Cisco Unified Communications Manager リリース 11.0(1) での IM and Presence サービスのドメイン間フェデレーション

初版：2015 年 06 月 08 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

この統合の概要

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 and Presence サービスが外部ドメイン ユーザとアベイラビリティ情報やインスタント メッセージング（IM）を交換したどのドメイン内からの IM and Presence サービス ユーザもイネーブルにします。異なる外部ドメインと連携するために、IM and Presence サービスが異なるプロトコルを使用します。

IM and Presence サービスでは、以下とのフェデレーションに対しては、標準的な Session Initiation Protocol（SIP RFC 3261）が使用されます。

- Microsoft Office Communications Server リリース 2（OCS R2）、OCS 2007、Microsoft Lync 2010

（注） IM and Presence サービス リリース 9.0 以降では、Microsoft Lync とのドメイン間フェデレーションがサポートされています。また IM and Presence サービス リリース 9.0 以降の場合、OCS とのドメイン間フェデレーションへの参照には、別途明示的な指定がない限り、Microsoft Lync が指定されます。

- AOL SIP Access Gateway（SAG）

（注） IM and Presence サービス リリース 9.0 以降では、AOL とのドメイン間フェデレーションがサポートされています。

AOL との SIP フェデレーションにより、IM and Presence サービス ユーザは次のユーザとフェデレーションを行うことが可能です。

- AOL パブリック コミュニティ（aim.com、aol.com など）のユーザ。
- ドメインが AOL によってホストされている企業のユーザ。
- AOL とフェデレーションを行っている外部企業のユーザ。IM and Presence サービスでは、こうした外部企業とフェデレーションを行う際、AOL をクリアリング ハウスとして使用することもできます。

IM and Presence サービスでは、以下とのフェデレーションに対しては、Extensible Messaging and Presence Protocol（XMPP）が使用されます。

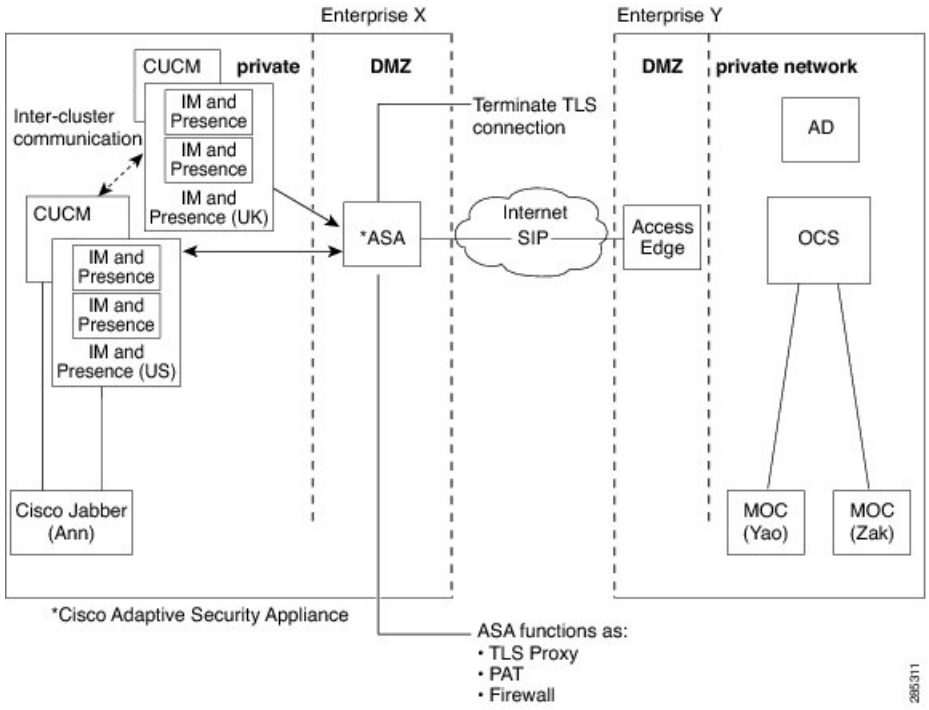
- IBM Sametime Server 8.2 および 8.5
- Cisco Webex Connect リリース 6
- Cisco Unified Presence リリース 8.x
- XMPP 標準に準拠したその他のサーバ
- IM and Presence サービス は IM and Presence サービス リリース 9.0 Enterprise と Cisco Unified Presence リリース 7.0（.x）Enterprise 間のフェデレーションをサポートしていません。

（注） 外部ドメインを使用して、XMPP フェデレーションをイネーブルにする場合、外部ドメインが Cisco Unified Presence の SIP フェデレーション ドメインとして設定されていないことを確認します。

例： example.com の Cisco Unified Presence 配置は、SIP ベースのフェデレーションとして過去に設定されています。ただし、example.com では、XMPP サポートが追加されています。したがって、ローカル管理者は代わりに XMPP ベース フェデレーションを有効にしようとします。この機能を使用するには、ローカル管理者は Cisco Unified Presence で SIP フェデレーション ドメインとして example.com を削除する必要があります。

次の図は、IM and Presence サービスのエンタープライズ導入と Microsoft OCS のエンタープライズ導入との間の SIP フェデレーテッド ネットワークの具体例を示したものです。

図 *1*：*IM and Presence* サービスと *Microsoft OCS* の間の基本的な *SIP* フェデレーテッド ネットワーク

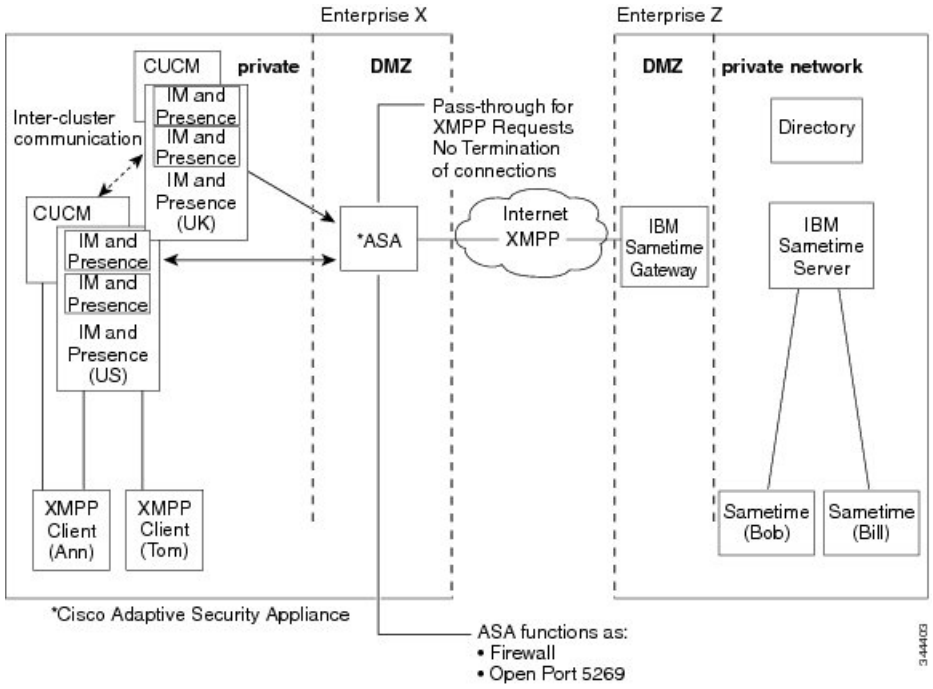


この図では、各内部企業ドメインがそれぞれの DMZ エッジ サーバとセキュアな TLS 接続を使用して、パブリック インターネット経由で相互接続されています。内部の IM and Presence サービスのエンタープライズ導入では、Cisco Adaptive Security Appliance（ASA）によってファイアウォール、ポート アドレス変換（PAT）、および TLS プロキシ機能が実現されています。Cisco Adaptive Security Appliance（ASA）では、外部ドメインからのすべての着信トラフィックが、指定された IM and Presence サービス ノードへルーティングされます。

次の図は、IM and Presence サービス のエンタープライズ展開と IBM Sametime のエンタープライズ展開との間の XMPP フェデレーテッド ネットワークの具体例を示したものです。XMPP フェデレーションでは、TLS はオプションです。XMPP フェデレーションの場合、Cisco Adaptive Security

Appliance（ASA）はファイアウォールとしてのみ機能し、TLS プロキシ機能や PAT を実行する役割は果たしません。

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



IM and Presence サービスの内部エンタープライズ導入には DNS サーバが 2 つ存在します。一方の DNS サーバは、IM and 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 サーバは、SIP フェデレーションに使用する IM and Presence サービスのパブリック アドレスと DNS SRV レコード（_sipfederationtls）、および IM and Presence サービスとの XMPP フェデレーションに使用する DNS SRV レコード（_xmpp-server）をホストします。IM and Presence サービスのパブリック アドレスをホストする DNS サーバは、ローカルの DMZ に配置します。

AOL との SIP フェデレーション

AOL フェデレーションを使用する場合の制限事項

AOL コミュニティ（aol.com、aim.com）のユーザは、既存の電子メール アドレスを AOL の画面名として使用することができます。既存の電子メールアドレスとは、`gmail.com`、`yahoo.com`、`msn.com` などの一般的な電子メール プロバイダで現在使用している電子メール アドレスのことです。このシナリオの場合、AOL では、これらのユーザに対して `user（gmail.com）@aol.com` などのアドレスを割り当てる際、マッピングされた JID が必要となります。また同様に AOL からは修正された JID が送信されます。

たとえば、AOL では次のようにして、画面名「user@gmail.com」を基にしたアドレスがユーザに割り当てられます。

```
SUBSCRIBE sip:user(gmail.com)@aol.com SIP/2.0From: sip:user@cisco.com;tag= To:
sip:user(gmail.com)@aol.com
```

AOL からは、このユーザの修正済み JID が送信されます。

```
SUBSCRIBE sip:user@cisco.com SIP/2.0From: sip:user(gmail.com)@aol.com;tag= To:
sip:user@cisco.com
```

AOL との SIP フェデレーションを導入する場合、IM and Presence サービスでは、画面名としてユーザ ID ではなく電子メール アドレスを使用するこのような AOL ユーザはサポートされません。

なお AOL のルーティングは OCS のルーティングとは異なり、SIP レコード ルートには従いません。AOL からのすべての要求は、それらが元々その他の IM and Presence サービス ノードから送信されたものであっても、ルーティング用の IM and Presence サービス ノードに送信されます。そのため、AOL フェデレーションを設定すると、OCS とのフェデレーションの場合に比べて、フェデレーションのルーティングを行う IM and Presence サービス サーバの負荷が大きくなる場合があります。

クラスタ間展開とマルチノード展開

（注） このマニュアルに記載されている IM and Presence サービスのクラスタ間配置に関連した設定手順はすべて、IM and Presence サービスのマルチノード配置にも適用することができます。

SIP フェデレーション導入

クラスタ間およびマルチノード クラスタの IM and Presence サービスの導入では、外部ドメインが新しいセッションを開始すると、Cisco Adaptive Security Appliance がすべてのメッセージをルーティング用に指定された IM and Presence サービス ノードにルーティングします。IM and Presence サービス ルーティング ノードが受信ユーザをホストしていない場合は、クラスタ間通信を介してクラスタ内の適切な IM and Presence サービス ノードにメッセージをルーティングします。システムは、ルーティング IM and Presence サービス ノードを介して、この要求に関連付けられたすべての応答をルーティングします。

IM and Presence サービス ノードは、Cisco Adaptive Security Appliance を介して外部ドメインへメッセージを送信します。OCS では、これらのメッセージに対して外部ドメインから応答があると、Cisco Adaptive Security Appliance を介してメッセージを送信した IM and Presence サービス ノードにその応答が直接返送されます。この動作は、Cisco Adaptive Security Appliance 上でポート アドレス変換（PAT）を設定すると有効になります。ただし、AOL フェデレーション用の場合、すべての応答が IM and Presence サービス ルーティング ノードにルーティングされます。200 OK 応答メッセージに対しては PAT が必要となるため、Cisco Adaptive Security Appliance 上で PAT を設定することを推奨します。

関連トピック

ポート アドレス変換（PAT），（80 ページ）

XMPP フェデレーション導入

単一のクラスタの場合、クラスタ内の 1 ノードでのみ XMPP フェデレーションをイネーブルにする必要があります。パブリック DNS では、そのエンタープライズに対してただ 1 つの DNS SRV レコードがパブリッシュされます。この DNS SRV レコードは、XMPP フェデレーションが有効な IM and Presence サービス ノードにマッピングされます。外部ドメインからの着信要求はすべて、パブリッシュされた SRV レコードに基づいて、XMPP フェデレーションが実行されているノードにルーティングされます。これらの要求は、内部的には IM and Presence サービスにより、各ユーザにとって適切なノードにルーティングされます。また、IM and Presence サービスは、XMPP フェデレーションを実行するノードを通じてすべての発信要求をルーティングします。

（規模を拡大する場合や、）複数の IM and Presence サービス クラスタをパブリッシュしたのに伴って XMPP フェデレーションを各クラスタにつき少なくとも 1 つずつ有効にする必要がある場合などには、複数の DNS SRV レコードをパブリッシュすることもできます。XMPP フェデレーションでは、SIP フェデレーションとは異なり、IM and Presence サービス が配置された企業ドメインに対してエントリ ポイントがただ 1 つである必要はありません。そのため IM and Presence サービスでは、パブリッシュされているノードのうち XMPP フェデレーションが有効であるいずれのノードに対しても、着信要求をルーティングすることができます。

クラスタ間およびマルチノード クラスタ IM and Presence サービス展開では、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、要求をルーティングする場所を設定するために DNS SRV ルックアップが実行されます。複数の DNS SRV レコードをパブリッシュした場合、DNS ルックアップでは複数の結果が返されます。IM and Presence サービスでは、DNS でパブリッシュされたいずれのサーバへも、要求をルーティングすることができます。これらの要求は、内部的には IM and Presence サービスにより、各ユーザにとって適切なノードにルーティングされます。IM and Presence サービスでは、発信要求は、XMPP フェデレーションが実行されているクラスタ内のいずれかのノードを経由してルーティングされます。

XMPP フェデレーションを実行しているノードが複数ある場合は、パブリック DNS 内でパブリッシュするノードを 1 つだけ選択することもできます。この設定の場合、XMPP フェデレーションを実行しているノード全体に着信要求がロード バランシングされるのではなく、IM and Presence サービスからその単一ノードを介してすべての着信要求がルーティングされます。IM and Presence サービス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。

ハイ アベイラビリティとフェデレーション

SIP フェデレーションのハイ アベイラビリティ

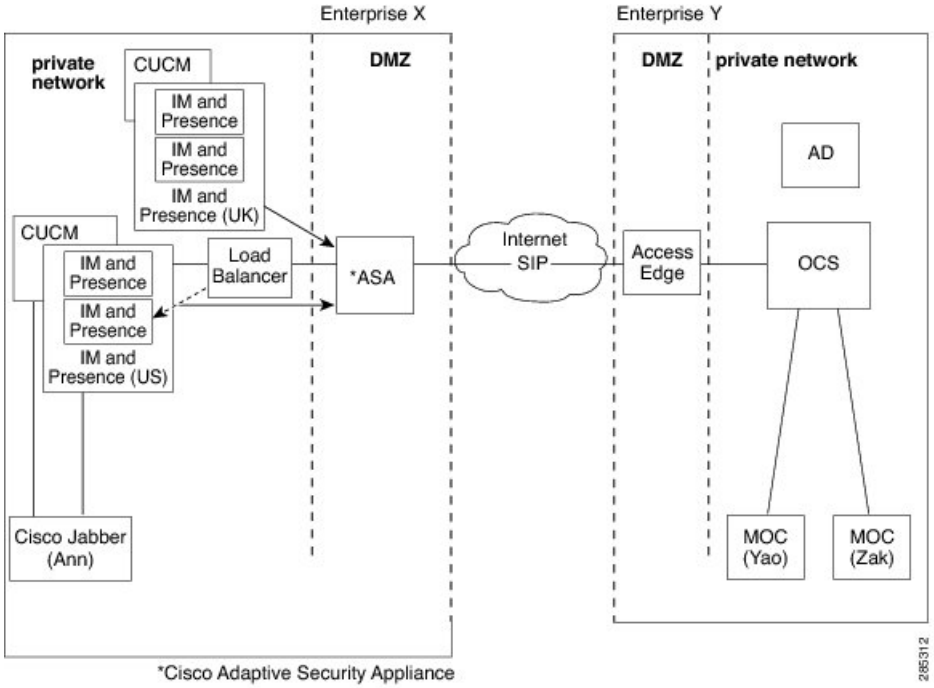
（注） ハイ アベイラビリティは、IM and Presence サービス リリース 8.5 以降でのみサポートされています。

Microsoft OCS の企業とフェデレーションを行う場合、Microsoft の Access Edge サーバでは、ホスト名とサーバ アドレスをそれぞれ 1 つだけ返す DNS SRV ルックアップしか実行できません。また Microsoft の Access Edge サーバでは、手動でプロビジョニングできる IP アドレスは 1 つだけです。

そのため、Microsoft OCS とのフェデレーションにおいてハイ アベイラビリティを実現するためには、以下の図のように IM and Presence サービス ノードと Cisco Adaptive Security Appliance との間にロードバランサを配置する必要があります。ロードバランサは、Cisco Adaptive Security Appliance からの着信 TLS 接続を終端したうえで、TLS 接続を新たに開始して適切なバックエンド IM and Presence サービス サーバへデータをルーティングします。

同様に、AOL とのフェデレーションにおいてハイ アベイラビリティを実現するためには、以下の図のように IM and Presence サービス ノードと Cisco Adaptive Security Appliance との間にロード バランサを配置する必要があります。

図 *3*：ハイ アベイラビリティのある *IM and Presence* サービスと *Microsoft OCS* との間のフェデレーテッド ネットワーク



関連トピック

冗長性確保のためのロード バランサの設定（SIP フェデレーションの場合），（129 ページ）

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 アベイラビリティには、IM and Presence サービスのその他の機能に対するハイ アベイラビリティとは異なる点があります。それは 2 ノード サブクラスタ モデルには限定されないという点です。

XMPP フェデレーションに対してハイ アベイラビリティを実現するためには、クラスタ内の 2 つ以上の IM and Presence ノードに対して XMPP フェデレーションを有効にする必要があります。複数のノードに対して XMPP フェデレーションを有効にすることで、規模が拡大されるだけでなく、いずれかのノードに障害が発生したときのための冗長性が確保されます。

発信要求のルーティングに対するハイ アベイラビリティ

IM and Presence サービスでは、クラスタ内部のユーザからの発信要求について、XMPP フェデレーションが有効になっているクラスタ内のすべてのノードに対して均等にロードバランシングが行

われます。いずれかのノードで障害が発生すると、発信トラフィックは IM and Presence サービスによって、クラスタ内に存在する残りのアクティブ ノード全体に動的に分散されます。

着信要求のルーティングに対するハイ アベイラビリティ

着信要求のルーティングに対してハイ アベイラビリティを実現するためには、さらなる対処が必要です。IM and Presence サービスのローカル配置を外部ドメインから検出できるようにするためには、パブリック DNS サーバ上で DNS SRV レコードをパブリッシュする必要があります。このレコードから、XMPP フェデレーションの有効なノードが解決されます。外部ドメインは、解決されたそのアドレスに接続します。

このモデルでハイ アベイラビリティを実現するためには、IM and Presence サービスのローカル配置に対して複数の DNS SRV レコードをパブリッシュする必要があります。これらの各レコードは、IM and Presence サービスのローカル配置内のノードのうち XMPP フェデレーションの有効なノードに解決されます。

ローカル配置に対する DNS SRV レコードは、これらのレコードの中から選択されます。XMPP フェデレーションが有効になっているノードに障害が発生した場合、外部システムは別のノードを選択し、そのノードから IM and Presence サービスのローカル配置に接続することになります。

（注）

- パブリッシュされた DNS SRV レコードの優先度および重み付けはすべて同じであることが必要です。これにより、すべての公開されたレコード間で負荷を分散させることができます。また、外部システムが正しく障害時に DNS SRV レコードと他のノードの 1 個に再接続できます。
- 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すべてのノードに対してパブリッシュできるほか、その一部に対してのみパブリッシュすることもできます。パブリッシュされたレコードの数が多いほど、着信要求の処理に関するシステムの冗長性は高くなります。
- XMPP フェデレーション配置の IM and Presence サービス ノード上でチャット機能を設定した場合は、チャット ノード エイリアスに対して複数の DNS SRV レコードをパブリッシュできます。これにより外部システムでは、XMPP フェデレーションが有効ないずれかのノードで障害が発生した場合に、XMPP フェデレーションが有効な他のノードを経由してその特定のチャット ノードに達する別の着信ルートを検索することができます。ただし、これはチャット機能そのものに対するハイ アベイラビリティではなく、チャット ノード エイリアス宛ての着信要求に対する XMPP フェデレーションのハイ アベイラビリティ機能を拡張したものです。

IBM Sametime フェデレーション

IM and Presence サービス リリース 9.0 では、IM and Presence サービスの企業と IBM Sametime の企業とのドメイン間フェデレーションに対するハイ アベイラビリティはサポートされていません。これは、IBM Sametime が DNS SRV ルックアップにより返された別のレコードに対して再試行を行わないためです。試行の対象となるのは最初に検出された DNS SRV レコードのみで、接続試行に失敗しても、重み付けの低いノードに対する再試行は行われません。

（注） IBM Sametime フェデレーション配置の IM and Presence サービスでも、状況によっては XMMP フェデレーションのハイ アベイラビリティが実現されているように見えることがあります。それは、重大なサービス障害に伴ってユーザがバックアップ ノードにフェールオーバーしても、プライマリ ノードでは引き続き Cisco XCP XMPP Federation Connection Manager が実行されているという状況です。この場合、着信トラフィックはこれまでどおりプライマリ ノードに転送され、その後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。そしてこのシナリオでは、XMPP フェデレーションは停止することなく、通常どおりの動作が続行されます。

関連トピック

XMPP フェデレーション用の DNS の設定，（144 ページ）
ノードで XMPP フェデレーションをオンにする，（142 ページ）

Cisco Adaptive Security Appliance（ASA）の配置オプション

IM and Presence サービスの内部エンタープライズ導入では、Cisco Adaptive Security Appliance（ASA）によってファイアウォール、ポート アドレス変換（PAT）、および TLS プロキシ機能が DMZ 内に実現されています。これにより、ハブリック インターネットからの着信接続を終端するとともに、特定のフェデレーテッド ドメインからのトラフィックを許可することができます。

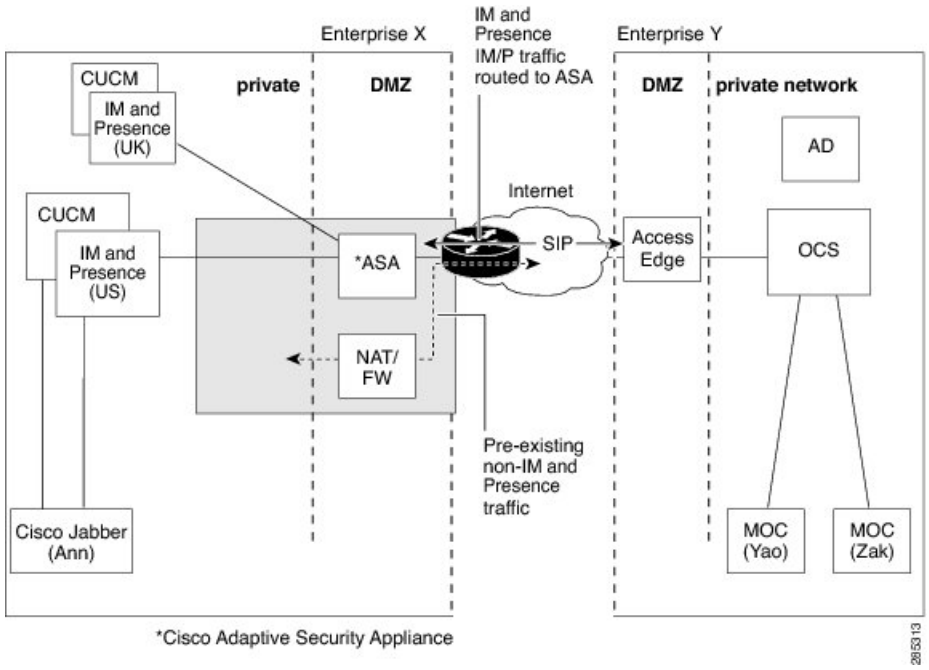
（注） XMPP フェデレーション配置の場合、Cisco Adaptive Security Appliance（ASA）によって実現されるのはファイアウォール機能だけです。すでにファイアウォールが配置されている場合は、XMPP フェデレーション用として Cisco Adaptive Security Appliance（ASA）を追加する必要ありません。

Cisco Adaptive Security Appliance（ASA）には、既存のネットワーク、および導入する必要があるファイアウォール機能の種類に応じて、さまざまな配置方法があります。ここでは、推奨される配置モデルの概要についてのみ説明します。詳細については、Cisco Adaptive Security Appliance（ASA）のマニュアルに記載されている展開に関するガイドラインを参照してください。ここで説明する Cisco Adaptive Security Appliance（ASA）の配置オプションは、SIP フェデレーションに適用されるものです。

Cisco Adaptive Security Appliance（ASA）は以下の 2 つの図のように、インスタント メッセージ（IM）のトラフィックやアベイラビリティのトラフィックなどさまざまなトラフィックを保護する企業ファイアウォールとして配置することができます。これはコスト効率が最も高く、新しいネットワークにも既存のネットワークにも推奨される配置方法です。また、Cisco Adaptive Security Appliance（ASA）を既存のファイアウォールと並行して配置することもできます（次の図を参照）。このように配置した場合、Cisco Adaptive Security Appliance（ASA）では、IM and Presence サービスとパブリック インターネットの間の IM and Presence サービス トラフィックが処理され、

既存のトラフィックにはそのまま既存のファイアウォールが使用されます。次の図では、配置された Cisco Adaptive Security Appliance（ASA）が IM and Presence サービス ノードに対するゲートウェイとしても機能しています。そのため、Cisco Adaptive Security Appliance（ASA）にトラフィックを転送するためのルートを別途用意する必要はありません。

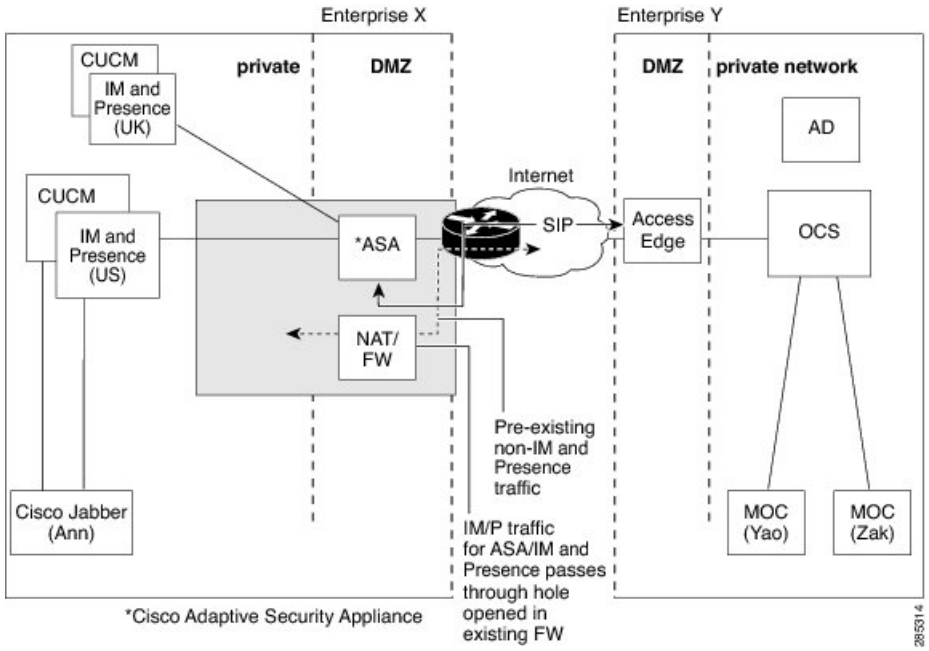
図 *4*：既存の *NAT/*ファイアウォールと並行して *Cisco ASA 5500* を配置する方法



既存のファイアウォールの背後に Cisco Adaptive Security Appliance（ASA）を配置することもできます。この場合は、IM and Presence サービス宛てのトラフィックが Cisco Adaptive Security Appliance（ASA）へ転送されるように既存のファイアウォールを設定します（次の図を参照）。このよう

に配置した場合、Cisco Adaptive Security Appliance（ASA）は IM and Presence サービス ノードに対するゲートウェアとして機能します。

図 *5*：既存の *NAT/*ファイアウォールの背後に *Cisco ASA 5500* を配置する方法



プレゼンス サブスクリプションとブロッキング レベル

x@externaldomain.com から user@local.com への新たなプレゼンス サブスクリプションはすべて、Cisco Adaptive Security Appliance により送信されます（以下の図を参照）。Cisco Adaptive Security Appliance では、許可されている外部ドメインのリストと着信 SIP サブスクリプションとの照合確認が行われます。許可されていないドメインのプレゼンス サブスクリプションは Cisco Adaptive Security Appliance により拒否されます。

（注） XMPP フェデレーションの導入の場合、Cisco Adaptive Security Appliance ではドメインの確認は行われません。

IM and Presence サービスでは、着信サブスクリプションを受信すると、その外部ドメインが許可フェデレーテッド ドメインに該当するかどうか検証が行われます。許可フェデレーテッド ドメインは IM and Presence サービス ノードにおいて管理レベルで定義します。SIP フェデレーションの場合は、フェデレーテッド ドメインを設定します。XMPP フェデレーションの場合は、XMPP フェデレーションに関する管理者ポリシーを定義します。許可ドメイン以外から受信したサブスクリプションは、IM and Presence サービスにより（ローカル ユーザに通知されることなく）拒否されます。

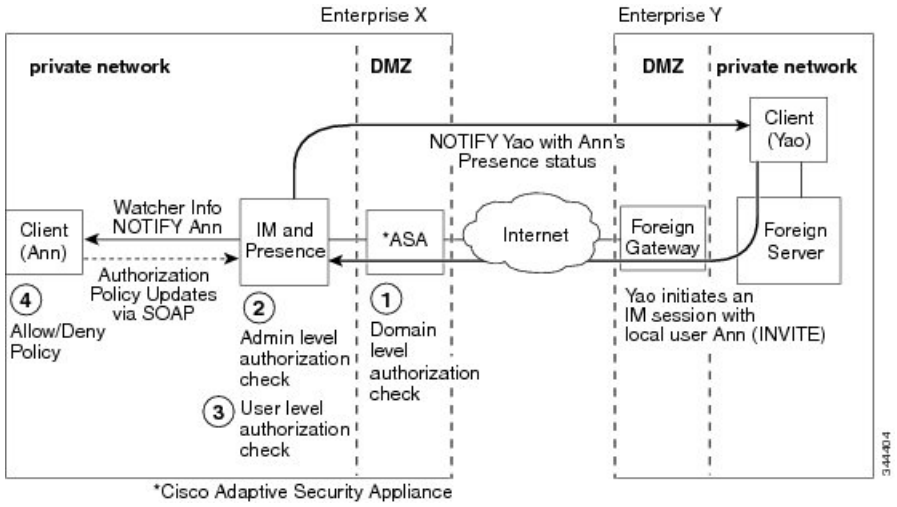
許可ドメインからサブスクリプションを受信した場合、IM and Presence サービスではローカル ユーザの承認ポリシーが確認された後、そのローカル ユーザが過去にフェデレーテッド ドメイン、またはプレゼンス サブスクリプションの送信ユーザをブロックまたは許可したことがあるかどうか検証が行われます。IM and Presence サービスは着信登録を承認し、それを保留中にします。

ここで、x@externaldomain.comからプレゼンスの閲覧要求があることをローカル ユーザに通知するため、IM and Presence サービスからクライアント アプリケーションに対してサブスクリプションに関する通知メッセージが送信されます。これを受けてクライアント アプリケーションには、ローカル ユーザがサブスクリプションを許可または拒否することができるダイアログ ボックスが表示されます。ユーザが承認または拒否の決定を下すと、クライアント アプリケーションから IM and Presence サービスに対してその決定内容が通知されます。承認または拒否の決定は、IM and Presence サービスに保存されているユーザのポリシー リストに追加されます。

拒否の決定が下されると、ポライト ブロッキングの措置が取られます。この場合、その外部クライアントに対してユーザのプレゼンス ステータスが「オフライン」と表示されます。ローカル ユーザがサブスクリプションを許可した場合は、IM and Presence サービスから外部ウォッチャに最新のプレゼンス情報が送信されます。

ユーザは、サブスクリプションをユーザ単位およびドメイン単位でブロックすることもできます。これは、Cisco Jabber クライアントで設定できます。

図 *6*：着信 *SIP* プレゼンス メッセージのフロー

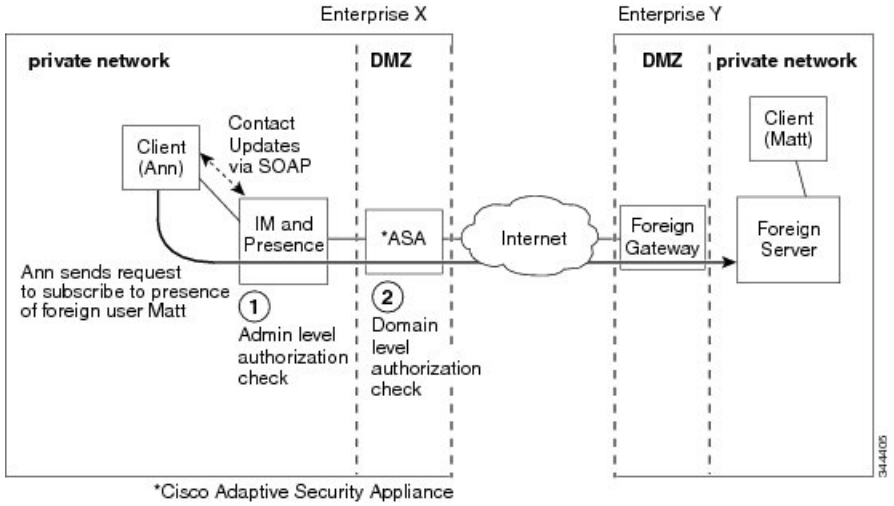


IM and Presence サービス は Cisco Adaptive Security Appliance を通じてすべての発信サブスクリプションを送信し、Cisco Adaptive Security Appliance はこれらのサブスクリプションを外部ドメインに転送します。その外部ドメインの同じ外部ユーザと、別のローカル ユーザとの間にアクティブなサブスクリプションがすでに存在する場合でも、IM and Presence サービスからは発信サブスクリプションが送信されます。次の図は、発信プレゼンス サブスクリプションのフローを図示したものです。

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

（注） XMPP フェデレーションの場合、Cisco Adaptive Security Appliance でのドメイン レベル認証チェックは行われません。

図 7：発信プレゼンス要求のフロー



（注）
- Microsoft OCS では、サブスクライブ更新が 1 時間 45 分間隔で実行されます。したがって、IM and Presence サービス ノードが再起動すると、Microsoft Office Communicator クライアントが IM and Presence サービスの連絡先のプレゼンス ステータスなしで存続する最大時間はおよそ 2 時間です。
- また Microsoft OCS が再起動した場合は、IM and Presence サービス クライアントで、Microsoft Office Communicator コンタクトのプレゼンス ステータスがない状態が最長で 2 時間前後続きます。

関連トピック

在席ステータスのマッピング，（15 ページ）
インスタント メッセージ，（21 ページ）

在席ステータスのマッピング

Microsoft OCS の在席ステータスのマッピング

次の表は、Microsoft Office Communicator から IM and Presence サービス、サードパーティの XMPP クライアント、および Cisco Jabber への在席ステータスのマッピング状況をまとめたものです。

表 *1*：*Microsoft Office Communicator* からのアベイラビリティ マッピング状態

Microsoft Office Communicator 設定	（IM and Presence サービスに接続された）サードパーティの XMPP クライアントでの設定	Cisco Jabber リリース 8.x での設定
応対可	応対可	応対可
ビジー	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
オフライン	オフライン	オフライン

この表の中で、Microsoft Office Communicator の「ビジー」および「サイレント」の各ステータスはいずれも「退席中」にマッピングされており、サードパーティの XMPP クライアントでは「ビジー」というステータスとして表されています。XMPP クライアントでは、この「退席中」ステータスの表示方法がそれぞれで異なります。たとえば、テキストのない「退席中」アイコンとして表示される XMPP クライアントもあれば、「ビジー」というテキストが付記された「退席中」アイコンとして表示される XMPP クライアントもあります。

次の表は、Cisco Jabber リリース 8.x から Microsoft Office Communicator に対する在席ステータスのマッピング状況を示したものです。

表 *2*：*Cisco Jabber* リリース *8.x* の在席ステータスのマッピング

Cisco Jabber リリース 8.x 設定	Microsoft Office Communicator 設定
応対可	応対可
ビジー	ビジー

Cisco Jabber リリース 8.x 設定	Microsoft Office Communicator 設定
サイレント	ビジー
オフライン	オフライン

次の表は、IM and Presence サービスに接続されたサードパーティの XMPP クライアントから Microsoft Office Communicator への在席ステータスのマッピング状況を示したものです。

表 *3*：サードパーティの *XMPP* クライアントの在席ステータスのマッピング

（IM and Presence サービスに接続された）サードパーティの XMPP クライアントでの設定	Microsoft Office Communicator 設定
応対可	応対可
退席中	退席中
退席中（延長）	退席中
サイレント	ビジー
オフライン	オフライン

関連トピック

プレゼンス サブスクリプションとブロッキング レベル，（12 ページ）

Microsoft Lync の在席ステータスのマッピング

次の表は、Microsoft Lync から IM and Presence サービス、サードパーティの XMPP クライアント、および Cisco Jabber への在席ステータスのマッピング状況をまとめたものです。

表 *4*：*Microsoft Lync* の在席ステータスのマッピング

Microsoft Lync 設定	（IM and Presence サービスに接続された）サードパーティの XMPP クライアントでの設定	Cisco Jabber リリース 8.x 設定
応対可	応対可	応対可
ビジー	退席中	ビジー

Microsoft Lync 設定	（IM and Presence サービスに接続された）サードパーティの XMPP クライアントでの設定	Cisco Jabber リリース 8.x 設定
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
オフライン	オフライン	オフライン

