可リストに追加されている可能性があります。Access Edge サーバーで、 IM and Presence Service ノードを指すすべてのエントリを許可リストから削除します。

**関連情報 -**

SIP フェデレーションの外部サーバー コンポーネントの構成

# NOTIFY メッセージのタイムアウト

TCP を使用して IM and Presence Service と Microsoft OCS の間で直接フェデレーションを行う場合、NOTIFY メッセージの送信時に IM and Presence Service がタイムアウトします。

IM and Presence Service ノードでは、**[Record-Route ヘッダーでトランスポートを使用（ Use Transport in Record-Route Header）]** を有効にする必要がある場合があります。

**ステップ 1** **Cisco Unified CM IM and Presence Administration** のユーザーインターフェイスにログインします。**[システム（System）] > [サービスパラメータ（Service Parameters）]** を選択します。

**ステップ 2** [サーバ（Server）] ドロップダウン リストからノードを選択します。

**ステップ 3** [サービス（Service）] ドロップダウン リストから、**[Cisco SIP プロキシ（Cisco SIP Proxy）]** サービスを選択します。

**ステップ 4** [SIP パラメータ（クラスタ全体）（SIP Parameters (Clusterwide)）] セクションで、[Record-Route ヘッダーでトランスポートを使用（Use Transport in Record-Route Header）] パラメータで **[オン（ On ）]** を選択します。

**ステップ 5** [保存（**Save**）] をクリックします。

# IM および Presence サービスの証明書は承認されません

Access Edge が IM and Presence Serviceからの証明書を受け入れていません。

IM and Presence Service/Cisco 適応型セキュリティアプライアンス と Access Edge 間の TLS ハンドシェイクが失敗している可能性があります。

**OCS/Access Edge**：

1. Access Edge の IM プロバイダー リストに IM and Presence Service ノードのパブリック FQDN が含まれており、 IM and Presence Service 証明書のサブジェクト CN と一致していることを確認します。許可リストに IM and Presence Serviceの FQDN を入力しないことを選択した場合は、 IM and Presence Service 証明書のサブジェクト CN が IM and Presence Service ドメインの SRV レコードの FQDN に解決されることを確認する必要があります。 。
2. Access Edge で FIPS が有効になっていることを確認します（TLSv1 を使用）。
3. フェデレーションが OCS でグローバルに有効になっており、フロント エンド サーバーで有効になっていることを確認します。
4. DNS SRV の解決に失敗した場合は、DNS が正しく設定されていることを確認し、Access Edge から type=srv の nslookup を実行します。
5. Access Edge のコマンドプロンプトから、 **`nslookup`**と入力します。
6. **`set type=srv`** と入力します。
7. たとえば、 IM and Presence Service ドメインの SRV レコードを入力します。 **_sipfederationtls._tcp.abc.com** ここで、 **abc.com** はドメイン名です。SRV レコードが存在する場合は、 IM and Presence Service/Cisco 適応型セキュリティ アプライアンス の FQDN が返されます。

IM and Presence サービス/Cisco 適応型セキュリティアプライアンス：

IM and Presence サービス と Cisco 適応型セキュリティアプライアンスの暗号を確認します。**IM and Presence Service Administration** にログインし、**[システム（System）]** > **[セキュリティ（Security）]** > **[TLS コンテンツ構成（TLS Context Configuration）]** > **[デフォルト Cisco SIP プロキシ ピア認証 TLS コンテンツ（Default Cisco SIP Proxy Peer Auth TLS Context）]**を選択し、「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。

# OCS でのフロントエンド サーバの起動に関する問題

OCS のフロントエンド サーバーが起動しない。

OCS では、Access Edge のプライベート インターフェイスの FQDN が承認済みホストのリストで定義されている可能性があります。OCS の承認済みホストのリストから Access Edge のプライベート インターフェイスを削除します。

OCS のインストール中に、RTCService と RTCComponentService という 2 つの Active Directory ユーザー アカウントが作成されます。これらのアカウントには管理者が定義したパスワードが与えられますが、これらのアカウントの両方で [パスワードを無期限にする（Password never expires）] オプションはデフォルトで選択されていないため、パスワードは定期的に期限切れになります。OCS サーバーの RTCService または RTCComponentService のパスワードをリセットするには、次の手順に従います。

**ステップ 1** ユーザー アカウントを右クリックします。
**ステップ 2** **[パスワードのリセット（Reset Password）]** を選択します。
**ステップ 3** ユーザー アカウントを右クリックします。
**ステップ 4** [プロパティ（Properties）] を選択します。
**ステップ 5** **[アカウント（Accounts）]** タブを選択します。
**ステップ 6** [パスワードを無期限にする（Password Never Expires）] チェックボックスをオンにします。
**ステップ 7** **[OK]** をクリックします。

# リモートデスクトップから Edge にアクセスできない

Windows XP で FIPS が有効になっている Access Edge Server に正常にリモート デスクトップを接続できません。

これは、既知の Microsoft 問題です。この問題を解決するための回避策には、Windows XP コンピュータにリモートデスクトップ接続アプリケーションをインストールする必要があります。リモート デスクトップ接続 6.0 をインストールするには、次の Microsoft URL の手順に従ってください。

http://support.microsoft.com/kb/811770

第 22 章

# XMPP フェデレーション統合のトラブルシューティング

このセクションでは、XMPP フェデレーション統合のトラブルシューティング方法について説明します。



## システムトラブルシュータの確認

複数の IM and Presence Service クラスタを展開し、XMPP フェデレーションを構成する場合は、クラスタごとに少なくとも 1 つのノードで XMPP フェデレーションをオンにする必要があります。各クラスタで同じ XMPP フェデレーション設定とポリシーを設定する必要があります。IM and Presence Service は、クラスタ全体で XMPP フェデレーション構成を複製しません。システム トラブルシュータは、クラスタ間の XMPP フェデレーション設定が同期されていない場合にレポートします。システム トラブルシュータは、次のチェックを実行します。

