CHAPTER 19

Cisco Unified Presence の設定

この章では、Cisco Unified Presence 向けに適応型セキュリティ アプライアンスを設定する方法を説明します。

この章の内容は、次のとおりです。

Cisco Unified Presence に関する情報

この項では、次のトピックについて取り上げます。

SIP フェデレーション配置の Cisco Unified Presence のアーキテクチャ

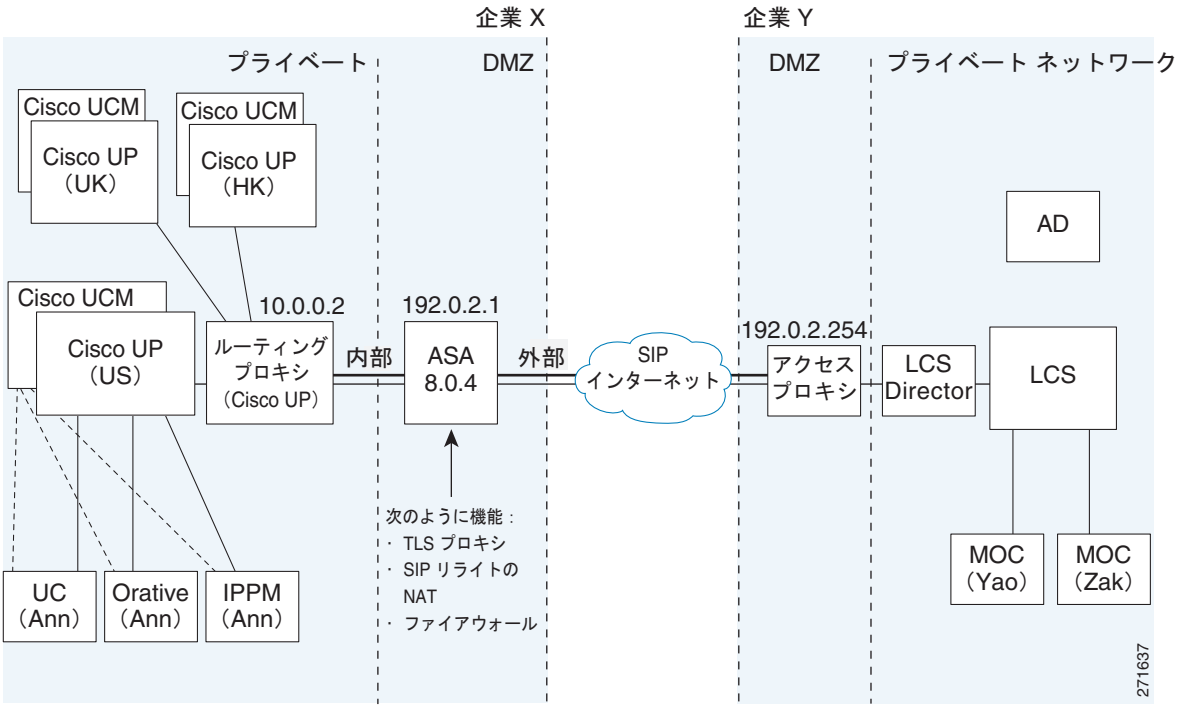
図 19-1 は、ASA を（TLS プロキシとして実装されている）プレゼンス フェデレーション プロキシとして使用する、Cisco Unified Presence/LCS フェデレーションのシナリオを示しています。TLS 接続を使用する 2 つのエンティティは、企業 X の「ルーティング プロキシ」（専用の Cisco UP）と、企業 Y の Microsoft アクセス プロキシです。ただし、構成はこのシナリオに制限されません。ASA の左側には、あらゆる Cisco UP または Cisco UP クラスタを展開できます。リモート エンティティには任意のサーバ（LCS、OCS、または別の Cisco UP）を使用できます。