この表の中で、Lyncクライアントの「ビジー（Busy）」および「サイレント（Do Not Disturb）」の各ステータスはいずれも「退席中（Away）」にマッピングされており、サードパーティのXMPPクライアントでは「ビジー（Busy）」というステータスとして表されています。XMPP クライアントでは、この「退席中」ステータスの表示方法がそれぞれで異なります。たとえば、テキストのない「退席中」アイコンとして表示される XMPP クライアントもあれば、「ビジー」というテキストが付記された「退席中」アイコンとして表示される XMPP クライアントもあります。

次の表は、Cisco Jabber リリース 8.x から Lync クライアントへの在席ステータスのマッピング状況を示したものです。

表 *5*：*Cisco Jabber* リリース *8.x* の在席ステータスのマッピング

Cisco Jabber リリース 8.x 設定	Microsoft Lync 設定
応対可	応対可
ビジー	ビジー
サイレント	ビジー
オフライン	オフライン

次の表は、IM and Presence サービスに接続されたサードパーティの XMPP クライアントから Lync クライアントへの在席ステータスのマッピング状況を示したものです。

表 *6*：サードパーティの *XMPP* クライアントの在席ステータスのマッピング

（IM and Presence サービスに接続された）サードパーティの XMPP クライアントでの設定	Microsoft Lync 設定
応対可	応対可

（IM and Presence サービスに接続された）サードパーティの XMPP クライアントでの設定	Microsoft Lync 設定
退席中	退席中
退席中（延長）	退席中
サイレント	ビジー
オフライン	オフライン

関連トピック

プレゼンス サブスクリプションとブロッキング レベル, （12 ページ）

AOL Instant Messenger の在席ステータスのマッピング

次の表は、AOL Instant Messenger から Cisco Jabber への在席ステータスのマッピング状況を示したものです。

表 *7*：*AOL Instant Messenger* から *Cisco Jabber* への在席ステータスのマッピング

AOL Instant Messenger 設定	Cisco Jabber リリース 8.x 設定
応対可	応対可
退席中	退席中
非表示	オフライン
オフライン	オフライン

次の表は、Cisco Jabber から AOL Instant Messenger への在席ステータスのマッピング状況を示したものです。

表 *8*：*Cisco Jabber* から *AOL Instant Messenger* への在席ステータスのマッピング

Cisco Jabber リリース 8.x での設定	AOL Instant Messenger
応対可	応対可
サイレント	退席中

Cisco Jabber リリース 8.x での設定	AOL Instant Messenger
ビジー	退席中
アイドル	退席中
オフライン	オフライン

関連トピック

プレゼンス サブスクリプションとブロッキング レベル, （12 ページ）

XMPP フェデレーションの在席ステータスのマッピング

次の表は、IBM Sametime 8.2 から IM and Presence サービス上のサードパーティの XMPP クライアント、および Cisco Jabber への在席ステータスのマッピング状況を示したものです。

表 *9*：*IBM Sametime 8.2* クライアントの在席ステータスのマッピング

IBM Sametime クライアントでの設定	（IM and Presence サービスに接続された）サードパーティの XMPP クライアントでの設定	Cisco Jabber リリース 8.x での設定
応対可	応対可	ステータス メッセージで使用可能
サイレント	サイレント	ステータス メッセージでのサイレント
連絡可能（「“会議中”」ステータスも表示）	連絡可能（「“会議中”」ステータスも表示）	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も表示）
オフライン	オフライン	オフライン

次の表は、webex Connect から IM and Presence サービス上のサードパーティの XMPP クライアント、および Cisco Jabber への在席ステータスのマッピング状況を示したものです。

表 *10*：*Webex Connect* の在席ステータスのマッピング

Webex Connect での設定	（IM and Presence サービスに接続された）サードパーティの XMPP クライアントでの設定	Cisco Jabber リリース 8.x での設定
応対可	応対可	応対可
サイレント	サイレント	サイレント
応答可能（「“会議中”」ステータスも表示）	連絡可能（「“会議中”」ステータスも表示）	応答可能（「“会議中”」ステータスも表示）
退席中	退席中	退席中
オフライン	オフライン	オフライン

次の表は、Cisco Jabber リリース 8.x からフェデレーションが有効な他のクライアントへの在席ステータスのマッピング状況を示したものです。

表 *11*：*Cisco Jabber* リリース *8.x* の在席ステータスのマッピング

Cisco Jabber リリース 8.x での設定	フェデレーションが有効な Cisco Jabber リリース 8.x での設定	フェデレーションが有効な（IM and Presence サービスに接続されている）サードパーティの XMPP クライアントでの設定	Webex Connect クライアントでの設定	IBM Sametime クライアント サーバ
応対可	応対可	応対可	応対可	応対可
サイレント	サイレント	サイレント	サイレント	サイレント
ビジー	ビジー	退席中	アイドル	退席中
アイドル	アイドル	アイドル	アイドル	アイドル
オフライン	オフライン	オフライン	オフライン	オフライン

次の表は、IM and Presence サービス上のサードパーティの XMPP クライアントからフェデレーションが有効な他のクライアントへの在席ステータスのマッピング状況を示したものです。

表 *12* : *IM and Presence* サービスに接続されている *XMPP* クライアントの在席ステータスのマッピング

（IM and Presence サービスに接続された）サードパーティの XMPP クライアントでの設定	フェデレーションが有効な Cisco Jabber リリース 8.x での設定	フェデレーションが有効な（IM and Presence サービスに接続されている）XMPP クライアントでの設定	Webex Connect クライアントでの設定	IBM Sametime クライアント サーバ
応対可	応対可	応対可	応対可	応対可
サイレント	サイレント	サイレント	サイレント	サイレント
退席中	退席中	退席中	退席中	退席中
退席中（延長）	退席中	退席中（延長）	退席中（延長）	退席中
退席中（「“アイドル”」ステータスも表示）	アイドル	退席中（「“アイドル”」ステータスも表示）	退席中（「“アイドル”」ステータスも表示）	退席中（「“アイドル”」ステータスも表示）
オフライン	オフライン	オフライン	オフライン	オフライン

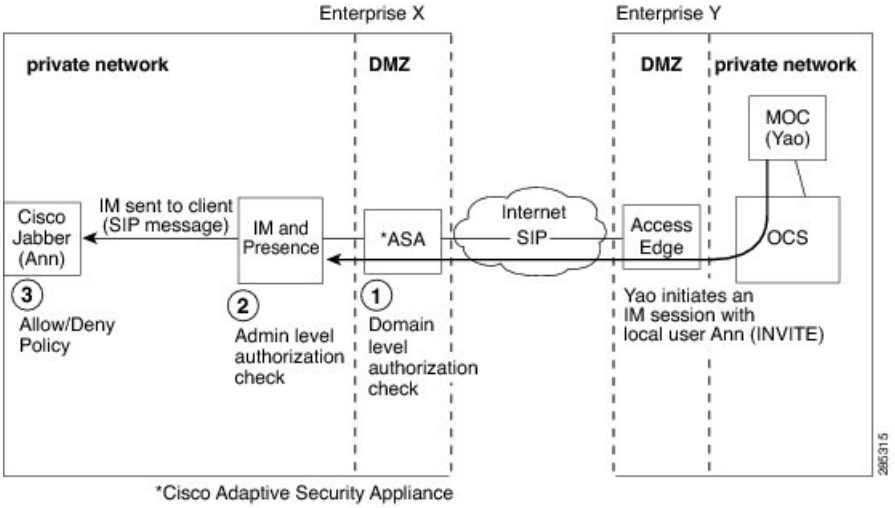
インスタント メッセージ

SIP フェデレーションに関するインスタント メッセージのフロー

2 つのエンタープライズ導入間でインスタント メッセージ（IM）を送信する場合には、セッション モードが使用されます。外部ドメインのユーザが IM and Presence サービス ドメインのローカル ユーザへ IM を送信するとき、外部サーバは次の図のように INVITE メッセージを送信します。この INVITE メッセージは、Cisco Adaptive Security Appliance によって IM and Presence サービスに転送されます。IM and Presence サービスでは外部サーバに対し 200 OK メッセージが返信され、外部サーバからはテキスト データを含む SIP メッセージが送信されます。IM and Presence サービス

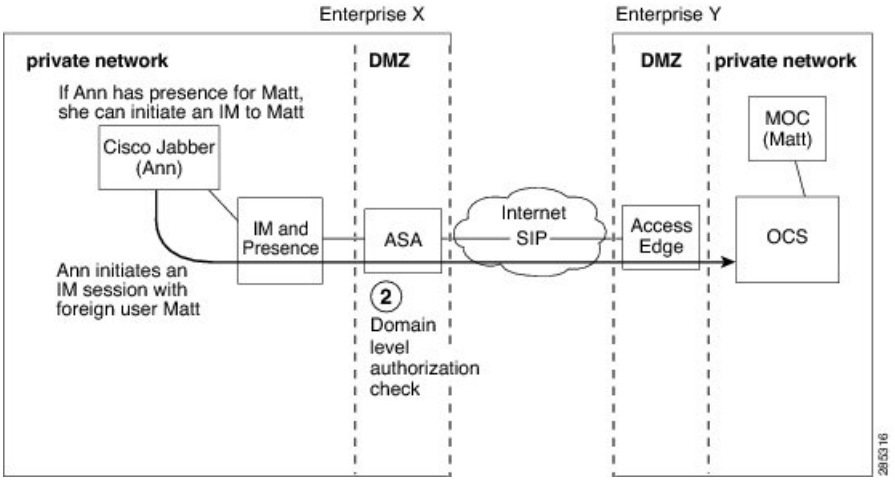
では、適切なプロトコルを使用して、ローカルユーザのクライアントアプリケーションにそのテキスト データが転送されます。

図 *8*：着信インスタント メッセージのフロー



IM and Presence サービス ドメインのローカル ユーザが外部ドメインのユーザに IM を送信する場合、その IM は IM and Presence サービス ノードへ送信されます。これらの 2 つのユーザ間にまだ既存の IM セッションが確立されていない場合は、新しいセッションを確立するために IM and Presence サービスから外部ドメインに INVITE メッセージが送信されます。IM and Presence サービスでは、これ以降両ユーザから送信されるメッセージ トラフィックはいずれも、このセッションを使用して処理されます。ただし、Cisco Jabber およびサードパーティの XMPP クライアントについては、利用可能でない場合でもユーザは IM を開始することができます。

図 *9*：発信インスタント メッセージのフロー



（注） IM and Presence サービスでは、Microsoft OCS コンタクトを使用した 3 者間 IM セッション（グループ チャット）はサポートされていません。

関連トピック

プレゼンス サブスクリプションとブロッキング レベル, （12 ページ）

XMPP フェデレーションに関する在席情報およびインスタント メッセージのフロー

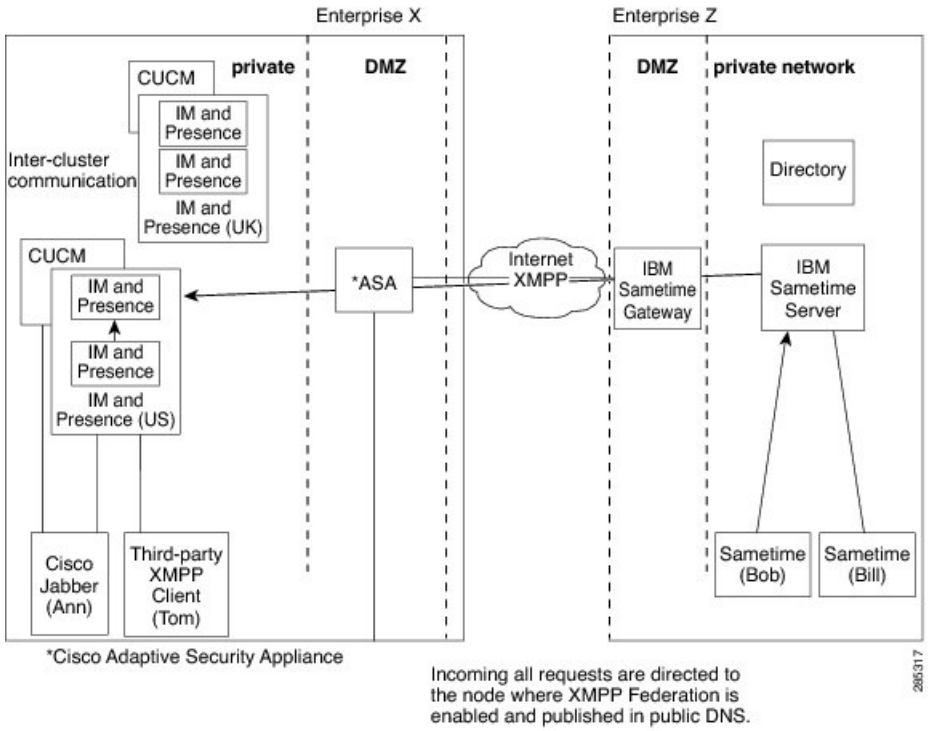
XMPP フェデレーションの着信/発信のアベイラビリティと IM 要求のフローは、IM and Presence サービスのマルチノード配置で違いがあります。

マルチノード配置では、クラスタ内の各ノードで XMPP フェデレーションを有効にできるほか、クラスタ内のいずれか 1 つのノードでのみ XMPP フェデレーションを有効にすることも可能です。さらに DNS SRV レコードについても、いずれか 1 つだけをパブリッシュすることも、複数のレコード（ただし XMPP フェデレーションを有効にしたノードごとに 1 つずつ）をパブリッシュすることもできます。

DNS SRV レコードを 1 つだけパブリッシュした場合は、そのレコードに対応するただ 1 つのノードにすべての着信要求がルーティングされ、内部的には IM and Presence サービスによりクラスタ間ルーティングを使用して正しいノードにトラフィックがルーティングされます（次の図を参

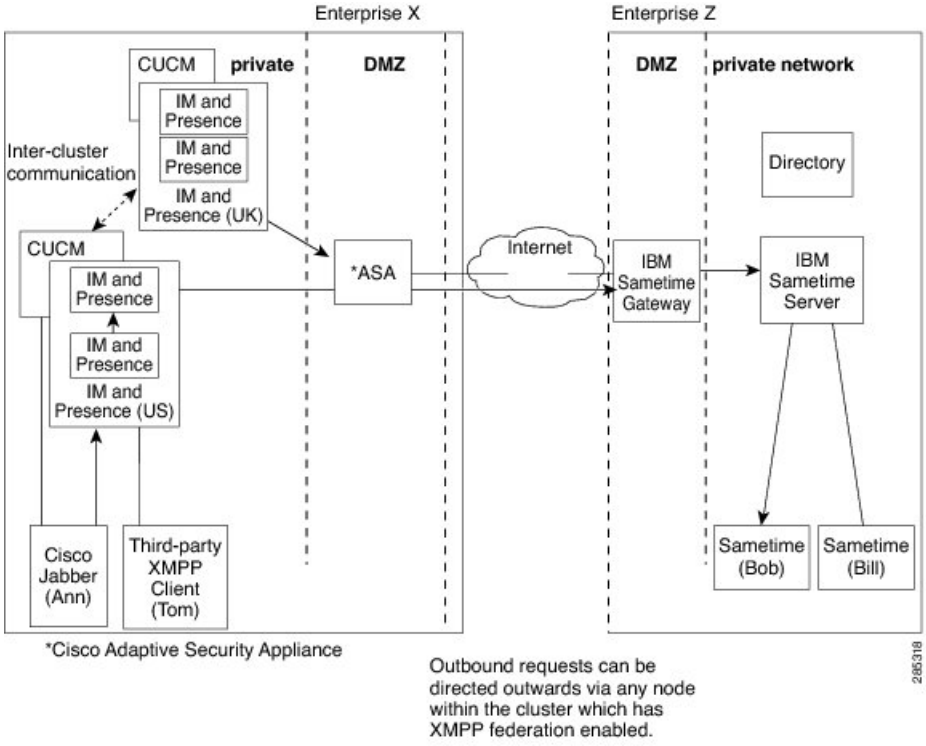
照）。複数のDNS SRV レコードをパブリッシュした場合は、SRV レコードの設定方法に応じて、各ノードに対して着信要求のロードバランシングが行われます。

図 *10*：*XMPP* 着信要求のフロー



発信要求については、IM and Presence サービスから、XMPP フェデレーションが有効なクラスタ内のいずれのノードにもルーティングされます。そのノードは、要求を送信したユーザのホームノードである必要はありません。

図 *11* : *XMPP* 発信要求のフロー



関連トピック

XMPP フェデレーションのハイ アベイラビリティ, （8 ページ）

複数のドメインとのフェデレーション導入

リモート ドメインが IM and Presence サービス ローカル導入で管理されないとき、フェデレーションは複数ドメインのある IM and Presence サービス導入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の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は、cup-xmpp セキュリティ証明書でサブジェクト代替名としてすべてのローカル ドメインが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

IM and Presence サービスは次のサブドメインのシナリオをサポートします。

- IM and Presence サービスは、外部ドメインのサブドメインに属します。たとえば、IM and Presence サービスはサブドメイン「imp.cisco.com」に属します。IM and Presence サービスでは、ドメイン「cisco.com」に属する外部企業とフェデレーションできます。この場合、IM and Presence サービス ユーザには「impuser@imp.cisco.com」という URI に割り当てられ、外部ユーザには「foreignuser@cisco.com」という URI が割り当てられます。
- IM and Presence サービスは親ドメイに属し、外部企業はその親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 サービスはドメイン「cisco.com」に属します。IM and Presence サービスでは、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できます。この場合、IM and Presence サービス ユーザには「impuser@cisco.com」という URI に割り当てられ、外部ユーザには「foreignuser@foreign.cisco.com」という URI が割り当てられます。
- IM and Presence サービスと外部企業は、それぞれ別々のサブドメインに属していますが、どちらのサブドメインも親ドメインは同じです。たとえば、IM and Presence サービスは「cup.cisco.com」というサブドメイン、外部企業は「foreign.cisco.com」というサブドメインに属しています。また、どちらのサブドメインも「cisco.com」という親ドメインに属しています。この場合、IM and Presence サービス ユーザには「impuser@cisco.com」という URI に割り当てられ、外部ユーザには「foreignuser@foreign.cisco.com」という URI が割り当てられます。

サブドメインとフェデレーションを行う場合は、DNS ドメインを別途設定するだけで十分です。Active Directory を分割する必要はありません。企業内部でフェデレーションを設定する場合、IM and Presence サービス ユーザまたは外部ユーザを同じ Active Directory ドメインに所属させることができます。たとえば上記 3 番目のシナリオの場合、Active Directory が親ドメイン「cisco.com」に属すことができます。各ユーザは「imp.cisco.com」と「foreign.cisco.com」のどちらかのサブドメインに所属し、かつ「impuser@cup.cisco.com」と「foreignuser@foreign.cisco.com」のどちらかの URI を割り当てられていますが、このような場合でもすべてのユーザを「cisco.com」ドメイン配下の Active Directory に設定することが可能です。

ただし、Cisco Jabber から LDAP 検索を実行すると、他のドメインまたはサブドメインのユーザが返される場合がありますが、Cisco Jabber ユーザが Cisco Jabber での LDAP ルックアップからこれらのフェデレーション ユーザを追加することはできません。Cisco Jabber ユーザは、これらのユーザを外部（フェデレーション）コンタクトとして追加する必要があります。これにより IM and Presence サービスでは、ローカル ドメインではなく正しいドメインが適用されます。

（注） IM and Presence サービスでは、IM and Presence サービスの 2 つのエンタープライズ導入の間にフェデレーションを設定する場合にも、上記のシナリオがサポートされています。

第 2 章

この統合のための準備

サポートされているドメイン間フェデレーションの統合

このマニュアルでは、IM and Presence サービスと外部ドメイン間にフェデレーテッド 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 サービス ノードがフェデレーション可能な、サポートされた外部ドメインは次のとおりです。

- Microsoft Office Communications Server リリース 2007、R2、Microsoft Lync 2010（SIP 経由）

（注） IM and Presence サービス リリース 9.0 では、Microsoft Lync とのドメイン間フェデレーションがサポートされています。OCS とのドメイン間フェデレーションへの参照には、別途明示的な指定がない限り、Microsoft Lync が指定されます。

- AOL（SIP 経由）
- Cisco Webex Connect リリース 6.x（XMPP 経由）
- IBM Sametime Server リリース 8.2、8.5（XMPP 経由）
- Cisco Unified Presence リリース 8.x（XMPP 経由）
- IM and Presence サービス リリース 9.x 以降（XMPP 経由）

（注） それぞれ IM and Presence サービスが導入されている 2 つのエンタープライズ間にフェデレーションを設定する場合は、XMPP フェデレーションの設定方法について記載されている手順に従ってください。

関連トピック

ハードウェア要件, （28 ページ）
ソフトウェア要件, （29 ページ）

Presence Web Service の API サポート

オープン インターフェイスである Presence Web Service を使用すると、クライアント アプリケーションはユーザ プレゼンス情報を IM and Presence サービスと共有できます。サードパーティ開発者は、このインターフェイスを使用して、ユーザのプレゼンス状態に関する更新を送信および取得するクライアント アプリケーションを構築できます。Presence Web Service の API サポートについて、次の制限事項に注意してください。

- SIP を使用したドメイン間フェデレーションでは、Presence Web Service の API を使用し、シスコ以外のクライアントから多くのプレゼンス情報を取得することができます。ただし、シスコ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ません。
- XMPP を使用したドメイン間フェデレーションでは、Presence Web Service の 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の『*IM and Presence Service Developer Guide*』を参照してください。

ハードウェア要件

シスコ ハードウェア

- IM and Presence サービス ノード。IM and Presence サービス ハードウェア サポートについては、IM and Presence サービス互換性マトリクスを参照してください。
- Cisco Unified Communications Manager のノード。Cisco Unified Communications Manager のハードウェア サポートについては、Cisco Unified Communications Manager の互換性マトリクスを参照してください。
- IM and Presence サービスの企業内の 2 つの DNS サーバ
- Cisco Adaptive Security Appliance（ASA）5500 シリーズ

- SIP フェデレーションの場合のみ、TLS プロキシ機能を実現できる Cisco Adaptive Security Appliance（ASA）の使用を推奨します。XMPP フェデレーションの場合は、いずれのファイアウォールでも十分です。
- Cisco Adaptive Security Appliance（ASA）モデルを選択する場合は、http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_models_home.html にアクセスしてください。TLS プロキシコンポーネントは、すべての 5500 モデルで使用可能です。
- 必ず目的の配置に適したバージョンの Cisco Adaptive Security Appliance（ASA）ソフトウェアを使用してください。ドメイン間フェデレーションを新たに設定する場合は、IM and Presence サービスの互換性マトリクスで、Cisco Adaptive Security Appliance（ASA）ソフトウェアの適切なバージョンを確認してください。

関連トピック

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html
ソフトウェア要件，（29 ページ）

ソフトウェア要件

シスコ ソフトウェア

- IM and Presence サービス リリース 9.0
- Cisco Unified Communications Manager Server リリース 9.0
- Cisco Adaptive Security Appliance v8.3(1)
- Cisco Adaptive Security Device Manager（ASDM）v6.3
- サポートされている XMPP クライアント：
  - Cisco Unified Personal Communicator リリース 8.5
  - Cisco Jabber for Mac
  - Cisco Jabber for Windows
  - モバイル向け Cisco Jabber IM（Cisco Jabber IM for iPhone、Android、Blackberry）
  - Cisco Jabber for iPad
  - Cisco Jabber for Cius

Microsoft の SIP フェデレーション用ソフトウェア

- Microsoft Lync 2010
- Microsoft OCS 2007 リリース 2 Server Standard または Enterprise
- Microsoft Office Communicator 2007 リリース 2

- Microsoft Active Directory

AOL の SIP フェデレーション用ソフトウェア

- AOL SIP Access Gateway（SAG）
- AOL Instant Messenger リリース 7.2.6.1 以降

XMPP フェデレーション用ソフトウェア

- Cisco Webex Connect リリース 6.x
- IBM Sametime Server リリース 8.2

関連項目

ハードウェア要件, （28 ページ）

統合の準備

この統合については、綿密な計画を立てることが重要です。この統合に関する設定を開始する前に、以下の各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 ネットワークでのルーティングをどのように設定するかを考えます。まず外部ドメイン宛てのメッセージを、IM and Presence サービス から Cisco Adaptive Security Appliance を経由して外部ドメインにルーティングする方法について考える必要があります。その 1 つの選択肢として、IM and Presence サービスのエンタープライズ導入と Cisco Adaptive Security Appliance との間に、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）を導入するという方法があります。この場合、メッセージはルーティング エンティティから Cisco Adaptive Security Appliance にルーティングされ、さらに Cisco Adaptive Security Appliance から外部ドメインにルーティングされます。

一方、IM and Presence サービスと外部ドメインとの間に Cisco Adaptive Security Appliance をゲートウェイとして導入することもできます。Cisco Adaptive Security Appliance をローカルのエンタープライズ導入内の IM and Presence サービスのゲートウェイとして使用する場合は、Cisco Unified Communications Manager と IM and Presence サービス クライアントが IM and Presence サービス ノードにどのようにアクセスするかを考慮する必要があります。Cisco Unified Communications Manager と IM and Presence サービス クライアントが IM and Presence サービスとは異なるサブネットにある場合、それらは Cisco Adaptive Security Appliance を使用して IM and Presence サービス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 Adaptive Security Appliance を導入する場合は、Cisco Adaptive Security Applianceおよび IM and Presence サービスにトラフィックをルーティングする方法について考慮します。既存のファイアウォール上では、IM and Presence サービスの

パブリックアドレスにトラフィックをルーティングするための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も設定する必要があります。

関連トピック

Cisco Adaptive Security Appliance（ASA）の配置オプション，（10 ページ）
SIP フェデレーションに関する Cisco Adaptive Security Appliance（ASA）の設定，（77 ページ）

パブリック IP アドレス

SIP フェデレーションの場合、IM and Presence サービスのパブリック アドレスとして、パブリックにアクセスできるIPアドレスが必要です。割り当てることができるIPアドレスがない場合は、Cisco Adaptive Security Appliance の外部インターフェイスを IM and Presence サービス アドレスのパブリック アドレスとして使用します（Cisco Adaptive Security Appliance を在席情報および IM トラフィック用としてのみ使用している場合）。

Microsoft OCS R2 との SIP フェデレーションでは、複数の IM and Presence サービス ノードを導入する場合でも、必要となるパブリック IP アドレスは 1 つだけです。Cisco Adaptive Security Appliance では、ポート アドレス変換（PAT）を使用して、OCS から適切な IM and Presence サービス ノードへ要求がルーティングされます。

XMPP フェデレーションの場合は、XMPP フェデレーションを有効にした IM and Presence サービス ノードごとにパブリック IP アドレスを公開するか、ただ 1 つのパブリック IP アドレスを公開するかを選択することができます。

- 複数の IP アドレスを公開する場合は、Cisco Adaptive Security Appliance 上で 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 を使用すると、x.x.x.x:5269 および y.y.y.y:5269 というパブリック アドレスをそれぞれ、a.a.a.a:5269 および b.b.b.b:5269 というプライベート アドレスに変換できます。
- 1 つのパブリック IP アドレスを公開する場合は、Cisco Adaptive Security Appliance 上で PAT を使用して、正しい IM and Presence サービス ノードにマッピングします。たとえば、使用するパブリック IP アドレスが x.x.x.x で、かつ _xmpp-server の DNS SRV レコードが複数あるとします。各レコードのポートはそれぞれ異なりますが、レコードはすべて x.x.x.x に解決されます。そして外部サーバからは、Cisco Adaptive Security Appliance を経由して x.x.x.x:5269、x.x.x.x:15269、x.x.x.x.25269 に要求が送信されるとします。この場合、Cisco Adaptive Security Appliance では、それらの IP アドレスを対象に PAT が実行されます。これにより、それぞれのアドレスは、対応する各 IM and Presence サービス ノードの内部 IP アドレスにマッピングされます。

  たとえば、パブリック IP アドレス x.x.x.x:5269 は a.a.a.a:5269 というプライベート IP アドレス、パブリック IP アドレス x.x.x.x:15269 は b.b.b.b.b:5269 というプライベート IP アドレス、パブリック IP アドレス x.x.x.x:25269 は c.c.c.c:5269 というプライベート IP アドレスにそれぞれマッピングされます。内部的には、すべての IP アドレスが IM and Presence サービス上の同一ポート（5269）にマッピングされます。

関連トピック

外部および内部インターフェイスの設定，（78 ページ）
DNS の設定，（33 ページ）

パブリック FQDN

SIP フェデレーションの場合、要求メッセージのルーティングは FQDN に基づいて行われます。そのため、ルーティングする IM and Presence サービス 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 Access Gateway では、企業の SIP/SIMPLE ベースのインスタント メッセージ サーバと、ネットワーク上のインスタント メッセージ ユーザとの通信を可能にするフェデレーション サービスが提供されます。AOL SIP Access Gateway を使用すると、企業の SIP/SIMPLE ベースのインスタント メッセージ サーバを利用するユーザは、AIM サービスや AOL サービスのパブリック ユーザと対話することができるほか、その在席情報を取得することもできます。また AOL SIP Access Gateway により、AIM システムや AOL システムのユーザはインスタント メッセージを送信したり、社内の SIP/SIMPLE ベース システムのユーザに関する在席情報を表示したりすることもできます。

AOL SIP Access Gateway は、内部 AOL プロトコルの変換を行うフロント エンドとして機能します。企業のサーバと AOL との間の通信は、すべて SIP を使用して行われます。内部の AOL システムで必要なプロトコルへの変換処理は、AOL SIP Access Gateway で行われます。外部サーバに変換機能を追加する必要はありません。そのため、AOL プロトコルは外部からは認識されません。企業のサーバは、SIP/SIMPLE を使用して通信している場合でも、AOL SIP Access Gateway を介して AOL に接続することが可能です。

AOL SIP Access Gateway は、TLS over TCP を介した接続のみサポートしています。AOL SIP Access Gateway サーバは、次のアドレスを持つインスタント メッセージ サーバまたはプロキシの内部で定義する必要があります。

サーバ名：`sip.oscar.aol.com`

サーバ ポート：5061

サーバ名 `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いずれかの場所で静的に設定した場合は、これらのアドレスが変更されていないかどうか AOL で定期的に確認することをお勧めします。
- また、AOL SIP Access Gateway の FQDN（sip.oscar.aol.com）についても、場合によっては変更される可能性があるため、ping を実行してその IP アドレスを確認することが推奨されます（**ping sip.oscar.aol.com** など）。

冗長性およびハイ アベイラビリティ

フェデレーテッドネットワークに冗長性を確保する方法についても考える必要があります。Cisco Adaptive Security Appliance では、アクティブ/スタンバイ（A/S）導入モデルにより冗長性がサポートされています。

IM and Presence サービスのフェデレーション機能に対してハイ アベイラビリティを実現する必要がある場合は、指定した（フェデレーション）IM and Presence サービス クラスタの手前にロードバランサを導入することができます。

DNS の設定

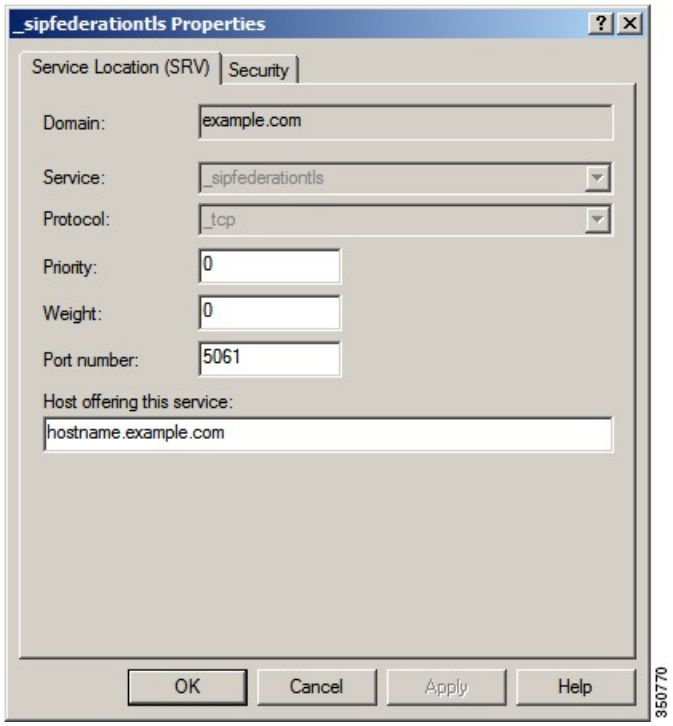
ローカル IM and Presence サービス企業展開では、DNS SRV を通じて他のドメインが IM and Presence サービス ノードを確認できるように、IM and Presence サービスがローカル IM and Presence サービス ドメインに DNS SRV レコードをパブリッシュしなければなりません。DNS SRV レコードは、企業の DMZ 内にある DNS サーバに保管されています。

ローカル IM and Presence サービス展開が複数のドメインを管理している場合は、各ローカル ドメインの DNS SRV レコードを公開します。ユーザが各ローカル ドメインに対して公開する DNS SRV レコードは、同一の FQDN パブリック IP アドレスに解決される必要があります。

Microsoft OCS R2 との SIP フェデレーションの場合は、DNS SRV レコード「_sipfederationtls」をパブリッシュする必要があります。Microsoft 製品のエンタープライズ導入では、IM and Presence サービスを Access Edge サーバ上で Public IM Provider として設定するため、このレコードが必要となります。外部のエンタープライズ導入で IM and Presence サービスから Microsoft ドメインを検出できるようにするためには、そ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 サービス 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、IM and Presence サービス上で、その外部ドメインのパブリック インターフェイスに向かうスタティック ルートを設定する必要があります。

DNS SRV レコード「_sipfederationtls_tcp.example.com」の DNS 設定例については、次の図を参照してください。

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



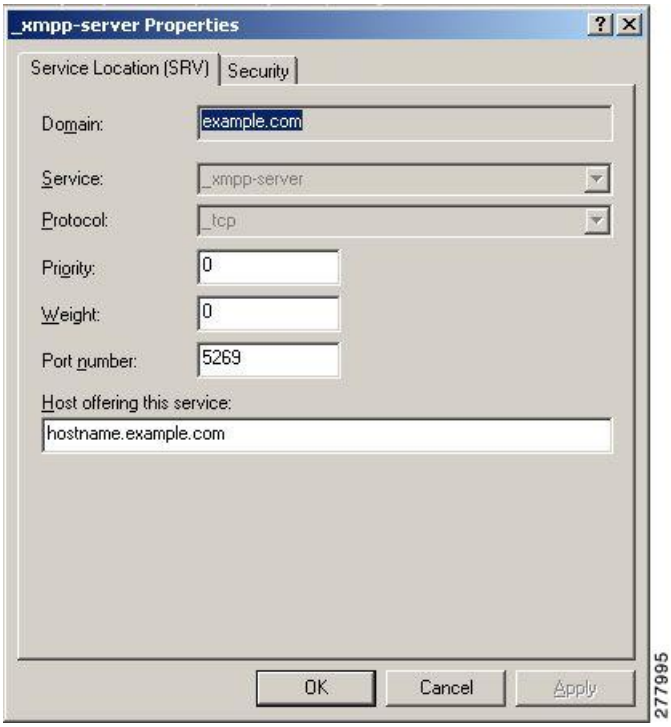
AOL フェデレーションの場合、AOL では「aol.com」ドメインのパブリック DNS サーバで DNS SRV レコード「_sipfederationtls_tcp.aol.com」がパブリッシュされます。このレコードは、AOL SIP Access Gateway に対応する「sip.oscar.aol.com」に解決されます。

DNS SRV レコードはパブリックに解決可能です。そのため、ローカルのエンタープライズ導入内で DNS 転送を有効にしている場合は、DNS クエリーを実行することで、外部のパブリック ドメインに関する情報を取得することができます。DNS クエリーがローカルのエンタープライズ導入内の DNS 情報に全面的に依存している（ローカルのエンタープライズ導入内で DNS 転送を有効にしていない）場合は、外部ドメインを指定する DNS SRV レコード/FQDN/IP アドレスをパブリッシュしなければなりません。スタティック ルートを設定することもできます。

XMPP フェデレーションの場合は、DNS SRV レコード「_xmpp-server」をパブリッシュする必要があります。このレコードにより、フェデレーション XMPP ドメインから IM and Presence サービス ドメインを検出することができるため、両ドメインのユーザは XMPP を介して IM や在席情報をやり取りすることが可能です。同様に外部ドメインでは、IM and Presence サービスから検出できるよう、パブリック DNS サーバで「_xmpp-server」レコードをパブリッシュする必要があります。

DNS SRV レコード "_xmpp-server" の DNS 設定例については、次の図を参照してください。

図 *13*：「*_xmpp-server*」の *DNS SRV*



関連トピック

AOL との SIP フェデレーションのルート SIP 要求，（53 ページ）
AOL との SIP フェデレーションに使用するデフォルト フェデレーション ルーティング ドメインの変更，（54 ページ）

認証権限サーバ

SIP フェデレーションの場合、IM and Presence サービスのエンタープライズ導入内の Cisco Adaptive Security Appliance（ASA）と、外部のエンタープライズ導入とは、セキュアな TLS/SSL 接続を介して IM および在席情報を共有します。

各エンタープライズ導入では外部認証局（CA）により署名された証明書を提示する必要があります。ただし、エンタープライズ導入ごとに別々の CA が使用される場合もあります。したがって両者間の相互信頼を実現するためには、それぞれのエンタープライズ導入に他方のエンタープライズ導入の外部 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は、セキュアな TLS 接続を設定するかどうかを選択することができます。TLS を設定する場合は、IM and Presence サービス上で、外部企業の証明書に署名している認証局（CA）のルート証明書をアップロードする必要があります。この証明書は、IM and Presence サービス上の証明書信頼ストア内に存在する必要があります。これは、Cisco Adaptive

Security Appliance（ASA）では XMPP フェデレーション用の TLS 接続が終端されないためです。Cisco Adaptive Security Appliance（ASA）は XMPP フェデレーション用のファイアウォールとして機能します。

この統合の前提条件となる設定タスク

統合に関する IM and Presence サービスの設定

（注） ここで説明する前提条件タスクは、SIP フェデレーションと XMPP フェデレーションのどちらにも共通するものです。

手順

ステップ 1 IM and Presence サービスをインストールし、設定します。
ここでは、IM and Presence サービスが正常に動作することを保証するため、以下の確認を行います。

- IM and Presence サービス システム設定トラブルシュータを実行します。
- ローカルな連絡先を IM and Presence サービスに追加できることを確認します。
- クライアントが IM and Presence サービス ノードからアベイラビリティ ステータスを受信していることを確認します。

ステップ 2 IM and Presence サービス ノードと Cisco Unified Communications Manager ノードを『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』の説明のとおりに設定します。IM and Presence サービス ノードが動作しており、問題がないことを確認します。