**ステップ 1**
a) XMPP フェデレーションは、クラスタ間ピア全体で一貫して有効になります。
b) SSL モードは、クラスタ間ピア全体で一貫して構成されます。
c) 「Required Valid client-side certificates」は、クラスタ間ピア全体で一貫して構成されます。
d) SASL 設定は、クラスタ間ピア全体で一貫して構成されます。
e) ダイヤルバック秘密は、クラスタ間ピア全体で一貫して構成されます。
f) XMPP フェデレーションのデフォルトの管理ポリシーは、クラスタ間ピア全体で一貫して構成されます。
g) ポリシーホストは、クラスタ間ピア全体で一貫して構成されます。

**ステップ 2** **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。[診断（Diagnostics）] > [システムのトラブルシューティングツール（System Troubleshooter）] の順に選択します。 >

**ステップ 3** 次の横に緑色のチェックマークがあることを確認します。

- XMPP フェデレーション設定がすべてのクラスタ間ピアで一致していることを確認します。

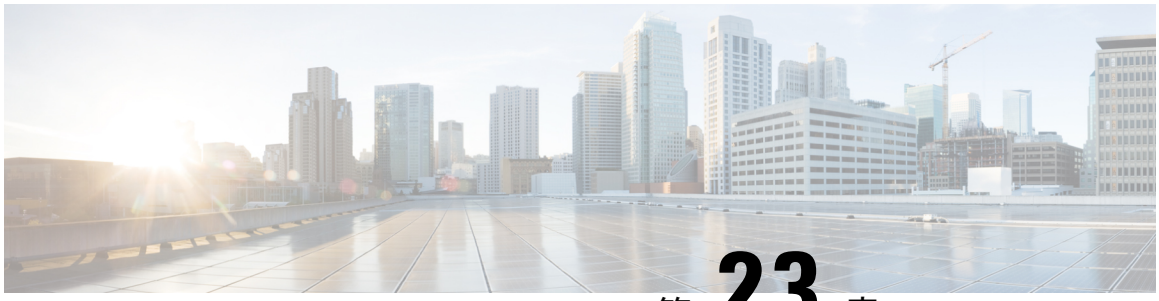
- SASL 設定がすべてのクラスタ間ピアに対して正しく構成されていることを確認します。
- XMPP がすべてのクラスタの少なくとも 1 つのノードで均一に無効または有効になっていることを確認します。
- デフォルトの管理ポリシーがすべてのクラスタ間ピアで一貫していることを確認します。
- ホスト ポリシーがすべてのクラスタ間ピアで一貫していることを確認します。

システム トラブルシュータは、これらのチェックのいずれかで問題が報告された場合に推奨されるアクションを提供します。

（注）
- システム トラブルシュータのすべてのテストに合格しても、IM の交換と可用性に関する問題が解決しない場合は、**[プレゼンス設定（Presence Settings）]** ページの **[フェデレーション時に電子メール アドレスの使用を有効にする（Enable use of Email Address when Federating）]** 設定がクラスタ間ピア全体で一貫して構成されているかどうかを確認します。
- システム トラブルシュータのすべてのテストに合格しても、IM の交換と可用性に関する問題が解決しない場合は、**[プレゼンス設定（Presence Settings）]** ページの **[ドメイン間フェデレーションでの電子メール アドレスの使用を有効にする（Enable use of Email Address for Inter-domain Federation）]** 設定がクラスタ間ピア全体で一貫して構成されているかどうかを確認します。

### 次のタスク

XMPP フェデレーションのログ ファイルの場所 （197 ページ）



第 23 章

# Cisco 適応型セキュリティ アプライアンスの構成例

ここでは、Cisco 適応型セキュリティ アプライアンスの構成例について説明します。



## SIP フェデレーション用の PAT コマンドとアクセス リストの構成例

このセクションでは、外部 OCS エンタープライズ展開とフェデレートしている IM および Presence サービス ノードの設定例を示します。ローカル エンタープライズ展開には、2 つの追加のクラスタ間 IM および Presence サービス ノードがあります。

以下の値は、以下のサンプル例で使用されています。

- パブリック IM および Presence サービス IP アドレス = 10.10.10.10
- プライベート ルーティング IM および Presence サービス IP アドレス = 1.1.1.1
- プライベート セカンド IM および Presence サービス IP アドレス = 2.2.2.2
- プライベート サード IM および Presence サービス IP アドレス = 3.3.3.3
- IM および Presence サービスのピア認証リスナー ポート= 5062
- Netmask = 255.255.255.255
- 外部ドメイン = abc.com
- Microsoft OCS 外部インターフェイス = 20.20.20.20

次の PAT コマンドは、（ルーティング） IM および Presence サービス ノードに対して定義されます。

（Cisco 適応型セキュリティ アプライアンス リリース 8.2:）

```
static (inside,outside) tcp 10.10.10.10 5061 1.1.1.1 5062 netmask 255.255.255.255
static (inside,outside) tcp 10.10.10.10 5080 1.1.1.1 5080 netmask 255.255.255.255
static (inside,outside) tcp 10.10.10.10 5060 1.1.1.1 5060 netmask 255.255.255.255
```

