Cisco Unified Communication Wizard の使用

この章では、Cisco Unified Communications プロキシ機能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について説明します。

この章は、次の項で構成されています。

Cisco Unified Communication Wizard に関する情報

（注） Unified Communication Wizard は、ASA バージョン 8.3(1) 以降でサポートされています。

Unified Communication Wizard は、ASA 上で次のような Unified Communications プロキシを設定する場合に役立ちます。

- Cisco 電話プロキシ

  「Unified Communication Wizard を使用した電話プロキシの設定」（P.15-5）を参照してください。

- Cisco Mobility Advantage Proxy

  「Unified Communication Wizard を使用した Mobility Advantage の設定」（P.15-12）を参照してください。

- Cisco Presence Federation Proxy

  「Unified Communication Wizard を使用したプレゼンス フェデレーション プロキシの設定」（P.15-14）を参照してください。

- Cisco Intercompany Media Engine Proxy

「Unified Communication Wizard を使用した UC-IME の設定」（P.15-17）を参照してください。

このウィザードにより、Unified Communications プロキシの設定は次のように簡略化されます。

- ウィザードの手順の中で必要なデータをすべて入力します。Unified Communications プロキシを設定するために ASDM の画面をあちこち移動する必要はありません。
- Unified Communications プロキシのコンフィギュレーション設定は、このウィザードによって可能な限り自動生成されるようになり、設定者がデータを入力する必要がなくなります。ウィザードによって設定される内容には、必要なアクセス リスト、IP アドレス変換（NAT および PAT）文、自己署名証明書、TLS プロキシ、アプリケーション インスペクションなどがあります。
- ウィザードにはデータの収集を示すネットワーク図が表示されます。

Unified Communication Wizard にアクセスするには、メイン ASDM アプリケーション ウィンドウで、次のいずれかのパスを選択します。

- [Wizards] > [Unified Communication Wizard] を選択します。
- [Configuration] > [Firewall] > [Unified Communications] を選択して、[Unified Communication Wizard] をクリックします。

電話プロキシ：シスコ暗号化エンドポイントのセキュアなリモート アクセスと Cisco SoftPhone の VLAN トラバーサル

電話プロキシ機能は、セキュアなリモート アクセスのために Cisco Secure Real-time Transport Protocol（SRTP）および Transport Layer Security（TLS）暗号化エンドポイントの終端をイネーブルにします。電話プロキシを使用すると、大規模な VPN リモート アクセス ハードウェア構成を使用することなく、セキュアな電話を大規模に展開できます。エンドユーザのインフラストラクチャは、VPN トンネルまたはハードウェアを使用しない、単なる IP エンドポイントに制限されます。

Cisco 適応型セキュリティ アプライアンスの電話プロキシは、Cisco Unified Phone Proxy の代わりになる製品です。また、電話プロキシを、ソフトフォン アプリケーションの音声およびデータ VLAN トラバーサルに対して展開できます。Cisco IP Communicator（CIPC）トラフィック（メディアとシグナリングの両方）は、ASA を通じてプロキシで処理できるため、コールは音声 VLAN とデータ VLAN 間を安全に通過できます。

TLS プロキシと電話プロキシの違いについては、次の URL で Unified Communications に関するコンテンツ（ホワイト ペーパーの『TLS Proxy vs Phone Proxy』など）を参照してください。ホワイト ペーパーもあります。

http://www.cisco.com/go/secureuc

Mobility Advantage Proxy：Cisco Mobility Advantage サーバと Cisco Unified Mobile Communicator クライアント間のセキュアな接続

Cisco Mobility Advantage ソリューションには、企業向け通信アプリケーションとサービスを携帯電話に拡張する、モバイル ハンドセット用の使いやすいソフトウェア アプリケーションである Cisco Unified Mobile Communicator（Cisco UMC）と Cisco Unified Mobility Advantage（Cisco UMA）サーバが含まれています。Cisco Mobility Advantage ソリューションは通信のエクスペリエンスを効率化し、シングル ナンバー リーチおよびモバイル エンドポイントの Unified Communications インフラストラクチャへの統合を実現します。

セキュリティ アプライアンスはプロキシとして機能し、Cisco UMC と Cisco UMA 間の TLS シグナリングを終端し、再発信します。プロキシ セキュリティ機能の一部として、Cisco UMC と Cisco UMA 間のプロトコルである Cisco UMA Mobile Multiplexing Protocol（MMP）に対するインスペクションがイネーブルになります。