関連トピック

統合に関する Cisco Adaptive Security Appliance の設定, （37 ページ）

統合に関する Cisco Adaptive Security Appliance の設定

（注）
- SIP フェデレーションには、Cisco Adaptive Security Appliance が必要です。
- XMPP フェデレーションには、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 機能を実現するためであれば、Cisco Adaptive Security Appliance を含め任意のファイアウォールを使用することができます。XMPP フェデレーションで TLS プロキシ機能を実現する場合には、Cisco Adaptive Security Appliance は使用しません。

Cisco Adaptive Security Appliance をインストールし、設定します。そのうえで、Cisco Adaptive Security Appliance について次のような基本設定の確認を行います。

手順

ステップ 1 コンソール、HyperTerminal または Web ベースの Adaptive Security Device Manager（ASDM）を介して Cisco Adaptive Security Appliance にアクセスします。

ステップ 2 Cisco Adaptive Security Appliance の適切なライセンスを取得します。Cisco Adaptive Security Appliance の TLS プロキシにはライセンスが必要です。ライセンス情報については、シスコ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 次のコマンドを使用してホスト名を設定します。

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

ステップ 5 [デバイス設定（Device Setup）] > [システム時間（System Time）] > [時計（Clock）] を選択するか、CLI から **clock set** コマンドを使用することにより、ASDM で時間帯、日付、および時刻を設定します。次の点に注意してください。

- TLS プロキシを設定する前に、Cisco Adaptive Security Appliance 5500 で時計を設定します。
- Cisco Adaptive Security Appliance では IM and Presence サービス クラスタと同じ NTP サーバを使用することが推奨されます。Cisco Adaptive Security Appliance と IM and Presence サービス ノードとの間で時計が同期されていない場合は、証明書の有効性が確認できないために TLS 接続が正常に確立されないことがあります。
- NTP サーバ アドレスを表示するには、**ntp server** *server_address* コマンドと **show ntp associat | status** コマンドを使用して、NTP サーバのステータスを表示します。

ステップ 6 Cisco Adaptive Security Appliance 5500 のモードを確認します。Cisco Adaptive Security Appliance 5500 は、デフォルトでシングルモードおよびルーテッドモードが使用されるよう設定されています。

- 現在のモードを確認します。この値は、デフォルトでシングル モードとなります。

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

- 現在のファイアウォール モードを確認します。この値は、デフォルトでルーテッド モードとなります。

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

- 外部インターフェイスおよび内部インターフェイスを設定します。
- 基本 IP ルートを設定します。

関連トピック

外部および内部インターフェイスの設定, （78 ページ）
スタティック IP ルートの設定, （79 ページ）
統合に関する IM and Presence サービスの設定, （36 ページ）

第 3 章

ドメイン間フェデレーションの設定ワークフロー

（注） IM and Presence サービス リリース 9.0 以降では、Microsoft Lync とのドメイン間フェデレーションがサポートされています。また IM and Presence サービス リリース 9.0 以降の場合、OCS とのドメイン間フェデレーションへの参照には、別途明示的な指定がない限り、Microsoft Lync が指定されます。

ASA ファイアウォールを使用した Microsoft OCS との SIP フェデレーションに関する設定ワークフロー

- IM and Presence サービス上で Microsoft OCS フェデレーション用のフェデレーテッド ドメインを設定します。詳細については、SIP フェデレーテッド ドメインの追加，（45 ページ）を参照してください。

- DNS SRV レコードを設定します。詳細については、SIP フェデレーションの DNS 設定, （47 ページ）を参照してください。
- IM and Presence サービス上で Microsoft Lync フェデレーションのルーティングに関する設定を行います。詳細については、を参照してください。 IM and Presence サービスでのルーティング設定, （47 ページ）
- フェデレーション機能用の電子メール アドレスを設定します。、を参照してください。
- IM and Presence サービス上で TLS セキュリティの設定を行います。詳細については、を参照してください。 IM and Presence サービスでのセキュリティの設定, （51 ページ）
- Microsoft OCS フェデレーションに関する Cisco Adaptive Security Appliance の設定を行います。詳細については、SIP フェデレーションに関する Cisco Adaptive Security Appliance（ASA）の設定, （77 ページ）および Cisco Adaptive Securiy Appliance での TLS プロキシ設定, （91 ページ）を参照してください。
- Microsoft OCS フェデレーションでの証明書交換に関する設定を行います。詳細については、を参照してください。 Cisco Adaptive Security Appliance による SIP フェデレーション セキュリティ証明書の設定, （57 ページ）
- Microsoft OCS サーバの設定を行います。詳細については、 SIP フェデレーション用の外部サーバ コンポーネントの設定, （121 ページ）を参照してください。
- （任意）冗長性確保のためのロードバランサの設定を行います。詳細については、を参照してください。 冗長性確保のためのロード バランサの設定（SIP フェデレーションの場合）, （129 ページ）
- Microsoft OCS フェデレーションに関するトラブルシューティング情報については、を参照してください。 SIP フェデレーション統合に関するトラブルシューティング, （181 ページ）

ASA ファイアウォールを使用した Microsoft Lync との SIP フェデレーションに関する設定ワークフロー

- IM and Presence サービス上で Microsoft Lync フェデレーション用のフェデレーテッド ドメインを設定します。詳細については、SIP フェデレーテッド ドメインの追加, （45 ページ）を参照してください。
- DNS SRV レコードを設定します。詳細については、SIP フェデレーションの DNS 設定, （47 ページ）を参照してください。
- IM and Presence サービス上で Microsoft Lync フェデレーションのルーティングに関する設定を行います。詳細については、を参照してください。 IM and Presence サービスでのルーティング設定, （47 ページ）
- フェデレーション機能用の電子メール アドレスを設定します。
- IM and Presence サービス上で TLS セキュリティの設定を行います。詳細については、を参照してください。 IM and Presence サービスでのセキュリティの設定, （51 ページ）

- Microsoft Lync フェデレーションに関する Cisco Adaptive Security Appliance（ASA）の設定を行います。詳細については、SIP フェデレーションに関する Cisco Adaptive Security Appliance（ASA）の設定, （77 ページ）およびCisco Adaptive Securiy Appliance での TLS プロキシ設定, （91 ページ）を参照してください。
- Microsoft Lync フェデレーションでの証明書交換に関する設定を行います。詳細については、TLS フェデレーション用の Lync エッジ サーバでのセキュリティ証明書の設定, （73 ページ）を参照してください。
- ドメイン間フェデレーションに関する Lync Server 2010 および Edge サーバの設定は、このマニュアルに記載されている OCS についての設定とは異なります。IM and Presence サービスとのドメイン間フェデレーションを行えるよう Lync のエンタープライズ導入を設定する詳しい方法については、Microsoft のドキュメント（http://technet.microsoft.com/en-us/library/gg399048.aspx）を参照してください。

AOLとのSIPフェデレーションに関する設定ワークフロー

- AOL ライセンスを設定して AOL フェデレーションを有効にします。詳細については、AOL フェデレーションのライセンス要件, （125 ページ）、AOL ルーティング情報の要件, （125 ページ）、およびAOL プロビジョニング情報要件, （126 ページ）を参照してください。
- IM and Presence サービス上で AOL フェデレーション用のフェデレーテッド ドメインを設定します。詳細については、SIP フェデレーテッド ドメインの追加, （45 ページ）を参照してください。
- DNS SRV レコードを設定します。詳細については、SIP フェデレーションの DNS 設定, （47 ページ）を参照してください。DNS を使用しない場合は、次の手順に進んでください。
- AOL フェデレーションのルーティングに関する設定を行います。詳細については、TLS を使用したスタティック ルートの設定, （48 ページ）を参照してください。
- （任意）AOL ホステッド ドメインのデフォルト フェデレーション ルーティング ドメインについて確認および設定を行います。詳細については、AOL フェデレーションに関するルーティング情報の設定, （53 ページ）を参照してください。
- フェデレーション機能用の電子メール アドレスを設定します。、を参照してください。
- IM and Presence サービス上で TLS セキュリティおよびその証明書の設定を行います。詳細については、IM and Presence サービスでのセキュリティの設定, （51 ページ）およびCisco Adaptive Security Appliance と AOL SIP Access Gateway の間でのセキュリティ証明書の交換, （74 ページ）を参照してください。
- AOL に関する Cisco Adaptive Security Appliance の設定を行います。AOL FQDN、サーバ ポート、およびパブリック IP アドレスに関する詳細については、AOL SIP アクセス ゲートウェイ, （32 ページ）を参照してください。
- （任意）冗長性確保のためのロードバランサの設定を行います。詳細については、冗長性確保のためのロードバランサの設定（SIP フェデレーションの場合）, （129 ページ）を参照してください。

XMPP フェデレーションに関する設定ワークフロー

（注） WebEx、IM and Presence サービス、IBM Sametime については、以下のワークフローに従ってください。

- XMPP フェデレーション用の IM and Presence サービスの設定については、XMPP フェデレーション用の IM and Presence サービスの設定，（139 ページ）を参照してください。
- XMPP フェデレーション用のセキュリティ設定については、XMPP フェデレーションに使用するセキュリティ証明書の設定，（157 ページ）を参照してください。
- フェデレーション機能用の電子メール アドレスを設定します。
- XMPP フェデレーション サービスを有効にします。詳細については、XMPP フェデレーション サービスをオンにする，（154 ページ）を参照してください。
- XMPP フェデレーションに関する Cisco Adaptive Security Appliance（ASA）の設定を行います。詳細については、XMPP フェデレーション用に Cisco Adaptive Security Appliance を設定する，（153 ページ）を参照してください。
- XMPP フェデレーションに関するトラブルシューティング情報については、を参照してください。 XMPP フェデレーション統合に関するトラブルシューティング，（193 ページ）

ASA ファイアウォールを使用しない企業内における Microsoft OCS/Lync との SIP フェデレーションに関する設定ワークフロー

- IM and Presence サービス上で Microsoft OCS フェデレーション用のフェデレーテッド ドメインを設定します。詳細については、エンタープライズ内での Microsoft サーバ ドメインの追加，（100 ページ）を参照してください。
- Microsoft OCS/Lync とのダイレクト フェデレーションに使用するスタティック ルートを設定します。詳細については、企業内の Microsoft OCS/Lync コンフィギュレーション ドメイン間フェデレーション，（99 ページ）を参照してください。
- （任意）IM and Presence サービス上で TLS セキュリティおよびその証明書の設定を行います。詳細については、

SIP フェデレーションに関する Cisco Adaptive Security Appliance の設定ワークフロー

- Cisco Adaptive Security Appliance（ASA）と IM and Presence サービス（Inside インターフェイス）との間の証明書を設定します。詳細については、IM and Presence サービスと Cisco Adaptive Security Appliance の間でのセキュリティ証明書交換, （58 ページ）を参照してください。
- Cisco Adaptive Security Appliance（ASA）とフェデレーテッド ドメイン（outside インターフェイス）との間の証明書を設定します。詳細については、Microsoft CA を使用した Cisco Adaptive Security Appliance と Microsoft Access Edge（外部インターフェイス）の間でのセキュリティ証明書交換, （62 ページ）およびCisco Adaptive Security Appliance と AOL SIP Access Gateway の間でのセキュリティ証明書の交換, （74 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に関する PAT を設定します。詳細については、ポート アドレス変換（PAT）, （80 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に関するスタティック PAT を設定します。詳細については、スタティック PAT コマンドの例, （85 ページ）を参照してください。
- 必要なアクセス リストを設定します。詳細については、アクセス リストの設定の要件, （92 ページ）を参照してください。
- TLS プロキシ インスタンスを設定します。詳細については、TLS プロキシ インスタンスの設定, （94 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。詳細については、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, （96 ページ）を参照してください。

第 4 章

SIP フェデレーション用の IM and Presence サービスの設定

IM and Presence サービス リリース 9.0 以降では、Microsoft Lync とのドメイン間フェデレーションがサポートされています。また IM and Presence サービス リリース 9.0 以降の場合、OCS とのドメイン間フェデレーションへの参照には、別途明示的な指定がない限り、Microsoft Lync が指定されます。

SIP フェデレーテッド ドメインの追加

（注） IM and Presence サービス リリース 9.0 では、AOL との SIP フェデレーションがサポートされています。

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 サービスは自動的にフェデレーテッド ドメイン エントリに着信 ACL を追加します。[Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにフェデレーテッド ドメインに関連付けられた着信 ACL を表示できますが、変更または削除できません。着信 ACL を削除できるのは、（関連付けられた）フェデレーテッド ドメイン エントリを削除する場合だけです。

AOL との SIP フェデレーションを設定する場合は、以下の点に注意してください。

- AOL ネットワークは、パブリック コミュニティとホステッド ネットワークの両方を使用して構成することができます。これらの各ドメインは、IM and Presence サービス でタイプが AOL である SIP フェデレーテッド ドメインとして設定する必要があります。
- 「user@acompany.com」などのホステッド ドメインのユーザに対応するためには、IM and Presence サービス でタイプが AOL である SIP フェデレーテッド ドメインを「acompany.com」用に設定する必要があります。
- 「aol.com」ドメインおよび「aim.com」ドメインのユーザに対応するためには、IM and Presence サービスで「aol.com」用の SIP フェデレーテッド ドメインを 1 つ追加するだけで十分です。AOL ネットワークでは、「user@aim.com」を「user@aol.com」として処理することができます。

手順

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

ステップ 2 [新規追加（Add New）] をクリックします。

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

ステップ 4 [説明（Description）] フィールドにフェデレーテッド ドメインを識別する説明を入力します。[Manage Domains（ドメインの管理）] タブからアクセスできる Cisco Jabber リリース 8.x のプライバシー設定では、ユーザに対してこのテキスト文字列が表示されます。そのため、ユーザにとって分かりやすいドメイン名を入力するようにしてください。

ステップ 5 次の統合のいずれかを選択します。

a) **ドメイン間から OCS/Lync（Inter-domain to OCS/Lync）**

b) **ドメイン間から AOL（Inter-domain to AOL）**

ステップ 6 Microsoft OCS とのフェデレーションを設定する場合は、[ダイレクト フェデレーション（Direct Federation）] 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] 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。これにより、Cisco XCP ルータを再起動すると、IM and Presence サービス ですべての XCP サービスが再起動されます。

IM and Presence サービスでのルーティング設定

SIP フェデレーションの DNS 設定

ローカル IM and Presence サービス企業では、DNS SRV を通じて他のドメインが IM and Presence サービス ノードを確認できるように、IM and Presence サービスが各ローカル IM and Presence サービス ドメインに DNS SRV レコードをパブリッシュしなければなりません。DNS SRV レコードにそれぞれが同じパブリック IP アドレスに解決される必要があります。

Microsoft のエンタープライズ導入では、IM and Presence サービスが IM and Presence サービス ドメインの DNS SRV レコードを公開することが求められます。IM and Presence サービスを Access Edge サーバのパブリック IM プロバイダとして設定するからです。

IM and Presence サービスのエンタープライズ導入では、ポート 5061 で _sipfederationtls._tcp.*imp_domain* をポイントする DNS SRV レコードを設定する必要があります。ここで、*imp_domain* は IM and Presence サービス ドメインの名前です。この DNS SRV は、ルーティング用 IM and Presence サービス ノードのパブリック FQDN を指定している必要があります。この FQDN は、パブリックに解決可能であることが必要です。

IM and Presence サービスが外部ドメインを確認できるようにするには、外部ドメインの外部インターフェイスの FQDN を指定する外部ドメインの DNS サーバに DNS SRV レコードが存在する必要があります。

AOL との SIP フェデレーションを設定した場合、AOL では FQDN をベースにルーティングが行われます。そのため、ルーティング用 IM and Presence サービス ノードの FQDN は、パブリックに解決可能であることが必要です。AOL では、DNS SRV ルックアップは実行されず、代わりに IM and Presence サービスの FQDN が静的に設定されます。そのため、この FQDN はパブリックに解決可能であることが必要です。

ヒント　DNS SRV ルックアップを実行するには、次のコマンド シーケンスを使用します。

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

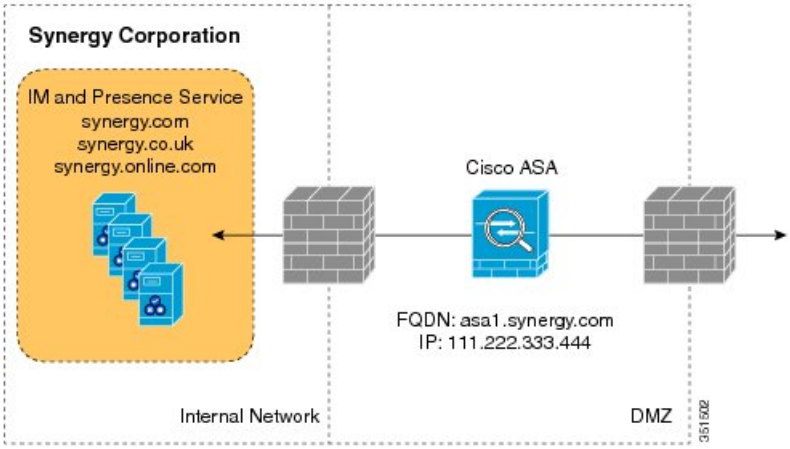
IM and Presence サービスがパブリック DNS lookup で外部企業を解決できない場合は、配置のスタティック ルートを設定しなければなりません。

ドメイン間フェデレーション導入の SIP DNS SRVs

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 に解決し、DNS SRV レコードを IM and Presence サービス展開でホストされたドメインごとに公開しなければなりません。次

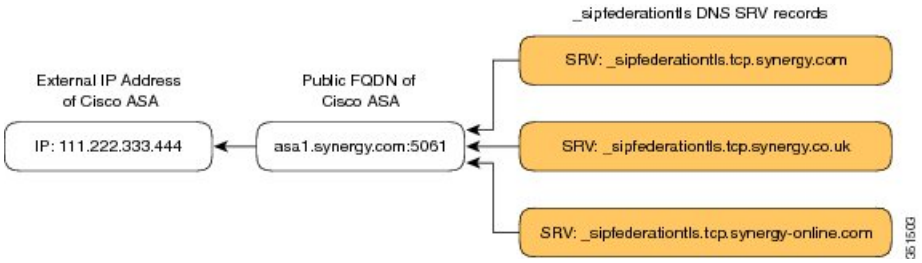
の図は、3 つのローカル ドメインが存在するドメイン間フェデレーション導入の例を示しています。各ドメインの_sipfederationtls DNS SRV レコードを公開します。

図 *14*：*SIP* ベースのフェデレーテッド ドメイン間導入の複数ドメイン



各 DNS SRV レコードは、次の図が示すように DMZ（ポート 5061）に配置された Cisco Adaptive Security Appliance の外部（パブリック）IP アドレスの FQDN に解決されなければなりません。

図 *15*：*Cisco Adaptive Security Appliance* の *FQDN* を解決する *SIP DNS SRV*



関連項目

TLS を使用したスタティック ルートの設定, （48 ページ）

TLS を使用したスタティック ルートの設定

（注） スタティック ルートの設定は、SIP フェデレーションの場合のみ行います。

IM and Presence サービス 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、IM and Presence サービス上で、その外部ドメインの外部インターフェイスに向かうスタティック ルートを設定する必要があります。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[プレゼンス（Presence）] > [ルーティング（Routing）] > [スタティック ルート（Static Routes）] を選択します。

ステップ 2 スタティック ルートに関するパラメータを以下のように設定します。

- 宛先パターンには、外部エンタープライズ ドメイン名を反転させた値を設定する必要があります。たとえば、ドメインが `domaina.com` であれば、[宛先パターン（Destination Pattern）] の値は `.com.domaina.*` となります。
- [ネクスト ホップ（Next Hop）] の値は、Microsoft OCS とのフェデレーションの場合は外部 Access Edge の FQDN または IP アドレス、AOL とのフェデレーションの場合は AOL SIP Access Gateway の FQDN または IP アドレスです。
- [ネクスト ホップ ポート（Next Hop Port）] の番号は **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。

関連トピック

フェデレーションのルーティング パラメータの設定

はじめる前に

初めて IM and Presence サービスをインストールする場合、フェデレーション ルーティング パラメータは、パブリッシャ ノードの FQDN に自動的に設定され、IM and Presence サービスは、各サブスクライバ ノードにこの値を渡します。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[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 サービス（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 and Presence の FQDN（Federation Routing IM and Presence FQDN）] パラメータの値として、パブリック FQDN を入力します。

- この FQDN 値は、その IM and Presence サービス ドメインのパブリック DNS にある _sipfederationtls エントリに一致している必要があります。次に、例を示します。
  - プレゼンス サーバ FQDN が imp1.cisco.com 、DNS SRV が *_sipinternaltls.*_tcp.cisco.com（FQDN imp1-public.cisco.com をポイント）の場合、フェデレーション ルーティング FQDN は imp1-public.cisco.com になることがあります。
  - プレゼンス サーバ FQDN が imp1.cisco.com 、DNS SRV が *_sipinternaltls.*_tcp.cisco.com（imp1-public.ciscoext.com）の場合、フェデレーション ルーティング FQDN は imp1-public.ciscoext.com になることがあります。

（注） このパラメータは、プレゼンス サーバと Lync サーバ間にファイアウォール（ASA）と TLS プロキシが存在するフェデレーション、および [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）] の下の [ダイレクト 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。

- ユーザをルーティング用 IM and Presence サービス ノードに割り当てる場合、この FQDN 値を IM and Presence サービス ノードの実際の FQDN と同じにすることはできません。

ステップ 5 [保存（Save）] をクリックします。

次の作業

IM and Presence サービス 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 UP XCP ルータを再起動します。**Cisco Unified Serviceability** のユーザ 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 - Cisco Unified Serviceability のネットワーク サービス（Control Center - Network Services in Cisco Unified Serviceability）] を選択します。

Cisco UP XCP ルータを再起動すると、それにより IM and Presence サービスのすべての XCP サービスが再起動します。

関連トピック

フェデレーション用電子メールの有効化, （169 ページ）

IM and Presence サービスでのセキュリティの設定

（注） この設定手順が適用されるのは、企業内にフェデレーションを導入する際にセキュアな TLS 接続を必要とする場合など、フェデレーションを導入するにあたって Cisco Adaptive Security Appliance を使用しない場合のみです。

新規 TLS ピア サブジェクトの作成

Cisco Adaptive Security Appliance セキュリティ証明書を IM and Presence サービスにインポートすると、IM and Presence サービス は Cisco Adaptive Security Appliance を TLS ピア サブジェクトとして自動的に追加します。そのため、IM and Presence サービスでは、Cisco Adaptive Security Appliance を TLS ピア サブジェクトとして手動で追加する必要はありません。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[システム（System）] > [セキュリティ（Security）] > [TLS ピア サブジェクト（TLS Peer Subjects）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 次のいずれかの値を入力します。

a) Microsoft OCS 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、Access Edge サーバの外部 FQDN を入力します。この値は、Microsoft の Access Edge サーバによって提示される証明書の件名 CN と一致する必要があります。

b) AOL との SIP フェデレーションを設定する場合は、AOL SIP Access Gateway の外部 FQDN を入力します。この値は、AOL SIP Access Gateway サーバによって提示される証明書の件名 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。

次の作業

選択した TLS ピア サブジェクト リストへの TLS ピアの追加, （52 ページ）

関連トピック

IM and Presence サービスへの自己署名証明書のインポート, （60 ページ）

選択した TLS ピア サブジェクト リストへの TLS ピアの追加

はじめる前に

新規 TLS ピア サブジェクトの作成

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[システム（System）] > [セキュリティ（Security）] > [TLS コンテキスト設定（TLS Context Configuration）] を選択します。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 [Default_Cisco_SIP_Proxy_Peer_Auth_TLS_Context] をクリックします。

ステップ 4 使用可能な TLS 暗号のリストからすべての暗号を選択します。

ステップ 5 矢印をクリックして、[選択された TLS 暗号（Selected TLS Ciphers）] までこれらの暗号を移動します。

ステップ 6 使用可能な TLS ピア サブジェクトのリストから、前の項で設定した TLS ピア サブジェクトをクリックします。

ステップ 7 矢印をクリックして、選択されている TLS ピア サブジェクトを [選択された TLS ピア サブジェクト（Selected TLS Peer Subjects）] に移動します。

ステップ 8 Microsoft OCS とフェデレーションを行う場合は、[空の TLS フラグメントの無効化（Disable Empty TLS Fragments）] チェックボックスをオンにします。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 Cisco SIP プロキシ サービスを再起動します。

（注） AOL フェデレーションと Microsoft OCS フェデレーションを同じ IM and Presence サービス ノード上に導入する場合、[空の TLS フラグメントの無効化（Disable Empty TLS Fragments）] チェックボックスをオンにしても、AOL フェデレーションに影響はありません。

関連トピック

新規 TLS ピア サブジェクトの作成, （51 ページ）

AOL フェデレーションに関するルーティング情報の設定

AOL との SIP フェデレーションのルート SIP 要求

（注） IM and Presence サービス リリース 9.0 では、AOL との SIP フェデレーションがサポートされています。

AOL との SIP フェデレーションにより、IM and Presence サービス ユーザは次のユーザとフェデレーションを行うことが可能です。

- AOL パブリック コミュニティ（aim.com、aol.com など）のユーザ。
- ドメインが AOL によってホストされている企業のユーザ。
- AOL とフェデレーションを行っている外部企業のユーザ。IM and Presence サービスでは、こうした外部企業とフェデレーションを行う際、AOL をクリアリング ハウスとして使用することもできます。

たとえば、「hosteddomain.com」というドメインを持つ企業を AOL がホストしており、かつ「acompany.com」というドメインを持つ企業が AOL とフェデレーションを行っているとします。このとき、IM and Presence サービス上でこれらの各ドメインに対して SIP フェデレーション ドメイン エントリを追加することにより、IM and Presence サービス ユーザは users@hosteddomain.com および users@acompany.com とフェデレーションを行うことができます。

IM and Presence サービスでは、AOL を介してフェデレーションを行うドメインへのルーティングをサポートするため、ルーティング ロジックが強化されています。AOL との SIP フェデレーションを設定すると、IM and Presence サービスでは、デフォルト 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のルーティングが行われます。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が適用されるのは、「ドメイン間から AOL」というタイプのフェデレーテッド ドメインを設定した場合のみです。

フェデレーション ユーザが AOL のいずれかのホステッド ドメイン（aol.com 以外のドメイン）に属している場合、IM and Presence サービスでは次のような順序で処理が実行されます。

手順

ステップ 1 ホステッドドメインのスタティックルートについてルックアップが実行されます。スタティックルートがない場合、IM and Presence サービスは、

ステップ 2 ホストされたドメインの DNS SRV ルックアップを実行します。ルックアップが何も返さない場合、IM and Presence サービス は、

ステップ 3 デフォルト フェデレーション ルーティング ドメイン（デフォルトは aol.com）のスタティックルートについてのルックアップを実行します。スタティック ルートがない場合、IM and Presence サービスは、

ステップ 4 デフォルト フェデレーション ルーティング ドメイン（デフォルトは aol.com）の DNS SRV ルックアップを実行します。
フェデレーション ユーザがデフォルト AOL ドメイン（user@aol.com）に属している場合、IM and Presence サービスでは次のような順序で処理が実行されます。

ステップ 5 デフォルト AOL ドメイン（デフォルトは aol.com）のスタティック ルートについてのルックアップ。スタティック ルートがない場合、IM and Presence サービスは、

ステップ 6 デフォルト フェデレーション ルーティング ドメイン（デフォルトは aol.com）の DNS SRV ルックアップを実行します。

関連トピック

AOL との SIP フェデレーションに使用するデフォルト フェデレーション ルーティング ドメインの変更, （54 ページ）

AOL との SIP フェデレーションに使用するデフォルト フェデレーション ルーティング ドメインの変更

（注） IM and Presence サービス リリース 9.0 では、AOL との SIP フェデレーションがサポートされています。

通常は、AOL のエンタープライズ導入において AOL から解決されたドメインが変更されない限り、デフォルト フェデレーション ルーティング ドメインの値を変更する必要はありません。

はじめる前に

AOL との SIP フェデレーションのルーティング SIP 要求に関するトピックに目を通します。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[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 サービス（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 [フェデレーションのルーティング パラメータ（クラスタ全体）（Federation Routing Parameters (Clusterwide)）] 領域で、[デフォルト フェデレーション ルーティング ドメイン（Default Federation Routing Domain）] のパラメータの値を確認または編集します。

ステップ 5 [デフォルト フェデレーション ルーティング ドメイン（Default Federation Routing Domain）] のパラメータの値を変更した場合は、[保存（Save）] を選択します。

ステップ 6 [デフォルト フェデレーション ルーティング ドメイン（Default Federation Routing Domain）] パラメータの値を変更した場合は、Cisco XCP ルータを再起動する必要があります。[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[ツール（Tools）] > [コントロール センター - ネットワーク サービス（Control Center - Network Services）] を選択し、Cisco XCP ルータを再起動します。

関連トピック

AOL との SIP フェデレーションのルート SIP 要求, （53 ページ）

SIP フェデレーション サービスの有効化

各 IM and Presence サービス ノード上では、Cisco XCP XMPP Federation Connection Manager サービスを有効にする必要があります。このサービスを有効にすると、それぞれのノード上でプロビジョニングした各ユーザに対して SIP フェデレーション機能が有効になります。この作業は、クラスタ内のノードごとに実行する必要があります。

手順

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

ステップ 2 [ホスト（Host）] 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 Services）] セクションで、[Cisco XCP SIP Federation Connection Manager] サービスの横にあるボタンを選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 SIP フェデレーションを利用するためには、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] 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。

関連トピック

フェデレーションでのロギングの使用, （173 ページ）

第 5 章

Cisco Adaptive Security Appliance による SIP フェデレーション セキュリティ証明書の設定

（注） IM and Presence サービス リリース 9.0(1) 以降では、Microsoft Lync とのドメイン間フェデレーションがサポートされています。OCS とのドメイン間フェデレーションへの参照には、別途明示的な指定がない限り、Microsoft Lync が指定されます。

IM and Presence サービスと Cisco Adaptive Security Appliance の間でのセキュリティ証明書交換

Cisco Adaptive Security Appliance でのキーペアとトラスト ポイントの生成

この証明書に対してキー ペア（例、**cmp_proxy_key**）を作成し、Cisco Adaptive Security Appliance から IM and Presence サービスへの自己署名証明書を識別するトラストポイント（例、**imp_proxy**）を設定する必要があります。CiscoAdaptive Security Appliance で自己署名証明書を作成していることを示すために登録タイプを“self”と指定するとともに、証明書のサブジェクト名にインターフェイス内の IP アドレスを指定する必要があります。

はじめる前に

次の章に記載されている設定タスクを実行したことを確認します。

- SIP フェデレーション用の IM and Presence サービスの設定, （45 ページ）
- SIP フェデレーションに関する Cisco Adaptive Security Appliance（ASA）の設定, （77 ページ）

手順

ステップ 1 Cisco Adaptive Security Appliance で、設定モードに入ります。

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

ステップ 2 次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 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 サービス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 ペアが生成されていることを確認します。

次の作業

Cisco Adaptive Security Appliance での自己署名証明書の作成, （59 ページ）

Cisco Adaptive Security Appliance での自己署名証明書の作成

はじめる前に

- Cisco Adaptive Security Appliance でのキーペアとトラスト ポイントの生成, （58 ページ）の手順を実行します。
- この手順を実行するには、UNIX 対応のテキスト 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 Service Pack 2 を推奨します。

手順

ステップ 1 次のコマンドを入力して、自己署名証明書を作成します。

```
(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ことを確認するメッセージが表示されたら、**no** と入力します。

ステップ 3 自己署名証明書を作成するよう求めるプロンプトに対して、**yes** で応答します。

ステップ 4 次のコマンドを入力して、IM and Presence サービスにエクスポートする証明書を作成します。

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

これによって、たとえば、PEM でエンコードされたアイデンティティ証明書が画面に表示されます。

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

ステップ 5 Cisco Adaptive Security Appliance 証明書の内容全体をコピーし、ワードパッドかメモ帳のファイル（.pem の拡張子を付ける）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。

次の作業

IM and Presence サービスへの自己署名証明書のインポート, （60 ページ）

IM and Presence サービスへの自己署名証明書のインポート

はじめる前に

の手順を実行します。 Cisco Adaptive Security Appliance での自己署名証明書の作成, （59 ページ）

手順

ステップ 1 [Cisco Unified IM and Presence Operating System Administration] ユーザ インターフェイスにログインします。[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 [証明書のアップロード（Upload Certificate）] をクリックします。

ステップ 3 [Certificate Purpose（証明書目的）] で、[cup-trust] を選択します。

（注） ルート名のフィールドは空白のままにしておきます。

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（前の手順で作成した）Cisco Adaptive Security Appliance の .pem 証明書ファイルを特定します。

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

トラブルシューティングのヒント

証明書の一覧で、`<asa ip address>.pem` と `<asa ip address>.der` を検索すると、見つかります。

次の作業

IM and Presence サービスでの新しい証明書の生成, （60 ページ）

IM and Presence サービスでの新しい証明書の生成

（注） Cisco ASA ファイアウォールの証明書は、内外でサーバ認証属性とクライアント認証属性が設定されている必要があります。これは、証明書の強化キー使用（EKU）パラメータ、または次のオブジェクト ID（OID）の値を調べ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

はじめる前に

の手順を実行します。 IM and Presence サービスへの自己署名証明書のインポート, （60 ページ）

手順

ステップ 1 **[Cisco Unified IM and Presence Operating System Administration]** ユーザ インターフェイスにログインします。[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 [新規作成（Generate New）] をクリックします。

ステップ 3 [証明書目的（Certificate Purpose）] ドロップダウン リストで、cup を選択します。

ステップ 4 [生成（Generate）] をクリックします。

次の作業

Cisco Adaptive Security Appliance への IM and Presence サービス証明書のインポート, （61 ページ）

Cisco Adaptive Security Appliance への IM and Presence サービス証明書のインポート

IM and Presence サービス証明書を Cisco Cisco Adaptive Security Appliance にインポートするには、IM and Presence サービスからインポートした証明書を識別するためのトラストポイント（たとえば **cert_from_imp**）を作成し、“terminal” として登録タイプを指定し、IM and Presence サービスから取得した証明書が端末に張り付けられることを表示する必要があります。

（注） IM and Presence サービスと Cisco Unified Communications Manager のノード、ならびに Cisco Adaptive Security Appliance は、同じ NTP ソースから同期する必要があります。

はじめる前に

- IM and Presence サービスでの新しい証明書の生成, （60 ページ）の手順を実行します。
- この手順を実行するには、UNIX 対応のテキスト 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 Service Pack 2 を推奨します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

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

ステップ 2 次のコマンド シーケンスを入力して、インポートした IM and Presence サービス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 次のコマンドを入力して、IM and Presence サービスから証明書をインポートします。
crypto ca authenticate *cert_from_imp*

ステップ 4 [Cisco Unified IM and Presence Operating System Administration] ユーザ インターフェイスにログインします。IM and Presence サービスで [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 サービス証明書を特定します。

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 推奨されているテキスト エディタの 1 つを使用して、imp.pem ファイルを開きます。

ステップ 9 imp.pem の内容を切り取って、Cisco Adaptive Security Appliance 端末に貼り付けます。

ステップ 10 **quit** を入力します。

ステップ 11 証明書の承認を確認するメッセージが表示されたら、**yes** と入力します。

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。

次の作業

Microsoft CA を使用した Cisco Adaptive Security Appliance と Microsoft Access Edge（外部インターフェイス）の間でのセキュリティ証明書交換, （62 ページ）

Microsoft CA を使用した Cisco Adaptive Security Appliance と Microsoft Access Edge（外部インターフェイス）の間でのセキュリティ証明書交換

次の手順は、Microsoft CA を使用して証明書を設定する方法を示した例です。

（注） VeriSign CA を使用した手順の例は、このマニュアル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作成する場合、トラストポイントに対して使用する登録方法を指定する必要があります。登録方法としては、Simple Certificate Enrollment Process（SCEP）を使用できます（Microsoft CA を使用する場合）。SCEP では、**enrollment url** コマンドを使用して、宣言したトラストポイントの SCEP による登録に使用する URL を定義します。定義した URL は、使用する CA の URL にする必要があります。

このほかに使用できる登録方法には、手動登録があります。手動登録では、**enrollment terminal** コマンドを使用して、CAから受信した証明書をターミナルに貼り付けます。いずれの登録方法の

手順についても、この項で説明します。登録方法の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』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、証明書を設定する 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、実行します。
- [ローカル システム アカウント（local system account）] 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。

[終了（Finish）] をクリックして、SCEP の URL を取得します。この URL は、Cisco Adaptive Security Appliance（ASA）でのトラストポイントの登録時に使用します。

SCEP を使用した Cisco Adaptive Security Appliance での証明書の設定

手順

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 次のコマンドを入力して、CA を識別するトラストポイントを作成します。
crypto ca trustpoint *trustpoint_name*

ステップ 3 **client-types** コマンドを使用して、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。クライアント接続タイプは、ユーザ接続に関連付けられた証明書を確認するのに使用できます。**client-types ssl** 設定を指定する次のコマンドを入力することで、このトラストポイントを使用して SSL クライアント接続が確認できることを指定します。
`(config-ca-trustpoint)#` **client-types ssl**

ステップ 4 次のコマンドを入力して、パブリック IM and Presence サービス アドレスの FQDN を設定します。
fqdn *fqdn_public_imp_address*

（注） ここで、VPN 認証に関する警告が発行される場合があります。

ステップ 5 次のコマンドを入力して、トラストポイントのキー ペアを設定します。
keypair *public_key_for_ca*

ステップ 6 次のコマンドを入力して、トラストポイントの登録方法を設定します。
enrollment url http://*ca_ip_address***/certsrv/mscep/mscep.dll**

ステップ 7 次のコマンドを入力して、設定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*

```
INFO: Certificate has the following attributes: Fingerprint: cc966ba6 90dfe235 6fe632fc
2e521e48
```

ステップ 8 CA からの証明書の承認を確認するメッセージが表示されたら、**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*

次の警告の出力が表示されます。

```
%WARNING: The certificate enrollment is configured with an fqdn that differs from the system
fqdn.If this certificate will be used for VPN authentication this may cause connection
problems.
```

ステップ 10 登録の続行を確認するメッセージが表示されたら、**yes** と入力します。

```
Would you like to continue with this enrollment?[yes/no]: yes

% Start certificate enrollment..
```

ステップ 11 チャレンジ パスワードを作成するよう求めるプロンプトに対して、パスワードを入力します。

```
% Create a challenge password.You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate.For security reasons your password will
not be saved in the configuration.Please make a note of it.