（Cisco 適応型セキュリティ アプライアンス リリース 8.3:）

```
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5061 obj_tcp_source_eq_5062
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5080 obj_tcp_source_eq_5080
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5060 obj_tcp_source_eq_5060
```

次の PAT コマンドは、エンタープライズ展開の 2 つの追加のクラスタ間 IM および Presence サービス ノードに対して定義されます。

（Cisco 適応型セキュリティ アプライアンス リリース 8.2:）

```
static (inside,outside) tcp 10.10.10.10 45080 2.2.2.2 5080 netmask 255.255.255.255
static (inside,outside) udp 10.10.10.10 55070 3.3.3.3 5070 netmask 255.255.255.255
static (inside,outside) tcp 10.10.10.10 55070 3.3.3.3 5070 netmask 255.255.255.255
static (inside,outside) udp 10.10.10.10 45062 2.2.2.2 5062 netmask 255.255.255.255
static (inside,outside) tcp 10.10.10.10 55062 3.3.3.3 5062 netmask 255.255.255.255
```

（Cisco 適応型セキュリティ アプライアンス リリース 8.3:）

```
nat (inside,outside) source static obj_host_2.2.2.2 obj_host_10.10.10.10 service
obj_tcp_source_eq_5080 obj_tcp_source_eq_45080
nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_tcp_source_eq_5070 obj_tcp_source_eq_55070
nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_udp_source_eq_5070 obj_udp_source_eq_55070
nat (inside,outside) source static obj_host_2.2.2.2 obj_host_10.10.10.10 service
obj_tcp_source_eq_5062 obj_tcp_source_eq_45062
nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_tcp_source_eq_5062 obj_tcp_source_eq_55062
```

この構成に対応するアクセス リストを次に示します。フェデレーションする外部ドメインごとに、ドメイン abc.com のアクセス リストと同様のアクセス リストを追加する必要があることに注意してください。

（Cisco 適応型セキュリティ アプライアンス リリース 8.2:）

```
access-list ent_imp_to_abc extended permit tcp host 1.1.1.1 host 20.20.20.20 eq 5061
access-list ent_abc_to_imp extended permit tcp host 20.20.20.20 host 10.10.10.10 eq 5061
```

```
access-list ent_second_imp_to_abc extended permit tcp host 2.2.2.2 host 20.20.20.20 eq
5061

access-list ent_third_imp_to_abc extended permit tcp host 3.3.3.3 host 20.20.20.20 eq
5061

access-list ent_abc_to_second_imp extended permit tcp host 20.20.20.20 host 10.10.10.10
eq 45061

access-list ent_abc_to_third_imp extended permit tcp host 20.20.20.20 host 10.10.10.10
eq 55061
```

**（Cisco 適応型セキュリティ アプライアンス リリース 8.3:）**

```
access-list ent_imp_to_abc extended permit tcp host 1.1.1.1 host 20.20.20.20 eq 5061

access-list ent_abc_to_imp extended permit tcp host 20.20.20.20 host 1.1.1.1 eq 5062

access-list ent_second_imp_to_abc extended permit tcp host 2.2.2.2 host 20.20.20.20 eq
5061

access-list ent_third_imp_to_abc extended permit tcp host 3.3.3.3 host 20.20.20.20 eq
5061

access-list ent_abc_to_second_imp extended permit tcp host 20.20.20.20 host 2.2.2.2 eq
5062

access-list ent_abc_to_third_imp extended permit tcp host 20.20.20.20 host 3.3.3.3 eq
5062
```

各アクセス リストをクラス マップに関連付けます。

```
class-map ent_imp_to_abc

match access-list ent_imp_to_abc

class-map ent_abc_to_imp

match access-list ent_abc_to_imp

class-map ent_second_imp_to_abc

match access-list ent_second_imp_to_abc

class-map ent_third_imp_to_abc

match access-list ent_third_imp_to_abc

class-map ent_abc_to_second_imp

match access-list ent_abc_to_second_imp

class-map ent_abc_to_third_imp

match access-list ent_abc_to_third_imp
```

作成した各クラスマップのグローバル ポリシーマップを更新します。この例では、IMおよびPresence サービスによって開始された TLS 接続の TLS プロキシ インスタンスは「「imp_to_external」」と呼ばれ、外部ドメインによって開始された TLS 接続の TLS プロキシインスタンスは「external_to_imp」と呼ばれます。

```
policy-map global_policy
```

```
class ent_imp_to_abc
inspect sip sip_inspect tls-proxy ent_imp_to_external
policy-map global_policy
class ent_abc_to_imp
inspect sip sip_inspect tls-proxy ent_external_to_imp
policy-map global_policy
class ent_second_imp_to_abc
inspect sip sip_inspect tls-proxy ent_imp_to_external
policy-map global_policy
class ent_third_imp_to_abc
inspect sip sip_inspect tls-proxy ent_imp_to_external
policy-map global_policy
class ent_abc_to_second_imp
inspect sip sip_inspect tls-proxy ent_external_to_imp
policy-map global_policy
class ent_abc_to_third_imp
inspect sip sip_inspect tls-proxy ent_external_to_imp
```