プレゼンス フェデレーション プロキシ：Cisco Unified Presence サーバとシスコまたは Microsoft 社のプレゼンス サーバ間のセキュアな接続

Cisco Unified Presence ソリューションは、ユーザの可用性とステータスに関する情報（ユーザが特定の時間に IP 電話などの通信デバイスを使用しているかどうかなど）を収集します。また、Web コラボレーションやビデオ会議がイネーブルになっているかどうかなど、通信機能に関する情報も収集します。Cisco Unified Presence でキャプチャされたユーザ情報を使用すると、Cisco Unified Personal Communicator や Cisco UCM などのアプリケーションで、ユーザは最も効率のよい協調的な通信方法を確認して同僚との接続を効率化できるので、生産性が向上します。

ASA をセキュア プレゼンス フェデレーション プロキシとして使用すると、企業は Cisco Unified Presence（Cisco UP）サーバをシスコまたは Microsoft 社の他のプレゼンス サーバに安全に接続し、企業間通信をイネーブルにできます。セキュリティ アプライアンスは、サーバ間の TLS 接続を終端し、サーバ間の SIP 通信に対するポリシーを検査および適用できます。

Cisco Intercompany Media Engine Proxy：異なる企業内の Cisco UCM サーバ間での IP フォン トラフィック用のセキュアな接続

統合された通信が多くの企業内で展開されるにつれ、企業間コールの両側で統合された通信が使用され、その間に Public Switched Network（PSTN）が存在するケースが一般的になりつつあります。すべての外部コールが回線を介して電話のプロバイダーに到達し、そこからすべての外部の宛先に配信されます。

Cisco Intercompany Media Engine（UC-IME）は、ビジネス間にダイナミックで、暗号化された VoIP 接続を徐々に作成します。それにより、連携する企業の集合は、それらの間にセキュアな VoIP 相互接続を持つ 1 つの巨大なビジネスと見なすことが最終的にできるようになります。

企業内での Cisco Intercompany Media Engine 配置には、Cisco Intercompany Media Engine サーバ、コール エージェント（Cisco Unified Communications Manager）、および Cisco Intercompany Media Engine Proxy を稼働している ASA からなる 3 つのコンポーネントがあります。

ASA は、企業間のシグナリング接続を暗号化し、不正なコールを防ぐことにより、境界セキュリティを提供します。Cisco Intercompany Media Engine Proxy を稼働している ASA は、インターネット ファイアウォールとして配置することも、Cisco Intercompany Media Engine Proxy として DMZ（通常のインターネット トラフィックのパス外）に配置することもできます。

Unified Communication Wizard のライセンス要件

ASDM で Unified Communication Wizard を実行するには、次のライセンスが必要です。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ただし、ウィザードで作成された Unified Communications プロキシ機能のそれぞれを実行するには、適切な Unified Communications Proxy のライセンスが必要です。

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

- Cisco 電話プロキシ
- 暗号化音声インスペクションの TLS プロキシ
- プレゼンス フェデレーション プロキシ
- Cisco Intercompany Media Engine Proxy

詳細については、「Cisco Unified Communications プロキシ機能のライセンス」（P.14-4）を参照してください。

（注）　Cisco Intercompany Media Engine Proxy は、このプロキシに必要なライセンスが ASA にインストールされていなければ、Unified Communication Wizard にオプションとして表示されません。

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 アドレスをサポートしています。

その他のガイドラインと制限事項

Unified Communication Wizard を使用した Unified Communications プロキシの作成には、次の制限および要件があります。

- ASA 上に少なくとも 2 つのインターフェイスを設定し、UC Wizard を使用して Unified Communications プロキシを設定する必要があります。
- すべての Unified Communications プロキシを正しく機能させるには、ASA および各プロキシに関連付けられたすべてのサーバ（Cisco Unified Communication Manager サーバ、Cisco Mobility Advantage サーバ、Cisco Unified Presence サーバ、Cisco Intercompany Media Engine サーバなど）上の時計を同期する必要があります。
- Cisco Intercompany Media Engine Proxy をパス外配置に設定する場合は、Cisco Unified Communications Manager サーバのパブリック IP アドレスとポートおよびメディア ターミネーション アドレス用のパブリック IP アドレスが、インターネットからアクセス可能になっている必要があります。Unified Communication Wizard のサマリー ページに要件が記載されています。
- Cisco Mobility Advantage Proxy および Cisco Presence Federation Proxy を設定する ASA が別のファイアウォールの背後に配置されている場合は、Cisco Mobility Advantage サーバおよび Cisco Unified Presence サーバのパブリック IP アドレスが、インターネットからアクセス可能になっている必要があります。
- Unified Communication Wizard を使用してプレゼンス フェデレーション プロキシおよび Cisco Intercompany Media Engine Proxy を作成する場合は、各プロキシにウィザードが自動的に作成したアクセス リストの設定を調整する必要がある場合があります。各プロキシに必要なアクセス リスト要件の詳細については、第 19 章「Cisco Unified Presence の設定」および第 20 章「Cisco Intercompany Media Engine Proxy の設定」をそれぞれ参照してください。