Password: <password>

********** Re-enter password: **********
```

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ことを確認するメッセージが表示されたら、**no** と入力します。

ステップ 13 CA に証明書を要求するよう求めるメッセージが表示されたら、**yes** と入力します。

```
Request certificate from CA?[yes/no]: yes

% Certificate request sent to Certificate Authority
```

ステップ 14 CA に移動し、保留されていた証明書を発行します（証明書が自動的に発行されていなかった場合）。

次の作業

外部 Access Edge インターフェイスの証明書の設定, （66 ページ）

手動による登録を使用した Cisco Adaptive Security Appliance での証明書の設定

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：

手順

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 次のコマンド シーケンスを入力して、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 サービス アドレスの FQDN である必要があります。
- キー ペア値は、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法を設定します。
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 の 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] を選択します。
d) CA 証明書のダウンロード
e) 証明書を .cer ファイルとして保存します（例：`CARoot.cer`）。

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

ステップ 7 Cisco Adaptive Security Appliance 端末に証明書の内容をコピー アンド ペーストします。

ステップ 8 証明書の承認を確認するメッセージが表示されたら、**yes** と入力します。
Cisco Adaptive Security Appliance のパブリック証明書に CSR を生成します。

ステップ 9 次のコマンドを入力して、CA に対する登録要求を送信します。
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るプロンプトに対して、**no** で応答します。

ステップ 11 証明書要求を表示するよう求めるプロンプトに対して、**yes** で応答します。

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（後の手順で使用するため）。

ステップ 13 登録要求を再表示するよう求めるプロンプトに対して、**no** で応答します。

ステップ 14 （手順 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 の Web ページに移動します（例：`http(s)://ca_ip_address/certsrv`）。
b) [証明書を要求（Request a certificate）] をクリックします。
c) [証明書の要求の詳細設定（Advanced certificate request）] をクリックします。
d) [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 orPKCS#10 file...）] を選択します。
e) （手順 4 でコピーした）base-64 証明書を貼り付けます。
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) 証明書をテキスト エディタで開き、内容をコピーしてターミナルに貼り付けます。別の行に **quit** という単語を入力して終了します。

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るプロンプトに対して、**yes** で応答します。

次の作業

外部 Access Edge インターフェイスの証明書の設定, （66 ページ）

外部 Access Edge インターフェイスの証明書の設定

この手順では、スタンドアロン CA を使用して Access Edge サーバ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

手順

ステップ 1 Access Edge サーバで、[スタート（Start）] > [実行（Run）] を選択します。

ステップ 2 http://<name of your Issuing CA Server>/certsrv を入力し、[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 [ファイルのダウンロード（File Download）] ダイアログボックスで、[保存（Save）] をクリックします。

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 .p7b です。この .p7b ファイルを開くと、チェーンに次の 2 つの証明書が表示されます。

a) スタンドアロンのルート CA 証明書の名前

b) スタンドアロンの下位 CA 証明書の名前（ある場合）

次の作業

CA 証明書チェーンのインストール, （67 ページ）

CA 証明書チェーンのインストール

はじめる前に

の手順を実行します。CA 証明書チェーンのダウンロード, （67 ページ）

手順

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

ステップ 2 `mmc` を入力し、[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と削除（Add/Remove Snap-in）] を選択します。

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

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 [Certificates（証明書）] を選択します。

ステップ 6 [追加（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) [<ローカル コンピュータ>（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（Finish）] 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 [信頼されたルート証明機関（Trusted Root Certification Authorities）] を展開します。

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）] をクリックして、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 [証明書をすべてストアに配置する（Place all certificates in the store）] というデフォルト値のままにして、[証明書ストア（Certificate store）] の下に [信頼されるルート証明機関（Trusted Root Certification Authorities）] が表示されていることを確認します。

ステップ 21 [次へ（Next）] をクリックします。

ステップ 22 [終了（Finish）] をクリックします。

次の作業

CA サーバからの証明書の要求，（69 ページ）

CA サーバからの証明書の要求

はじめる前に

の手順を実行します。 CA 証明書チェーンのインストール, （67 ページ）

手順

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

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

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 [証明書の要求の詳細設定（Advanced certificate request）] をクリックします。

ステップ 5 [この CA への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 [必要な証明書の種類（Type of Certificate Needed）] リストから **[その他（Other）]** をクリックします。

ステップ 7 件名共通名に Access Edge 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 ID（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 を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 を使用する場合は、[主要オプション（Key Options）] で [ローカル コンピュータ証明書ストアに証明書を格納（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、この項の「トラブルシューティングのヒント」で説明し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 [送信（Submit）] をクリックします。

次の作業

CA サーバからの証明書のダウンロード, （69 ページ）

CA サーバからの証明書のダウンロード

はじめる前に

の手順を実行します。 CA サーバからの証明書の要求, （69 ページ）

手順

ステップ 1 [スタート（Start）] > [管理ツール（Administrative Tools）] > [認証局（Certificate Authority）] を選択して、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、ユーザが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）] > [発行（Issue）] を選択します。

ステップ 5 CA を実行している Access Edge サーバで `http://local_server/certsrv` を開きます。

ステップ 6 [保留中の証明書要求の状態の表示（View the Status of a Pending Certificate Request）] をクリックし、証明書要求をクリックします。

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

次の作業

Access Edge への証明書のアップロード, （70 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 サーバに証明書をアップロードする方法について説明します。また、Access Edge サーバには手動で証明書をインポートすることもできます。それには、[Microsoft Office Communications Server 2007] > [プロパティ（Properties）] > [エッジ インターフェイス（Edge Interfaces）] を選択します。

はじめる前に

の手順を実行します。 CA サーバからの証明書のダウンロード, （69 ページ）

手順

ステップ 1 Access Edge サーバで、[スタート（Start）] > [管理ツール（Administrative Tools）] > [コンピュータの管理（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 [証明書（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 [既存の証明書を割り当てる（Assign an existing certificate）] タスク 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 [エッジ サーバのパブリック 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 [終了（Finish）] をクリックします。

次の作業

Cisco Adaptive Securiy Appliance での TLS プロキシ設定, （91 ページ）

エンタープライズ認証局を使用した Access Edge のカスタム証明書の作成

次の手順を参照する必要があるのは、Microsoft エンタープライズ Certificate Authority を使用して Access Edge の外部インターフェイスまたは Cisco Adaptive Security Appliance にクライアント/サーバ ロール証明書を発行する場合です。

はじめる前に

次の手順を実行するには、認証局がエンタープライズ CA で、Windows Server 2003 または 2008 の Enterprise Edition にインストールされている必要があります。

この手順の詳細については、http://technet.microsoft.com/en-us/library/bb694035.aspx に記載されている Microsoft の指示を参照してください。

カスタム証明書テンプレートの作成および発行

手順

ステップ 1 次の URL にある Microsoft サイト「Creating and Issuing the Site Server Signing Certificate Template on the Certification Authority」の手順 1 ～ 6 を実行します。
http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver1

ヒント 手順 5 では、この特別なテンプレートに相互認証証明書などの適切な名前を使用します。

ステップ 2 Microsoft サイトの手順 7 ～ 12 の代わりに次の手順を実行します。

a) [拡張（Extensions）] タブを選択します。[アプリケーションのポリシー（Application Policies）] の下に [クライアント認証（Client Authentication）] および [サーバ認証（Server Authentication）] があり、他のポリシーがないことを確認します。これらのポリシーがない場合は、続行する前に追加する必要があります。

- [アプリケーション ポリシーの拡張の編集（Edit Application Policies Extension）] ダイアログボックスで、[追加（Add）] を選択します。
- [アプリケーションのポリシーの追加（Add Application Policy）] ダイアログボックスで、[クライアント認証（Client Authentication）] を選択し、Shift を押してから [サーバ認証（Server Authentication）] を選択して、[追加（Add）] をクリックします。
- [アプリケーション ポリシーの拡張の編集（Edit Application Policies Extension）] ダイアログボックスで、他にポリシーがあれば、それを選択して [削除（Remove）] を選択します。

[新しいテンプレートのプロパティ（Properties of New Template）] ダイアログボックスに、[アプリケーションのポリシー（Application Policies）] の説明として、クライアント認証（Client Authentication）とサーバ認証（Server Authentication）のリストが表示されます。

b) [発行要件（Issuance Requirement）] タブを選択します。証明書が自動的に発行されないようにしたい場合は、[CA 証明書マネージャの許可（CA certificate manager approval）] を選択します。これ以外の場合は、このオプションは空白のままにしておきます。

c) [セキュリティ（Security）] タブを選択し、必要なすべてのユーザとグループに読み取り権限と登録権限を必ず付与します。

d) [要求の処理（Request Handling）] タブを選択し、[CSP] ボタンをクリックします。

e) [CSP の選択（CSP Selection）] ダイアログボックスで、[要求で次の CSP のいずれかを使用（Requests must use one of the following CSP's）] をオンにします。

f) CSP のリストから、[Microsoft Basic Cryptographic Provider v1.0 および Microsoft Enhanced Cryptographic Provider v1.0（Microsoft Basic Cryptographic Provider v1.0 and Microsoft Enhanced Cryptographic Provider v1.0）] を選択し、[OK] を選択します。

ステップ 3 次の URL にある Microsoft サイト「Creating and Issuing the Site Server Signing Certificate Template on the Certification Authority」の手順 13 ～ 15 に進みます。
http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver1

次の作業

サイト サーバ署名証明書の要求, （73 ページ）

サイト サーバ署名証明書の要求

手順

ステップ 1 次の URL にある Microsoft サイト「Site Server Signing Certificate for the Server That Will Run the Configuration Manager 2007 Site Server」の手順 1 ～ 6 を実行します。
http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver2

ヒント 手順 5 では、相互認証証明書など、以前に作成した証明書テンプレートの名前を選択し、[名前（Name）] フィールドに Access Edge の外部 FQDN を入力します。

ステップ 2 Microsoft サイトの手順 7 ～ 8 の代わりに次の手順を実行します。

a) 証明書要求が自動的に発行される場合は、署名証明書をインストールするオプションが提示されます。[この証明書のインストール（Install this Certificate）] を選択します。

b) 証明書要求が自動的に出されなければ証明書を導入するために管理者を待ちます。発行されたら、次を実行します。

- メンバ サーバで、Internet Explorer をロードし、`http://<server>/certsrv` のアドレスを使用して Web 登録サービスに接続します。ここで、`<server>` はエンタープライズ CA の名前または IP アドレスです。
- [ようこそ（Welcome）] ページで、[保留中の証明書の要求の状態（View the status of a pending certificate request）] を選択します。

c) 発行された証明書を選択し、[この証明書のインストール（Install this Certificate）] を選択します。

TLS フェデレーション用の Lync エッジ サーバでのセキュリティ証明書の設定

Microsoft Lync との TLS フェデレーション用に Access Edge 上で証明書を設定する方法については、URL http://technet.microsoft.com/en-us/library/gg398409.aspx にある Microsoft TechNet ライブラリの文書を参照してください。IM and Presence サービスでフェデレーテッド接続を行うには相互 TLS 認証が必要なため、サーバ認証とクライアント認証を両方サポートするよう Microsoft Lync 証明書を設定する必要があります。上記のガイドに従う場合は、2 番目の項をスキップして 3 番目の項に移動します。この項には、AOL とのパブリック IM 接続をサポートするエッジ サーバの外部

インターフェイスに対して証明書要求を作成する方法が記載されています。AOL にも、IM and Presence サービスと同じ相互 TLS 認証要件があります。このガイドは、TLS 上で IM and Presence サービスとのフェデレーションを直接行うよう Lync Server を設定するのにも使用できます。

ダイレクト フェデレーションを行えるよう Lync Server でスタティック ルートを設定する方法については、Microsoft Lync サーバ コンフィギュレーション タスク リストにフェデレーション リンク，（108 ページ）を参照してください。

Cisco Adaptive Security Appliance と AOL SIP Access Gateway の間でのセキュリティ証明書の交換

AOL を使用するには、Cisco Adaptive Security Appliance の証明書が信頼済み認証局（CA）によって署名されている必要があります。AOL は、Windows でよく使用される CA や、主なブラウザで配信されるライブラリに含まれている CA から成る、確立された信頼リストを持っています。AOL の信頼リストにない CA を使用する場合は、この情報を AOL に提供するため、シスコのサポート担当者と連携されることが推奨されます。

Verisign CA を使用して Cisco Adaptive Security Appliance と外部ドメイン（Microsoft Access Edge）の間での証明書交換を設定する方法を詳細に示した設定ワークフローの例が、このマニュアルの付録に記載されています。この手順を基準として使用して、Verisign CA を使用した Cisco Enterprise EditionAdaptive Security Appliance と AOL SIP Access Gateway の間での証明書交換を設定します。設定手順の大まかな概要を下記に示します。

Verisign CA を使用した Cisco Adaptive Security Appliance と AOL SIP Access Gateway の間での証明書交換を設定するには、次の手順を実行します。

- https://pki-info.aol.com/AOL/ から AOL のルート証明書をダウンロードします。
- https://pki-info.aol.com/AOLMSPKI/index.html から AOL のメンバ証明書をダウンロードします。
- Cisco Adaptive Security Appliance で、ルート証明書のトラストポイントおよび古い中間証明書や署名証明書があればすべて削除します。
- AOL ルート証明書用に Cisco Adaptive Security Appliance で新しいトラストポイントを作成します。Cisco Adaptive Security Appliance への IM and Presence サービス証明書のインポート，（61 ページ）の項（手順 1 ～ 3）を参照してください。
- AOL メンバ証明書用に Cisco Adaptive Security Appliance で新しいトラストポイントを作成します。
- Cisco Adaptive Security Appliance で Verisign CA 用に新しいトラストポイントを作成します。
- Cisco Adaptive Security Appliance で、ルート証明書をインポートし、証明書署名要求（CSR）を作成します。類似の手順を手動による登録を使用した Cisco Adaptive Security Appliance での証明書の設定，（65 ページ）の項で参照してください。

（注） IM and Presence サービス サーバ証明書の件名 CN は、IM and Presence サービス ノードの FQDN と一致する必要があります。Cisco Adaptive Security Appliance での IM and Presence サービス用パブリック証明書と CN は、[フェデレーション ルーティング IM and Presence の FQDN（Federation Routing IM and Presence FQDN）] サービス パラメータの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 により、次の証明書が提供されます。
  - Verisign 署名付き証明書
  - Verisign 下位/中間/ルート証明書
  - Verisign ルート CA 証明書
- Cisco Adaptive Security Appliance で、証明書署名要求の作成に使用する一時ルート証明書を削除します。
- Verisign 下位/中間/ルート証明書を Cisco Adaptive Security Appliance にインポートします。
- Cisco Adaptive Security Appliance 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 Adaptive Security Appliance にインポートし、続いて Verisign 署名付き証明書を Cisco Adaptive Security Appliance にインポートします。
- VeriSign ルート証明書および中間証明書を AOL に提供します。

（注） AOL 信頼リストにこのルート CA がまだない場合は、AOL にこの CA を提供する必要があります。

関連トピック

Cisco Adaptive Security Appliance への IM and Presence サービス証明書のインポート, （61 ページ）
手動による登録を使用した Cisco Adaptive Security Appliance での証明書の設定, （65 ページ）
Cisco Adaptive Security Appliance と Microsoft Access Edge との間における VeriSign を使用したセキュリティ証明書交換, （203 ページ）
AOL ルーティング情報の要件, （125 ページ）

第 6 章

SIPフェデレーションに関するCiscoAdaptive Security Appliance（ASA）の設定

（注） IM and Presence サービス リリース 9.0 以降では、Microsoft Lync とのドメイン間フェデレーションがサポートされています。また IM and Presence サービス リリース 9.0 以降の場合、OCS とのドメイン間フェデレーションへの参照には、別途明示的な指定がない限り、Microsoft Lync が指定されます。

Cisco Adaptive Security Appliance（ASA）の ユニファイド コミュニケーション ウィザード

ご使用のドメイン間フェデレーション導入に単一の IM and Presence サービスを導入する場合は、Cisco Adaptive Security Appliance でユニファイド コミュニケーション ウィザードを使用して、Cisco Adaptive Security Appliance と IM and Presence サービスの間のプレゼンス フェデレーション プロキシを設定できます。

ユニファイド コミュニケーション ウィザードが表示されている設定例を、次の URL にある IM and Presence サービスに関するドキュメンテーション wiki でご確認ください。

関連トピック

http://docwiki.cisco.com/wiki/Cisco_Unified_Presence%2C_Release_8.x

外部および内部インターフェイスの設定

Cisco Adaptive Security Appliance で 2 つのインターフェイスを設定するには、次のようにします。

- 1 つのインターフェイスを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（例、Microsoft Access Edge/アクセス プロキシ）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として使用します。これは、ご使用の導入に応じて、IM and Presence サービスへのインターフェイスか、ロード バランサのインターフェイスになります。
- インターフェイスを設定する際、イーサネットやギガビット イーサネットなどのインターフェイス タイプ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 Adaptive Security Appliance のスロット 0 には、4 つのイーサネット ポートまたはギガビット ポートが備わっています。任意に、スロット 1 に SSM-4GE モジュールを追加して、スロット 1 で 4 つのギガビット イーサネット ポートを実現することもできます。
- ルート トラフィックへのインターフェイスごとに、インターフェイス名と IP アドレスを設定する必要があります。内部インターフェイスの IP アドレ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含まれる必要があります。つまり、異なるサブマスクがある必要があります。
- 各インターフェイスのセキュリティ レベルは、0（最低）～ 100（最高）の間である必要があります。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、最もセキュアでないインターフェイスです。内部インターフェイスや外部インターフェイスに対してセキュリティ レベルを明示的に設定しない場合、Cisco Adaptive Security Appliance によりデフォルトで 100 に設定されます。
- CLI を使用して外部インターフェイスおよび内部インターフェイスを設定する方法の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

（注） 内部インターフェイスおよび外部インターフェイスは、ASDM 起動（ASDM startup）ウィザードを使用して設定することもできます。また、ASDM で [設定（Configuration）] > [デバイス設定（Device Setup）] > [インターフェイス（Interfaces）] を選択することによって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 ルートの設定

Cisco Adaptive Security Appliance は、OSPF、RIP および EIGRP などのダイナミック ルーティング プロトコルとスタティック ルートを両方ともサポートしています。本統合を実現するには、Cisco Adaptive Security Appliance 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に対するネクストホップアドレスを定義するスタティック ルートを設定する必要があります。次の手順で、dest_ip マスクは接続先ネットワークの IP アドレス、gateway_ip 値はネクスト ホップのルータまたはゲートウェイのアドレスです。

Cisco Adaptive Security Appliance でデフォルト ルートおよびスタティック ルートを設定する方法の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

はじめる前に

の手順を実行します。 外部および内部インターフェイスの設定, （78 ページ）

手順

ステップ 1 コンフィギュレーション モードを開始します。

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

ステップ 2 次のコマンドを入力して、内部インターフェイスにスタティック ルートを追加します。

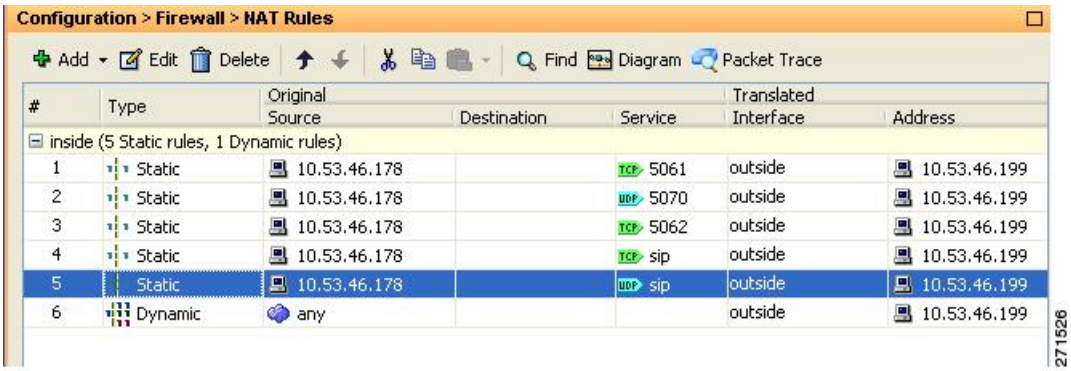
```
hostname(config)# route inside dest_ip mask gateway_ip
```

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にスタティック ルートを追加します。

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

（注） また、ASDM で [設定（Configuration）] > [デバイス設定（Device Setup）] > [ルーティング（Routing）] > [スタティック ルート（Static Route）] を選択することによってスタティック ルートを表示および設定することもできます。

図 *16*：***ASDM*** を使用したビューのスタティック ルート



次の作業

ポート アドレス変換（PAT），（80 ページ）

ポート アドレス変換（PAT）

本統合に必要なポート アドレス変換

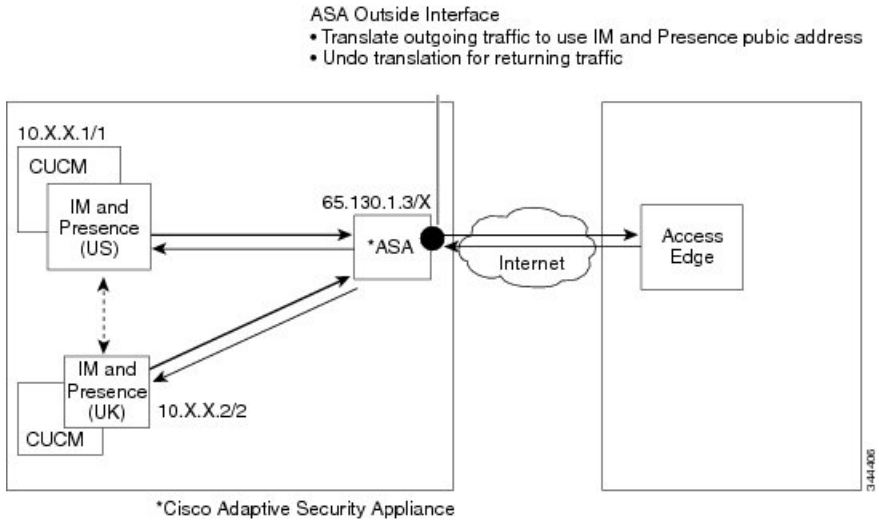
（注） 外部ドメインで別の IM and Presence サービスのエンタープライズ導入とのフェデレーションを行う場合は、ポート アドレス変換も使用します。

本統合を実現するため、Cisco Adaptive Security Appliance ではポート アドレス変換（PAT）およびスタティック PAT を使用してメッセージ アドレス変換を行っています。Cisco Adaptive Security Appliance では、本統合を実現するためにネットワーク アドレス変換（NAT）は使用していません。

本統合では、PAT を使用して、IM and Presence サービスから送信されたメッセージを外部ドメインに（プライベート メッセージをパブリック メッセージに）変換します。ポート アドレス変換（PAT）とは、パケット内の実際のアドレスおよびソース ポートが接続先ネットワーク上でルーティング可能なマップされたアドレスおよび固有のポートに置換されることを意味します。この変換方法で使用される二段階のプロセスでは、実際の IP アドレスとポートをマップされた IP アドレスとポートに変換します。戻ってくるトラフィックでは、変換が“元に戻されます”。

Cisco Adaptive Security Appliance は、IM and 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 and 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（プライベート メッセージからパブリック メッセージに）変換します。このため、ローカルの IM and Presence サービス ドメインでは 1 つのパブリック IP アドレスのみを使用します。Cisco Adaptive Security Appliance は、外部インターフェイスに NAT コマンドを割り当て、そのインターフェイスで受信された任意のメッセージの IP アドレスおよびポートを次の図に示すように変換します。

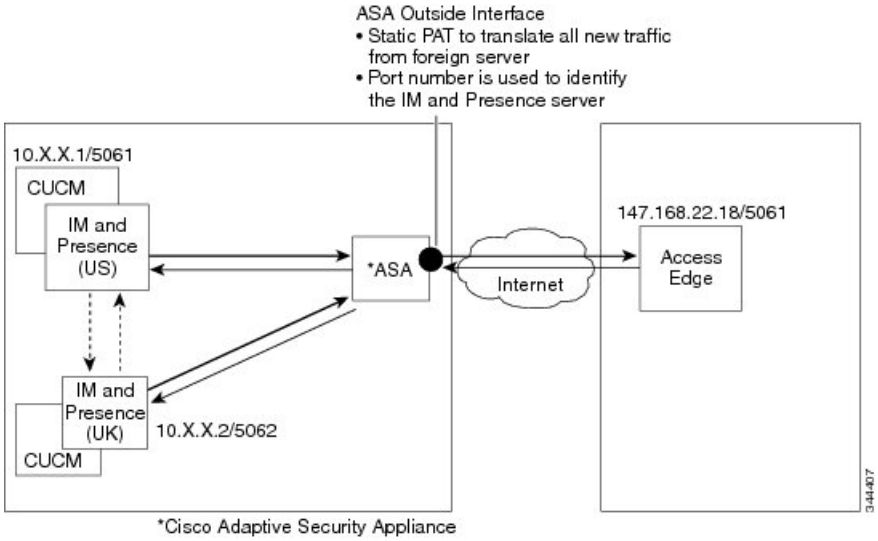
図 *17*：*IM and Presence* サービスから外部ドメインへのメッセージの *PAT* の例



外部ドメインから IM and Presence サービスへ送信された新しいメッセージの場合、Cisco Adaptive Security Appliance はスタティック PAT を使用して IM and 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 and Presence サービス ノードにマッピングします。スタティック PAT を使用することで、実際の IP アドレスをマップされた IP アドレスに変換し、実際のポート番号をマップされた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にも異なるポート番号にも変換することができます。この場合、ポート番号は次の図に示すように、適切な IM and Presence サービス ノードを識別して、メッセージ要求を処理します。

（注） IM and Presence サービス ノードにユーザが存在しない場合、IM and 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。すべての応答が、IM and Presence サービス ルーティング ノードから Cisco Adaptive Security Appliance に送信されます。

図 *18*：外部ドメインから送信されたメッセージに対してスタティック *PAT*



プライベート要求のポート/アドレスのパブリック要求のポート/アドレスへの変換（PAT）

本統合を実現するため、プライベート メッセージ ドレスのパブリック メッセージ ドレスへの変換には次の設定が必要になります。

- 変換したい実際の IP アドレスおよび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 Adaptive Security Appliance が内部インターフェイスで受信された任意のメッセージに NAT 操作を適用するという NAT ルールを設定します。
- 外部インターフェイスから発信されるメッセージに使用するマップされたアドレスを指定するグローバル NAT 操作を設定します。本統合を実現するには、ただ 1 つのアドレスを指定します（PAT を使用するため）。NAT 操作では、（内部インターフェイスで受信されたメッセージの）IP アドレスを IM and Presence サービスのパブリック アドレスにマップします。

プライベート要求のポート/アドレスのパブリック要求のポート/アドレスへの変換（PAT），（82 ページ） に、Cisco Adaptive Security Appliance リリース 8.2 と 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 and Presence サービスの導入でも複数の IM and Presence サービスの導入でも必須です。2 番目の行は、単一の IM and Presence サービスの導入の

みを対象としています。3 番目の行は、複数の IM and Presence サービスの導入を対象としています。

表 *13*：グローバル アドレス変換コマンドの例

設定例	Cisco Adaptive Security Appliance リリース 8.2 グローバル コマンド	Cisco Adaptive Security Appliance 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 and Presence サービス ノードがあり、それ以外のファイアウォール トラフィックがない導入で使用できます。	**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 and Presence サービス ノードとその他のファイアウォール トラフィックがある導入で使用できます。	**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* **object network** *my_inside***subnet 0.0.0.0 0.0.0.0 nat (inside,outside) dynamic interface**
この NAT 設定例は、内部インターフェイスに複数の IM and Presence サービス ノードとその他のファイアウォール トラフィックがある導入で使用できます。	**global (outside) 1** *public_imp_ip* **nat (inside) 1** *private_imp_net private_imp_netmask* **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* **object network** *my_inside***subnet 0.0.0.0 0.0.0.0 nat (inside,outside) dynamic interface**

（注） プライベート要求のポート/アドレスのパブリック要求のポート/アドレスへの変換（PAT），（82 ページ）で最後の行に示した設定例では、Cisco Adaptive Security Appliance の背後に複数の IM and Presence サービス ノードがある場合に、これらの IM and Presence サービス ノードがすべて同じサブネットに含まれることを想定しています。具体例を挙げると、すべての内部 IM and Presence サービス ノードが 2.2.2.x/24 ネットワーク内にある場合、NAT コマンドは nat (inside) 1 2.2.2.0 255.255.255.0 となります。

関連トピック

本統合に必要なポート アドレス変換, （80 ページ）

新規要求に対するスタティック PAT

本統合を実現するため、プライベート メッセージ ドレスのパブリック メッセージ ドレスへの変換には次の設定が必要になります。

- TCP でポート 5060、5061、5062 および 5080 に対してスタティック PAT コマンドを設定します。
- UDP でポート 5080 に対して別のスタティック PAT コマンドを設定します。

本統合で使用するポートの説明は、次のとおりです。

- 5060：このポートは、Cisco Adaptive Security Appliance で一般的な SIP 検査を行うために使用されます。
- 5061：このポートに SIP 要求が送信され、それによって TLS ハンドシェイクがトリガーされます。
- 5062、5080：これらのポートは、IM and Presence サービスにより SIP VIA/CONTACT ヘッダー内で使用されます。

（注） IM and Presence サービスのピア認証リスナーを確認するには、**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。

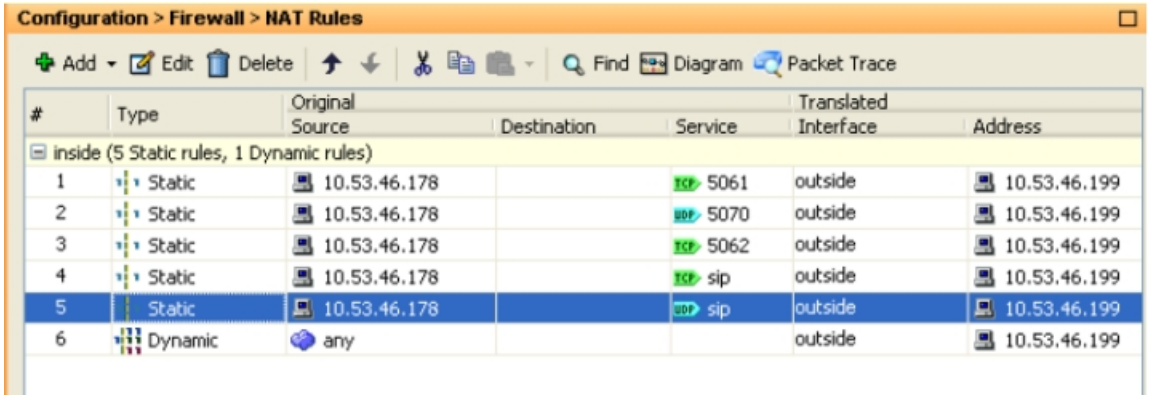
関連トピック

スタティック PAT コマンドの例, （85 ページ）
Cisco Adaptive Security Appliance の設定例, （195 ページ）

ASDM での NAT ルール

ASDM で NAT ルールを表示するには、[設定（Configuration）]>[ファイアウォール（Firewall）]>[NAT ルール（NAT Rules）] を選択します。次の図に示されている最初の 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 エントリはすべての発信トラフィックをパブリック IM and Presence サービス IP アドレスおよびポートにマップする発信 PAT 設定です。

図 *19*：*ASDM* での *NAT* ルールの表示



関連トピック

スタティック PAT コマンドの例, （85 ページ）
Cisco Adaptive Security Appliance の設定例, （195 ページ）

スタティック PAT コマンドの例

（注） この項では、Cisco Adaptive Security Appliance リリース 8.3 および リリース 8.2 のコマンドの例を示します。これらのコマンドは、フェデレーション用に Cisco Adaptive Security Appliance の新規設定を行う場合に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 設定

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

（注） Cisco Adaptive Security Appliance（ASA） 8.3 設定の場合、オブジェクトは一度定義するだけで複数のコマンド内で参照できます。同じオブジェクトを何度も定義する必要はありません。

表 *14*：*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 Adaptive Security Appliance リリース 8.2 のスタティック コマンド	Cisco Adaptive Security Appliance リリース 8.3 の NAT コマンド
static (inside,outside) tcp *public_imp_ip_address* **5061** *routing_imp_private_address***5062 netmask 255.255.255.255** ルーティングする IM and Presence サービスの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。 **static (inside,outside) tcp** *public_imp_ip_address* **5061** *routing_imp_private_address***5061 netmask 255.255.255.255** **static (inside,outside) tcp** *public_imp_ip_address* **5080** *routing_imp_private_address* **5080 netmask 255.255.255.255** **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_address* (for example **object network** *obj_host_10.10.10.10*) **#host** *public_imp_ip_address* **object network** *obj_host_routing_imp_private_address***host** *routing_imp_private_address* **object service** *obj_tcp_source_eq_5061***service tcp source eq 5061** **object service** *obj_tcp_source_eq_5062***service tcp source eq 5062** **nat (inside,outside) source static** *obj_host_routing_imp_private_address* *obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_5062 obj_tcp_source_eq_5061* ルーティングする IM and Presence サービスの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。 **nat (inside,outside) source static** *obj_host_routing_imp_private_address* *obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_5061 obj_tcp_source_eq_5061*
	object service *obj_tcp_source_eq_5080* **service tcp source eq 5080 nat (inside,outside) source static** *obj_host_routing_imp_private_address* *obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_5080 obj_tcp_source_eq_5080*
	object service *obj_tcp_source_eq_5060* **service tcp source eq 5060** （注） 5060 displays as "sip" in the service object. **nat (inside,outside) source static** *obj_host_routing_imp_private_address* *obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_5060* *obj_tcp_source_eq_5060*

Cisco Adaptive Security Appliance リリース 8.2 のスタティック コマンド	Cisco Adaptive Security Appliance リリース 8.3 の NAT コマンド
static (inside,outside) tcp *public_imp_ip_address* **5062** *routing_imp_private_address***5062 netmask 255.255.255.255**	**nat (inside,outside) source static** *obj_host_routing_imp_private_address obj_host_public_imp_ip_address* **service obj_tcp_source_eq_5062 obj_tcp_source_eq_5062**

関連トピック

新規要求に対するスタティック PAT, （84 ページ）
クラスタ間およびクラスタ内 IM and Presence サービス ノードの PAT 設定, （87 ページ）

クラスタ間およびクラスタ内 IM and Presence サービス ノードの PAT 設定

マルチノードまたはクラスタ間の IM and Presence サービスの導入で IM and Presence サービス クラスタ内の非ルーティング ノードが直接 Cisco Adaptive Security Appliance と通信する場合、これらのノードごとにスタティック PAT コマンドのセットを設定する必要があります。次にリストするコマンドは、単一のノードに対して設定する必要があるスタティック PAT コマンドのセットの例です。

任意のポートを使用できますが、未使用のポートである必要があります。対応する番号を選択することを推奨します。たとえば、5080 の場合は、未使用の任意のポート X5080 を使用します。ここで、X は IM and Presence サービス クラスタ間またはクラスタ内サーバに固有にマップされている番号に相当します。例を挙げると、45080 は特定のノードに固有にマップされており、55080 は別のノードに固有にマップされています。

次の表に、非ルーティング IM and Presence サービス ノードに対する NAT コマンドを示します。非ルーティング IM and Presence サービス ノードごとにコマンドを繰り返します。

（注） Cisco Adaptive Security Appliance（ASA） 8.3 設定の場合、オブジェクトは一度定義するだけで複数のコマンド内で参照できます。同じオブジェクトを何度も定義する必要はありません。

表 *15*：非ルーティング *IM and Presence* サービス ノードに対する *NAT* コマンド

Cisco Adaptive Security Appliance（ASA）リリース 8.2 のスタティック コマンド	Cisco Adaptive Security Appliance（ASA）リリース 8.3 の NAT コマンド
static (inside,outside) tcp *public_imp_address* **45062** *intercluster_imp_private_address* **5062 netmask 255.255.255.255** クラスタ間 IM and Presence サービスの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。 **static (inside,outside) tcp** *public_imp_address* **45061** *intercluster_imp_private_address* **5061 netmask 255.255.255.255**	**object network** *obj_host_intercluster_imp_private_address***host** *intercluster_imp_private_address* **object service** *obj_tcp_source_eq_45062***service tcp source eq 45062** **nat (inside,outside) source static** *obj_host_intercluster_imp_private_address obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_5062 obj_tcp_source_eq_45062* クラスタ間 IM and Presence サービスの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。 **object service** *obj_tcp_source_eq_45061* **service tcp source eq 45061 nat (inside,outside) source static** *obj_host_intercluster_imp_private_address obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_5061 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* **service tcp source eq 45080 nat (inside,outside) source static** *obj_host_intercluster_imp_private_address obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_5080 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* **service tcp source eq 45060 nat (inside,outside) source static** *obj_host_intercluster_imp_private_address obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_5060 obj_tcp_source_eq_45060*

関連トピック

新規要求に対するスタティック PAT, （84 ページ）
IM and Presence サービス ノードをルーティングするための PAT 設定, （85 ページ）

既存の導入に対する Cisco Adaptive Security Appliance（ASA）アップグレードオプション

Cisco Adaptive Security Appliance（ASA）のリリース 8.2 をリリース 8.3 にアップグレードすると、Cisco Adaptive Security Appliance（ASA）では既存のコマンドがシームレスに移行されます。

（注） IM and Presence サービス リリース 9.0 にアップグレードした場合は、Cisco Adaptive Security Appliance（ASA）に管理されている IM and Presence サービス 9.0 ノードごとに、Cisco Adaptive Security Appliance（ASA）のポート 5080 をオープンする必要があります。これは、Cisco Adaptive Security Appliance（ASA）もアップグレードしたかどうかには無関係です。

既存のフェデレーション導入で IM and Presence サービスと Cisco Adaptive Security Appliance（ASA）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てください。

アップグレード手順オプション 1：

1. IM and Presence サービスを リリース 9.0 にアップグレードする手順について説明します。
2. Cisco Adaptive Security Appliance（ASA）のポート 5080 に NAT ルールを設定します。
3. IM and Presence サービス のアップグレード後にフェデレーションが導入で機能していることを確認します。
4. Cisco Adaptive Security Appliance（ASA）を リリース 8.3 にアップグレードします。
5. Cisco Adaptive Security Appliance（ASA）のアップグレード後にフェデレーションが導入で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 サービス ノードを リリース 9.0、Cisco Adaptive Security Appliance（ASA）を リリース 8.3 にそれぞれアップグレードします。
2. 両方のアップグレード後、Cisco Adaptive Security Appliance（ASA）のポート 5080 に NAT ルールを設定します。
3. フェデレーションが導入で機能していることを確認します。

Cisco Adaptive Security Appliance（ASA）に管理されているすべての IM and Presence サービス リリース 9.0 ノードに対してポート 5080 をオープンするには、必要なコマンドがあります。

表 *16*：ポート *5080* への *Cisco ASA* コマンド

Cisco Adaptive Security Appliance（ASA）リリース 8.2 のスタティック コマンド	Cisco Adaptive Security Appliance（ASA）リリース 8.3 の NAT コマンド
static (inside,outside) tcp *public_imp_ip_address* **5080** *routing_imp_private_address***5080 netmask 255.255.255.255** **static (inside,outside) tcp** *public_imp_ip_address* **45080** *intercluster_imp_private_address* **5080 netmask 255.255.255.255** （注） クラスタ間 IM and Presence サービス 9.0 ノードごとにこれらのコマンドを設定し、サーバごとに異なる任意のポートを使用します。	**object service** *obj_tcp_source_eq_5080***# service tcp source eq 5080** **nat (inside,outside) source static** *obj_host_routing_imp_private_address obj_host_public_imp_ip_address***service** *obj_tcp_source_eq_5080 obj_tcp_source_eq_5080* **object service** *obj_tcp_source_eq_45080***# service tcp source eq 45080** **nat (inside,outside) source static***obj_host_intercluster_imp_private_address obj_host_public_imp_ip_address* **service***obj_tcp_source_eq_5080 obj_tcp_source_eq_45080* （注） クラスタ間 IM and Presence サービス 9.0 ノードごとにこれらのコマンドを設定し、サーバごとに異なる任意のポートを使用します。

第 7 章

Cisco Adaptive Securiy Appliance での TLS プロキシ設定

IM and Presence サービス リリース 8.5(2) 以降では、Microsoft Lync とのドメイン間フェデレーションがサポートされています。また IM and Presence サービス リリース 8.5(2) 以降の場合、OCS とのドメイン間フェデレーションへの参照には、別途明示的な指定がない限り、Microsoft Lync が指定されます。

TLS プロキシ設定の最新のリリース情報については、『*Cisco Adaptive Security Appliance Configuration Guide*』を参照してください。

TLS プロキシ

Cisco Adaptive Security Appliance は、IM and Presence サービスと外部サーバの間の TLS プロキシとして機能します。つまり、Cisco Adaptive Security Appliance は、（TLS 接続を開始した）サーバの代わりに TLS メッセージを仲介し、プロキシとしての自分からクライアントに TLS メッセージをルーティングします。TLS プロキシは、着信レッグの TLS メッセージを必要に応じて復号化、検査および変更してから、応答レッグの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 Adaptive Security Appliance と IM and Presence サービス間と、Cisco Adaptive Security Appliance と外部サーバ間に Cisco Adaptive Security Appliance 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する必要があります。

- IM and Presence サービスと Cisco Adaptive Security Appliance の間でのセキュリティ証明書交換, （58 ページ）
- Microsoft CA を使用した Cisco Adaptive Security Appliance と Microsoft Access Edge（外部インターフェイス）の間でのセキュリティ証明書交換, （62 ページ）

関連トピック

一般的な Cisco Adaptive Security Appliance の問題と推奨される操作, （181 ページ）

アクセス リストの設定の要件

この項では、単一の IM and Presence サービス導入に必要なアクセス リストの設定をリストします。

（注）
- アクセス リストごとに、対応するクラスマップを設定するとともに、ポリシーマップのグローバル ポリシーにエントリを設定する必要があります。
- IM and Presence サービスのピア認証リスナー ポートを調べるには、[Cisco Unified Communications Manager 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。

表 *17*：単一の *IM and Presence* サービス アクセス リスト設定の要件

項目	説明
配置シナリオ：1 つ以上の外部ドメインと連携する IM and Presence サービス ノード	

項目	説明
設定要件：	IM and 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 リストを設定します。 • IM and 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 リストを設定します。 • IM and 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 リストを設定します。Cisco Adaptive Security Appliance リリース 8.3 を使用する場合は、IM and 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 and Presence サービス ピア認証のリスナー ポートを確認してください）。
設定例：	**access-list** *ent_imp_to_external_server* **extended permit tcp host** *routing_imp_private_address* **host** *external_public_address* **eq 5061** Cisco Adaptive Security Appliance リリース 8.2: **access-list** *ent_external_server_to_imp* **extended permit tcp host** *external_public_address***host** *imp_public_address* **eq 5061** Cisco Adaptive Security Appliance リリース 8.3: **access-list** *ent_external_server_to_imp* **extended permit tcp host** *external_public_address* **host** *imp_private_address* **eq 5061** （注） 前述のアクセス リストで、5061 は、SIP メッセージングが行われていないかどうかを IM and Presence サービスがリッスンするポートです。IM and Presence サービスがポート 5062 をリッスンする場合は、アクセス リストに 5062 を指定します。
配置シナリオ：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。	
設定要件：	クラスタ間 IM and Presence サービス ノードごとに、次の 2 つのアクセス リストを設定します。 • IM and 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 リストを設定します。 • IM and Presence サービスが任意ポート 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 リストを設定します。Cisco Adaptive Security Appliance リリース 8.3 を使用する場合は、IM and 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 and Presence サービス ピア認証のリスナー ポートを確認してください）。

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** Cisco Adaptive Security Appliance リリース 8.2: **access-list** *ent_external_server_to_intercluster_imp* **extended permit tcp host***external_public_address* **host** *imp* **public address eq** *arbitrary_port* Cisco Adaptive Security Appliance リリース 8.3: *ent_external_server_to_intercluster_imp* **extended permit tcp host***external_public_address* **host** *imp_private_address* **eq** *5061* 前述のアクセス リストで、5061 は、SIP メッセージングが行われていないかどうかを IM and Presence サービスがリッスンするポートです。IM and Presence サービスがポート 5062 をリッスンする場合は、アクセス リストに 5062 を指定します。

関連トピック

Cisco Adaptive Security Appliance の設定例, （195 ページ）
TLS プロキシ インスタンスの設定, （94 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, （96 ページ）
TLS プロキシの有効化, （97 ページ）

TLS プロキシ インスタンスの設定

本統合を実現するには、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 プロキシでは、IM and Presence サービスが開始した TLS 接続を処理します。ここでは、IM and Presence サービスがクライアント、外部ドメインはサーバです。この場合、Cisco Adaptive Security Appliance が、IM and Presence サービスをクライアントとする TLS サーバとして機能します。2 番目の TLS プロキシでは、外部ドメインによって開始された TLS 接続を処理します。ここで、外部ドメインはクライアントで、IM and Presence サービスがサーバです。

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に対して“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た方向によって、サーバおよびクライアントのコマンドで定義されるトラストポイントが決定されます。

- TLS ハンドシェイクが IM and Presence サービスから外部ドメインに向かって開始された場合は、サーバ コマンドで指定するトラストポイントには、Cisco Adaptive Security Appliance 自己署名証明書を含めます。クライアント コマンドで指定するトラストポイントには、Cisco Adaptive Security Appliance と外部ドメインの間の TLS ハンドシェイクで使用される Cisco Adaptive Security Appliance 証明書を含めます。

- ハンドシェイクが外部ドメインから IM and Presence サービスに向かって開始された場合は、サーバ コマンドで指定するトラストポイントには、Cisco Adaptive Security Appliance と外部ドメインの間の TLS ハンドシェイクで使用する Cisco Adaptive Security Appliance 証明書を含めます。クライアント コマンドで指定するトラストポイントには、Cisco Adaptive Security Appliance 自己署名証明書を含めます。

はじめる前に

- アクセス リストの設定の要件, （92 ページ）の手順を実行します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

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

ステップ 2 IM and Presence サービスによって開始された TLS 接続に対して、TLS プロキシ インスタンスを作成します。次の例では、imp_to_external という TLS プロキシ インスタンスが作成されます。