# XMPP フェデレーションのアクセス リストの構成例

（注） このセクションの例は、Cisco 適応型セキュリティ アプライアンス リリース 8.3 に適用されます。

### ポート 5269 の任意のアドレスへの任意のアドレスアクセス

このアクセス リストの設定例では、任意のアドレスから任意のアドレスへのポート 5269 を許可します。

```
access-list ALLOW-ALL extended permit tcp any any eq 5269
```

### ポート 5269 での任意の単一 XMPP フェデレーション ノードへの任意のアドレス アクセス

このアクセス リストの設定例では、任意のアドレスからポート 5269の任意の単一の XMPP フェデレーション ノードへのアクセスを許可します。この例では、次の値を使用します。

- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1
- XMPP federation listening port = 5269

```
access-list ALLOW-ALL extended permit tcp any host 1.1.1.1 eq 5269
```

### DNS で公開された特定の XMPP フェデレーション ノードへの任意のアドレス アクセス

このアクセス リストの構成例では、任意のアドレスから DNS で公開された特定の XMPP フェデレーション ノードへのアクセスを許可します。

（注） パブリック アドレスは DNS で公開されますが、プライベート アドレスは access-list コマンドで構成されます。

この構成例では、次の値が使用されています。

- • XMPP フェデレーション IM and Presence Service リリース 9.x のプライベート IP アドレス = 1.1.1.1
- • 2 番目の IM and Presence Service リリース 9.x のプライベート IP アドレス = 2.2.2.2
- • 3 番目 の IM and Presence Service リリース 9.x のプライベート IP アドレス = 3.3.3.3
- • XMPP フェデレーション リスニング ポート = 5269

```
access-list ALLOW-ALL extended permit tcp any host 1.1.1.1 eq 5269
access-list ALLOW-ALL extended permit tcp any host 2.2.2.2 eq 5269
access-list ALLOW-ALL extended permit tcp any host 3.3.3.3 eq 5269
```

### DNS で公開された特定の XMPP フェデレーション ノードへの特定のフェデレーション ドメインのみのアクセス

このアクセス リストの設定例では、特定のフェデレーション ドメイン インターフェイスから、DNS でパブリッシュされた特定の XMPP フェデレーション ノードへのアクセスのみを許可します。

（注） パブリック アドレスは DNS で公開されますが、プライベート アドレスは access-list コマンドで設定されます。

この設定例では、次の値が使用されています。

- XMPP フェデレーション IM and Presence Service リリース 9.x プライベート IP アドレス = 1.1.1.1
- 2 番目 の IM and Presence Service リリース 9.x のプライベート IP アドレス = 2.2.2.2

- 3 番目 の IM and Presence Service リリース 9.x のプライベート IP アドレス = 3.3.3.3
- XMPP フェデレーション リスニング ポート = 5269
- 外部 XMPP エンタープライズの外部インターフェイス = 100.100.100.100

```
access-list ALLOW-ALL extended permit tcp host 100.100.100.100 host 1.1.1.1 eq
5269
access-list ALLOW-ALL extended permit tcp host 100.100.100.100 host 2.2.2.2 eq
5269
access-list ALLOW-ALL extended permit tcp host 100.100.100.100 host 3.3.3.3 eq
5269
```

# XMPP フェデレーションの NAT 構成の例

**例 1**：XMPP フェデレーションが有効になっている単一ノード

以下の値は、以下のサンプル例で使用されています。

- Public IM and Presence Service IP address = 10.10.10.10
- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1
- XMPP federation listening port = 5269

```
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
```

**例 2**：XMPP フェデレーションを備えた複数のノード（それぞれが DNS にパブリック IP アドレスを持つ）

以下の値は、以下のサンプル例で使用されています。

- Public IM and Presence Service IP addresses = 10.10.10.10, 20.20.20.20, 30.30.30.30
- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1
- Private second IM and Presence Service Release 9.x IP address = 2.2.2.2
- Private third IM and Presence Service Release 9.x IP address = 3.3.3.3
- XMPP federation listening port = 5269

```
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
nat (inside,outside) source static obj_host_2.2.2.2 obj_host_20.20.20.20 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269
```

```
nat (inside,outside) source static obj_host_2.2.2.2 obj_host_20.20.20.20 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_30.30.30.30 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_30.30.30.30 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
```

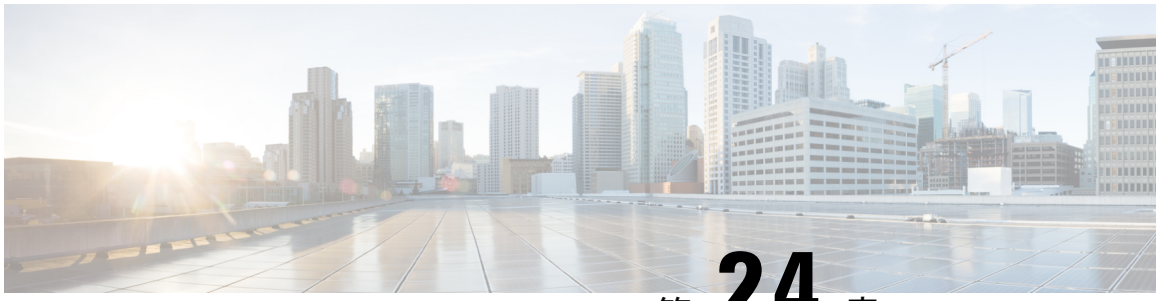
**例 3**： XMPP フェデレーションを使用する複数のノード、ただし DNS 内の単一のパブリック IP アドレスが任意の