次のアーキテクチャは、TLS 接続で SIP（または他の ASA 検査対象のプロトコル）を使用する 2 つのサーバの一般的なアーキテクチャです。

エンティティ X：企業 X の Cisco UP/ルーティング プロキシ

エンティティ Y：企業 Y の LCS/OCS 用の Microsoft アクセス プロキシ/エッジ サーバ

図 19-1　標準的な Cisco Unified Presence/LCS フェデレーション シナリオ



上記のアーキテクチャでは、ASA はファイアウォール、NAT、および TLS プロキシとして機能します。これは推奨のアーキテクチャです。ただし、ASA は、NAT および TLS プロキシのみとして機能し、既存のファイアウォールを使用することもできます。

いずれかのサーバが TLS ハンドシェイクを開始できます（クライアントだけが TLS ハンドシェイクを開始できる IP テレフォニーまたは Cisco Unified Mobility とは異なります）。双方向の TLS プロキシ ルールと設定があります。各企業は、ASA を TLS プロキシとして使用できます。

図 19-1 では、NAT または PAT を使用して、エンティティ X のプライベート アドレスを非表示にできます。この状況では、スタティック NAT または PAT を、接続または TLS ハンドシェイク（着信）を開始した外部サーバ（エンティティ Y）に設定する必要があります。通常、パブリック ポートは 5061 にする必要があります。次のスタティック PAT コマンドは、着信接続を受け入れる Cisco UP で必要です。

```
hostname(config)# object network obj-10.0.0.2-01
hostname(config-network-object)# host 10.0.0.2
hostname(config-network-object)# nat (inside,outside) static 192.0.2.1 service tcp 5061
5061
```

次のスタティック PAT は、（SIP SUBSCRIBE を送信して）外部サーバへの接続を開始できる各 Cisco UP に対して設定する必要があります。

アドレスが 10.0.0.2 の Cisco UP の場合は、次のコマンドを入力します。

```
hostname(config)# object network obj-10.0.0.2-02
hostname(config-network-object)# host 10.0.0.2
hostname(config-network-object)# nat (inside,outside) static 192.0.2.1 service tcp 5062
5062
hostname(config)# object network obj-10.0.0.2-03
hostname(config-network-object)# host 10.0.0.2
hostname(config-network-object)# nat (inside,outside) static 192.0.2.1 service udp 5070
5070
hostname(config)# object network obj-10.0.0.2-04
hostname(config-network-object)# host 10.0.0.2
```

```
hostname(config-network-object)# nat (inside,outside) static 192.0.2.1 service tcp 5060
5060
```