```
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 接続に対して、TLS プロキシ インスタンスを作成します。次の例では、foreign_to_cup という TLS プロキシ インスタンスが作成されます。

```
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
```

次の作業

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, （96 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

クラス マップ 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。

はじめる前に

の手順を実行します。 TLS プロキシ インスタンスの設定, （94 ページ）

手順

ステップ 1 コンフィギュレーション モードを開始します。

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

ステップ 2 各アクセス リストに、クラス マップが使用する TLS プロキシ インスタンスを関連付けます。クラス マップが IM and Presence サービスから外部ドメインへのメッセージ用か、外部ドメインから IM and Presence サービスへのメッセージ用かによって、選択する TLS プロキシが異なります。次の例では、IM and Presence サービス外部ドメインへ送信されたメッセージのアクセス リストが、IM and Presence サービスによって開始された TLS 接続の “ent_imp_to_external” という TLS プロキシ インスタンス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 サービスに送信されるメッセージのアクセス リストが、「ent_external_to_imp」という外部サーバによって開始された TLS 接続の TLS プロキシ インスタンスと関連付けられます。

```
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 サービス導入を使用している場合は、各 IM and Presence サービス ノードにクラスマップを設定し、以前に定義したサーバの該当する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
```

次の作業

TLS プロキシの有効化, （97 ページ）

TLS プロキシの有効化

ポリシー マップ コマンドを使用して、前の項で作成したクラス マップごとに TLS プロキシを有効化する必要があります。

（注） フェデレーテッド導入に対し、Cisco Adaptive Security Appliance で高レベル セキュリティの sip-inspect ポリシー マップは、設定しても失敗するため使用できません。低レベル/中のセキュリティ ポリシー マップを使用する必要があります。

はじめる前に

の手順を実行します。 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，（96 ページ）

手順

ステップ 1 コンフィギュレーション モードを開始します。

```
> 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
```

Cisco Adaptive Security Appliance のクラスタ間導入用設定

クラスタ間 IM and Presence サービス導入では、IM and Presence サービス ノードを追加するたびに、Cisco Adaptive Security Appliance で次の設定を行う必要があります。

手順

ステップ 1 IM and Presence サービス ノードに対する追加アクセス リストを作成します。

ステップ 2 Cisco Adaptive Security Appliance セキュリティ証明書を生成し、IM and Presence サービス ノードにインポートします。

ステップ 3 IM and Presence サービス セキュリティ証明書を生成し、Cisco Adaptive Security Appliance 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 マップを設定します。

ステップ 5 クラス マップをグローバル ポリシー マップに追加します。

関連トピック

IM and Presence サービスと Cisco Adaptive Security Appliance の間でのセキュリティ証明書交換, （58 ページ）
IM and Presence サービスと Cisco Adaptive Security Appliance の間でのセキュリティ証明書交換, （58 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, （96 ページ）
TLS プロキシの有効化, （97 ページ）
クラスタ間展開とマルチノード展開, （5 ページ）

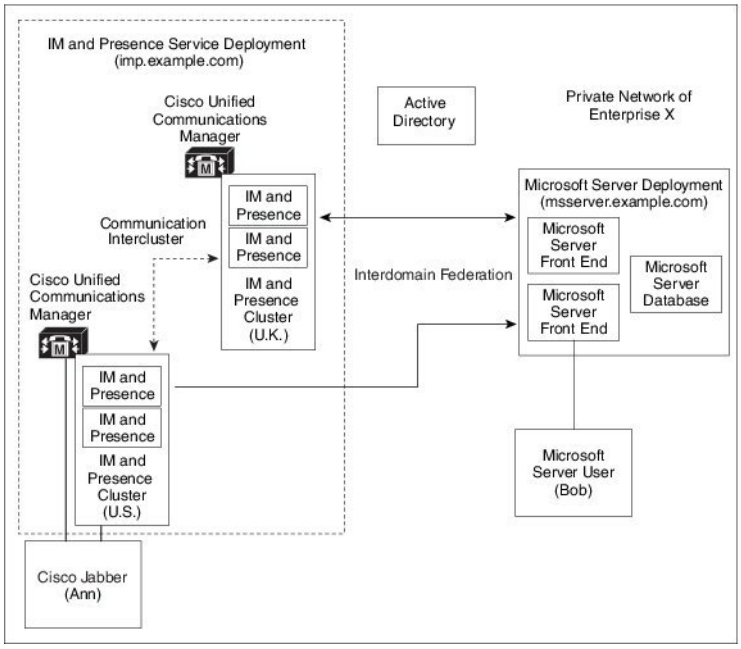
第 8 章

企業内の Microsoft OCS/Lync コンフィギュレーション ドメイン間フェデレーション

エンタープライズ内のサーバへのドメイン間フェデレーション

（注） 次のワークフローの適切な段階で、この章の手順を実行することを確認します（ASA ファイアウォールを使用しない企業内における Microsoft OCS/Lync との SIP フェデレーションに関する設定ワークフロー，（42 ページ））。全体のワークフローを実行することも、確認してください。

図 *20*：エンタープライズ内のサーバへのドメイン間フェデレーション



Microsoft サーバおよび IM and Presence サービス ドメインが異なる場合、企業内フェデレーションを設定できます。ドメインが異なればそれらは同等に適用することができるため、サブドメインを使用する必要はありません。詳細については、フェデレーションとサブドメインのトピックを参照してください。

エンタープライズ内での Microsoft サーバ ドメインの追加

OCS サーバや Lync サーバ用のフェデレーテッド ドメイン エントリを設定すると、IM and Presence サービス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。この着信

ACL がフェデレーテッド ドメインと関連付けられたことを [IM and Presence Administration] で確認できますが、着信 ACL は変更したり削除したりすることはできません。着信 ACL を削除できるのは、（関連付けられた）フェデレーテッド ドメイン エントリを削除する場合だけです。

手順

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

ステップ 2 [新規追加（Add New）] をクリックします。

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

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

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

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

ステップ 7 [保存（Save）] をクリックします。

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

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

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

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

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

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

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[プレゼンス（Presence）] > [ルーティング（Routing）] > [スタティック ルート（Static Routes）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 ドメイン、つまり FQDN が元に戻るよう [宛先パターン（Destination Pattern）] 値を入力します。次に、例を示します。

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

ステップ 4 その他のパラメータは次のように入力します。

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

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

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

  Microsoft OCS サーバは TCP および TLS 経由のフェデレーションをサポートします。TCP は Microsoft OCS サーバでのみサポートされます。

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

  Microsoft Lync サーバは、TLS 経由のフェデレーションのみをサポートします。TCP は Lync ではサポートされません。

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

ステップ 5 [保存（Save）] をクリックします。

次の作業

IM and Presence サービス用の Microsoft サーバのスタティック ルートを設定します。

Microsoft OCS サーバ コンフィギュレーション タスク リストへのフェデレーテッド リンク

次の表では、IM and Presence サービスと Microsoft OCS サーバ間のフェデレーション リンクを設定する手順の概要を示します。

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

- Standard Edition では Standard Edition サーバのスタティック ルートを設定する必要があります。
- Enterprise Edition では、すべてのプールにスタティック ルートを設定する必要があります。

表 *18*：*Microsoft OCS* サーバへのフェデレーション リンクのエンドツーエンド設定のタスク リスト

手順	説明
IM and Presence サービスのスタティック ルートの設定	TLS または TCP がサポートされています。 TLS では、[プロトコル タイプ（Protocol Type）] に [TLS]、[ネクスト ホップ ポート（Next Hop Port）] の番号として [5061] を選択します。 TCP では、[プロトコル タイプ（Protocol Type）] に [TCP]、[ネクスト ホップ ポート（Next Hop Port）] の番号として [5060] を選択します。
OCS での IM and Presence サービスのスタティック ルートの設定	TLS または TCP がサポートされています。 TLS の場合、スタティック ルート ポートは 5061 になります。 TCP の場合、スタティック ルート ポートは 5060 になります。 **重要** OCS のスタティック ルートとともに TLS を使用する場合は、IM and Presence サービス ノードの IP アドレスでなく FQDN を指定する必要があります。 ピア認証リスナー ポートを 5061 に設定し、サーバ承認リスナー ポートを変更します。 **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。 • 必ずピア認証リスナー ポートを 5061 にします。 • サーバ認証リスナー ポートが 5061 に設定されている場合は、別の値（5063）に変更する必要があります。

手順	説明
IM and Presence サービス用のホスト認証エントリを設定します。	この手順は、TLS および TCP に適用されます。 TLS では、IM and Presence サービス ノードそれぞれについて、1 つのエントリにIM and Presence サービス ノードの IP アドレスを使用し、2 つ目のエントリに IM and Presence サービス FQDN を使用して、2 つのホスト認証エントリを追加する必要があります。 TCP の場合、IM and Presence サービス IP アドレスを使用する 1 つのホスト認証エントリのみを各 IM and Presence サービス ノードに追加する必要があります。
OCS での証明書の設定	この手順は TLS の場合だけです。 CA ルート証明書および OCS の署名付き証明書を取得するには、次の手順を実行します。 • CA 証明書チェーンをダウンロードおよびインストールします。 • CA サーバの証明書を要求します。 • CA サーバから証明書をダウンロードします。 OCS の[フロントエンド サーバ プロパティ（Front End Server Properties）] で、OCS のポート 5061 で TLS リスナーが設定されていることを確認します（トランスポートは MTLS または TLS の場合もあります）。 [OCS フロント エンド サーバのプロパティ（OCS Front End Server Properties）] で、[証明書（Certificates）] タブを選択し、[証明書の選択（Select Certificate）] をクリックして、OCS 署名証明書を選択します。

手順	説明
FIPS（SSLv3 よりも、TLSv1）を使用するように OCS を設定し CA ルート証明書をインポートします。	この手順は TLS の場合だけです。 1 OCS のローカル セキュリティ設定を開きます。 2 コンソール ツリーから、[ローカル ポリシー（Local Policies）] を選択します。 3 [セキュリティ オプション（Security Options）] を選択します。 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）] をダブルクリックします。 5 セキュリティ設定を有効にします。 6 [OK] をクリックします。 （注） 有効にするには、OCS を再起動する必要があります。 7 IM and Presence サービス証明書に署名した CA の CA ルート証明書をインポートします。証明書スナップインを使用して OCS の信頼ストアに CA ルート証明書をインポートします。
IM and Presence サービス証明書の設定	この手順は TLS の場合だけです。 IM and Presence サービスに OCS サーバ証明書に署名した CA のルート証明書をアップロードします。また、IM and Presence サービス用の CSR を生成し、CA によって署名されるようにします。CA 署名付き証明書を IM and Presence サービスにアップロードします。 その後、OCS サーバの IM and Presence サービスで TLS ピア サブジェクトを追加します。詳細な手順については、証明書のセットアップに関するトピックを参照してください。

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

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

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

手順

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

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

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

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

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

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

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

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

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

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

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

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

次の作業

ホスト認証を IM and Presence サービスの OCS に追加します。

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

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

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

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

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

次の手順では、必要なホスト認証エントリを追加する方法について説明します。

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

手順

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

ステップ 2 次のいずれかの手順を実行します。

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

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

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [IP] を選択します。

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

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

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

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

ステップ 8 [OK] をクリックします。

OCS サーバでのポート 5060/5061 の有効化

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

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

手順

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

ステップ 2 フロント エンド サーバの FQDN を右クリックします。

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

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

ステップ 5 次のように、ポート値を設定します。

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

b) ポート値を選択します。

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

c) 輸送値を選択します。

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

ステップ 6 [OK] をクリックします。

Microsoft Lync サーバ コンフィギュレーション タスク リストにフェデレーション リンク

次の項に、IM and Presence サービス と Microsoft Lync サーバとの間のフェデレーション リンクを設定するエンド―ツーエンドの手順の概要を示します。

次の表に、IM and Presence サービス ノードと Microsoft Lync サーバとの間のフェデレーション リンクにスタティック ルートを設定する手順の概要を示します。 IM and Presence サービスとフェデ

レーション用 Microsoft Lync 間の TLS のスタティック ルートを設定します。 Microsoft Lync サーバにフェデレーションされているリンクに使用するスタティック ルートの設定に関する詳細については、https://technet.microsoft.com/en-us/library/gg615051.aspx を参照してください。

IM and Presence サービス ドメインごとにスタティック ルートを作成します。

表 *19*：*Microsoft Lync* サーバに連合リンクのスタティック ルートを設定するためのタスク リスト

手順	説明
IM and Presence サービスのスタティック ルートの設定	IM and Presence サービス上で、Lync サーバにスタティック ルートを作成します。 [プロトコル タイプ（Protocol Type）] に [TLS]、[次のホップ ポート（Next Hop Port）] の番号として [5061] を選択します。
Lync での IM and Presence サービスのスタティック ルートの設定	IM and Presence サービスの Lync のサーバのスタティック ルートを作成します。 IM and Presence サービス ルーティング ノード（ルータ ノードとして設定されているノードがない場合はパブリッシャ ノード）だけにスタティック ルートを作成しなければなりません。 IM and Presence サービス導入に複数のクラスタがある場合でも、加入者ノードにスタティック ルートとクラスタ間ピア ノードはいずれも作成する必要はありません。 ただし、スタティック ルートは、各 IM and Presence サービス プレゼンス ドメインで必要です。 （注） TLS で、IM and Presence サービス ピアの認証のリスナー ポートはデフォルトで 5062 に設定されます。 Microsoft サーバのスタティック ルートに合わせてピア認証のリスナー ポートを 5061 に切り替えてください。 ただし、サーバ認証のリスナー ポートはデフォルトで 5061 であるため、これを別のポートに変更する必要があります。 ポート 5061 を使用するように IM and Presence サービスのピア認証のリスナーポートを設定し、サーバ認証のリスナーポートを 変更します。 **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。 • 必ずピア認証リスナー ポートを 5061 にします。 • サーバ認証のリスナー ポートが 5061 に設定されている場合は、5063 など、別の値に変更する必要があります。
ルートの永続	この手順は、ルーティング ノードにのみ必要です。

スタティック ルートを設定した後、ホスト認証を設定し、トポロジをパブリッシュします。以下の表は、ホスト認証をセット アップし、トポロジをパブリッシュするタスクを示します。

表 *20*：ホスト認証の設定およびトポロジのパブリッシュのためのタスク リスト

手順	説明
信頼できるアプリケーション プールの作成	エンタープライズ エディションの場合は、IM and Presence サービス ノードを表す信頼済みアプリケーションのコンピュータを保存する単一の信頼できるアプリケーション プールを作成する必要があります。 標準エディションの場合は、各 IM and Presence サービス ノードの信頼済みアプリケーション プールを作成しなければなりません。
作成されたプールに信頼できるアプリケーションのコンピュータを追加する	ルーティング IM and Presence サービス ノードを除き、各 IM and Presence サービス ノードに作成されたプールに信頼できるアプリケーションのコンピュータを追加する必要があります。 Enterprise Edition の構成にだけこの手順を実行します。
作成されたプールへの信頼済みアプリケーション サーバの追加	エンタープライズ エディションの場合は、IM and Presence サービス導入に対して作成されたプールにアプリケーション サーバを追加します。 スタンダードエディションの場合は、ノード用に作成された各プールにアプリケーション サーバを追加します。
トポロジをイネーブルにします。	トポロジをイネーブルにする前に、次の項目が完了したことを確認してください。 • IM and Presence サービス ノードのルーティングに TLS ルートを定義します。 • IM and Presence サービス ノードのルーティングに新しいスタティック ルートを持続します。 • IM and Presence サービス展開の信頼済みアプリケーション プールを作成します。 • 各 IM and Presence サービス ノードに作成されたプールに信頼済みアプリケーションのコンピュータを追加します。 • IM and Presence サービスの展開に作成されたプールに信頼済みアプリケーション サーバを追加します。

Microsoft Lync サーバと IM and Presence サービス ノードに CA 署名付き証明書を追加しなければなりません。

表 *21*：*Microsoft Lync* サーバと *IM and Presence* サービス ノードの証明書を設定するためのタスク リスト

手順	説明
Lync の各サーバの証明書を設定します。	CA ルート証明書および Lync の署名付き証明書を取得するには、次の手順を実行します。 • CA 証明書チェーンをダウンロードおよびインストールします。 • CA サーバの署名付き証明書を要求します。 • Lync の証明書をインポートして割り当てます。 Lync サーバ証明書をインポートし、割り当てる詳細については Microsoft Lync のマニュアルを参照してください（http://technet.microsoft.com/en-us/library/gg558664.aspx）。
IM and Presence サービスでの証明書の設定	IM and Presence サービスに Lync サーバ証明書に署名した CA のルート証明書をアップロードします。 また、IM and Presence サービス用の CSR を生成し、CA によって署名されるようにします。 CA 署名付き証明書を IM and Presence サービスにアップロードします。 その後、Lync サーバの IM and Presence サービスで TLS ピア サブジェクトを追加します。 詳細な手順については、証明書のセットアップに関するトピックを参照してください。

フェデレーション用の Microsoft Lync のスタティック ルートを設定

IM and Presence サービスは Microsoft Lync サーバとのフェデレーションの Transport Layer Security（TLS）をサポートします。IM and Presence サービス ルーティング ノードのみにスタティック ルートを作成する必要があります。IM and Presence サービス展開に複数のクラスタがある場合でも、加入者ノードにスタティック ルートとクラスタ間ピア ノードはいずれも作成する必要はありません。

ただし、スタティック ルートは、各 IM and Presence サービス ドメインで必要です。

次の表に、この手順で使用した設定パラメータ例を示します。

表 *22*：*Microsoft Lync* の *TLS* スタティック ルート用のサンプル パラメータ

説明	サンプル パラメータ
IM and Presence サービス ノード FQDN（IM and Presence サービス ノードをルーティング） FQDN が正しい IP アドレスに解決できることを確認します。	impserverPub.sip.com

説明	サンプル パラメータ
IM and Presence サービス ノード IP アドレス（IM and Presence サービス ノードをルーティング）	10.10.1.10
IM and Presence サービス ノードの TLS ポート TLS ポート値が設定されたインターフェイスのユーザ インターフェイスと一致させる必要があります。値を確認するには、**[Cisco Unified CM IM and Presence Administration]** ユーザ インターフェイスにログインし、[システム（System）] > [アプリケーション リスナー（Application Listeners）] > [デフォルト Cisco SIP プロキシ TLS リスナー - ピア認証（Default Cisco SIP Proxy TLS Listener - Peer Auth）] を選択します。 （注） シスコはポート 5061 を推奨します。ただし、ポート 5062 を使用できます。	5061
IM and Presence サービス ノードのドメイン	sip.com
Lync 登録サーバ	lyncserver.synergy.com

（注）
- Transport Layer Security（TLS）を使用する場合は、スタティック ルートの宛先パターンで使用する FQDN は、Lync のフロント 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 and Presence サービス ノードの IP アドレスに解決されることを確認します。
- Lync FQDN をパーティション イントラドメイン フェデレーションに使用される IM and Presence サービス ドメインに一致させることはできません。

手順

ステップ 1 Lync Server サーバ管理シェルがインストールされたコンピュータに、ドメイン管理者などのロールでログインします。

ヒント RTCUniversalServerAdmins グループのメンバか、**New-CsStaticRoute** コマンドレットを割り当てたロールベース アクセス コントロール（RBAC）ロールとして、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 管理シェル（Lync Server Management Shell）] の順に選択します。

ヒント Microsoft Lync サーバのバージョンに応じて、Microsoft Lync Server 2010 または 2013 を入力します。

ステップ 3 TLS ルートを定義するには、次のコマンドを入力します。

```
$tlsRoute = New-CsStaticRoute -TLSRoute
-Destinationfqdn_of_imp_routing_node-Portlistening_port_imp_routing_node-usedefaultcertificate
$true -MatchUridestination_domain
```

例：

```
$tlsRoute = New-CsStaticRoute -TLSRoute
-Destinationimpserver Pub.sip.com-Port5061-usedefaultcertificate $true -MatchUrisip.com
```

引数の説明

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

（注）
- ドメインの子ドメインに一致させるには、**-MatchUri** パラメータに、たとえば *.sip.com などのワイルドカード値を指定できます。この値は sip.com サフィックスを持つどのドメインにも一致します。
- Microsoft Lync Server 2013 で IPv6 を使用する場合、**-MatchUri** パラメータの * ワイルドカード オプションはサポートされていません。
- **-usedefaultcertificate** を FALSE に設定した場合は、TLSCertIssuer および 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には、それぞれ、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指定します。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 新しく作成されたスタティック ルートを中央管理ストアで保持されていることを確認します。次のコマンドを入力します。

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

（注） IM and Presence サービス ノードをルーティングする場合のみこの手順を実行します。

ステップ 5 新しいスタティック ルートを保持するように設定した場合、コマンドが正常に実行され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 [外部ユーザ アクセス（External User Access）] エリアで、Lync のコントロール パネルを開きます。

a) [新規（New）] をクリックし、Lync が（IM and Presence サービスと）IM and Presence サービス ノードの FQDN とのフェデレーションを実行しているドメインのパブリック プロバイダーを作成します。

b) 新しいパブリック プロバイダーで、このプロバイダーとのすべての通信を許可するユーザ レベルの検証を設定します。

Enterprise Edition Lync Server での IM and Presence サービスに対するホスト認証の追加

Lync が許可を求められることなく SIP 要求を IM and Presence サービス から受け入れられるようにするには、IM and Presence サービス ノードごとに Lync でホスト認証のエントリを設定する必要があります。Enterprise Edition の場合、すべてのプールでこの手順を実行する必要があります。

（注） Lync とのパーティション イントラドメイン フェデレーションの TLS を設定する必要があります。TCP はサポートされません。

Lync と IM and Presence サービス間の TLS 暗号化に必要なホスト認証エントリを設定するには、各 IM and Presence サービス ノードの FQDN のホスト認証エントリを追加する必要があります。

手順

ステップ 1 以下のコマンドを使用して、IM and Presence サービス展開に対して信頼できるアプリケーション サーバを作成します。

ヒント プールの登録サービスの FQDN 値を検証するために **Get-CsPool** を入力できます。

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*

引数の説明

パラメータ	説明
-Identity	IM and Presence サービス展開の信頼済みアプリケーション プールの名前を入力します。これは FQDN 形式である必要があります。例：`trustedpool.sip.com` **ヒント** Active Directory にはないマシンに関する警告メッセージを無視し、変更を適用します。
-Registrar	プールのレジストラ サービス ID または FQDN。例：`lyncserver.synergy.com` この値は、コマンド Get-CsPool を使用して確認できます。
-Site	信頼できるアプリケーション プールを作成するサイトの数値。 **ヒント** Get-CsSite 管理シェルコマンドを使用します。
-Computerfqdn	IM and Presence サービス ルーティング ノードの FQDN。例：`impserverPub.sip.com` • impserverPub = IM and Presence サービス ホスト名。 • sip.com = IM and Presence サービス ドメイン。

ステップ 2 各IM and Presence サービス ノードに次のコマンドを入力し、新しいアプリケーション プールに信頼できるアプリケーションのコンピュータとしてノードの FQDN を追加します。

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

例：

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

引数の説明

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

ステップ 3 新しい信頼済みアプリケーションを作成し、それを新規アプリケーション プールに追加するには、次のコマンドを入力します。

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**

引数の説明

パラメータ	説明
-ApplicationID	アプリケーションの名前。これは任意の値にすることができます。例：imptrustedapp.sip.com。
-TrustedApplicationPoolFqdn	IM and Presence サービス展開の信頼済みアプリケーション プール サーバの FQDN。例：`trustedpool.sip.com`
-Port	IM and Presence サービス ノードの SIP リスニング ポート。TLS の場合、ポートは 5061 です。

次の作業

トポロジのパブリッシュを続行します。

関連トピック

統合のトラブルシューティング

IM and Presence サービスのホスト認証をスタンダード エディションの Lync サーバに追加

Lync が認証確認を求められずに IM and Presence サービスから SIP 要求を受け入れられるようにするには、展開しているすべての標準エディション Lync サーバの各 IM and Presence サービス ノードのホスト認証エントリを設定しなければなりません。Lync サーバ上で各 IM and Presence サービス ノードの 1 本の信頼済みアプリケーション プールを作成します。

（注） Lync とのパーティション イントラドメイン フェデレーションの TLS を設定する必要があります。TCP はサポートされません。

Lync と IM and Presence サービス間の TLS 暗号化に必要なホスト認証エントリを設定するには、各 IM and Presence サービス ノードの FQDN のホスト認証エントリを追加する必要があります。

手順

ステップ 1 次のコマンドを使用して各 IM and Presernce サービスの信頼済みアプリケーション サーバ プールを作成します。

ヒント プールの登録サービスの FQDN 値を検証するために **Get-CsPool** を入力できます。

```
New-CsTrustedApplicationPool
-Identity fqdn_of_the_im_and_presence_service_node -Registrar fqdn_of_the_lync_registrar_service -Site site_id_for_where_you_want_to_create_trusted_app_pool -TreatAsAuthenticated
$true -ThrottleAsServer $true -RequiresReplication $false -OutboundOnly $false
```

例：

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

引数の説明

パラメータ	説明
-Identity	信頼できるアプリケーション プールとして IM and Presence サービス ノードの FQDN 名を入力します。例：`impserverPub.sip.com` **ヒント** Active Directory にはないマシンに関する警告メッセージを無視し、変更を適用します。
-Registrar	プールのレジストラ サービス ID または FQDN。例：`lyncserver.synergy.com` この値は、コマンド Get-CsPool を使用して確認できます。
-Site	信頼できるアプリケーション プールを作成するサイトの数値。 **ヒント** Get-CsSite 管理シェルコマンドを使用します。

ステップ 2 各 IM and Presence サービス ノードの場合は、ノードの信頼済みアプリケーションを作成し、そのノードの信頼できるアプリケーションのサーバ プールに割り当てるには、次のコマンドを入力します。

```
New-CsTrustedApplication
-ApplicationID new_app_name -TrustedApplicationPoolFqdn new_trusted_app_pool_fqdn -Port 5061
```

例：

```
New-CsTrustedApplication
-ApplicationID imptrustedapp.sip.com -TrustedApplicationPoolFqdn impserverPub.sip.com -Port
5061
```

引数の説明

パラメータ	説明
-ApplicationID	ノードの FQDN にもなる信頼済みアプリケーションのコンピュータのアプリケーション ID。例：`impserverPub.sip.com`
-TrustedApplicationPoolFqdn	IM and Presence サービス導入で使用される信頼済みアプリケーション プールの FQDN。例：`impserverPub.sip.com`
-Port	IM and Presence サービス ノードの SIP リスニング ポート。TLS の場合、ポートは 5061 です。

次の作業

トポロジのパブリッシュ，（118 ページ）

関連トピック

統合のトラブルシューティング

トポロジのパブリッシュ

次の手順は、トポロジをコミットする例を示します。

手順

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

```
Enable-CsTopology
```

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

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

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

ステップ 3 `topology.xml` ファイルを開きます。

ステップ 4 クラスタの FQDN セクションで、信頼できるプールに追加した各 IM and Presence サービス ノードの IP アドレスを *"0.0.0.0"* から IP アドレス パラメータに変更します。

ステップ 5 `topology.xml` ファイルを保存します。

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

```
Publish-CsTopology -FileName "C:\topology.xml"
```

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

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

手順

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

- CUP 信頼証明書として証明書をアップロードします。
- [ルート証明書（Root Certificate）] フィールドは空白のままにします。
- IM and Presence サービスに自己署名証明書をインポートします。

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

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

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

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

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

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

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

次の作業

Microsoft Lync または OCS サーバで、「サーバ認証」と「クライアント認証」の両方で「強化キー」を保有している証明書を設定します。参照先：

- CA サーバからの証明書の要求, （69 ページ）
- Microsoft TechNet Library, Windows Server — Implementing and Administering Certificate Templates：http://technet.microsoft.com/en-us/library/cc731256(v=ws.10).aspx

第 9 章

SIP フェデレーション用の外部サーバ コンポーネントの設定

SIP フェデレーションを行うための Microsoft コンポーネントの設定

次の表に、Microsoft OCS サーバおよび Access Edge サーバでフェデレーションを設定するための簡単なチェックリストを示します。OCS サーバおよび Access Edge サーバの設定および導入の詳細な手順については、Microsoft のマニュアルを参照してください。

表 *23*：*Microsoft* コンポーネントの設定タスク - *OCS* サーバ

タスク	手順
グローバル フェデレーション設定の有効化	1 左側のペインのグローバル フォレスト ブランチで、[プロパティ（Properties）] > [グローバル プロパティ（Global Properties）] > [フェデレーション（Federation）] を選択します。 2 [フェデレーションとパブリック IM 接続の有効化（Enable Federation and Public IM Connectivity）] チェックボックスをオンにします。 3 Access Edge サーバの内部インターフェイスの FQDN およびポート番号を入力します。

タスク	手順
Access Edge サーバのアドレスの設定	1 左側のペインのグローバル フォレスト ブランチで、[プロパティ（Properties）] > [グローバル プロパティ（Global Properties）] > [エッジ サーバ（Edge Servers）] を選択します。 2 [Access Edge および Web 会議サーバ（Access Edge and Web Conferencing Edge Servers）] ウィンドウで、[追加（Add）] をクリックします。 3 Access Edge サーバの内部インターフェイスの FQDN を入力します。
各フロントエンドのフェデレーション設定の有効化	フェデレーションを行うフロントエンド サーバごとに、フェデレーション設定を有効化する必要があります。 1 左側のペインのフロントエンド サーバ ブランチで、[プロパティ（Properties）] > [フロント エンド プロパティ（Front End Properties）] > [フェデレーション（Federation）] を選択します。 2 [フェデレーションとパブリック IM 接続の有効化（Enable Federation and Public IM Connectivity）] チェックボックスをオンにします。
ユーザが MOC（Microsoft Office Communicator）およびフェデレーションを使用できるようなっていることを確認する	• [ユーザ（Users）] タブを選択し、ユーザが MOC を使用できるようになっていることを確認します。 • ユーザがこのリストにない場合、管理者は Microsoft Active Directory でユーザが MOC を使用できるようにする必要があります。 • また、Microsoft Active Directory でユーザが**パブリック IM 接続**を使用できるようにする必要があります。 次の URL にある Microsoft Active Directory のマニュアルを参照してください。 http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx
セキュリティ証明書の設定	• OCS サーバと Access Edge サーバの間のセキュリティ証明書を設定する必要があります。 • CA サーバは、この手順を実行する必要があります。 • これらのサーバ間のセキュリティ証明書を設定する方法の詳細については、Microsoft のマニュアルを参照してください。