DNS（PAT）で公開されているポート。

以下の値は、以下のサンプル例で使用されています。

- Public IM and Presence Service IP Address = 10.10.10.10
- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1, port 5269
- Private second IM and Presence Service Release 9.x IP address = 2.2.2.2, arbitrary port 25269
- Private third IM and Presence Service Release 9.x IP address = 3.3.3.3, arbitrary port 35269

```
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

nat (inside,outside) source static obj_host_2.2.2.2 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_25269

nat (inside,outside) source static obj_host_2.2.2.2 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_25269

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_35269

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_35269
```



第 24 章

# VeriSign を使用した Cisco 適応型セキュリティアプライアンスと Microsoft Access Edge 間のセキュリティ証明書の交換

ここでは、VeriSign を使用した Cisco 適応型セキュリティ アプライアンスと Microsoft Access Edge 間のセキュリティ証明書交換について説明します。



## Cisco 適応型セキュリティ アプライアンスでのセキュリティ証明書の設定

ここでは、Cisco 適応型セキュリティ アプライアンスでのセキュリティ証明書の構成について説明します。

### 古い証明書とトラストポイントの削除

この手順では、Cisco 適応型セキュリティ アプライアンスで古い中間証明書と署名付き証明書、およびルート証明書のトラストポイントを削除する方法について説明します。

#### 始める前に

以下の章で説明されている構成タスクを実行していることを確認してください。

- IM および Presence サービスでセキュリティ設定の構成
- SIP フェデレーション向け Cisco 適応型セキュリティ アプライアンスのワークフロー

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** トラストポイントを表示するには、次のコマンドを入力します。

```
show crypto ca trustpoints
```

**ステップ 3** トラストポイントおよび関連する証明書を削除するには、次のコマンドを入力します。

```
no crypto ca trustpoint trustpoint_name
```

次の警告が表示されます。

警告：登録済みのトラストポイントを削除すると、関連する認証局から受信したすべての証明書が破棄されます。

**ステップ 4** トラストポイントを削除するように求められたら、**[はい（yes）]** と入力します。

### 次のタスク

VeriSign の新しいトラストポイントの生成 （228 ページ）

# VeriSign の新しいトラストポイントの生成

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** このコマンドを入力して、この証明書のキー ペアを生成します。

```
crypto key generate rsa label keys_for_verisign
```

**ステップ 3** 次の一連のコマンドを入力して、 IM and Presence Serviceのトラストポイントを作成します。

```
(config)# crypto ca trustpoint trustpoint_name
(config-ca-trustpoint)# enrollment terminal
(config-ca-trustpoint)# subject-name
cn=fqdn,OU=organisational_unit,O=organisation_name,C=country,St=state,L=locality
(config-ca-trustpoint)# keypair keys_for_verisign
(config-ca-trustpoint)# fqdn none
(config-ca-trustpoint)# exit
```

（注） 証明書の更新署名要求（CSR）ファイルを VeriSign に送信する場合は、subject-name の値に次の情報を含める必要があります。

- 国（2 文字の国コードのみ）
- 州（略語なし）
- 地域（略語なし）
- 組織名
- 組織単位
- [共通名（FQDN）（Common Name (FQDN)）]：この値は、パブリック IM and Presence サービスの FQDN である必要があります。

### トラブルシューティングのヒント

コマンド **show crypto key mypubkey rsa** を入力して、キー ペアが生成されていることを確認してください。

### 次のタスク

中間証明書のインポート （232 ページ）

# ルート証明書のインポート

### 始める前に

VeriSign の新しいトラストポイントの生成 （228 ページ）の手順を完了します。

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次のコマンドを入力して、証明書を Cisco 適応型セキュリティアプライアンスにインポートします。

```
crypto ca authenticate trustpoint_name
```

**ステップ 3** CA 証明書を入力します。次に例を示します。

```
-----BEGIN CERTIFICATE-----MIIDAzCCAmwCEQC5L2DMiJ+hekYJuFtwbIqvMA0GCSqGSIb3DQEBBQUAMIH... -----END CERTIFICATE-----
quit
```

（注） 別の行に「quit」という単語を入力して終了します。

**ステップ 4** 証明書を受け入れるように求められたら、**yes** を入力します。

**次のタスク**

証明書署名要求の生成 （230 ページ）

# 証明書署名要求の生成

**始める前に**

ルート証明書のインポート （229 ページ）の手順を完了します。

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** CA に登録要求を送信するには、次のコマンドを入力します。

```
(config)# crypto ca enroll trustpoint_name
```

次の警告が表示されます。

```
%警告：証明書の登録は、システム fqdn とは異なる fqdn で構成されています。この証明書が VPN 認証に使用される場合、接続の問題が発生する可能性があります。
```

**ステップ 3** 証明書の登録を続行するように求められたら、**yes** と入力します。

```
% 証明書の登録を開始します。% 証明書のサブジェクト名は次のようになります。<fqdn>,
OU=<organisational_unit>,O=<organisation_name>,C=<country>,St=<state>,L=<locality>
```