アドレスが 10.0.0.3 の別の Cisco UP の場合は、45062 または 45070 などの PAT ポートの異なるセットを使用する必要があります。

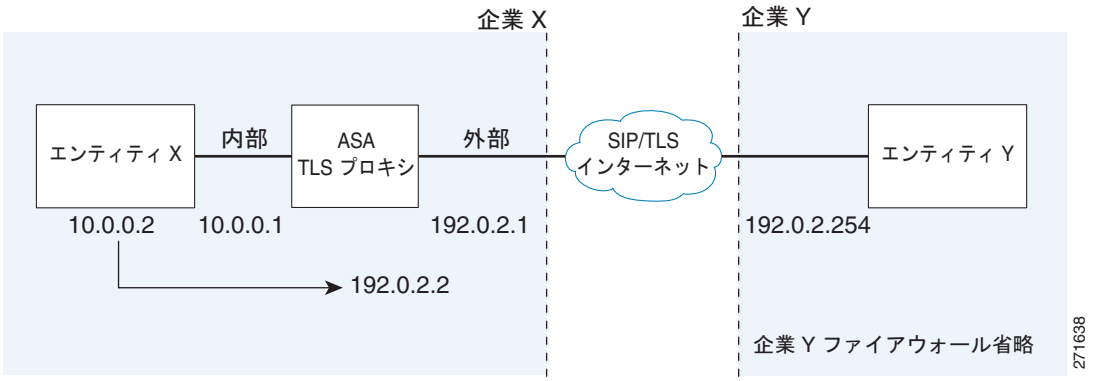
```
hostname(config)# object network obj-10.0.0.3-01
hostname(config-network-object)# host 10.0.0.3
hostname(config-network-object)# nat (inside,outside) static 192.0.2.1 service tcp 5061
45061
hostname(config)# object network obj-10.0.0.3-02
hostname(config-network-object)# host 10.0.0.3
hostname(config-network-object)# nat (inside,outside) static 192.0.2.1 service tcp 5062
45062
hostname(config)# object network obj-10.0.0.3-03
hostname(config-network-object)# host 10.0.0.3
hostname(config-network-object)# nat (inside,outside) static 192.0.2.1 service udp 5070
5070
hostname(config)# object network obj-10.0.0.2-03
hostname(config-network-object)# host 10.0.0.2
hostname(config-network-object)# nat (inside,outside) static 192.0.2.1 service tcp 5070
45070
hostname(config)# object network obj-10.0.0.3-04
hostname(config-network-object)# host 10.0.0.3
hostname(config-network-object)# nat (inside,outside) static 192.0.2.1 service tcp 5060
45060
```

ダイナミック NAT または PAT を、発信接続または TLS ハンドシェイクの残りに対して使用できます。ASA SIP インスペクション エンジンは、必要な変換（フィックスアップ）を処理します。

```
hostname(config)# object network obj-0.0.0.0-01
hostname(config-network-object)# subnet 0.0.0.0 0.0.0.0
hostname(config-network-object)# nat (inside,outside) dynamic 192.0.2.1
```

図 19-2 は、ASA 上のプレゼンス フェデレーション プロキシを通じてエンティティ Y に接続されているエンティティ X を抽象化したシナリオを示しています。プロキシは、エンティティ X と同じ管理ドメイン内に存在します。エンティティ Y は別の ASA をプロキシとして使用できますが、ここでは簡略化のために省略されています。

図 19-2　2 つのサーバ エンティティ間の抽象化されたプレゼンス フェデレーション プロキシ シナリオ



ASA がそのクレデンシャルを保持している場合にエンティティ X のドメイン名を正しく解決するには、ASA を、エンティティ X に対して NAT を実行するように設定します。またドメイン名は、ASA がプロキシ サービスを提供するエンティティ X のパブリック アドレスとして解決されます。

SIP フェデレーション用の Cisco Unified Presence Federation の設定方法の詳細については、『Integration Guide for Configuring Cisco Unified Presence for Interdomain Federation』を参照してください。