表 *24* : ***Microsoft*** コンポーネントの設定タスク - ***Access Edge*** サーバ

タスク	手順
DNS の設定	Microsoft のエンタープライズ導入では、_sipfederationtls._tcp.*domain* をポイントするすべての Access Edge サーバにポート 5061 を介して外部 SRV を設定する必要があります。ここでは、*domain* は組織の SIP ドメイン名です。この SRV は、Access Edge サーバの外部 FQDN をポイントしている必要があります。
IM Provider としてIM and Presence サービス を設定する	**1** 外部 Access Edge サーバで、[スタート（Start）] > [管理ツール（Administrative Tools）] > [コンピュータの管理（Computer Management）] を選択します。 **2** 左側のペインで、[Microsoft Office Communications Server 2007] を右クリックします。 **3** [IM プロバイダ（IM Provider）] タブを選択します。 **4** [追加（Add）] をクリックします。 **5** [IM サービス プロバイダを許可する（Allow the IM service provider）] チェックボックスをオンにします。 **6** IM サービス プロバイダ名（例：IM and Presence ノード）を定義します。 **7** IM サービス プロバイダのネットワーク アドレス（この場合、IM and Presence サービス のノードのパブリック FQDN）を定義します。 **8** IM サービス プロバイダが “public”（パブリック）とマークされていないことを確認します。 **9** フィルタ オプション、[このプロバイダとのすべての通信を許可する（Allow all communications from this provider）] オプションをクリックします。 **10** [OK] をクリックします。 IM and Presence サービスのエンタープライズ導入では、各 IM and Presence サービス ドメインの DNS SRV レコードを設定する必要があります。DNS SRV レコードがポート 5061 を介して _sipfederationtls._tcp.*IM and Presence_domain* をポイントする必要があります。ここで、*IM and Presence _domain* は IM and Presence Service ドメインの名前です。この DNS SRV は IM and Presence サービス ノードのパブリック FQDN を指定する必要があります。

タスク	手順
アクセス方法の設定の確認	1 コンソール ツリーで、[Microsoft Office Communications Server 2007] を右クリックします。 2 [プロパティ（Properties）] > [アクセス方法（Access Methods）] をクリックします。 3 [フェデレーション（Federation）] チェックボックスをオンにします。 4 DNS SRV を使用している場合は、[検出を許可する（Allow discovery）] チェックボックスをオンにします。
TLSv1 を使用するよう Access Edge を設定する	1 ローカルセキュリティポリシーを開くには、[スタート（Start）] > [管理ツール（Administrative Tools）] > [ローカル セキュリティ ポリシー（Local Security Policy）] を選択します。 （注） これをドメインコントローラで設定する場合は、パスが [スタート（Start）] > [管理ツール（Administrative Tools）] > [ドメインコントローラ セキュリティ ポリシー（Domain Controller Security Policy）] となります。 2 コンソールで、[セキュリティ設定（Security Settings）] > [ローカル ポリシー（Local Policies）] > [セキュリティ オプション（Security Options）] を選択します。 3 詳細ペインでFIPSセキュリティ設定をダブルクリックします。 4 FIPS セキュリティ設定を有効化します。 5 [OK] をクリックします。 （注） Windows XP で FIPS を有効化した場合、Access Edge サーバのリモートデスクトップに問題が発生することがわかっています。この問題の解決策については、Access Edge に対してリモート デスクトップを実行できない，（191 ページ）を参照してください。
セキュリティ証明書の設定	• OCS サーバと Access Edge サーバの間のセキュリティ証明書を設定する必要があります。 • CA サーバは、この手順を実行する必要があります。 • これらのサーバ間のセキュリティ証明書を設定する方法の詳細については、Microsoft のマニュアルを参照してください。

関連トピック

企業内の Microsoft OCS/Lync コンフィギュレーション ドメイン間フェデレーション, （99 ページ）

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 サービスと AOL の間のドメイン間フェデレーションを有効化できるようにするには、シスコから AOL-FEDERATION SKU ライセンスを購入する必要があります。このライセンス要求を送信すると、シスコでは、このトピックの後続の項に記載する AOL カスタマー ルーティングおよび連絡先情報をお尋ねします。シスコがお客様の AOL カスタマー ルーティングおよび連絡先情報を受信すると、IM and Presence サービスと AOL の間での AOL フェデレーションが有効化されます。

関連トピック

AOL ルーティング情報の要件, （125 ページ）
AOL プロビジョニング情報要件, （126 ページ）

AOL ルーティング情報の要件

IM and Presence サービスと AOL SIP Access Gateway の間のドメイン間フェデレーションを設定する場合、AOL に次の情報を提供する必要があります。

展開タイプ	（各ドメインに）提供する情報	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 サービス ノードのパブリック FQDN：<sip.domain.com> • IM and Presence サービス ノードのドメイン名：@<domain.com>	• IM and Presence サービス サーバ証明書の件名 CN は、IM and Presence サービス ノードの FQDN と一致する必要があります。 • IM and Presence サービス サーバ証明書に署名する CA は、AOL サーバによって信頼されている必要があります。

展開タイプ	（各ドメインに）提供する情報	注記
ロード バランサ	• ロード バランサの FQDN：<lb.domain.com> • ロードバランサのドメイン名：@<domain.com>	• IM and Presence サービス サーバ証明書の件名 CN は、ロード バランサの FQDN と一致する必要があります。 • IM and Presence サービス サーバ証明書に署名する CA は、AOL サーバ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 サービス サーバのセキュア SIP フェデレーション ポート	AOL SIP Access Gateway 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 ポートは 5061 です。

この情報を AOL に提供するにあたっては、シスコのサポート担当者と連携されることを推奨します。

AOL プロビジョニング情報要件

- エンタープライズまたは会社などの名前。
- フェデレーションに使用されるすべてのローカル ドメイン名（companyabc.com、sales-companyabc.com）。
- フェデレーションに使用する IM and Presence サービス ノードの FQDN。
- カスタマーの連絡先詳細：名前、電子メール アドレス、電話番号。
- 証明書のコピー：
  - 証明書が認証局によって署名されている場合、認証局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
CgmSJomT8ixkARkWA2NvbTEZMBcGCgmSJomT8ixkARkWCWhpY3k2md[illegible]
4zd4FeZvoCzyVglPkoLvA0Z+AJyOkO7/tie4EF3n/kEedaPWimv2TpRrlAP5lBXn
tbM82NpEDaSqzg0d4Dswqe7W30CKGgUBYS1fO7xJHSRju719D+H7XivmjvU= -----END
CERTIFICATE-----

この情報をAOLに提供するにあたっては、シスコのサポート担当者と連携されることを推奨します。

第 10 章

冗長性確保のためのロードバランサの設定（SIP フェデレーションの場合）

ロード バランサについて

冗長性とハイ アベイラビリティを持たせるために、フェデレーテッド ネットワークにロード バランサを組み込むことができます。ロード バランサは、IM and Presence サービス ノードと Cisco Adaptive Security Appliance の間に配置されます（SIP フェデレーションのハイ アベイラビリティ，（7 ページ）を参照）。

ロードバランサは、Cisco Adaptive Security Appliance からの着信 TLS 接続を終端したうえで、TLS 接続を新たに開始して適切なバックエンド IM and Presence サービス ノードへデータをルーティングします。

IM and Presence サービス 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 サービスのパブリッシャ ノードおよびサブスクライバ 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、[サービス（Service）] メニューから [システム（System）] > [サービス パラメータ（Service Parameters）] > [Cisco SIP プロキシ（Cisco SIP Proxy）] を選択し、これらの値を入力します。 • [仮想 IP アドレス（Virtual IP Address）]：ロード バランサに設定されているバーチャル IP アドレスを入力します。 1 [サーバ名（Server Name）]：ロード バランサの FQDN に設定します。 2 [フェデレーション ルーティング IM and Presence FQDN（Federation Routing IM and Presence FQDN）]：ロード バランサの FQDN に設定します。
新規 TLS ピア サブジェクトの作成	1 [Cisco Unified IM and Presence Administration] にログインし、[システム（System）]>[セキュリティ（Security）] > [TLS ピア サブジェクト（TLS Peer Subjects）] を選択します。 2 [新規追加（Add New）] をクリックして、次の値を入力します。 • [ピア サブジェクト名（Peer Subject Name）]：ロード バランサの外部 FQDN を入力します。 • [説明（Description）]：ロード バランサの名前を入力します。
TLS ピア サブジェクト リストへの TLS ピアの追加	1 [Cisco Unified IM and Presence Administration] にログインし、[システム（System）]>[セキュリティ（Security）] > [TLS コンテキスト設定（TLS Context Configuration）] を選択します。 2 [検索（Find）] をクリックします。 3 [Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context] をクリックします。 4 ロード バランサ フェデレーション TLS ピア サブジェクトを選択した TLS ピア サブジェクト リストに移動します。

関連トピック

フェデレーションのルーティング パラメータの設定, （49 ページ）
新規 TLS ピア サブジェクトの作成, （51 ページ）
選択した TLS ピア サブジェクト リストへの TLS ピアの追加, （52 ページ）

Cisco Adaptive Security Appliance（ASA）の更新

ロードバランサを使用しても、外部ドメインはメッセージをパブリック IM and Presence サービス アドレスに送信しますが、Cisco Adaptive Security Appliance によって、このアドレスはロードバランサのバーチャル IP アドレスにマップされます。つまり、Cisco Adaptive Security Appliance は、外部ドメインからメッセージを受信した場合、それをロード バランサに転送するということです。ロード バランサは適切な IM and Presence サービス ノードへ渡します。

このような設定を実現するには、Cisco Adaptive Security Appliance を一部変更する必要があります。

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むよう、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 Adaptive Security Appliance（ASA）リリース 8.2 のコマンド	Cisco Adaptive Security Appliance（ASA）リリース 8.3 のコマンド
IM and Presence サービス パブリッシュに対して必要な変更		

タスク	Cisco Adaptive Security Appliance（ASA）リリース 8.2 のコマンド	Cisco Adaptive Security Appliance（ASA）リリース 8.3 のコマンド
パブリック IM and Presence サービス アドレスに対して未使用の任意のポートを使用するよう、スタティック PAT を変更します。	変更前： **static (inside,outside) tcp** *public_imp_ip_address 5061 routing_imp_private_ip_address 5062* **netmask***255.255.255.255* 変更後： **static (inside,outside) tcp** *public_imp_ip_address 55061 routing_imp_publisher_ private_ip_address 5062* **netmask** *255.255.255.255*	変更前： **object service** *obj_tcp_source_eq_5061* **# service tcp source eq** *5061* **nat (inside,outside) source static***obj_host_routing_imp_private_ip_address obj_host_public_imp_ip_address* **service***obj_tcp_source_eq_5062 obj_tcp_source_eq_5061* 変更後 **object service** *obj_tcp_source_eq_55061***# service tcp source eq***55061* **nat (inside,outside) source static** *obj_host_routing_imp_private_ip_address obj_host_public_imp_ip_address* **service***obj_tcp_source_eq_5062 obj_tcp_source_eq_55061*
（どのポートでロード バランサが TLS メッセージをリッスンする場合でも）パブリック IM and Presence サービス アドレスに送信されたメッセージを仮想ポート アドレスに転送できるようにする、新しいスタティック PAT を追加します。	**static (inside,outside) tcp** *public_imp_address 5061 load_balancer_vip 5062* **netmask** *255.255.255.255*	**object network** *obj_host_load_balancer_vip* **# host** *routing_imp_private_address* **object service** *obj_tcp_source_eq_5061***# service tcp source eq***5061* **nat (inside,outside) source static***obj_host_load_balancer_vip obj_host_public_imp_ip_address* **service***obj_tcp_source_eq_5062 obj_tcp_source_eq_5061*
IM and Presence サービス サブスクライバに対して必要な変更		

タスク	Cisco Adaptive Security Appliance（ASA）リリース 8.2 のコマンド	Cisco Adaptive Security Appliance（ASA）リリース 8.3 のコマンド
ロード バランサのバーチャル IP アドレスへの新規アクセス リストを追加します。IM and Presence サービスがアクセスする必要の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。	**access-list** *ent_lber_to_external_ocs* **extended permit tcp host** *subscriber_private_ip_address* **host** *external_domain_public_ip_address 5061* **access-list** *ent_lcs_to_lber_routg_imp* **extended permit tcp host** *external_domain_public_ip_address* **host** *imp_public_ip_address 65061*	
ロード バランサのバーチャル IP アドレスが設定されている場合に IM and Presence サービス サーバへのメッセージを開始できるようにするには、**拡張許可TCP ホスト**外部ドメインの新規アクセス リストを追加します。IM and Presence サービスにアクセスする必要の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。		

関連トピック

スタティック IP ルートの設定, （79 ページ）
ポート アドレス変換（PAT）, （80 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 Adaptive Security Appliance のアクセス リストを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 Adaptive Security Appliance で DNS レコードに設定されされた、IM and Presence サービス ドメインのパブリック IP アドレスのことです。このレコードには、Cisco Adaptive Security Appliance のパブリック IP を含む、ロード バランサの FQDN が記載されます。

手順

配置シナリオ：1 つ以上の外部ドメインと連携する IM and Presence サービス ノード

タスク	設定例
新しいロードバランサのバーチャル IP アドレスへの新規アクセス リストを追加します。IM and Presence サービスがアクセスする必要の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。	パブリッシャの場合 Cisco Adaptive Security Appliance リリース 8.2 および 8.3 のコマンド： **access-list** *ent_lber_to_external_ocs* **extended permit tcp host** *virtual_IP_address* **host** *external_domain_public_ip_address* **eq 5061**
ロード バランサの仮想 IP アドレスが、IM and Presence サービス ノードに初期メッセージに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 サービスにアクセスする必要の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。	パブリッシャの場合 Cisco Adaptive Security Appliance リリース 8.2 のコマンド **access-list** *ent_lcs_to_lber_routgimp* **extended permit tcp host** *external_domain_public_ip_address* **host** *imp_public_ip_address* **eq 5062** Cisco Adaptive Security Appliance リリース 8.3 のコマンド **access-list** *ent_external_server_to_lb***extended permit tcp host***external_public_address***host** *loadbalancer_virtual_ip_address* **eq 5062**
アクセス リストごとに、新しいアクセス リストを組み込むための新しいクラスを追加します。	**class** *ent_lber_to_external_ocs* **match access-list** *ent_lber_to_external_ocs*
クラスごとに、IM and Presence サービスによって開始されたメッセージのエントリを policy-map global_policy に作成します。	**policy-map global_policy class** *ent_lber_to_external_ocs***inspect sip** *sip_inspect* **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エントリを policy-map global_policy に作成します。	**policy-map global_policy class** *ent_lcs_to_lber_routgimp***inspect sip** *sip_inspect* **tls-proxy** *ent_external_to_imp*

導入シナリオ：外部ドメインが 1 つ以上のクラスタ間 IM and Presence サービス ノードに追加される IM and Presence サービス フェデレーションへの IM and Presence サービス

タスク	設定例
外部ドメインの Adaptive Security Appliance は、ローカル ドメインのパブリッシャとサブスクライバ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* **extended permit tcp host** *external_domain_private_imp_address* **host** *public_imp_address_local_domain 55061* **access-list** *ent_imp_to_externalSubimpwlber* **extended permit tcp host** *external_domain_private_imp_address* **host** *public_imp_address_local_domain 65061*
アクセスリストごとに、新しいアクセスリストを組み込むための新しいクラスを追加します。	
クラスごとに、policy-map global_policy にエントリを作成します。	

関連トピック

アクセス リストの設定の要件, （92 ページ）

TLS プロキシ インスタンスの更新

Cisco Adaptive Security Appliance で TLS プロキシ インスタンスを更新します。

手順

変更前：

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

変更後：

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 インスタンスの設定, （94 ページ）

CA 署名付きセキュリティ証明書の更新

設定にロード バランサを追加する場合は、次の項で説明する、ロード バランサと Cisco Adaptive Security Appliance および IM and Presence サービス ノードの間の CA 署名付きセキュリティ証明書も作成する必要があります。

ロード バランサと Cisco Adaptive Security Appliance 間のセキュリティ証明書の設定

このトピックでは、ロード バランサと Cisco Adaptive Security Appliance の間で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
Cisco Adaptive Security Appliance でロードバランサ用の CA 署名付き証明書を作成します。	**crypto ca enroll** コマンドを使用して、ロードバランサの FQDN を指定します。
Cisco Adaptive Security Appliance 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い。
ロードバランサで Cisco Adaptive Security Appliance 用の CA 署名付き証明書を作成します。	ロード バランサのマニュアルを参照してください。
ロード バランサから Cisco Adaptive Security Appliance に CA 署名付き証明書をインポートします。	**crypto ca trustpoint** コマンドを使用します。 証明書がインポートされたことを確認するには、**show crypto ca certificate** コマンドを使用します。

関連トピック

SCEP を使用した Cisco Adaptive Security Appliance での証明書の設定 , （63 ページ）

Cisco Adaptive Security Appliance への IM and Presence サービス証明書のインポート, （61 ページ）
Microsoft CA を使用した Cisco Adaptive Security Appliance と Microsoft Access Edge（外部インターフェイス）の間でのセキュリティ証明書交換, （62 ページ）

ロード バランサと IM and Presence サービス ノード間のセキュリティ証明書の設定

このトピックでは、ロード バランサと IM and Presence サービス ノードの間で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署名付き証明書を作成します。	CA 署名付き証明書を使用して証明書を交換する手順に従ってください。
（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
FQDN のすべてのインスタンスをロードバランサのFQDNに一致するよう更新します。	

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 サーバで、[スタート（Start）] > [管理ツール（Administrative Tools）] > [コンピュータの管理（Computer Management）] を選択します。 2 左側のペインで、[Microsoft Office Communications Server 2007] を右クリックします。 3 [IM プロバイダ（IM Provider）] タブをクリックします。 4 [追加（Add）] をクリックします。 5 [Allow the IM service provider（IM サービス プロバイダを許可する）] チェックボックスをオンにします。 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 バランサのパブリック FQDN として定義します。

関連トピック

SIP フェデレーション用の外部サーバ コンポーネントの設定, （121 ページ）

AOL コンポーネントの更新

ご使用の AOL フェデレーション導入にロード バランサを組み込む場合は、ロード バランサに関するいくつかの細目を AOL に提供する必要があります。詳細については、関連項目内の項を参照してください。

関連トピック

AOL との SIP フェデレーションの要件, （125 ページ）

第 11 章

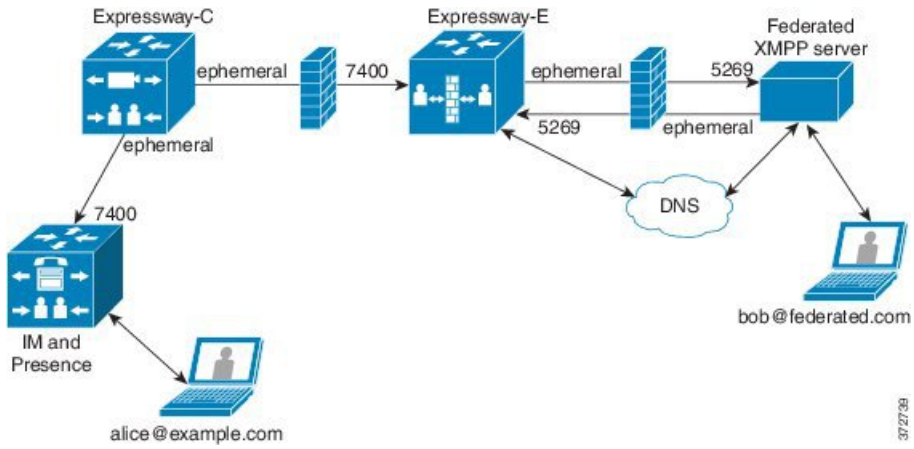
XMPP フェデレーション用の IM and Presence サービスの設定

Cisco Expressway 経由の外部 XMPP フェデレーション

外部 XMPP フェデレーションを導入するために推奨される方法は、Cisco Expressway を経由することです。Cisco Expressway は、別の XMPP 導入の Expressway-E ユーザと通信するため、IM and Presence サービスに登録されたユーザをイネーブルにします。次の図は、XMPP メッセージが Expressway-C、Expressway-E のコラボレーション エッジ ソリューションを介してオンプレミス IM and Presence サービス サーバからフェデレーテッド XMPP サーバへどのように経路指定されているかを示します。また、メッセージが DMZ ファイアウォールを通過するときに使用される接続とポートを示しています。

（注） Expressway-C、Expressway-E の組み合わせはここに表示されますが、VCS Control および VCS Expressway の組み合わせを使用している場合、同じ外部の XMPP フェデレーション機能も使用できます。Express シリーズ オプションの詳細については、『Cisco Expressway Administrator Guide (X8.2)』を参照してください。VCS オプションの詳細については、『Cisco TelePresence Video Communication Server Administrator Guide (X8.2)』を参照してください。

図 *21*：*Cisco Expressway* 経由の外部 *XMPP* フェデレーション



（注） SIP および XMPP フェデレーションは別のものであり、相互に影響を与えません。たとえば、IM and Presence サービスの SIP フェデレーションと Cisco Expressway の外部 XMPP フェデレーションを展開することができます。

サポートされるフェデレーション

Expressway E は次の企業との XMPP フェデレーションをサポートします。

- Cisco Unified Communications Manager IM and Presence サービス リリース 9.1 以降
- Cisco Webex Connect リリース 6.x
- XMPP 規格準拠サーバ

サポートされる導入設定

次の XMPP フェデレーションの導入オプションが使用可能です。

- 外部の XMPP フェデレーションのみ（Cisco Expressway で終了）
- 内部の XMPP フェデレーションのみ（IM and Presence サービスで終端）

- 内部および外部の XMPP フェデレーション（IM and Presence サービスで終端）が着信接続を許可するようにファイアウォールを設定する必要があります。

Cisco Expressway 経由の外部 XMPP フェデレーションについての詳細については、『Cisco Expressway Administrator's Guide（X8.2）』を参照してください。

制約事項

- 同時内部 XMPP フェデレーションは IM and Presence サービスで終端され、Cisco Expressway で終端する外部 XMPP フェデレーションはサポートされません。

重要 Cisco Expressway を通じて外部 XMPP フェデレーションを導入する場合、IM and Presence サービス上で Cisco XCP XMPP Federation Connection Manager 機能サービスをアクティブ化しないでください。

- Expressway-E は（電子メールアドレスなどの）XMPP のアドレス変換をサポートしません。XMPP フェデレーションに Expressway-E を使用する場合は、IM and Presence サービスからネイティブ プレゼンス Jabber ID を使用しなければなりません。

XMPP フェデレーションの一般的な設定の指定

XMPP フェデレーションの概要

IM and Presence サービス リリース 9.0 以降では、次のエンタープライズとの XMPP フェデレーションをサポートしています。

- Cisco WebEx Messenger Release 7.x
- IBM Sametime リリース 8.2 および 8.5
- Cisco Unified Presence リリース 8.x
- IM and Presence リリース 9.x 以上

（注） IM and Presence サービス は IM and Presence サービス リリース 9.x Enterprise と Cisco Unified Presence リリース 7.x Enterprise 間の XMPP フェデレーションをサポートしていません。

IM and Presence サービス と WebEx Enterprise のフェデレーションを実行する場合、WebEx Connect クライアント ユーザは IM and Presence サービス ユーザを一時的なチャット ルームまたはパーシステント チャット ルームに招待できません。これは、WebEx Connect クライアントにある設計の制約のためです。

IM and Presence サービスを XMPP でフェデレーションを実行できるようにするには、この章の手順に従って IM and Presence サービス で XMPP フェデレーションを有効にし、設定する必要があります。

複数の IM and Presence サービス クラスタがある場合、1 つのクラスタに少なくとも 1 つのノードで XMPP フェデレーションを有効にし、設定する必要があります。また、すべてのクラスタで XMPP フェデレーション設定を同じにする必要があります。**トラブルシュータ診断**では、クラスタ全体の XMPP フェデレーション設定が比較され、クラスタ全体で XMPP フェデレーション設定が同じかどうかがレポートされます。

ファイアウォールのために Cisco Adaptive Security Appliance を導入する場合、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 権限の考慮事項については、統合の準備に関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設定については、Cisco Adaptive Security Appliance を設定するタスクを参照してください。

XMPP フェデレーション用サービスの再起動に関する特記事項

XMPP フェデレーション設定のいずれかを変更する場合は、Cisco XCP Router および 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 のサービスアビリティ（IM and Presence Serviceability）] ユーザ インターフェイスにログインします。

- Cisco XCP ルータは、[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 フェデレーション接続マネージャで、[ツール（Tools）] > [コントロール センター - 機能サービス（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 サービスによってすべての XCP サービスが再起動されます。

1 つのノードで XMPP フェデレーションをイネーブルまたはディセーブルにする場合、XMPP フェデレーションをイネーブルまたはディセーブルにしたノードだけでなく、クラスタ内にあるすべてのノードの Cisco XCP ルータを再起動する必要があります。Cisco XCP ルータのその他すべての XMPP フェデレーション設定については、設定を変更したノードのみを再起動する必要があります。

ノードで XMPP フェデレーションをオンにする

デフォルトでこの設定は無効です。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[プレゼンス（Presence）] > [ドメイン間フェデレーション（Inter Domain Federation）] > [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 ノードのステータス（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イネーブルにしないと IM and Presence サービス ノードで XCP XMPP Federation Connection Manager サービスを起動できません。

次の作業

XMPP フェデレーションのセキュリティ設定を指定する, （143 ページ）

XMPP フェデレーションのセキュリティ設定を指定する

はじめる前に

- フェデレーション対象の外部ドメインが TLS 接続をサポートするかどうかを決定します。
- TLS および SASL 固有の設定は、SSL モードの “[TLS（オプション）（TLSOptional）]” または “[TLS（必須）（TLS Required）]” を選択した場合にのみ変更できます。
- TLS を使用して IM and Presence サービスと IBM 間のフェデレーションを設定している場合、SSL モードの “[TLS（必須）（TLS Required）]” を設定し、SASL を有効にする必要があります。

手順

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）] > [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 サービスで、外部ドメインとの TLS 接続が確立されません。外部ドメインとのフェデレーションには暗号化されていない接続が使用され、他のサーバの ID を識別するにはサーバ ダイヤルバック メカニズムが使用されます。

b) [TLS（オプション）（TLS Optional）]：IM and Presence サービスで、外部ドメインとの TLS 接続が試行されます。IM and Presence サービスで TLS 接続の確立に失敗すると、サーバダイヤルバックに戻り、他のサーバの ID が検証されます。

c）[TLS（必須）（TLS Required）]：外部ドメインとのセキュア（暗号化）接続が保証されます。

ステップ 3 ルート CA 証明書に対して外部ドメイン サーバの証明書を厳密に検証することを必須にするには、[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）] のセキュリティ設定を選択すると、デフォルトでこの設定はオンです。

（注） WebEx との XMPP フェデレーションを設定している場合、[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ないでください。

ステップ 4 [すべての着信接続の 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、IM and Presence サービスが着信接続試行の SASL EXTERNAL のサポートをアドバタイズし、SASL EXTERNAL 検証を実行します。

ステップ 5 外部サーバが SASL EXTERNAL を要求する場合に、IM and Presence サービスによって SASL 認証 ID が外部ドメインに確実に送信されるようにするには、[アウトバウンド接続で SASL を有効化（Enabling SASL on outbound connections）] チェックボックスをオンにします。

ステップ 6 IM and Presence サービスへの接続を試行する外部サーバの ID を検証するために DNS を使用する場合、ダイヤルバック シークレットを入力します。IM and Presence サービスは、DNS が外部サーバの ID を検証するまでは、外部サーバ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
- セキュリティ設定の詳細については、オンライン ヘルプを参照してください。
- サーバがクラスタ間導入の一部の場合、同じセキュリティ設定を使用して各クラスタを設定する必要があります。すべてのノードで同じ設定になるように、システム トラブルシュータを実行します。

関連トピック

ノードで XMPP フェデレーションをオンにする，（142 ページ）

XMPP フェデレーション用の DNS の設定

XMPP フェデレーション用 DNS SRV レコード

IM and Presence サービスで特定の 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 エンタープライズからパブリック DNS サーバの _xmpp-server DNS SRV レコードを公開する必要があります。同様に、IM and Presence サービスでドメイン用に DNS と同じ DNS SRV レコードを公開する必要があります。両方のエンタープライズはポート 5269 を公開する必要があります。公開された FQDN は、DNS で IP アドレスに解決できる必要があります。

DNS SRV レコードは、IM and Presence サービス導入環境内の各ドメインに対して公開する必要があります。[Cisco Unified Communications Manager IM and Presence Administration] ユーザ 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。システム内のすべてのドメイ

ンのリストを表示するには、[プレゼンス ドメイン（Presence Domains）] ウィンドウに移動します。[Cisco Unified 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。

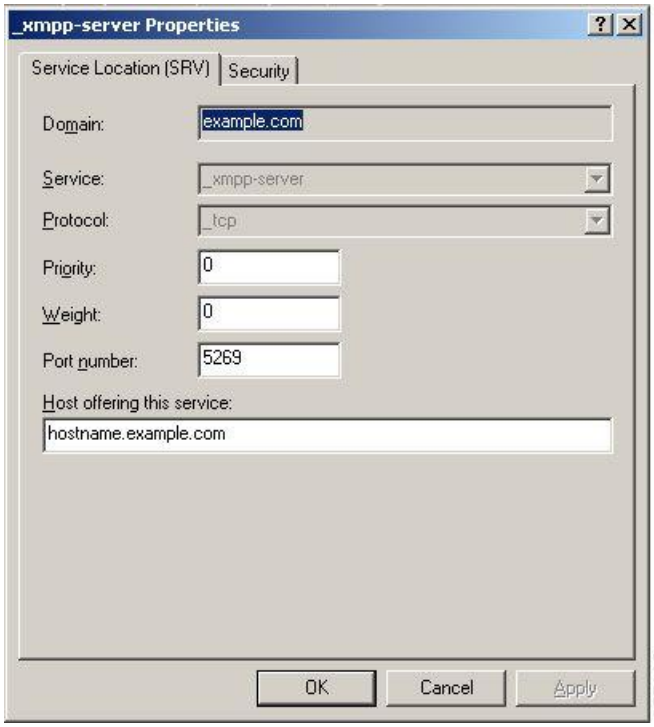
フェデレーション機能の電子メール アドレスが有効な場合は、[フェデレーション用電子メール ドメイン（Email Domains for Federation）] ウィンドウを使用して、システム内のすべてのメール ドメインのリストを表示することもできます。[Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。[プレゼンス（Presence）] > [ドメイン間フェデレーション（Inter-Domain Federation）] > [電子メール フェデレーション ドメイン（Email Federated Domains）] 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*

次の図は、ドメイン **example.com** の _xmpp-server DNS SRV レコードの DNS 設定例を示しています。

図 *22*：*"_xmpp-server" の DNS SRV*



クラスタではサーバごとに 2 つの DNS レコードが必要です。つまり、IPv4 用の DNS レコードが 1 つに IPv6 用の DNS レコードがもう 1 つです。レコードが IPv4 または IPv6 バージョンの場合は、[このサービスを提供中のホスト（Host offering this service）] フィールドで *[hostname]* の値を使用することにより、表示してください。次に、例を示します。

- 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 サービス に対するリモート ルート アクセス権がある場合、**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判断できます。

ヒント DNS SRV ルックアップを実行するには、次のコマンド シーケンスを使用します。

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）

このコマンドは、次の例のような出力を返します。「example.com」はフェデレーテッド サーバのドメインです。

```
_xmpp-server._tcp.example.com service = 0 0 5269 hostname.example.com.
```

単一のクラスタの場合、クラスタ内の 1 ノードでのみ XMPP フェデレーションをイネーブルにする必要があります。パブリック DNS でエンタープライズの 1 DNS SRV レコードを公開します。IM and Presence サービスによって、すべての着信要求は、外部ドメインからフェデレーションを実行するノードにルーティングされます。これらの要求は、内部的には IM and Presence サービスにより、各ユーザにとって適切なノードにルーティングされます。また、IM and Presence サービスによって、すべての発信要求は、XMPP フェデレーションを実行するノードにルーティングされます。

（規模を拡大する場合や、）複数の IM and Presence サービス クラスタをパブリッシュしたのに伴って XMPP フェデレーションを各クラスタにつき少なくとも 1 つずつ有効にする必要がある場合などには、複数の DNS SRV レコードをパブリッシュすることもできます。XMPP フェデレーションでは、SIP フェデレーションとは異なり、IM and Presence サービス が配置された企業ドメインに対してエントリ ポイントがただ 1 つである必要はありません。そのため、IM and Presence サービス は、XMPP フェデレーション用にイネーブルにするクラスタ内の公開されているノードのいずれかに対して、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 サービス展開では、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、要求をルーティングする場所を設定するために DNS SRV ルックアップが実行されます。各ドメインに対して複数の DNS SRV レコードをパブリッシュした場合、DNS ルックアップでは複数の結果が返されます。IM and Presence サービスでは、DNS でパブリッシュされたいずれのサーバへも、要求をルーティングすることができます。これらの要求は、内部的には IM and Presence サービスにより、各ユーザにとって適切なノードにルーティングされます。IM and Presence サービス によって、発信要求は XMPP フェデレーションを実行するノードにルーティングされます。

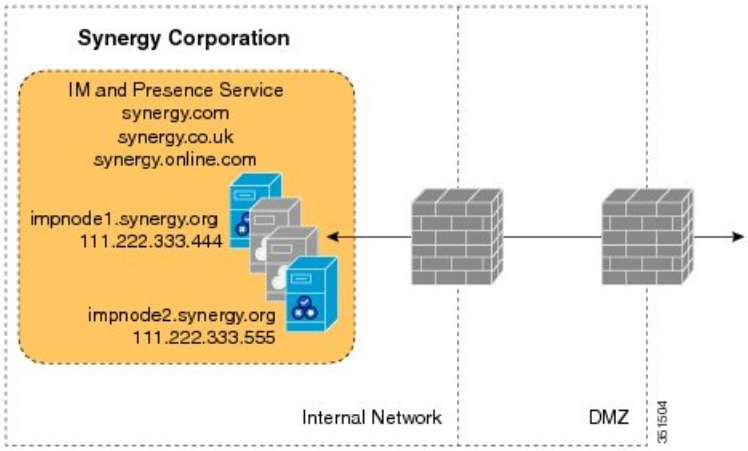
XMPP フェデレーションを実行しているノードが複数ある場合は、パブリック DNS 内でパブリッシュするノードを 1 つだけ選択することもできます。この設定の場合、XMPP フェデレーションを実行しているノード全体に着信要求がロード バランシングされるのではなく、IM and Presence サービスからその単一ノードにすべての着信要求がルーティングされます。IM and Presence サービスは、発信要求をロード バランシングし、XMPP フェデレーションを実行するノードからの発信要求を送信します。

（注） 公開する DNS SRV レコードとともに、対応する DNS A および AAAA レコードを追加する必要があります。

ドメイン間フェデレーション配置の XMPP DNS SRV

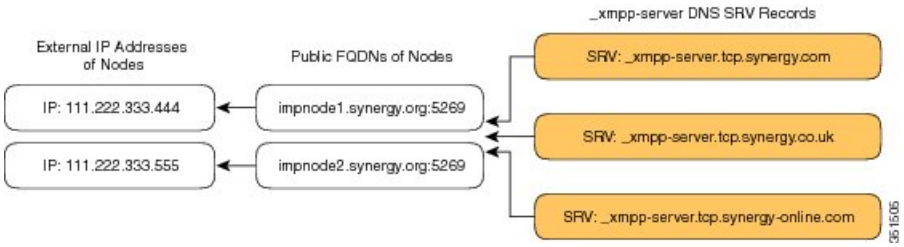
次の例のドメイン間フェデレーション導入では、2 つの IM and Presence サービス ノードが XMPP フェデレーション用に有効になります。DNS SRV レコードは、IM and Presence サービス導入環境でホストされる各ドメインに対して公開する必要があります。次の図は、3 つのローカル ドメインが存在するドメイン間フェデレーション導入の例を示しています。ドメインごとに、_xmpp-server DNS SRV レコードを公開する必要があります。

図 *23*：*Interdomain* の *XMPP* ベースの連合環境複数ドメイン



各 DNS SRV レコードは、XMPP フェデレーション トラフィックに指定される IM and Presence サービス ノードの両方のパブリック FQDN に解決される必要があります。FQDN は IM and Presence サービス ノードの外部 IP アドレスに解決される必要があります。

図 *24*：*IM and Presence* サービス ノードのパブリック *FQDN* に解決される *XMPP DNS SRV*



（注） DMZ 内に配置されたファイアウォールはノードの内部 IP アドレスに IP アドレス（NAT）を変換できます。ノードの FQDN がパブリック IP アドレスに解決できる必要があります。

関連トピック

XMPP フェデレーションのチャット機能用 DNS SRV レコード, （148 ページ）

XMPP フェデレーションのチャット機能用 DNS SRV レコード

XMPP フェデレーション導入環境で IM and Presence サービス ノードのチャット機能を設定するには、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 レコードを解決したホスト名は、パブリック IP アドレスに解決されます。導入環境によっては、パブリック IP アドレスが 1 つの場合と、ネットワーク内のチャット ノードごとにパブリック IP アドレスが 1 つの場合があります。

表 *25*：チャット要求のルーティング

展開	チャット要求のルーティング
1 つのパブリック IP アドレス、内部的に複数のノード	XMPP フェデレーション ノードにすべてのチャット要求を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。 **1** チャット ノード エイリアスの DNS SRV をポート 5269 に設定します。 **2** publicIPAddress:5269 を XMPPFederationNodePrivateIPAddress:5269 にマップする NAT コマンドを Cisco Adaptive Security Appliance または firewall\NAT サーバに設定します。
複数のパブリック IP アドレス、内部的に複数のノード	パブリック IP アドレスが複数ある場合、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できます。 **1** 5269 以外の任意のポート（25269 など）を使用するには、チャット ノード用の DNS SRV を設定します。 **2** textChatServerPublicIPAddress:25269 を textChatServerPrivateIPAddress:5269 にマップする NAT コマンドを Cisco Adaptive Security Appliance または firewall\NAT サーバに設定します。 （注） チャット ノードで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 XMPP Federation Connection Manager を有効にする必要があります。

IM and Presence サービスでチャット機能を設定する詳細については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

関連トピック

XMPP フェデレーションのチャット ノード用 DNS SRV レコードの設定, （149 ページ）

XMPP フェデレーションのチャット ノード用 DNS SRV レコードの設定

手順

ステップ 1 チャット ノード 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] 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) `conference-2.StandAloneCluster.example.com` など、DNS で公開するチャット ノード エイリアスを選択します。

ステップ 2 `example.com` ドメインのパブリック DNS サーバで、ドメイン StandAloneCluster を作成します。

ステップ 3 StandAloneCluster ドメインで、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 用の 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 設定レコードの例については、次の図を参照してください。