**ステップ 4** サブジェクト名にデバイスのシリアル番号を含めるように求められたら、**no** と入力します。

**ステップ 5** ターミナルに証明書要求を表示するプロンプトが表示されたら、**yes** と入力します。

証明書要求（Certificate Request）が表示されます。

**次のタスク**

VeriSign に証明書署名要求を送信する （230 ページ）

# VeriSign に証明書署名要求を送信する

証明書署名要求を送信すると、VeriSign から次の証明書ファイルが提供されます。

- `verisign-signed-cert.cer` （署名付き証明書）

- Trial-inter-root.cer （下位の中間ルート証明書）
- verisign-root-ca.cer （ルート CA 証明書）

証明書ファイルをダウンロードしたら、別のメモ帳ファイルに保存します。

**始める前に**

- 証明書署名要求の生成 （230 ページ）の手順を完了します。
- 証明書署名要求の生成時に定義したチャレンジ パスワードが必要です。

**ステップ 1** VeriSign Web サイトに移動します。
**ステップ 2** 証明書署名要求を入力するする手順に従います。
**ステップ 3** プロンプトが表示されたら、証明書署名要求のチャレンジ パスワードを送信します。
**ステップ 4** 表示されたウィンドウに証明書署名要求を貼り付けます。

（注） **-----BEGIN CERTIFICATE-----** から **-----END CERTIFICATE-----** までを貼り付ける必要があります。

**次のタスク**

証明書署名要求に使用される証明書の削除 （231 ページ）

# 証明書署名要求に使用される証明書の削除

証明書署名要求の生成に使用された一時ルート証明書を削除する必要があります。

**始める前に**

VeriSign に証明書署名要求を送信する （230 ページ）の手順を完了します。

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次のコマンドを入力して、証明書を表示します。

```
(config)# show running-config crypto calook for crypto ca certificate chain trustpoint_name
```

**ステップ 3** 証明書を削除するには、次のコマンドを入力します。

```
(config)# crypto ca certificate chain trustpoint_name
(config-cert-chain)# no certificate ca 00b92f60cc889fa17a4609b85b70$
```

次の警告が表示されます。

警告：CA 証明書はこのトラストポイントから関連付け解除され、他のトラストポイントに関連付けられていない場合は削除されます。この CA によって発行され、このトラストポイントに関連付けられている他の証明書も削除されます。

**ステップ 4** トラストポイントを削除するように求められたら、**[はい（yes）]** と入力します。

### 次のタスク

中間証明書のインポート （232 ページ）

# 中間証明書のインポート

### 始める前に

証明書署名要求に使用される証明書の削除 （231 ページ）の手順を完了します。

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次のコマンドを入力して、Cisco 適応型セキュリティアプライアンスに証明書をインポートします。

```
crypto ca authenticate trustpoint_name
```

**ステップ 3** CA 証明書を入力します。次に例を示します。

```
-----BEGIN CERTIFICATE-----MIIEwDCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0BAQU.... -----END CERTIFICATE-----
quit
```

（注） 別の行に「quit」という単語を入力して終了します。

**ステップ 4** 証明書を受け入れるように求められたら、**yes** を入力します。

### 次のタスク

ルート証明書のトラストポイントの作成 （233 ページ）

# ルート証明書のトラストポイントの作成

**始める前に**

中間証明書のインポート （232 ページ）の手順を完了します。

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次のコマンドを入力して、トラストポイントを生成します。

```
(config)# crypto ca trustpoint verisign_root
(config-ca-trustpoint)#
```

**ステップ 3** 次の順序でコマンドを入力します。

```
(config-ca-trustpoint)# revocation-check none
(config-ca-trustpoint)# keypair keys_for_verisign
(config-ca-trustpoint)# enrollment terminal
(config-ca-trustpoint)# exit
```

# ルート証明書のインポート

**始める前に**

ルート証明書のトラストポイントの作成 （233 ページ）の手順を完了します。

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次のコマンドを入力して、Cisco 適応型セキュリティアプライアンスに証明書をインポートします。

```
crypto ca authenticate verisign_root
```

**ステップ 3** CA 証明書を入力します。次に例を示します。

```
-----BEGIN CERTIFICATE-----MIICmDCCAgECECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQECBQAw.... -----END
CERTIFICATE-----
```

**quit**

（注） 別の行に「「quit」」という単語を入力して終了します。

**ステップ 4** 証明書を受け入れるように求められたら、**yes** を入力します。

### 次のタスク

署名付き証明書のインポート （234 ページ）

# 署名付き証明書のインポート

### 始める前に

ルート証明書のインポート （233 ページ）の手順を完了します。

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** 次のコマンドを入力して、Cisco 適応型セキュリティアプライアンスに証明書をインポートします。

**crypto ca import verisignca certificate**

次の警告が表示されます。

```
警告：証明書の登録は、システム fqdn とは異なる fqdn で構成されています。この証明書が VPN 認証に使用される場合、接続の問題が発生する可能性があります。
```

**ステップ 3** 証明書の登録を続行するように求められたら、**yes** と入力します。

**ステップ 4** CA 証明書を入力します。次に例を示します。

```
-----BEGIN CERTIFICATE-----MIIFYTCCBEmgAwIBAgIQXtEPGWzZ0b9gejHejq+HazANBgkqhkiG9w0B.... -----END CERTIFICATE-----
```