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

プレゼンス フェデレーションの信頼関係

企業内では、自己署名した証明書を使用して信頼関係を設定するか、内部 CA で信頼関係を設定できます。

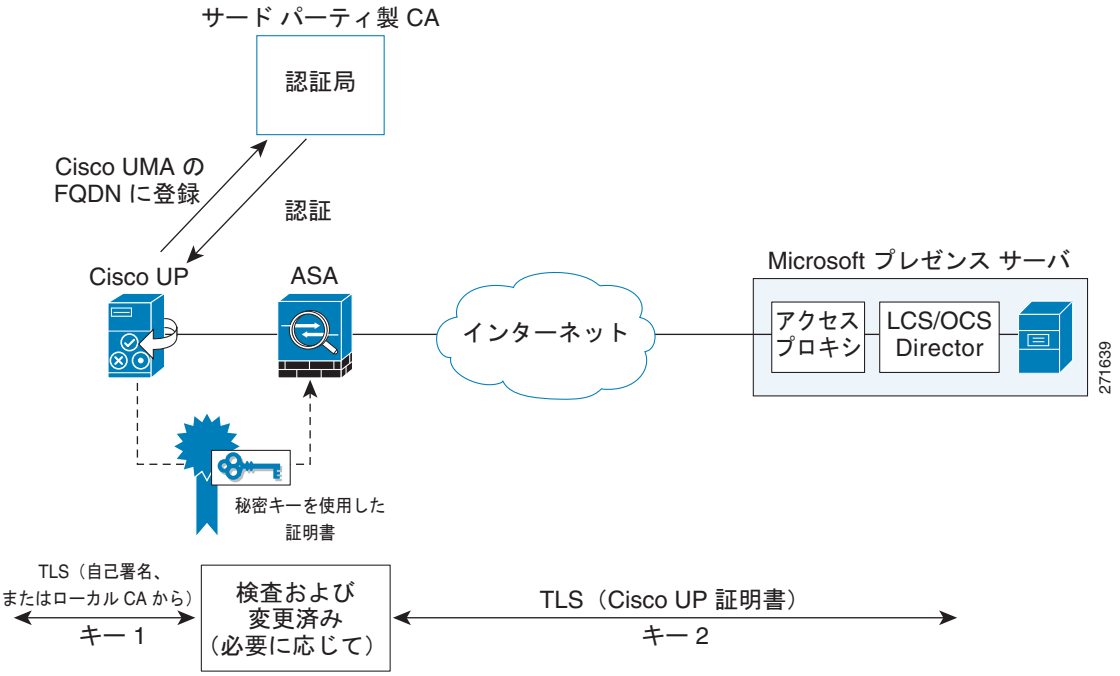
企業間または管理ドメイン間における信頼関係の確立は、フェデレーションにとって重要です。企業間では、信頼できるサードパーティ CA（VeriSign など）を使用する必要があります。ASA は、Cisco UP の Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を使用して証明書を取得します（証明書偽装）。

TLS ハンドシェイクの場合、2 つのエンティティが、信頼できるサードパーティ認証局への証明書チェーンを通じてピア証明書を検証できます。両方のエンティティが CA に登録されます。TLS プロキシとしての ASA は、両方のエンティティによって信頼されている必要があります。ASA は、企業のいずれかに常に関連付けられています。企業（図 19-1 の企業 X）内では、エンティティと ASA は、ローカル CA を通じて、または自己署名した証明書を使用して相互に認証を行うことができます。

ASA とリモート エンティティ（エンティティ Y）間で信頼関係を確立するために、ASA はエンティティ X（Cisco UP）の代わりに CA に登録できます。登録要求で、エンティティ X の ID（ドメイン名）が使用されます。

図 19-3 に、信頼関係を確立する方法を示します。ASA は、ASA が Cisco UP であるかのように、Cisco UP FQDN を使用してサードパーティ CA に登録します。