（注） 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 であり、手順 3 をスキップします。手順 4 で、conference-2-StandAloneCluster に _tcp ドメインを作成します。

図 *25*：チャット機能の*_xmpp-server* の *IPv4 DNS SRV* レコード

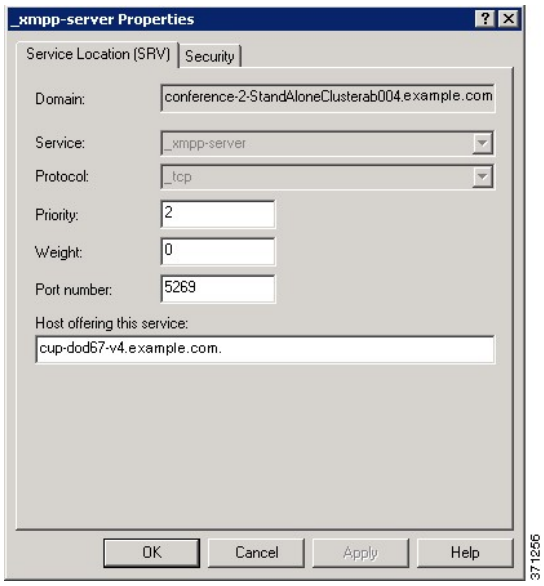


図 *26*：チャット機能の*_xmpp-server* の *IPv6 DNS SRV* レコード

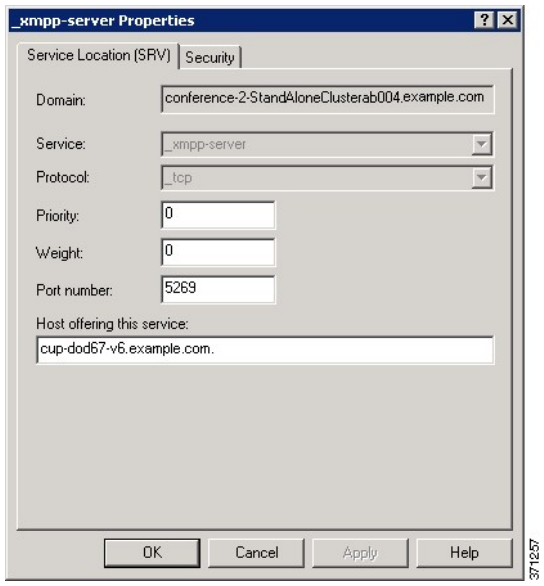
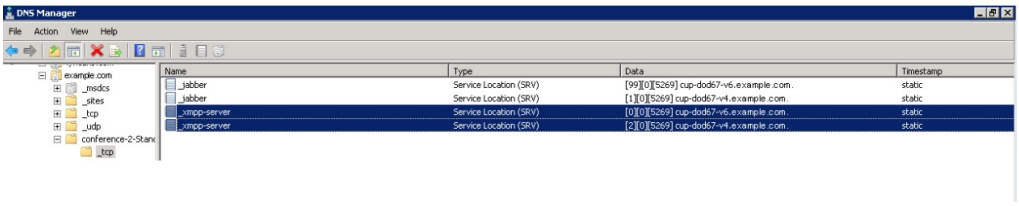


図 *27*：チャット機能用の *DNS* 設定



関連トピック

XMPP フェデレーション用 DNS SRV レコード, （144 ページ）

XMPP フェデレーションのポリシー設定

ポリシーの例外事項の設定

XMPP フェデレーションのデフォルト ポリシーには例外事項を設定できます。例外事項には、例外事項を適用する外部ドメインと、その例外事項に関する方向ルールを指定する必要があります。ポリシーの例外事項のドメイン名を設定する場合は、次の点に注意してください。

- ユーザの URI または JID が `user@example.com` の場合、例外事項の外部ドメイン名を `example.com` と設定します。
- 外部エンタープライズがユーザの URI または JID に hostname.domain を使用している場合（たとえば `user@hostname.example.com` など）、例外事項の外部ドメイン名を `hostname.example.com` に設定します。
- 例外事項の外部ドメイン名にはワイルドカード（*）を使用できます。たとえば、`*.example.com` の場合、`example.com` と example.com のすべてのサブドメイン（`somewhere.example.com` など）にポリシーが適用されます。

また、IM and Presence サービスがポリシーの例外事項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/ホストとの間でやり取りされるすべてのフェデレーテッド パケット（all federated packets from/to the above domain/host）] - IM and Presence サービスで、指定したドメインとの発着信トラフィックすべてを許可または拒否します。
- [上記のドメイン/ホストから着信するフェデレーテッドパケットのみ（Only incoming federated packets from the above domain/host）] - IM and Presence サービスは指定したドメインからの着信ブロードキャストを受信できますが、IM and Presence サービスから応答は送信しません。
- [上記のドメイン/ホストへ送信するフェデレーテッド パケットのみ（only outgoing federated packets to the above domain/host）] - IM and Presence サービス は指定したドメインへの送信ブロードキャストを送信できますが、IM and Presence サービス から応答は受信しません。

関連トピック

XMPP フェデレーションのポリシーを設定する，（152 ページ）

XMPP フェデレーションのポリシーを設定する

注意 XMPP フェデレーション設定のいずれかを変更する場合、[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスの Cisco XCP ルータ（[ツール（Tools）] > [コントロール センタのネットワーク サービス（Control Center - Network Services）] を選択）、Cisco XCP XMPP Federation Connection Manager（[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）] を選択）で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 サービスによってすべての XCP サービスが再起動されます。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[プレゼンス（Presence）] > [ドメイン間フェデレーション（Inter Domain 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 リストから次のポリシー設定を選択します。

- [許可（Allow）] - IM and Presence サービスは、ポリシーの例外事項の一覧で明示的に拒否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テッド トラフィックを許可します。
- [拒否（Deny）] - IM and Presence サービスは、ポリシーの例外事項の一覧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テッド トラフィックを拒否します。

ステップ 3 ポリシーの例外事項の一覧でドメインを設定するには、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) ポリシーの例外事項を適用する方向を指定します。
d) ポリシーの例外事項ウィンドウで [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。

関連トピック

ポリシーの例外事項の設定, （151 ページ）

XMPP フェデレーション用に Cisco Adaptive Security Appliance を設定する

Cisco Adaptive Security Appliance は、XMPP フェデレーションに対してファイアウォールとしてのみ機能します。Cisco Adaptive Security Appliance 上では、着信と発信の両方の XMPP フェデレーテッド トラフィックに対してポート 5269 を開く必要があります。

次に、Cisco Adaptive Security Appliance、リリース 8.3 でポート 5269 を開くアクセス リストの例を示します。

ポート 5269 上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する場合：

```
access-list ALLOW-ALL extended permit tcp any any eq 5269
```

ポート 5269 上で任意のアドレスから任意のシングル ノードへのトラフィックを許可する場合：

```
access-list ALLOW-ALL extended permit tcp any host private_imp_ip_address eq 5269
```

上述のアクセス リストを設定せずに、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、次の例のように、追加する各ノードへのアクセスを設定する必要があります。

```
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 コマンドを設定します。

```
nat (inside,outside) source static obj_host_private_imp1_ip obj_host_public_imp_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_private_imp1_ip obj_host_public_imp_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
```

単一のパブリック IP アドレスを DNS で公開し、任意のポートを使用する場合は、次を設定します。

（この例では、追加の XMPP フェデレーション ノードが 2 つあります）

```
nat (inside,outside) source static obj_host_private_imp2_ip obj_host_public_imp_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_25269

nat (inside,outside) source static obj_host_private_imp2_ip obj_host_public_imp_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_25269
```

```
nat (inside,outside) source static obj_host_private_imp3_ip obj_host_public_imp_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_35269
nat (inside,outside) source static obj_host_private_imp3_ip obj_host_public_imp_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_35269
```

すべてがポート 5269 を使用する複数のパブリック IP アドレスを DNS で公開する場合は、次を設定します。

（この例では、追加の XMPP フェデレーション ノードが 2 つあります）

```
nat (inside,outside) source static obj_host_private_imp2_ip obj_host_public_imp2_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_5269
nat (inside,outside) source static obj_host_private_imp2_ip obj_host_public_imp2_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
nat (inside,outside) source static obj_host_private_imp3_ip obj_host_public_imp3_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_5269
nat (inside,outside) source static obj_host_private_imp3_ip obj_host_public_imp_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
```

関連トピック

SIP フェデレーションに関する Cisco Adaptive Security Appliance（ASA）の設定, （77 ページ）

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 サービス ノードで、Cisco XCP XMPP Federation Connection Manager サービスでオンにする必要があります。[サービス アクティベーション（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 サービスによってサービスが自動的に起動されます。[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起動する必要はありません。

はじめる前に

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。詳細については、ノードで XMPP フェデレーションをオンにする, （142 ページ）を参照してください。

手順

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

関連トピック

フェデレーションに関するサービスアビリティの設定, （173 ページ）

第 12 章

XMPP フェデレーションに使用するセキュリティ証明書の設定

XMPP フェデレーションに使用するセキュリティ証明書の設定

XMPP フェデレーション用のセキュリティを設定するためには、以下のような操作を行う必要があります。

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設定されていることを確認し、必要に応じて、見つからないローカル 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作成します。

- XMPP フェデレーション用の自己署名付きの単一サーバ証明書
- XMPP フェデレーション用の CA 署名付きの単一サーバ証明書またはマルチサーバ証明書

3 ルート CA 証明書をインポートします。

まだ信頼していない CA を使用するエンタープライズとのフェデレーションを新たに設定するたびに、この操作を繰り返します。同様に、フェデレーションを新たに設定するエンタープラ

イズが自己署名証明書を使用している場合もこの操作を行う必要があります。この場合、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 ドメインは、生成された cup-xmpp-s2s の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ていて、[ドメイン（Domains）] ウィンドウに表示されることを確認します。計画に含まれているドメインを手動で追加しますが、ローカル ドメインのリストには表示されません。たとえば、ユーザが割り当てられていないドメインは、通常の場合ドメインのリストに表示されません。

[Cisco Unified CM IM and Presence Administration] ユーザ 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で作成されていることを確認した後は、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 証明書を作成する手順に進むことができます。フェデレーション用の電子メール アドレスが有効な場合は、すべての電子メール ドメインも証明書に含める必要があります。

ローカル ドメインを追加、更新または削除して、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。このサービスを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザ 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 - 機能サービス（Control Center - Feature Service）] を選択します。

関連トピック

電子メール ドメインを追加または更新する, （170 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, （159 ページ）
XMPP フェデレーションへの CA 署名付き証明書の使用, （159 ページ）
電子メール ドメインを表示する, （170 ページ）

マルチサーバ証明書の概要

IM and Presence サービスは、tomcat、cup-xmpp、および cup-xmpp-s2s の証明のために、マルチサーバ SAN ベースの証明書をサポートしています。適切な証明書署名要求（CSR）を生成するために、シングルサーバまたはマルチサーバ配布を選択できます。作成された署名付きマルチサーバ証明書と関連付けられたその一連の署名証明書は、クラスタ内の個々のサーバにマルチサーバ証明書をアップロードする際に、クラスタ内の他のサーバに自動的に配布されます。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 フェデレーションに自己署名証明書を使用する方法について説明します。CA 署名付き証明書の使用方法については、XMPP フェデレーションへの CA 署名付き証明書の使用，（159 ページ）を参照してください。

手順

ステップ 1 [Cisco Unified IM and Presence Operating System Administration] ユーザ インターフェイスにログインします。[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 [自己署名付きを生成（Generate Self-signed）] をクリックします。

ステップ 3 [証明書の用途（Certificate Purpose）] ドロップダウン リストから、[cup-xmpp-s2s] を選択して、[生成（Generate）] をクリックします。

ステップ 4 Cisco XCP XMPP Federation Connection Manager サービスを再起動します。[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[ツール（Tools）] > [コントロール センタ - ネットワーク サービス（Control Center - Network Services）] 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エンタープライズに送信して、XMPP サーバの信頼できる証明書として追加できます。これには、IM and Presence サービス ノードまたは別の XMPP サーバなどがあります。

次の作業

XMPP フェデレーションへの CA 署名付き証明書の使用，（159 ページ）

XMPP フェデレーションへの CA 署名付き証明書の使用

ここでは、CA 署名付き証明書を使用する方法について説明します。自己署名付き証明書の使用方法については、XMPP フェデレーションに自己署名証明書を使用する，（159 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を生成する

ここでは、Microsoft Certificate Services 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 Certificate Services CA の CSR を生成しますが、任意の認証局の証明書を要求する場合は、CSR を生成する手順（手順 1 ～ 3）が適用されます。

手順

ステップ 1 [Cisco Unified IM and Presence Operating System Administration] ユーザ インターフェイスにログインします。[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 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 リストから、証明書名に [cup-xmpp-s2s] を選択します。

c) 配信用には、単一署名された証明書を生成するローカル サーバ、またはマルチサーバ証明書を生成するマルチサーバ（SAN）の FQDN を選択します。

（注） 両方のディストリビューション オプションでは、すべての既存のドメイン、電子メール ドメインおよび [Cisco Unified IM and Presence Administration] ユーザ インターフェースで設定されたグループ チャットのサーバ エイリアスは、生成された CSR に自動的に含まれます。[Multi-server (SAN)（マルチサーバ（SAN））] オプションを選択した場合、各 IM and Presence サービス ノードのホスト名または FQDN は、生成された CSR に追加されます。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。

d) [生成（Generate）] をクリックします。

（注） [Multi-server（SAN）（マルチサーバ（SAN））] を選択した場合、CSR はクラスタの他のすべての 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 `.csr` ファイルをローカル マシンにダウンロードするには：

a) [CSR をダウンロード（Download CSR）] をクリックします。

b) [証明書目的（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 をダウンロード（Download CSR）] をクリックして、そ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 CSR ファイルの内容をコピーします。
次の行から、

- BEGIN CERTIFICATE REQUEST

次の行までの情報をすべてコピーします。

END CERTIFICATE REQUEST -

ステップ 6 インターネット ブラウザで、CA サーバを参照します。たとえば、次のように指定します。`http://<name of your Issuing CA Server>/certsrv`。

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 [証明書の要求の詳細設定（Advanced certificate request）] をクリックします。

ステップ 9 [ベース 64 エンコード CMC または PKCS #10 ファイルを使用して証明書要求を送信するか、ベース 64 エンコード PKCS #7 ファイルを使用して更新要求を送信する（Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file）] をクリックします。

ステップ 10 手順 5 でコピーした CSR ファイルの内容を [保存した要求（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、次の URL に戻ります。 `http://<name of your Issuing CA Server>/certsrv`

ステップ 13 [保留中の証明書の要求の状態（View the status of a pending certificate request）] をクリックします。

ステップ 14 前の項で発行した証明書の要求をクリックします。

ステップ 15 [ベース 64 エンコード（Base 64 encoded）] をクリックします。

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**セキュリティ証明書**として保存します。

次の作業

XMPP フェデレーションへの CA 署名付き証明書をアップロードする，（161 ページ）

トラブルシューティングのヒント

- IM and Presence サービスのサポートされるドメインのリストが変更される場合は、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。

XMPP フェデレーションへの CA 署名付き証明書をアップロードする

はじめる前に

XMPP フェデレーションの証明書署名要求を生成する，（159 ページ）の手順を実行します。

手順

ステップ 1 [Cisco Unified IM and Presence Operating System Administration] ユーザ インターフェイスにログインします。[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 証明書名に [cup-xmpp-s2s] を選択します。

ステップ 4 ローカル マシンに保存した CA 署名付き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）] をクリックします。

（注） マルチサーバの SAN ベースの証明書を生成した場合は、クラスタ内の任意の IM and Presence サービス ノードへこれをアップロードできます。これを実行すると、結果として署名証明書署名されたマルチ・サーバ証明書と関連チェーンがクラスタの個々のサーバがデバイスと証明書のアップロードのクラスタ内の他のサーバに自動的に配布されます。自己署名証明書がノードのいずれかにある場合、新しい複数サーバの証明書によって上書きされます。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。

ステップ 6 Cisco XMPP Federation Connection Manager サービスを再起動します。[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[ツール（Tools）] > [コントロール センタ - ネットワーク サービス（Control Center - Network Services）] を選択して、このサービスを再起動します。

（注） マルチサーバの証明書をアップロードするには、クラスタ内の**すべて**の IM and Presence サービス ノードで XCP ルータ サービスを再起動しなければなりません。

次の作業

同じクラスタ内のノード間でサービスアビリティ用のクロス ナビゲーションをサポートするために、IM and Presence サービスと Cisco Unified Communications Manager の間の Cisco Tomcat サービス信頼ストアが自動的に同期されます。

IM and Presence サービスまたは Cisco Unified Communications Manager のいずれかで元の自己署名信頼証明書を置き換えるためにCA署名付き証明書が生成されても、元の証明書は、ノードのサービス信頼ストアで保持されます。サービス信頼ストアに元の自己署名証明書を残しても、それらを表すサービスがないため、問題になりません。ただし、これらの証明書は削除できますが、削除は IM and Presence サービスと Cisco Unified Communications Manager の両方で実行する必要があります。

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.htmlの『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』の第 9 章「Security Configuration on IM and Presence Service」に含まれている第 II 部の「Delete Self-Signed Trust Certificates」セクションを参照してください。

XMPP フェデレーションのルート CA 証明書をインポートする

（注） ここでは、cup-xmpp-s2s 信頼証明書を IM and Presence サービス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、Certificate Import Tool 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。証明書のインポート ツール、ログインおよびプレゼンス管理**ユーザ インターフェイスに Cisco Unified** CM IM にアクセスする。[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、このツールを使用する手順を記載するオンライン ヘルプを参照してください。

IM and Presence サービスとエンタープライズのフェデレーションを行い、共通の信頼できる認証局（CA）がエンタープライズの証明書に署名する場合、CA のルート証明書を IM and Presence サービス ノードにアップロードする必要があります。

共通の信頼できる CA が署名した証明書ではなく、自己署名証明書を使用するエンタープライズと IM and Presence サービスのフェデレーションを行う場合、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。

はじめる前に

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。

手順

ステップ 1 [Cisco Unified IM and Presence Operating System Administration] ユーザ インターフェイスにログインします。IM and Presence サービスで、[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 証明書名に [cup-xmpp-trust] を選択します。

（注） ルート名のフィールドは空白のままにしておきます。

ステップ 4 [参照（Browse）] をクリック、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、証明書を IM and Presence サービス ノードにアップロードします。

（注） まだ信頼していない CA を使用するエンタープライズとのフェデレーションを新たに設定するたびに、この操作を繰り返します。同様に、フェデレーションを新たに設定するエンタープライズが自己署名証明書を使用している場合もこの操作を行う必要があります。この場合、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の場合、XMPP フェデレーションの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 13 章

フェデレーション設定の電子メール アドレス

この章では、フェデレーション機能と複数のドメインを設定する電子メール アドレスについての情報を提供します。

フェデレーション有効化用電子メール

フェデレーション機能用に電子メール アドレスをオンにすると、IM and Presence サービスによって、ローカル ユーザの JID が連絡先の電子メール アドレスに変更されます。

クラスタ間配置では、すべてのクラスタ間ノード上でフェデレーション用の電子メール アドレスを有効にする必要があります。フェデレーション機能用の電子メールをオンにした後は、Cisco XCP Router サービスを再起動する必要があります。

XMPP フェデレーション導入環境の場合、フェデレーション機能用の電子メール アドレスは、現在マルチクラスタ IM and Presence サービス導入での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 サービス クラスタがある導入シナリオでは、ローカル ユーザの実際の JID をフェデレーション対象ユーザに送信できます。チャット ルームに対する唯一の影響は、フェデレーション対象ユーザに表示される名前が、ローカル ユーザの電子メール アドレスではなくローカル ユーザのユーザ ID であることです。その他のチャット ルームの機能は通常どおりに機能します。このような状況は、フェデレーション対象ユーザとの一時的なチャット ルームとパーシステント 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 アドレスに関する詳細とこの機能を有効にする手順に関する詳細については、フェデレーション設定の電子メール アドレスに関するトピックを参照してください。

関連トピック

フェデレーション用電子メール アドレスの考慮事項, （166 ページ）
フェデレーション用電子メールの有効化, （169 ページ）

フェデレーション用電子メール アドレスの考慮事項

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ために IM and Presence サービスを設定する場合、IM and Presence サービスはローカル ユーザの IM アドレスをフェデレーションの連絡先とのすべての通信にユーザの電子メール アドレスと交換します。

ドメイン間フェデレーション用の電子メール アドレスを有効にする場合は、以下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はまだ行わないが、フェデレーション用の電子メール アドレスを有効にする必要がある場合は、ユーザがフェデレーテッド連絡先を追加する前にこの設定を有効にすることをお勧めします。
- フェデレーション用の電子メール アドレスを有効にした場合でも、ユーザが Active Directory で電子メール アドレスを設定していなければ、IM and Presence サービス ではそのユーザの JID がフェデレーション用として使用されます。
- この機能は、各ユーザに対する Cisco Unified Communications Manager の [メール ID（Mail ID）] が、そのユーザの完全な電子メール アドレスに一致していることが前提条件となります。

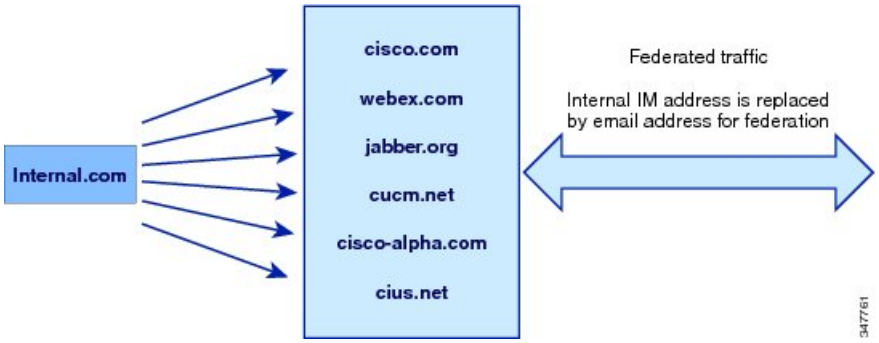
  ユーザの [メール ID（Mail ID）] フィールドに何も指定されていない場合、または完全な電子メール アドレスが指定されていない場合は、IM and Presence サービスのデフォルトの動作として、そのユーザの IM and Presence サービス JID がフェデレーション用に使用されます。
- フェデレーション用の電子メール アドレスを有効にした場合、フェデレーション コンタクトで使用されるのが電子メールではなく、IM and Presence サービス ユーザの JID であれば、（そのユーザに有効な電子メール アドレスが設定されているとしても）これらの要求は IM and Presence サービスによりドロップされます。
- IM and Presence サービスでは、フェデレーション機能用の電子メール アドレスに対する電子メール エイリアスはサポートされていません。

（注） この機能は、SIP フェデレーションと XMPP フェデレーションのどちらの場合にも適用することができます。

複数のドメイン間フェデレーション サポートの電子メール アドレス

フェデレーション機能用の電子メール アドレスは、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る複数の電子メール ドメインの例を示しています。

図 *28*：複数のドメインのフェデレーション サポート用電子メール アドレス



ローカルの IM and Presence サービス導入環境で、複数の電子メール ドメインを管理する場合は、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名代替名として含まれている必要があります。

電子メールのドメイン設定の概要

フェデレーション機能用の電子メールアドレスに使用する電子メール ドメインの手動による追加および編集は、オプションです。これは、IM and Presence サービスでは、それぞれのユーザの電子メール アドレスごとに一意のドメインが自動的に読み込まれ、その情報がフェデレーション機能用の電子メール アドレスに使用されるためです。

IM and Presence サービス用にまだ設定されていないユーザが存在するドメインがあり、それらのユーザを設定する予定であれば、**Cisco Unified CM IM and Presence Administration** のユーザ 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 サービスに手動で追加できます。現在ユーザが割り当てられていないドメインは、ユーザ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 ドメインは、[Cisco Unified CM IM and Presence Administration] ユーザ 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 インタフェースで設定できません。

外部ドメインの管理者に提供する情報

フェデレーション用の電子メール アドレスを有効にする場合は、外部ドメインのシステム管理者に対して以下のような注意事項を事前に通知する必要があります。

- フェデレーション用の電子メール アドレスを使用していること、および外部ドメイン内のユーザは、フェデレーテッド連絡先を連絡先リストに追加する際、電子メールアドレスを指定する必要があること。
- 外部ドメインとのフェデレーションをすでに行っており、かつフェデレーション用の電子メールを有効にする必要がある場合、外部ドメイン内のユーザは、連絡先リストにある既存のフェデレーテッド連絡先をいったん削除した後、それらのフェデレーテッド連絡先を再び追加したうえで、電子メール アドレスを指定する必要があること。

IM and Presence サービス ユーザに提供する情報

フェデレーション用の電子メール アドレスを有効にする場合は、すべての IM and Presence サービス ユーザに以下の情報を通知する必要があります。

- フェデレーテッド連絡先では、user_id@domain アドレスではなく、電子メールアドレスが使用されるようになったこと。
- フェデレーテッド連絡先は、新しいコンタクトを連絡先リストに追加する際、user_id@domain の代わりに IM and Presence サービス ユーザの電子メール アドレスを使用する必要があること。
- （フェデレーション ウォッチャの連絡先リスト上で）user_id@domain を指定して追加された既存の IM and Presence サービス コンタクトについては、いったん削除した後、IM and Presence サービス ユーザの電子メール アドレスを指定して追加し直す必要があります。
- IM and Presence サービスがフェデレーション コンタクトから受け取った user_id@domain アドレス宛てのメッセージはいずれもドロップされます（ただし、そのアドレスが Active Directory に設定されている電子メール アドレス、および IM and Presence サービスのユーザ テーブルに設定されているアドレスと同じである場合は除きます）。
- IM and Presence サービス ユーザの連絡先リストにフェデレーテッド連絡先がすでに追加されている場合は、その IM and Presence ユーザがクライアントに再度サイン インした時点でそのフェデレーテッド連絡先に対し電子メール アドレスをポップ アップで表示することができること。

（注） フェデレーション用の電子メール アドレスを有効にすると、IM and Presence サービス ユーザは、IM and Presence サービスへの接続時にクライアント上でデータを変更したり、別途 IM and Presence サービス ノードとデータのやり取りをしたりする必要がなくなります。

電子メールのドメイン管理の連携動作と制限事項

- 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 を介する 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に、TLS 証明書 cup-xmpp-s2s を再生成する必要があります。

フェデレーションの設定および電子メールのドメイン管理用電子メール アドレス

フェデレーション用電子メールの有効化

（注） クラスタ間導入では、すべてのクラスタ間ノード上でフェデレーション用の電子メール アドレスを有効にする必要があります。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[プレゼンス（Presence）] > [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で電子メール アドレスの使用を有効化（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 警告メッセージに目を通し、[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ら、Cisco XCP Router を再起動します。[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[ツール（Tools）] > [コントロール センタのネットワーク サービス（Control Center - Network Services）] を選択します。

関連トピック

フェデレーションのルーティング パラメータの設定, （49 ページ）

電子メール ドメインを表示する

システム管理ドメインおよび管理者によって管理されるローカル ドメインは、[Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスの [電子メール ドメインの検索/一覧表示（Find and List Email Domains）] ウィンドウに表示されます。また、このウィンドウでは、各管理者が管理するドメインがローカル クラスタ、ピア クラスタ、またはその両方で設定されたかどうかも示します。

手順

[Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[プレゼンス（Presence）] > [ドメイン間フェデレーション（Inter-Domain Federation）] > [電子メール フェデレーション 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/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 ドメインを追加または更新する

[Cisco Unified CM IM and Presence Administration] のユーザ 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 ドメインを追加することで、ローカル クラスタにある IM アドレス 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。使用できる値は、大文字または小文字（a ～ z、A ～ Z）、数字（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。

システムが管理するドメインと、管理者が管理するローカル ドメインが [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。また、このウィンドウでは、各管理者が管理するドメインがローカル クラスタ、ピア クラスタ、またはその両方で設定されたかどうかも示します。

システム管理ドメインは使用中のため、編集できません。その IM アドレス ドメインではシステムにすでにユーザが存在しない場合（たとえば、ユーザの削除により）、システム管理ドメインは、自動的に管理者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。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[プレゼンス（Presence）] > [ドメイン間フェデレーション（Inter-Domain Federation）] > [電子メール フェデレーション 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/一覧表示（Find and List Email Domains）] ウィンドウが開き、管理者およびシステムによって管理されたすべての電子メール ドメインが表示されます。

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 Domain）] 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 Domain）] ウィンドウが表示されます。

ステップ 3 新しいドメイン名を [ドメイン名（Domain Name）] フィールドに入力し、[保存（Save）] をクリックします。
最大 255 文字の一意のドメイン名を入力します。使用できる値は、大文字または小文字（a ～ z、A ～ Z）、数字（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めないでください。また、最後のラベル（たとえば、.com）は数字で始め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ている場合は、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 ドメインを削除する

Cisco Unified CM IM and Presence Administration のユーザ インターフェイスを使用して、ローカル クラスタ内にある管理者が管理する電子メール 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 ドメインではシステムにすでにユーザが存在しない場合（たとえば、ユーザの削除により）、システム管理ドメインは、自動的に管理者管理ドメインになります。管理者の管理ドメインを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。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[プレゼンス（Presence）] > [ドメイン間フェデレーション（Inter-Domain Federation）] > [電子メール フェデレーション 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/一覧表示（Find and List Email Domains）] ウィンドウが開き、管理者およびシステムによって管理されているすべての電子メール アドレス ドメインが表示されます。

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 14 章

フェデレーションに関するサービスアビリティの設定

フェデレーションでのロギングの使用

SIP フェデレーションのログ ファイルの場所

次のログ ファイルは SIP フェデレーションに適用できます。

- `sip-cm-3_0000000X.log`（`/var/log/active/epas/trace/xcp/log` にあります）
- `esp0000000X.log`（`/var/log/active/epas/trace/esp/sdi` にあります）

また、これらのログを 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。

- `xmpp-cm-4_0000000X.log`（`/var/log/active/epas/trace/xcp/log` にあります）

また、これらのログを RTMT から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

手順

ステップ 1 [Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログオンします。[トレース（Trace）] > [設定（Configuration）] を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストから、[IM and Presence サービス サーバ（IM and Presence Service server）] を選択し、[移動（Go）] をクリックします。

ステップ 3 [Service Group（サービス グループ）] リスト ボックスから、IM and Presence サービスを選択し、[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、[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、[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 [トレースを有効化（Trace On）] をクリックします。
[トレース フィルタの設定（Trace Filter Settings）] の [デバッグ トレース レベル（Debug Trace Level）] を選択します。トレースのデバッグ レベルをイネーブルにする場合、[デバッグ トレース レベル（Debug Trace Level）] に [デバッグ（Debug）] を選択します。

Cisco XCP Router を再起動する方法

Cisco XCP Router

SIP または XMPP フェデレーション設定の内容を変更した場合、IM and Presence サービスで Cisco XCP ルータをリスタートする必要があります。Cisco XCP ルータを再起動すると、IM and Presence サービスは自動的にすべてのアクティブ XCP サービスを再起動します。

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 ルータを再起動するのではなく停止した場合、IM and Presence サービスにより他のすべての XCP サービスが停止されます。その後 XCP ルータの電源をオンにしても、IM and Presence サービスにより他の XCP サービスは自動的に起動されません。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

手順

ステップ 1 [Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[ツール（Tools）] > [コントロール センタのネットワーク サービス（Control Center - Network Services）] を選択します。

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 Services）] エリアで、Cisco XCP XMPP ルータ 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 [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 15 章

フェデレーション統合の確認

SIP フェデレーション設定を検証する

この手順では、IM and Presence サービス エンタープライズ導入と Microsoft OCS エンタープライズ導入の間のフェデレーテッド ネットワークの設定を検証する方法について説明します。必要に応じて他の種類の統合を検証する場合、この手順をガイドとして使用してください。

（注） 複数のローカル IM and Presence サービス ドメインの場合、各ローカル ドメインのユーザについて、この手順を繰り返します。

手順

ステップ 1 Cisco Jabber クライアントまたはサードパーティの XMPP クライアントにログインします。

ステップ 2 2 つのフェデレーション対象の Microsoft Office Communicator クライアントにログオンします。

ステップ 3 1 つ目の Microsoft Office Communicator クライアントについて次の手順を実行します。

a) 連絡先として IM and Presence サービス ユーザを追加します。

b) Microsoft Office Communicator ユーザのプレゼンス サブスクリプションの受け入れ、ブロック、または無視を要求するポップアップ メッセージが IM and Presence サービスに表示されます。

c) IM and Presence サービス ユーザと Microsoft Office Communicator ユーザが相互のアベイラビリティを表示できることを確認します。

ステップ 4 IM and Presence サービス クライアントで、次の手順を実行します。

a) 連絡先として 2 つ目の Microsoft Office Communicator ユーザを追加します。

b) Microsoft Office Communicator ユーザのアベイラビリティを表示できることを確認します。

c) Microsoft Office Communicator ユーザのユーザ クライアントには、Cisco Jabber ユーザ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 サービス ユーザのクライアントと Microsoft Office Communicator クライアントの両方で、在席ステータスを切り替えます。各クライアントの連絡先について、在席ステータスが変わることを確認します。

ステップ 6 IM and Presence サービス ユーザのクライアントから、Microsoft Office Communicator ユーザに対して IM を開始します。

ステップ 7 Microsoft Office Communicator に、IM and Presence サービス ユーザからのメッセージがあるという IM ウィンドウが表示されることを確認します。

ステップ 8 IM and Presence サービス ユーザのクライアントの 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 ユーザから IM and Presence サービス ユーザに対して IM を開始します。

ステップ 10 IM and Presence サービス ユーザのクライアントに、Microsoft Office Communicator ユーザからのメッセージがあるという IM ウィンドウが表示され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 ユーザのいずれかをブロックします。

（注） XEP-0016 - Privacy Lists をサポートしないサードパーティ クライアントがあり、サードパーティの XMPP クライアントをブロックしている場合、IM のみがブロックされます。ユーザはアベイラビリティのステータスを交換できます。サーバ側の IM とアベイラビリティをブロックするには、IM and Presence の [ユーザ オプション（Users Options）] インターフェイスまたは Cisco Jabber の [プライバシー（Privacy）] 設定からプライバシー設定を変更します。

b) この Microsoft Office Communicator ユーザが、IM and Presence サービス ユーザのアベイラビリティがオフラインと表示されるようになったことを確認します。2 つ目の Microsoft Office Communicator ユーザは、IM and Presence サービス ユーザの在席ステータスを確認できます。

c) IM and Presence サービス ユーザのクライアントでは、ブロックした Microsoft Office Communicator ユーザがオンラインと表示され、ブロックした Microsoft Office Communicator ユーザに対して 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 サービス ユーザをブロックします。

ステップ 13 Microsoft Office Communicator ユーザのプレゼンスが IM and Presence サービス ユーザのクライアントで使用できなくなることを確認します。

XMPP フェデレーションの設定を検証する

この手順では、IM and Presence サービス リリース 9.0 エンタープライズ導入と、WebEx、IBM Sametime、または別の IM and Presence サービス リリース 9.0 エンタープライズ導入間のフェデレーテッド ネットワークの設定を検証する方法について説明します。以下の手順では、IM and

Presence サービス リリース 9.0 と WebEx 展開の場合について説明します。他の種類の XMPP フェデレーションについて検証する場合、この手順をガイドとして使用してください。

（注） 複数のローカル IM and Presence サービス ドメインの場合、各ローカル ドメインのユーザについて、この手順を繰り返します。

手順

ステップ 1 IM and Presence サービス リリース 9.0 サーバに接続する Cisco Jabber クライアントまたはサードパーティの XMPP クライアントにログオンします。

ステップ 2 2 つのフェデレーション対象 WebEx Connect クライアントにログオンします。

ステップ 3 1 つ目の WebEx Connect クライアントについて次の手順を実行します。

a) 連絡先として IM and Presence サービス ユーザを追加します。

b) WebEx Connect ユーザのプレゼンス サブスクリプションの受け入れ、ブロック、または無視を要求するポップアップメッセージが IM and Presence サービス ユーザのクライアントに表示されます。サブスクリプションを受け入れます。

c) IM and Presence サービス ユーザと WebEx Connect ユーザが相互のアベイラビリティを表示できることを確認します。

ステップ 4 IM and Presence サービス ユーザのクライアントで、次の手順を実行します。

a) 連絡先として 2 つ目の WebEx Connect ユーザを追加します。

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受け入れます。

c) WebEx Connect ユーザのアベイラビリティを表示できることを確認します。

ステップ 5 IM and Presence サービス ユーザのクライアントと WebEx Connect クライアントの両方で、在席ステータスを切り替えます。各クライアントの連絡先について、在席ステータスが変わることを確認します。

ステップ 6 IM and Presence サービス ユーザのクライアントから、WebEx Connect の連絡先に対して IM を開始します。

ステップ 7 WebEx Connect クライアントに、IM and Presence サービス ユーザからの IM があるという IM ウィンドウが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 ユーザから IM and Presence サービス ユーザに対して IM を開始します。

ステップ 10 IM and Presence サービス ユーザのクライアントに、WebEx Connect ユーザからの IM があるという IM ウィンドウが表示されることを確認します。

ステップ 11 IM and Presence サービス ユーザのクライアントで、次の手順を実行します。

a) いずれかの WebEx Connect ユーザをブロックします。

（注） サードパーティのXMPPクライアントをブロックしている場合、IMのみがブロックされます。ユーザはアベイラビリティのステータスは交換できます。サーバ側のIMとアベイラビリティをブロックするには、IM and Presence の [ユーザ オプション（Users Options）] インターフェイスまたはCisco Jabber の [プライバシー（Privacy）] 設定からプライバシー設定を変更します。

b) この WebEx Connect ユーザが、IM and Presence サービス ユーザのアベイラビリティがオフラインと表示されるようになったことを確認します。2 つ目の WebEx Connect ユーザは、IM and Presence サービス ユーザの在席ステータスを確認できます。

c) IM and Presence サービス ユーザのクライアントでは、ブロックした WebEx Connect ユーザはオンラインと表示されますが、ブロックした WebEx Connect ユーザに IM を送信することはできなくなります。

ステップ 12 WebEx Connect クライアントから IM and Presence サービス ユーザをブロックします。

ステップ 13 WebEx Connect ユーザのアベイラビリティが IM and Presence サービス ユーザのクライアントで使用できなくなることを確認します。

第 16 章

SIPフェデレーション統合に関するトラブルシューティング

一般的な Cisco Adaptive Security Appliance の問題と推奨される操作

証明書の設定に関する問題

IM and Presence サービスと Cisco Adaptive Security Appliance の間での証明書失敗

IM and Presence サービス と Cisco Adaptive Security Appliance 間の証明書の設定にエラーがあります。

Cisco Adaptive Security Appliance の時刻とタイム ゾーンが正しく設定されていない可能性があります。

- Cisco Adaptive Security Appliance で時刻とタイム ゾーンを設定します。
- IM and Presence サービス と Cisco Unified Communications Manager で時刻とタイム ゾーンが正しく設定されていることを確認します。

この統合の前提条件となる設定タスク, (36 ページ)

Cisco Adaptive Security Appliance と Microsoft Access Edge 間の証明書に関するエラー

Cisco Adaptive Security Appliance への証明書の登録時に、Cisco Adaptive Security Appliance と Microsoft Access Edge 間の証明書の設定が失敗しました。

Cisco Adaptive Security Appliance で SCEP の登録を使用している場合、SCEP アドオンのインストールと設定が正しく行わ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。

関連トピック

CA トラストポイント, （62 ページ）

SSL ハンドシェイクでの証明書に関するエラー

SSL ハンドシェイクで証明書のエラーが表示されます。

証明書に FQDN がありません。IM and Presence サービス CLI でドメインを設定し、IM and Presence サービスで FQDN がある証明書を再生成する必要があります。証明書を再生成する場合、IM and Presence サービスで SIP プロキシを再起動する必要があります。

関連トピック

CLI から IM and Presence サービス ドメインを設定します。

証明書署名要求を VeriSign に送信するときにエラーが発生する

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 の 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。

証明書署名要求の件名に情報が足りません。更新の証明書署名要求（CSR）ファイルを VeriSign に送信する場合、証明書署名要求の件名には次の情報を含める必要があります。

- 国（Country）（2 文字の国コードのみ）
- 都道府県（State）（省略なし）
- 市区町村（Locality）（省略なし）
- 組織名（Organization Name）
- 組織部門（Organizational Unit）
- 一般名（Common Name）（FQDN）

件名行エントリは次の形式にする必要があります。