**quit**

（注） 別の行に「「quit」」という単語を入力して終了します。

**ステップ 5** 証明書を受け入れるように求められたら、**yes** を入力します。

### 次のタスク

Microsoft Access Edge への VeriSign 証明書のインポート （235 ページ）

# Microsoft Access Edge への VeriSign 証明書のインポート

この手順では、VeriSign ルート証明書と中間証明書を Microsoft Access Edge サーバにインポートする方法について説明します。

### 始める前に

VeriSign から提供された証明書を Access Edge サーバー（C:\など）に保存します。

**ステップ 1** Access Edge サーバで、run コマンドから **mmc** を入力します。

**ステップ 2** **[ファイル（File）] > [スナップインの追加と削除（Add/Remove Snap-in）]** をクリックします。

**ステップ 3** [Add] をクリックします。

**ステップ 4** [Certificates] をクリックします。

**ステップ 5** [Add] をクリックします。

**ステップ 6** **[コンピュータ アカウント（Computer account）]** を選択します。

**ステップ 7** [次へ（Next)] をクリックします。

**ステップ 8** **[ローカル コンピュータ（Local Computer）]** を選択します。

**ステップ 9** **[終了]** をクリックします。

**ステップ 10** **[スナップインの追加と削除（Add/Remove Snap-In）]** ウィンドウを閉じるには、**[OK]** をクリックします。

**ステップ 11** メイン コンソールで、[証明書（Certificates）] ツリーを展開します。

**ステップ 12** **[信頼されたルート証明書（Trusted Root Certificates）]** ブランチを開きます。

**ステップ 13** **[証明書（Certificates）]** を右クリックします。

**ステップ 14** **[すべてのタスク（All Tasks）] > [インポート（Import）]**を選択します。

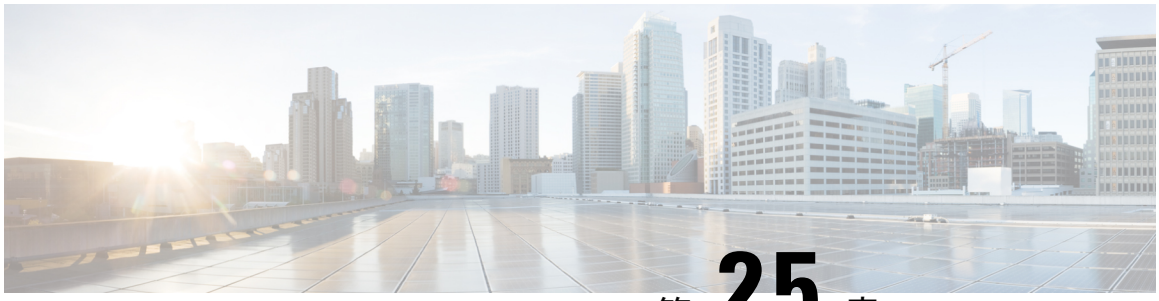
**ステップ 15** 証明書ウィザードで、**[次へ（Next）]** をクリックします。

**ステップ 16** C:\ ディレクトリで VeriSign 証明書を参照します。

**ステップ 17** **[証明書をすべて次のストアに配置する（Place all certificates in the following store）]** をクリックします。

**ステップ 18** 証明書ストアとして、**[信頼されるルート証明書認証局（Trusted Root Certification Authorities）]** を選択します。

**ステップ 19** 手順 13 ～ 18 を繰り返して、追加の VeriSign 証明書をインポートします。



第 25 章

# 統合デバッグ情報

このセクションでは、統合デバッグ情報について説明します。



## Cisco 適応型セキュリティ アプライアンスのデバッグ情報

ここでは、Cisco 適応型セキュリティ アプライアンスのデバッグ情報について説明します。

### Cisco 適応型セキュリティ アプライアンス デバッグ コマンド

次の表に、Cisco 適応型セキュリティ アプライアンスのデバッグ コマンドをリストします。

**表 *21 : Cisco* セキュリティ アプライアンスのデバッグ コマンド**

| 送信先 | コマンドを使用します。 | 注記 |
|---|---|---|
| Cisco 適応型セキュリティ アプライアンス インターフェイスへの ping の ICMP パケット情報を表示します。 | `debug icmp trace` | トラブルシューティングが完了グ メッセージを無効にするこます。すべてのデバッグ メッするには、`no debug icmp trac`用します。 |

| 送信先 | コマンドを使用します。 | 注記 |
|---|---|---|
| IM and Presence Service /Cisco 適応型セキュリティ アプライアンス または Cisco 適応型セキュリティ アプライアンス/外部ドメイン間の証明書検証に関連するメッセージを表示します。 | **debug crypto ca** | このコマンドに log level パラメーることで、Cisco 適応型セキュリアンス のログレベルを上げるこす。次に例を示します。<br>**debug crypto ca 3** |
| | **debug crypto ca messages** | 入力および出力メッセージのデバセージだけを表示します。 |
| | **debug crypto ca transactions** | トランザクションのデバッグ メッを表示します。 |
| Cisco 適応型セキュリティ アプライアンスを介して送信された SIP メッセージを表示します。 | **debug sip** | |
| ログメッセージをバッファに送信する（後で表示するため） | **terminal monitor** | |
| システム ログ メッセージを有効にします。 | **logging on** | トラブルシューティングが完了しテム ログ メッセージを無効にする推奨します。システム ログ メッセセーブルにするには、 **no logging** ドを使用します。 |
| バッファへのシステム ログ メッセージの送信 | **logging buffer debug** | |
| Telnet または SSH セッションに送信されるシステム ログ メッセージの設定 | **logging monitor debug** | |
| システム ログ メッセージを受信する（syslog）サーバーを指定します | **logging host** *interface_name ip_address* | • interface_name 引数は、syslog アクセスするときの Cisco 適リティ アプライアンス インタを指定します。<br>• ip_address 引数には、syslog サアドレスを指定します。 |