図 19-3　セキュリティ アプライアンスで Cisco Unified Presence を表す方法：証明書偽装



Cisco UP とセキュリティ アプライアンス間でのセキュリティ証明書の交換

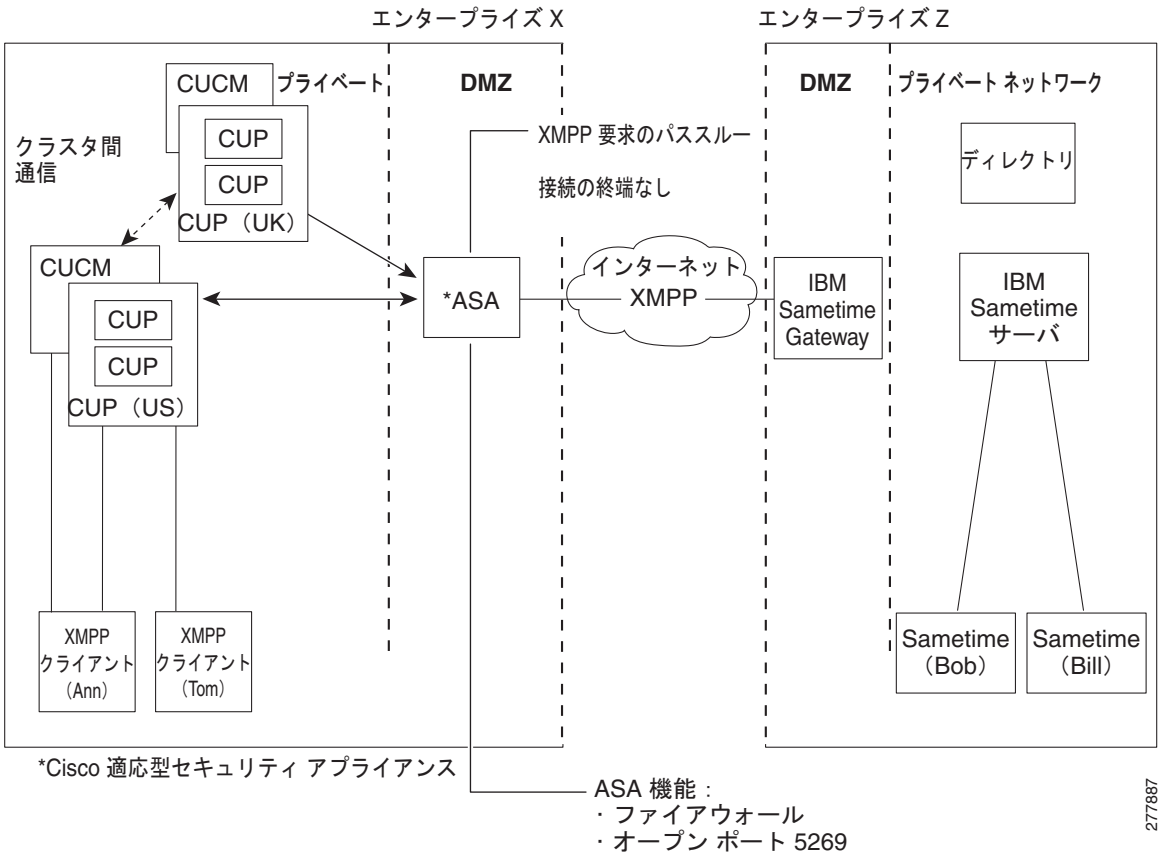
ASA で使用される証明書のキー ペア（cup_proxy_key など）を生成し、TLS ハンドシェイクで ASA から Cisco UP に送信された自己署名証明書を識別するためのトラストポイント（cup_proxy など）を設定します。

ASA で Cisco UP の証明書を信頼するためには、Cisco UP からの証明書を識別するトラストポイント（cert_from_cup など）を作成し、登録タイプを端末として指定して、Cisco UP から受信した証明書を端末に貼り付けることを示します。

XMPP フェデレーション配置

図 19-4 に、Cisco Unified Presence 企業配置と IBM Sametime 企業配置の間の XMPP フェデレーション ネットワークの例を示します。XMPP フェデレーションでは、TLS はオプションです。XMPP フェデレーションでは、ASA はファイアウォールとしてだけ機能します。TLS 機能や PAT は XMPP フェデレーションに対して提供されません。

図 19-4　　と IBM Sametime の間の基本的な XMPP フェデレーション ネットワーク



内部の Cisco Unified Presence 企業配置内には 2 台の DNS サーバが存在します。一方の DNS サーバは、Cisco Unified Presence 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 フェデレーション用の Cisco Unified Presence パブリック アドレスと DNS SRV レコード

（_sipfederationtle）、および Cisco Unified Presence による XMPP フェデレーション（_xmpp-server）をホストします。Cisco Unified Presence 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。

XMPP フェデレーション用の Cisco Unified Presence Federation の設定方法の詳細については、『*Integration Guide for Configuring Cisco Unified Presence Release 8.0 for Interdomain Federation*』を参照してください。