Unified Communication Wizard を使用した電話プロキシの設定

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、[Remote Access] セクションの下にある [Phone 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 Phone Proxy 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、Phone Proxy 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。

（注）　正しく同期を取るには、ウィザードで作成された設定はウィザードで管理する必要があります。たとえば、UC ウィザードを使用して電話プロキシ設定を作成し、この設定をウィザード以外で変更した場合、残りのウィザード設定は更新されず、ウィザード設定は同期化されません。

したがって、ウィザード以外で電話プロキシ設定の一部を変更する場合は、変更者の責任において残りの設定の同期を取ってください。

このウィザードでは、次の 4 つの手順を実行して電話プロキシを設定します。

ステップ 1　電話プロキシ オプションを選択します。

ステップ 2　Cisco Unified Communications Manager（UCM）サーバと TFTP サーバを定義する設定（各サーバの IP アドレスとアドレス変換設定など）および Cisco UCM クラスタのセキュリティ モードを指定します。「電話プロキシのプライベート ネットワークの設定」（P.15-5）および「電話プロキシのサーバの設定」（P.15-6）を参照してください。

ステップ 3　必要に応じて、Certificate Authority Proxy Function（CAPF）をイネーブルにします。「IP 電話に対する Certificate Authority Proxy Function（CAPF）のイネーブル化」（P.15-9）を参照してください。

ステップ 4　リモート IP 電話のアドレス変換設定、IP 電話のサービス設定をイネーブルにするかどうか、IP 電話が使用する HTTP プロキシなど、パブリック IP フォン ネットワークの設定を行います。「パブリック IP 電話ネットワークの設定」（P.15-10）

ステップ 5　Cisco UCM のメディア ターミネーション アドレス設定を指定します。「Unified Communication プロキシのメディア ターミネーション アドレスの設定」（P.15-11）。

このウィザードは、電話プロキシに対して作成される設定の概要を表示して完了します。

電話プロキシのプライベート ネットワークの設定

このページで指定する値によって、必要なアドレス変換設定とアクセス コントロール リスト エントリが作成され、ASA から Cisco UCM および TFTP サーバへの接続が設定されます。

また、Cisco UCM クラスタのセキュリティ モードも指定します。ノンセキュア クラスタ モードや、電話がノンセキュア モードに設定された混合モードの場合、電話プロキシは次のように動作します。

- 電話からの TLS 接続は ASA で終端され、Cisco UCM への TCP 接続が開始されます。
- 外部の IP フォンから内部ネットワークの IP フォンに ASA 経由で送信される SRTP は、Real-time Transport Protocol（RTP）に変換されます。

内部の IP 電話が認証モードに設定された混合モード クラスタの場合、TLS 接続は Cisco UCM への TCP に変換されませんが、SRTP は RTP に変換されます。

内部の IP フォンが暗号化モードに設定された混合モード クラスタの場合、TLS 接続は TLS のまま Cisco UCM に接続され、リモート電話からの SRTP は SRTP のまま内部の IP フォンに伝送されます。

ステップ 1　[Interface] ドロップダウン リストから、ASA が Cisco UCM サーバおよび TFTP サーバからの接続をリッスンするインターフェイスを選択します。Cisco UCM サーバと TFTP サーバが同じインターフェイス上に存在する必要があります。

ステップ 2　IP 電話が信頼する必要があるネットワーク内の各エンティティ（すべての Cisco UCM および TFTP サーバ）を指定します。[Add] をクリックして、サーバを追加します。「電話プロキシのサーバの設定」（P.15-6）を参照してください。