| 送信先 | コマンドを使用します。 | 注記 |
|---|---|---|
| インターフェイスを ping する | 一緒に | Cisco 適応型セキュリティ アプ<br>ンターフェイスへの ping の詳細<br>フィックが Cisco 適応型セキュ<br>イアンス を正常に通過できる<br>ための異なるインターフェイス<br>での ping の詳細については、<br>*Appliance Command Line Config*<br>の「Troubleshooting」セクショ<br>ださい。<br>[ ツール（**Tools**）] **[ping** > （**Pi**<br>て、ASDM のインターフェイス<br>することもできます。<br>（注） パブリック IM and Prese<br>IP アドレスに ping を実行<br>きません。ただし、Cisc<br>リティ アプライアンスの<br>フェイスの MAC アドレ<br>ブル（**arp –a**）に表示さ<br>ります。 |
| パケットのルートをトレースする | **traceroute** | ASDM でパケットのルートを<br>ともでき、**[ツール（Tools）]**><br>ト（**Traceroute**）] を選択しま |
| Cisco 適応型セキュリティ アプライアンスを介したパケットのライフスパンをトレースする | **packet-tracer** | ASDM でパケットのライフスパ<br>することもでき、**[ツール（To**<br>**ト トレーサー（Packet Tracer**<br>す。 |

**関連情報 -**

TLS プロキシ デバッグ コマンド

# 内部および外部インターフェイスでの出力のキャプチャ

**ステップ 1** 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

**ステップ 2** キャプチャするトラフィックを指定するアクセス リストを定義します。次に例を示します。

```
access-list cap extended permit ip 10.53.0.0 255.255.0.0 10.53.0.0 255.255.0.0
```

**ステップ 3** テストを開始する前に、キャプチャ コンテンツをクリアすることをお勧めします。内部インターフェイスのキャプチャをクリアするには、「clear capture in」 コマンドを使用し、外部インターフェイスのキャプチャをクリアするには、コマンド「clear capture out」 を使用します。

**ステップ 4** 次のコマンドを入力して、内部インターフェイスでパケットをキャプチャします。

```
cap in interface inside access-list cap
```

**ステップ 5** 次のコマンドを入力して、外部インターフェイスでパケットをキャプチャします。

```
cap out interface outside access-list cap
```

**ステップ 6** TLS 固有のパケットをキャプチャするには、次のコマンドを入力します。

```
capture capture_name type tls-proxy interface interface_name
```

**ステップ 7** パケット キャプチャを取得するには、次のコマンドを入力します。

```
copy /pcap capture:in tftp://xx.xx.xx.xx copy /pcap capture:out tftp://xx.xx.xx.xx
```

出力をディスクにコピーし、ASDM を使用して取得するには、次のコマンドを入力します（**[アクション（Actions）]**、> **[ファイル管理（File Management）]**、> **[ファイル転送（File Transfer）]** を選択）。

```
copy /pcap capture:in disk0:in_1
```

# TLS プロキシ デバッグ コマンド

次の表に、TLS プロキシのデバッグ コマンドを示します。

**表 *22 : TLS* プロキシ デバッグ コマンド**

| 送信先 | コマンドを使用 |
|---|---|
| TLS プロキシ関連のデバッグおよび syslog 出力の有効化 | **debug inspect tls-proxy events**<br>**debug inspect tls-proxy errors**<br>**debug inspect tls-proxy all** |
| TLS プロキシ セッションの出力を表示します。 | **show log** |
| アクティブな TLS プロキシ セッションを確認します。 | **show tls-proxy** |
| 現在のTLSプロキシセッションの詳細を表示します<br>（Cisco 適応型セキュリティ アプライアンス が IM and Presence サービス および外部ドメインとの接続を正常に確立した場合に使用） | **show tls-proxy session detail** |

# Access Edge および OCS サーバーのデバッグ

このセクションでは、Access Edge と OCS サーバーのデバッグについて説明します。

## OCS/アクセスエッジでのデバッグセッションの開始

**ステップ 1** 外部 Access Edge サーバーで、**[開始（Start）] > [管理ツール（Administrative Tools）] > [コンピュータ管理（Computer Management）]** を選択します。

**ステップ 2** 左側のペインで、**[Microsoft Office Communications Server 2007]** を右クリックします。

**ステップ 3** **[ロギング ツール（Logging Tool）] > [新しいデバッグセッション（New Debug Session）]** を選択します。

**ステップ 4** [ロギングオプション（Logging Options）] で、**[SIP スタック（SIP Stack）]** を選択します。

**ステップ 5** [レベル（Level）] の値として、**[すべて（All）]** を選択します。

**ステップ 6** **[ロギングの開始（Start Logging）]** をクリックします。

**ステップ 7** 完了したら、**[ロギングの停止（Stop Logging）]** をクリックします。

**ステップ 8** **[ログファイルの分析（Analyze Log Files）]**をクリックします。

## Access Edge 上での DNS 構成の確認

**ステップ 1** 外部 Access Edge サーバーで、**[開始（Start）] > [管理ツール（Administrative Tools）] > [コンピュータ管理（Computer Management）]** を選択します。

**ステップ 2** 左側のペインで **[Microsoft Office Communications Server 2007]** を右クリックします。

**ステップ 3** **[ブロック（Block）]** タブを選択します。

**ステップ 4** IM and Presence Service の管理対象ドメインがブロックされていないことを確認します。

**ステップ 5** **[アクセス方法（Access Methods）]** ペインで次のオプションが選択されていることを確認します。

a) 他のドメインとのフェデレーション

b) フェデレーション パートナーの検出を許可する

**ステップ 6** アクセス エッジが DNS SRV レコードを公開していることを確認します。

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。