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

XMPP フェデレーションの設定要件

XMPP フェデレーションの場合、ASA はファイアウォールとしてだけ機能します。ASA 上では、着信と発信の両方の XMPP フェデレーション 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、ASA 上でポート 5269 を開く ACL の例をいくつか示します。

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 cup IP address> eq 5269
```

上述の ACL 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 cup ip address>
#host <private cup ip address>
object network obj_host_<private cup2 ip address>
#host <private cup2 ip address>
object network obj_host_<public cup ip address>
#host <public cup ip address>
....
```

次の NAT コマンドを設定します。

```
nat (inside,outside) source static obj_host_<private cup1 IP> obj_host_<public cup IP>
service
obj_udp_source_eq_5269 obj_udp_source_eq_5269
nat (inside,outside) source static obj_host_<private cup1 IP> obj_host_<public cup 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 cup2 ip> obj_host_<public cup IP>
service
obj_udp_source_eq_5269 obj_udp_source_eq_25269
nat (inside,outside) source static obj_host_<private cup2 ip> obj_host_<public cup IP>
service
obj_tcp_source_eq_5269 obj_tcp_source_eq_25269

nat (inside,outside) source static obj_host_<private cup3 ip> obj_host_<public cup IP>
service
obj_udp_source_eq_5269 obj_udp_source_eq_35269
nat (inside,outside) source static obj_host_<private cup3 ip> obj_host_<public cup 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 cup2 ip> obj_host_<public cup2 IP>
service
obj_udp_source_eq_5269 obj_udp_source_eq_5269
nat (inside,outside) source static obj_host_<private cup2 ip> obj_host_<public cup2 IP>
service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

nat (inside,outside) source static obj_host_<private cup3 ip> obj_host_<public cup3 IP>
service
obj_udp_source_eq_5269 obj_udp_source_eq_5269
nat (inside,outside) source static obj_host_<private cup3 ip> obj_host_<public cup IP>
service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
```

Cisco Unified Presence のライセンス

ASA でサポートされる Cisco Unified Presence 機能には、Unified Communications Proxy ライセンスが必要です。

次の表に、Unified Communications Proxy ライセンスの詳細をプラットフォーム別に示します。

（注） この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件[1]
ASA 5505	基本ライセンスと Security Plus ライセンス：2 セッション。 *オプション ライセンス：24 セッション。*
ASA 5510	基本ライセンスと Security Plus ライセンス：2 セッション。 *オプション ライセンス：24、50、または 100 セッション。*
ASA 5520	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、または 1000 セッション。*
ASA 5540	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、または 2000 セッション。*
ASA 5550	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、または 3000 セッション。*
ASA 5580	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、3000、5000、または 10,000 セッション。*[2]
ASA 5512-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、または 500 セッション。*

モデル	ライセンス要件[1]
ASA 5515-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、または 500 セッション。*
ASA 5525-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、または 1000 セッション。*
ASA 5545-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、または 2000 セッション。*
ASA 5555-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、または 3000 セッション。*
ASA 5585-X（SSP-10）	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、または 3000 セッション。*
ASA 5585-X（SSP-20、-40、または -60）	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、3000、5000、または 10,000 セッション。*[2]
ASASM	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、3000、5000、または 10,000 セッション。*[2]

1. 次のアプリケーションでは、接続時に TLS プロキシ セッションを使用します。これらのアプリケーションで使用される各 TLS プロキシ セッション（およびこれらのアプリケーションのみ）は UC ライセンスの制限に対してカウントされます。
   - 電話プロキシ
   - プレゼンス フェデレーション プロキシ
   - 暗号化音声インスペクション

   TLS プロキシ セッションを使用するその他のアプリケーション（ライセンスが不要な Mobility Advantage Proxy、個別の IME ライセンスが必要な IME など）では、UC 制限に対してカウントしません。

   UC アプリケーションによっては、1 つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続が 2 つあるため、UC Proxy セッションも 2 つ使用されます。