```
(config-ca-trustpoint)# subject-name
cn=fqdn,U=organisational_unit_name,C=country,St=state,L=locality,O=organisation
```

関連トピック

VeriSign 用の新しいトラストポイントの生成, （204 ページ）

IM and Presence サービスのドメインまたはホスト名を変更する際の SSL エラー

CLI から IM and Presence サービス ドメインを変更すると、IM and Presence サービス と Cisco Adaptive Security Appliance 間で SSL 証明書のエラーが発生します。

CLI から IM and Presence サービス ドメイン名を変更する場合、IM and Presence サービスの自己署名証明書 sipproxy.pem が再生成されます。そのため、sipproxy.pem 証明書を Cisco Adaptive Security Appliance に再インポートする必要があります。具体的には、Cisco Adaptive Security Appliance の現在の sipproxy.pem 証明書を削除し、（再生成された）sipproxy.pem 証明書を再インポートします。

関連トピック

IM and Presence サービスと Cisco Adaptive Security Appliance の間でのセキュリティ証明書交換, （58 ページ）

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きに、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

ERROR: Specified ACL (ent_imp_to_external) either does not exist or its type is not supported
by the match command.

ciscoasa(config-cmap)# exit

ciscoasa(config)# class-map ent_external_to_imp

ciscoasa(config-cmap)# match access-list ent_external_to_imp

ERROR: Specified ACL (ent_external_to_imp) either does not exist or its type is not supported
by the match command.

ciscoasa(config-cmap)#
```

外部ドメインのアクセス リストが存在しません。前述の例では、ent_foreign_to_cup というアクセス リストが存在しません。**access list** コマンドを使用して、外部ドメインの拡張アクセス リストを作成してください。

関連トピック

アクセス リストの設定の要件, （92 ページ）
TLS プロキシのデバッグ コマンド, （216 ページ）

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 に到達しません。OCS から、ピアとしての Access Edge に関するネットワーク機能エラーがレポートされます。Access Edge サービスが起動しません。

Access Edge では、[許可（Allow）] タブと [IM プロバイダ（IM Provider）] タブの両方で IM and Presence サービス ドメインを設定できます。IM and Presence サービス ドメインは、[IM プロバイダ（IM Provider）] タブでのみ設定します。Access Edge の [許可（Allow）] タブから IM and Presence サービス ドメインを削除します。[IM Provider（IM プロバイダ）] タブに IM and Presence サービス ドメインのエントリがあることを確認します。

（注） IM and Presence サービスは複数のドメインをサポートします。各 IM and Presence ドメインを必ず確認し、[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ます。

アップグレード後の Cisco Adaptive Security Appliance の問題

ソフトウェアのアップグレード後に Cisco Adaptive Security Appliance がブートしません。

新しいソフトウェア イメージは、TFTP サーバおよび Cisco Adaptive Security Appliance の ROM Monitor（ROMMON）を使用して Cisco Adaptive Security Appliance にダウンロードできます。ROMMON は、TFTP や関連する診断ユーティリティでイメージのロードと取得を行うために使用できるコマンドライン インターフェイスです。

手順

ステップ 1 コンソール ポートから近くの TFTP サーバのポートにコンソール ケーブル（Cisco Adaptive Security Appliance に付属する青色のケーブル）を接続します。

ステップ 2 HyperTerminal または同等のものを開きます。

ステップ 3 表示されるすべてのデフォルト値を受け入れます。

ステップ 4 Cisco Adaptive Security Appliance をリブートします。

ステップ 5 ブート時に 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 Adaptive Security Appliance をイネーブルにし、TFTP サーバからイメージをダウンロードします。

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 Adaptive Security Appliance の Inside インターフェイスと一致する必要があります。

ステップ 7 TFTP サーバのソフトウェア イメージを推奨される場所（TFTP ソフトウェアによって異なります）に保存します。

ステップ 8 ダウンロードを開始するには、次のコマンドを入力します。

tftp dnld

（注） TFTP サーバが別のサブネットに属する場合、ゲートウェイを定義する必要があります。

署名付き Microsoft CA サーバ-クライアント認証証明書を Microsoft OCS 2008 で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は、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できません。現在のユーザ ストアからローカルのコンピュータ ストアへ証明書をコピーしようとすると、秘密キーがないというエラー メッセージで失敗します。

次の手順を実行できます。

1. ローカル ユーザとして OCS にログインします。
2. 証明書を作成します。
3. CA サーバから証明書を承認します。
4. OCS にログイン中に、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、この場合は OCS ドメイン ユーザとしてログインします。
7. 証明書ファイルをインポートするのに証明書ウィザードを使用します。証明書は、ローカル コンピュータ ストアにインストールされます。この時点で、[OCS 証明書（OCS Certificate）] タブで証明書を選択できるようになります。

一般的な Cisco Adaptive Security Appliance の問題と推奨される操作

アベイラビリティを交換できない

問題 Cisco Jabber と Microsoft Office Communicator 間でアベイラビリティ情報を交換できません。

解決法 OCS/Access Edge、IM and Presence サービス、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、1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2 という OID 値を使用していることを確認します。証明書の [全般（General）] タブには正しくない値が表示されます（正しい場合は表示されません）。また、IM and Presence サービスと Access Edge 間の TLS ハンドシェイクの Ethereal トレースでも正しくない値を確認できます。

証明書の種類が [その他（Other）] 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（Programs）] > [管理ツール（Administrative Tools）] > [コンピュータの管理（Computer Management）] を選択します。[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] サービスを確認します。実行されている場合、このサービスのステータスは [開始（Started）] です。

IM and Presence サービス：

1 IM and Presence サービ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。

IM and Presence サービスの正しい 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、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 ルートは「ドメイン」に設定されたルート タイプを持ち、反転した宛先パターンが設定されている必要があります。たとえば、フェデレーション ドメインが “abc.com” である場合は、宛先アドレスのパターンは .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、[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。

3 DNS SRV のチェックが実行され、両側が影響を受けるユーザ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 コンピュータから不正な DNS 設定を取得する可能性があります。以下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 設定を確認します。
2 DNS 設定を変更する場合は、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の設定, （66 ページ）
IM and Presence サービスでの新しい証明書の生成, （60 ページ）
SIP フェデレーションの DNS 設定, （47 ページ）

IM の送受信に関する問題

Microsoft Office Communicator ユーザと Cisco Jabber 8.0 ユーザ間で IM を送受信するときに問題があります。

DNS 設定、Access Edge、Microsoft Office Communicator クライアント、IM and Presence サービスについて記載されているトラブルシューティングを実行します。

DNS 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 と Access Edge の両方からの type=srv に対して nslookup を実行します。

Access Edge 側：

1. Access Edge のコマンド プロンプトに 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。たとえば、**_sipfederationtls._tcp.abc.com** と入力します（この **abc.com** はドメイン名です）。SRV レコードが存在する場合、IM and Presence サービスまたは Cisco Adaptive Security Appliance の FQDN が返されます。
   IM and Presence サービス：
4. リモート アクセス アカウントを使用し、ssh で IM and Presence サービス ノードにログインします。
5. 前述の Access Edge と同様の手順を実行します。ただし、ここでは 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 ユーザは、自分のプレゼンスを [取り込み中（Do Not Disturb）]（DND）に設定している可能性があります。Microsoft Office Communicator 2007 が DND に設定されている場合、他のユーザから IM を受信しません。Microsoft Office Communicator ユーザのプレゼンスを別の状態に設定します。

IM and Presence サービス：

1. DNS SRV ではなくスタティック ルートを使用している場合、スタティック ルートが正しく設定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 ルートを設定します。スタティック ルートは「ドメイン」に設定されたルート タイプを持ち、反転した宛先パターンが設定されている必要があります。たとえば、フェデレーション ドメインが “abc.com” である場合は、宛先アドレスのパターンは “.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** 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）] を選択して設定します。
2. [フェデレーション IM コントロール モジュールのステータス（Federation IM Control Module Status）] がディセーブルにされている可能性があります。**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 サービス（SIP Proxy service）] 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 パラメータが設定されていることを確認します。
3. フェデレーテッド 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、正しいフェデレーテッド ドメインが追加されていることを確認します。

関連トピック

SIP フェデレーションの DNS 設定, （47 ページ）
SIP フェデレーテッド ドメインの追加, （45 ページ）
エンタープライズ内での Microsoft サーバ ドメインの追加, （100 ページ）

少し時間が経つとアベイラビリティと IM の交換を利用できなくなる

Cisco Jabber と Microsoft Office Communicator 間でアベイラビリティと IM を共有できますが、少し時間が経つと、相互にアベイラビリティを確認できなくなり、IM も交換できなくなります。

OCS/Access Edge：

1. Access Edge で、内部エッジと外部エッジ両方の FQDN が同じである可能性があります。また、同じ FQDN の 2 つの「A」レコードのエントリが DNS にあり、一方が外部エッジの IP アドレスに解決され、もう一方が内部エッジの IP アドレスに解決される可能性があります。

   Access Edge で、内部エッジの FQDN を変更し、更新したレコード エントリを DNS に追加します。元々 Access Edge の内部 IP に解決されていた 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設定し直します。

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を設定し直します。

DNS 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。

関連トピック

SIP フェデレーション用の外部サーバ コンポーネントの設定, （121 ページ）

在席ステータスの変更と IM 配信の遅延

Cisco Jabber と Microsoft Office Communicator 間で、IM and Presence サービス状態の変更の配信が遅れます。

IM and Presence サービス ノードで、Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context に [Disable Empty TLS Fragments（空の TLS フラグメントの無効化）] オプションが選択されていない可能性があります。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[システム（System）] > [セキュリティ（Security）] > [TLS コンテキスト設定（TLS Context Configuration）] を選択します。

ステップ 2 Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context リンクをクリックします。

ステップ 3 TLS コンテキスト情報の領域で、[空の TLS フラグメントの無効化（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。

アベイラビリティ サブスクリプションを試行した後に 403 FORBIDDEN が返される

IM and Presence サービスで Microsoft Office Communicator ユーザのアベイラビリティにサブスクライブしようとすると、OCS サーバから 403 FORBIDDEN メッセージが送信されます。

Access Edge サーバで、IM and Presence サービス 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 サーバで、IM サービス プロバイダのリストに IM and Presence サービス ノードのエントリを追加します。Access Edge の DNS サーバに、IM and Presence サービス ノードのパブリック アドレスを指す IM and Presence サービス 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 サーバで、IM and Presence サービス ノードが [許可（Allow）] リストに追加されている可能性があります。Access Edge サーバで、IM and Presence サービス ノードを指す [許可（Allow）] リストからエントリを削除します。

関連トピック

SIP フェデレーション用の外部サーバ コンポーネントの設定, （121 ページ）

NOTIFY メッセージでのタイムアウト

NOTIFY メッセージを送信するときに IM and Presence サービスと Microsoft OCS 間で TCP を使用して直接フェデレーションが行われている場合、IM and Presence サービスがタイムアウトします。

場合によっては、IM and Presence サービス ノードで [レコード ルート ヘッダーでトランスポートを使用（Use Transport in Record-Route Header）] をイネーブルにする必要があります。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[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 ボックスで、[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（Clusterwide）（SIP Parameters (Clusterwide)）] セクションで、[レコード ルート ヘッダのトランスポートを使用（Use Transport in Record-Route Header）] パラメータの [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 and Presence サービス証明書が受け入れられない

Access Edge が IM and Presence サービスからの証明書を受け入れません。

IM and Presence サービス/Cisco Adaptive Security Appliance 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 DNS サーバに、IM and Presence サービス ノードのパブリック アドレスを指す IM and Presence サービス ドメインの _sipfederationtls レコードがあることを確認します。[許可（Allow）] リストに IM and Presence サービスの FQDN を設定しない場合、IM and Presence サービス証明書の件名の CN が IM and Presence サービス ドメインの SRV レコードの FQDN に解決される必要があります。
2. FIPS が Access Edge でイネーブルであること（TLSv1 を使用すること）を確認します。
3. OCS でグローバルにフェデレーションがイネーブルであり、フロントエンド サーバでフェデレーションがイネーブルであることを確認します。
4. DNS SRV を解決できない場合、DNS が正しく設定され、Access Edge から type=srv の nslookup が実行されることを確認します。
5. Access Edge のコマンド プロンプトに nslookup と入力します。
6. set type=srv と入力します。
7. たとえば、次のように IM and Presence サービス ドメインの SRV レコードを入力します。**_sipfederationtls._tcp.abc.com**（この **abc.com** はドメイン名です）。SRV レコードが存在する場合、IM and Presence サービス/Cisco Adaptive Security Appliance の FQDN が返されます。

IM and Presence サービス/Cisco Adaptive Security Appliance：

IM and Presence サービスと Cisco Adaptive Security Appliance で暗号を確認します。[IM and Presence Service Administration] にログインし、[システム（System）] > [セキュリティ（Security）] > [TLS

コンテキスト設定（TLS Context Configuration）] > [デフォルト Cisco SIP プロキシ ピア認証 TLS コンテキスト（Default Cisco SIP Proxy Peer Auth TLS Context）]を選択し、「TLS_RSA_WITH 3DES_EDE_CBC_SHA」暗号が選択することを確認します。

関連トピック

SIP フェデレーション用の外部サーバ コンポーネントの設定, （121 ページ）
選択した TLS ピア サブジェクト リストへの TLS ピアの追加, （52 ページ）

OCS でフロントエンド サーバの起動に問題がある

OCS でフロントエンド サーバが起動しません。

OCS で、Access Edge のプライベート インターフェイスの FQDN が [承認されたホスト（Authorized Hosts）] のリストに定義されている可能性があります。OCS の [承認されたホスト（Authorized Hosts）] 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 のインストール時に、RTCService と RTCComponentService という 2 つの Active Directory ユーザ 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付与されますが、これら両方のアカウントでは、[パスワードを無期限にする（Password never expires）] オプションがデフォルトで選択されないため、パスワードは定期的に期限切れになります。OCS サーバで RTCService または RTCComponentService のパスワードをリセットするには、次の手順を実行します。

手順

ステップ 1 ユーザ アカウントを右クリックします。
ステップ 2 [パスワードをリセット（Reset Password）] を選択します。
ステップ 3 ユーザ 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（Account）] 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。

Access Edge に対してリモート デスクトップを実行できない

Windows XP で FIPS を有効にしている場合、Access Edge サーバに対してリモート デスクトップを実行できません。

これは、Microsoft の既知の問題です。この問題を回避するには、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 の URL に記載されている順に従って操作してください。

http://support.microsoft.com/kb/811770

第 17 章

XMPP フェデレーション統合に関するトラブルシューティング

システム トラブルシュータを確認する

複数の IM and Presence サービス クラスタを配置し、XMPP フェデレーションを設定する場合、1 つのクラスタにつき少なくとも 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。各クラスタでは同じ XMPP フェデレーションの設定とポリシーを指定する必要があります。IM and Presence サービスでは、クラスタ全体に XMPP フェデレーション設定をレプリケートしません。システム トラブルシュータからは、クラスタ全体の XMPP フェデレーション設定が同期されていないかどうかがレポートされます。システム トラブルシュータは次の確認を実行します。

手順

ステップ 1
a) クラスタ間ピア全体で XMPP フェデレーションが一貫してイネーブルにされている。
b) クラスタ間ピア全体で SSL モードが一貫して設定されている。
c) クラスタ間ピア全体で「必要かつ有効なクライアント側の証明書」が一貫して設定されている。
d) クラスタ間ピア全体で SASL 設定が一貫して設定されている。
e) クラスタ間ピア全体でダイヤルバック シークレットが一貫して設定されている。
f) クラスタ間ピア全体で XMPP フェデレーションのデフォルト管理ポリシーが一貫して設定されている。
g) クラスタ間ピア全体でポリシー ホストが一貫して設定されている。

ステップ 2 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[診断（Diagnostics）] > [システム トラブルシュータ（System Troubleshooter）] を選択します。

ステップ 3 次の項目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することを確認する（Verify the XMPP Federation settings match on all interclustered peers.）
- SASL 設定がすべてのクラスタ間ピアで正しく設定されていることを確認する（Verify that SASL settings have been correctly configured for all intercluster peers.）
- XMPP が全体で無効になっているか、すべてのクラスタ内の少なくとも 1 つのノードで有効になっていることを確認する（Verify that XMPP has been uniformly disabled or enabled on at least one node in each all clusters.）
- すべてのクラスタ間ピアでデフォルトの管理者ポリシーが統一されていることを確認する（Verify that the default Admin Policy is consistent across all intercluster peers.）
- ホスト ポリシーがすべてのクラスタ間ピアで統一されていることを確認する（Verify that the Host Policy is consistent across all intercluster peers.）

これらのチェックのいずれかに問題があり、その問題をレポートする場合、システム トラブルシュータには推奨の操作が用意されています。

（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いても、IM とアベイラビリティの交換で問題が続く場合は、[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 for Inter-domain Federation）] がクラスタ間ピア全体に一貫して設定されているかを確認します。

関連トピック

XMPP フェデレーションのログ ファイルの場所, （173 ページ）

第 18 章

Cisco Adaptive Security Appliance の設定例

SIP フェデレーションの PAT コマンドとアクセス リスト設定の例

ここでは、外部 OCS のエンタープライズ導入とフェデレーションを実行する IM and Presence サービス ノードの設定例を示します。ローカルなエンタープライズ導入の場合は、さらに 2 つのクラスタ間 IM and Presence サービス ノードがあります。

この設定例では、次の値が使用されます。

- IM and Presence サービス のパブリック IP アドレス = 10.10.10.10
- IM and Presence のプライベート ルーティング IP アドレス = 1.1.1.1
- IM and Presence のプライベート セカンド IP アドレス = 2.2.2.2
- IM and Presence のプライベート サード IP アドレス = 3.3.3.3
- IM and Presence のピア認証リスナー ポート = 5062
- ネットマスク = 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 コマンドが（ルーティング）IM and Presence サービス ノード用に定義されています。

（Cisco Adaptive Security Appliance 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 Adaptive Security Appliance 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
serviceobj_tcp_source_eq_5060 obj_tcp_source_eq_5060
```

エンタープライズ導入の場合、さらに 2 つのクラスタ間 IM and Presence サービス ノード用に次の PAT コマンドを定義します。

（Cisco Adaptive Security Appliance 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 Adaptive Security Appliance 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
serviceobj_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
serviceobj_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
serviceobj_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
serviceobj_tcp_source_eq_5062 obj_tcp_source_eq_55062
```

この設定に対応するアクセス リストを次に示します。フェデレーションを行う外部ドメインごとに、ドメイン abc.com 用に次のようなアクセス リストを追加する必要があります。

（Cisco Adaptive Security Appliance 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 Adaptive Security Appliance 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
```

クラス マップにそれぞれのアクセス リストを関連付けます。

```
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 and Presence サービスから開始される TLS 接続の TLS プロキシ インスタンスは “imp_to_external” です。また、外部ドメインから開始される TLS 接続の TLS プロキシ インスタンスは "external_to_imp" です。

```
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 フェデレーション用のアクセス リストの設定例

（注） この項の例は、Cisco Adaptive Security Appliance リリース 8.3 に適用されます。

ポート 5269 のすべてのアドレスへのアクセスに対応します。

このアクセス リストの設定例では、ポート 5269 上で任意のアドレスから任意のアドレスへの転送が許可されます。

```
access-list ALLOW-ALL extended permit tcp any any eq 5269
```

任意のアドレスから ポート 5269 上の任意の単一 XMPP フェデレーション ノードへのアクセス

このアクセス リストの設定例では、ポート 5269 上で任意のアドレスから任意のシングル XMPP フェデレーション ノードへの転送が許可されます。この例では、次の値が使用されます。

- XMPP フェデレーション IM and Presence サービス リリース 9.x のプライベート IP アドレス = 1.1.1.1
- XMPP フェデレーションのリスニング ポート = 5269

```
access-list ALLOW-ALL extended permit tcp any host 1.1.1.1 eq 5269
```

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

このアクセス リストの設定例では、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 ノードへの転送が許可されます。

（注） これらのパブリック アドレスは DNS で公開されますが、access-list コマンドにはプライベート アドレスが設定されます。

この設定例では、次の値が使用されます。

- • XMPP フェデレーション IM and Presence サービス リリース 9.x のプライベート IP アドレス = 1.1.1.1
- • IM and Presence サービス リリース 9.x のプライベート セカンド IP アドレス = 2.2.2.2
- • IM and Presence サービス リリース 9.x IP のプライベート サード IP アドレス = 3.3.3.3
- • XMPP フェデレーションのリスニング 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
```

特定のフェデレーション ドメインから DNS で公開された特定の XMPP フェデレーション ノードへの専用アクセス

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 で公開された特定の XMPP フェデレーション ノードへの転送だけが許可されます。

（注） これらのパブリック アドレスは DNS で公開されますが、access-list コマンドにはプライベート アドレスが設定されます。

この設定例では、次の値が使用されます。

- XMPP フェデレーション IM and Presence サービス リリース 9.x のプライベート IP アドレス = 1.1.1.1
- IM and Presence サービス リリース 9.x のプライベート セカンド IP アドレス = 2.2.2.2
- IM and Presence サービス リリース 9.x IP のプライベート サード IP アドレス = 3.3.3.3
- XMPP フェデレーションのリスニング ポート = 5269
- 外部の XMPP 企業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 フェデレーション用の NAT の設定例

例 1：XMPP フェデレーションがイネーブルのシングル ノード

この設定例では、次の値が使用されます。

- IM and Presence サービス のパブリック IP アドレス = 10.10.10.10
- XMPP フェデレーション IM and Presence サービス リリース 9.x のプライベート IP アドレス = 1.1.1.1

- XMPP フェデレーションのリスニング ポート = 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
serviceobj_tcp_source_eq_5269 obj_tcp_source_eq_5269
```

例 2：XMPP フェデレーションが設定され、それぞれが DNS 内のパブリック IP アドレスを持つ複数のノード

この設定例では、次の値が使用されます。

- IM and Presence サービスのパブリック IP アドレス = 10.10.10.10, 20.20.20.20, 30.30.30.30
- XMPP フェデレーション IM and Presence サービス リリース 9.x のプライベート IP アドレス = 1.1.1.1
- IM and Presence サービス リリース 9.x のプライベート セカンド IP アドレス = 2.2.2.2
- IM and Presence サービス リリース 9.x IP のプライベート サード IP アドレス = 3.3.3.3
- XMPP フェデレーションのリスニング ポート = 5269

```
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10
serviceobj_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
serviceobj_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
serviceobj_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
serviceobj_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
serviceobj_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
serviceobj_tcp_source_eq_5269 obj_tcp_source_eq_5269
```

例 3：XMPP フェデレーションが設定されているが、DNS 内のパブリック IP アドレスは単一で、DNS で公開された任意のポートを持つ複数のノード（PAT）

DNS でパブリッシュされたポート（PAT）。

この設定例では、次の値が使用されます。

- IM and Presence サービス のパブリック IP アドレス = 10.10.10.10
- XMPP フェデレーション IM and Presence サービス リリース 9.x のプライベート IP アドレス = 1.1.1.1、ポート 5269
- IM and Presence サービス リリース 9.x のプライベート セカンド IP アドレス = 2.2.2.2、任意のポート 25269

- IM and Presence サービス リリース 9.x のプライベート サード IP アドレス = 3.3.3.3、任意のポート 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
serviceobj_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
serviceobj_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
serviceobj_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
serviceobj_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
serviceobj_tcp_source_eq_5269 obj_tcp_source_eq_35269
```

第 19 章

Cisco Adaptive Security Appliance と Microsoft Access Edge との間における VeriSign を使用したセキュリティ証明書交換

Cisco Adaptive Security Appliance でのセキュリティ証明書の設定

古い証明書およびトラストポイントの削除

この手順では、古い中間証明書、署名済み証明書、およびルート証明書のトラストポイントを Cisco Adaptive Security Appliance で削除する方法について説明します。

はじめる前に

次の章に記載されている設定タスクを実行したことを確認します。

- SIP フェデレーション用の IM and Presence サービスの設定，（45 ページ）
- SIP フェデレーションに関する Cisco Adaptive Security Appliance（ASA）の設定，（77 ページ）

手順

ステップ 1 コンフィギュレーション モードを開始します。

```
> 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表示します。

```
show crypto ca trustpoints
```

ステップ 3 次のコマンドを入力して、トラストポイントと関連する証明書を削除します。

```
no crypto ca trustpoint trustpoint_name
```

次の警告の出力が表示されます。

```
WARNING: Removing an enrolled trustpoint will destroy allcertificates received from the
related Certificate Authority.
```

ステップ 4 トラストポイントの削除を確認するメッセージが表示されたら、yes と入力します。

次の作業

VeriSign 用の新しいトラストポイントの生成, （204 ページ）

VeriSign 用の新しいトラストポイントの生成

手順

ステップ 1 コンフィギュレーション モードを開始します。

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

ステップ 2 次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 サービス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） 更新の証明書署名要求（CSR）ファイルを VeriSign に送信する場合、件名の値には次の情報を含める必要があります。

- 国（Country）（2 文字の国コードのみ）
- 都道府県（State）（省略なし）
- 市区町村（Locality）（省略なし）
- 組織名（Organization Name）
- 組織部門（Organizational Unit）
- 一般名（Common Name）（FQDN）- この値はパブリック IM and Presence の FQDN にする必要があります。

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 ペアが生成されていることを確認します。

次の作業

中間証明書のインポート, （208 ページ）

ルート証明書のインポート

はじめる前に

VeriSign 用の新しいトラストポイントの生成, （204 ページ）の手順を実行します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

```
> 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 Adaptive Security Appliance にインポートします。

```
crypto ca authenticate trustpoint_name
```

ステップ 3 次のように CA 証明書を入力します。

```
-----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 証明書の承認を確認するメッセージが表示されたら、**yes** と入力します。

次の作業

証明書署名要求の生成，（206 ページ）

証明書署名要求の生成

はじめる前に

ルート証明書のインポート，（205 ページ）の手順を実行します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

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

ステップ 2 次のコマンドを入力して、CA に対する登録要求を送信します。

```
(config)# crypto ca enroll trustpoint_name
```

次の警告の出力が表示されます。

```
%WARNING: The certificate enrollment is configured with an fqdnthat differs from the system fqdn.If this certificate will be used for VPN authentication this may cause connection problems.
```

ステップ 3 登録の続行を確認するメッセージが表示されたら、**yes** と入力します。

```
% Start certificate enrollment..%The subject name in the certificate will be: <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ことを確認するメッセージが表示されたら、**no** と入力します。

ステップ 5 端末に証明書要求を表示することを確認するメッセージが表示されたら、**yes** と入力します。証明書要求が表示されます。

次の作業

証明書署名要求を VeriSign に送信する，（207 ページ）

証明書署名要求を VeriSign に送信する

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`（署名済み証明書）
- `trial-inter-root.cer`（下位中間ルート証明書）
- `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証明書ファイルを保存します。

はじめる前に

- 証明書署名要求の生成, （206 ページ）の手順を実行します。
- 証明書署名要求を生成するときは、定義したチャレンジ パスワードが必要になります。

手順

ステップ 1 VeriSign Web サイトにアクセスします。

ステップ 2 記載されている手順に従って証明書署名要求を入力します。

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 表示される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（これらの文字列を含めて）貼り付けなければなりません。

次の作業

証明書署名要求に使用した証明書の削除, （207 ページ）

証明書署名要求に使用した証明書の削除

証明書署名要求の生成に使用した一時ルート証明書は削除する必要があります。

はじめる前に

証明書署名要求を VeriSign に送信する, （207 ページ）の手順を実行します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

```
> 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 次のコマンドを入力して、証明書を削除します。

```
(config)# crypto ca certificate chain trustpoint_name

(config-cert-chain)# no certificate ca 00b92f60cc889fa17a4609b85b70$
```

次の警告の出力が表示されます。

```
WARNING: The CA certificate will be disassociated from this trustpoint andwill be removed
if it is not associated with any other trustpoint.Any other certificates issued by this CA
and associated with this trustpoint will also be removed.
```

ステップ 4 トラストポイントの削除を確認するメッセージが表示されたら、**yes** と入力します。

次の作業

中間証明書のインポート, （208 ページ）

中間証明書のインポート

はじめる前に

証明書署名要求に使用した証明書の削除, （207 ページ）の手順を実行します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

```
> 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 Adaptive Security Appliance にインポートします。

```
crypto ca authenticate trustpoint_name
```

ステップ 3 次のように CA 証明書を入力します。

```
-----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 証明書の承認を確認するメッセージが表示されたら、**yes** と入力します。

次の作業

ルート証明書のトラストポイントの作成, （209 ページ）

ルート証明書のトラストポイントの作成

はじめる前に

中間証明書のインポート, （208 ページ）の手順を実行します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

```
> 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 次の一連の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

はじめる前に

ルート証明書のトラストポイントの作成, （209 ページ）の手順を実行します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

```
> 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 Adaptive Security Appliance にインポートします。

```
crypto ca authenticate verisign_root
```

ステップ 3 次のように CA 証明書を入力します。

```
-----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 証明書の承認を確認するメッセージが表示されたら、**yes** と入力します。

次の作業

署名付き証明書のインポート, （210 ページ）

署名付き証明書のインポート

はじめる前に

ルート証明書のインポート, （209 ページ）の手順を実行します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

```
> 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 Adaptive Security Appliance にインポートします。

```
crypto ca import verisignca certificate
```

次の警告の出力が表示されます。

```
WARNING: The certificate enrollment is configured with an fqdn that differs from the system
fqdn.If this certificate will be used for VPN authentication this may cause connection
problems.
```

ステップ 3 証明書の登録の続行を確認するメッセージが表示されたら、**yes** と入力します。

ステップ 4 次のように CA 証明書を入力します。

```
-----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 証明書の承認を確認するメッセージが表示されたら、**yes** と入力します。

次の作業

VeriSign 証明書を Microsoft Access Edge にインポートする, （211 ページ）

VeriSign 証明書を Microsoft Access Edge にインポートする

この手順では、VeriSign のルート証明書と中間証明書を Microsoft の Access Edge サーバにインポートする方法について説明します。

はじめる前に

VeriSign から提供された証明書を Access Edge サーバ（C:\ など）に保存します。

手順

ステップ 1 Access Edge サーバで、run コマンドから **mmc** を実行します。
ステップ 2 [ファイル（File）] > [スナップインを追加/削除（Add/Remove Snap-in）] を選択します。
ステップ 3 [追加（Add）] をクリックします。
ステップ 4 [証明書（Certificates）] をクリックします。
ステップ 5 [追加（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（Finish）] をクリックします。
ステップ 10 [スナップインを追加/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）] の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 証明書ウィザードの [次へ（Next）] をクリックします。
ステップ 16 C:\ ディレクトリにある 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、[信頼されたルート証明機関（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 20 章

統合のデバッグ情報

Cisco Adaptive Security Appliance のデバッグ情報

Cisco Adaptive Security Appliance のデバッグ コマンド

次の表は、Cisco Adaptive Security Appliance のデバッグ コマンドの一覧です。

表 *26*：*Cisco Security Appliance* のデバッグ コマンド

目的	使用するコマンド	注記
Cisco Adaptive Security Appliance インターフェイスに ping を送信するための 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終わったら、デバッグ メッセージをディセーブルにすることを強くお勧めします。ICMP デバッグ メッセージをディセーブルにするには、`no debug icmp trace` コマンドを使用します。

目的	使用するコマンド	注記
IM and Presence サービス/Cisco Adaptive Security Appliance または Cisco Adaptive Security Appliance/外部ドメイン間の証明書の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 パラメータを追加して、Cisco Adaptive Security Appliance でログ レベルをさらに強化できます。例： **debug crypto ca 3**
	debug crypto ca messages	入力および出力メッセージのデバッグ メッセージのみ表示します。
	debug crypto ca transactions	トランザクションのデバッグ メッセージのみを表示します。
Cisco Adaptive Security Appliance を介して送信された SIP メッセージを表示します。	**debug sip**	
（後で確認するために）ログ メッセージをバッファに送信します。	**terminal monitor**	
システム ログ メッセージをイネーブルにします。	**ログイン**	トラブルシューティングが終わったら、システム ログをディセーブルにすることを強くお勧めします。システム ログ メッセージをディセーブルにするには、**no logging on** コマンドを使用します。
システム ログ メッセージをバッファに送信します。	**logging buffer debug**	
Telnet セッションまたは SSH セッションに送信するシステム ログメッセージを設定します。	**logging monitor debug**	
システム ログ メッセージを受信する（syslog）サーバを指定します。	**logging host** *interface_name ip_address*	• interface_name 引数に、syslog サーバにアクセスする Cisco Adaptive Security Appliance インターフェイスを指定します。 • ip_address 引数には、syslog サーバの IP アドレスを指定します。

目的	使用するコマンド	注記
インターフェイスに ping を送信します。	**ping**	トラフィックが Cisco Adaptive Security Appliance を経由できることを確認するために、Cisco Adaptive Security Appliance インターフェイスに ping を送信する操作、異なるインターフェイスにあるホスト間で ping を送信する操作の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の「Troubleshooting」を参照してください。 また、ADSM で [ツール（Tools）] > [ping] を選択してインターフェイスに ping を送信することもできます。 （注） パブリックの IM and Presence サービス IP アドレスへの ping を実行できません。ただし、インターフェイスではない Cisco Adaptive Security Appliance の MAC アドレスが ARP テーブルに表示されます（**arp –a**）。
パケットのルートをトレースします。	**traceroute**	[ツール（Tools）] > [トレースルート（Traceroute）] を使用して ASDM のパケットのルートをトレースすることもできます。
Cisco Adaptive Security Appliance を介するパケットの存続期間をトレースします。	**packet-tracer**	[ツール（Tools）] > [パケット トレーサ（Packet Tracer）] を選択して ASDM のパケットの存続期間をトレースすることもできます。

関連トピック

TLS プロキシのデバッグ コマンド, （216 ページ）

内部インターフェイスと外部インターフェイスの出力のキャプチャ

手順

ステップ 1 コンフィギュレーション モードを開始します。

```
> 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 キャプチャ内容をクリアしてから、テストすることを推奨します。“clear capture in” コマンドを使用して内部インターフェイスのキャプチャをクリアし、“clear capture out” コマンドを使用して外部インターフェイスのキャプチャをクリアします。

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の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の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 次のコマンドを入力して、TLS 固有のパケットをキャプチャします。

```
capture capture_name type tls-proxy interface interface_name
```

ステップ 7 次のコマンドを入力して、パケットのキャプチャを取得します。

```
copy /pcap capture:in tftp://xx.xx.xx.xx copy /pcap capture:out tftp://xx.xx.xx.xx
```

次のコマンドを入力して、出力をディスクにコピーし、ASDM（[操作（Actions）] > [ファイル管理（File Management）] > [ファイル転送（File Transfer）]）を使用して取得します。

```
copy /pcap capture:in disk0:in_1
```

TLS プロキシのデバッグ コマンド

次の表は、TLS プロキシのデバッグ コマンドの一覧です。

表 *27* : *TLS* プロキシのデバッグ コマンド

目的	使用するコマンド
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** **debug inspect tls-proxy errors** **debug inspect tls-proxy all**

目的	使用するコマンド
TLS プロキシ セッション出力の表示	**show log**
アクティブな TLS プロキシ セッションの確認	**show tls-proxy**
現在の TLS プロキシ セッションに関する詳細情報の表示 （Cisco Adaptive Security Appliance が IM and Presence サービスと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 サーバのデバッグ

OCS/Access Edge でデバッグ セッションを開始する

手順

ステップ 1 外部 Access Edge サーバで、[スタート（Start）] > [管理ツール（Administrative Tools）] > [コンピュータの管理（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）] > [新規デバッグ セッション（New Debug Session）] を選択します。

ステップ 4 [ロギング（Logging）] オプションで、[SIP スタック（SIP Stack）] を選択します。

ステップ 5 レベル値に対して [すべて（All）] を選択します。

ステップ 6 [ログの開始（Start Logging）] をクリックします。

ステップ 7 完了したら、[ロギングを停止（Stop Logging）] をクリックします。

ステップ 8 [ログ ファイルを分析（Analyze Log Files）] をクリックします。

Access Edge の DNS 設定を検証する

手順

ステップ 1 外部 Access Edge サーバで、[スタート（Start）] > [管理ツール（Administrative Tools）] > [コンピュータの管理（Computer Management）] を選択します。

ステップ 2 左側のペインの [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 サービスで管理されるドメインがいずれもブロックされ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) [他のドメインとフェデレーションを行う（Federate with other domains）]

b) [フェデレーション パートナーの検出を許可する（Allow discovery of federation partners）]

ステップ 6 Access Edge が DNS SRV レコードを公開していることを確認します。