   [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して個別に TLS プロキシの制限を設定します。デフォルトの TLS プロキシ制限よりも高い UC ライセンスを適用する場合、ASA では、その UC 制限に一致するように TLS プロキシの制限が自動的に設定されます。UC ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限を UC ライセンスよりも少なく設定すると、UC ライセンスですべてのセッションを使用できません。

   注：「K8」で終わるライセンス製品番号（たとえばユーザ数が 250 未満のライセンス）では、TLS プロキシ セッション数は 1000 までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザ数が 250 以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。

   注：設定をクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトが UC ライセンスの制限よりも低い場合、制限を再度引き上げるようにエラー メッセージが表示されます（ASDM の [TLS Proxy] ペインを使用します）。フェールオーバーを使用して、プライマリ ユニットで [File] > [Save Running Configuration to Standby Unit] を使用して設定の同期を強制する場合、**clear configure all** コマンドがセカンダリ ユニットに自動的に生成されるので、セカンダリ ユニットに警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。

   接続には、SRTP 暗号化セッションを使用する場合もあります。
   - K8 ライセンスでは、SRTP セッション数は 250 までに制限されます。
   - K9 ライセンスに制限はありません。

   （注）メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。
2. 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシ セッションの最大数は 5000 です。

ライセンスの詳細については、一般的な操作のコンフィギュレーション ガイドの Chapter 3, “Managing Feature Licenses for Cisco ASA Version 9.1,” を参照してください。

SIP フェデレーション用の Cisco Unified Presence Proxy の設定

ここでは、次の内容について説明します。

SIP フェデレーション用の Cisco Unified Presence Federation Proxy の設定のタスク フロー

ローカル ドメイン内にある単一の Cisco UP を含み Cisco UP と ASA の間で自己署名した証明書を使用する（図 19-1 のシナリオを参照）ASA を TLS プロキシとして使用する Cisco Unified Presence/LCS フェデレーション シナリオを設定するには、次のタスクを実行します。

ASDM を使用して Cisco Unified Presence プロキシを設定するには、メニューから [Wizards] > [Unified Communication Wizard] を選択します。Unified Communications Wizard が開きます。最初のページから、[Business-to-Business] セクションで [Cisco Unified Presence Proxy] オプションを選択します。

このウィザードにより、必要な TLS プロキシが自動的に作成されます。その後、ウィザードの指示に従って Unified Presence プロキシ インスタンスを作成し、必要な証明書のインポートとインストールを行います。最後に、プレゼンス フェデレーション トラフィックの SIP および SCCP インスペクションが自動的にイネーブルになります。

このウィザードでは、次の 4 つのステップでプレゼンス フェデレーション プロキシを作成します。

ステップ 1　[Presence Federation Proxy] オプションを選択します。

ステップ 2　プロキシ トポロジを定義するための設定（たとえばプレゼンス フェデレーション サーバの IP アドレス）を指定します。

ステップ 3　ローカル側の証明書管理、つまりローカルの Unified Presence Federation サーバと ASA 間で交換される証明書を設定します。

ステップ 4　リモート側の証明書管理を設定します。つまり、リモート サーバと ASA の間で交換される証明書を設定します。

ウィザードの完了時に、プレゼンス フェデレーションに対して作成される設定の要約が表示されます。詳細については、このマニュアル内の Unified Communications Wizard に関するセクションを参照してください。

Cisco Unified Presence の機能履歴

表 19-1 に、この機能のリリース履歴を示します。

表 19-1　Cisco Unified Presence の機能履歴

機能名	リリース	機能情報
Cisco Presence Federation Proxy	8.0(4)	Cisco Unified Presence プロキシ機能が導入されました。
Cisco Presence Federation Proxy	8.3(1)	Unified Communications Wizard が ASDM に追加されました。このウィザードを使用することにより、Cisco Presence Federation Proxy を設定できます。 XMPP フェデレーションのサポートが導入されました。