すでにコンフィギュレーションに追加されているサーバの設定を変更するには、テーブルでサーバを選択して [Edit] をクリックします。[Edit Server] ダイアログが表示されます。「電話プロキシのサーバの設定」（P.15-6）を参照してください。電話プロキシには少なくとも 1 つの Cisco UCM および少なくとも 1 つの TFTP サーバを設定する必要があります。

ステップ 3　[Unified CM Cluster Mode] フィールドで、次のいずれかのオプションをクリックして、Cisco UCM クラスタのセキュリティ モードを指定します。

- [Non-secure]：電話プロキシ機能の設定時に非セキュア モードになるクラスタを指定します。
- [Mixed]：電話プロキシ機能の設定時に混合モードになるクラスタを指定します。

  [Mixed] セキュリティ モードを選択した場合は、[Generate and Export LDC Certificate] ボタンが使用できるようになります。

ステップ 4　[Mixed] セキュリティ モードの場合のみ、次の手順を実行して、IP 電話のローカル ダイナミック証明書（LDC）を設定します。

a. [Generate and Export LDC Certificate] ボタンをクリックします。

「Enrollment succeeded」というダイアログボックスが表示され、LDC が生成されたことが示されます。

b. [OK] をクリックして、[Enrollment Status] ダイアログボックスを閉じます。[Export Certificate] ダイアログボックスが表示されます。

c. [Export to File] フィールドで、LDC のファイル名およびパスを入力するか、または [Browse] をクリックして既存のファイルを見つけて選択します。

d. [Export Certificate] ボタンをクリックします。ファイルが正常にエクスポートされたことを示すダイアログボックスが表示されます。

e. [OK] をクリックして、ダイアログボックスを閉じます。Cisco UCM に LDC をインストールするよう通知するダイアログボックスが表示されます。

f. [OK] をクリックして、ダイアログボックスを閉じます。

設定が完了すると、ASA はこの動的に作成された一意な証明書を IP 電話に代わって Cisco UCM に提示します。

ステップ 5　[Next] をクリックします。

電話プロキシのサーバの設定

このページで指定する値によって、各サーバのアドレス変換設定、アクセス リスト エントリ、トラストポイント、および対応する CTL ファイル エントリが生成されます。

IP 電話が信頼する必要があるネットワーク内のエンティティごとに、サーバを追加する必要があります。これらのサーバには、クラスタ内のすべての Cisco UCM サーバおよびすべての TFTP サーバがあります。

電話プロキシには少なくとも 1 つの TFTP サーバおよび少なくとも 1 つの Cisco UCM サーバを追加する必要があります。電話プロキシに対して最大 5 つの TFTP サーバを設定できます。TFTP サーバは、信頼ネットワーク上のファイアウォールの背後に存在すると想定されます。そのため、電話プロキシは IP 電話と TFTP サーバの間の要求を代行受信します。

（注） ウィザードの手順 2 で [Server] リストから、TFTP サーバを削除すると、ASDM はコンフィグレーションから TFTP サーバの IP アドレスだけを削除し、TFTP サーバに接続されたすべてのアクセス リスト、NAT ステートメント、オブジェクト グループなどはコンフィグレーションから削除されません。これらの接続されたコンフィグレーション ステートメントを削除するには、ASDM 内の適切な領域を使用して手動で削除するか、または Unified Communications ウィザードを変更せずに再実行し、コンフィギュレーションを適用して、これらのステートメントを削除します。

IP 電話が信頼する必要があるサーバは、次のいずれかの方法でネットワークに配置できます。

- Cisco UCM サーバが必要とするすべてのサービス（つまり、Cisco UCM、TFTP、および CAPF サービス）は、1 つのサーバ上で実行されます。この配置では、各サービスのインスタンスが 1 つだけ存在します。この配置の場合は、サーバ タイプとして [Unified CM+ TFTP] を選択できます。アドレス変換には [Address only] または [Address and ports] を使用できます。セキュリティを強化するために、[Address and ports] を指定することを推奨します。
- 大規模な企業への配置では、冗長化された Cisco UCM や、TFTP と CAPF サービスの専用サーバを使用する場合があります。このような配置では、音声のアドレス変換には [Address only] を使用し、TFTP には [Address only] または [Address and ports] を使用します。

表 15-1 に、アドレスとポートの変換用にデフォルトで設定されているポートを示します。

表 15-1　ポート設定

アドレス	デフォルト ポート	説明
TFTP サーバ	69	TFTP の着信を許可する
Cisco UCM	2000	ノンセキュア SCCP の着信を許可する
Cisco UCM	2443	セキュア SCCP の着信を許可する
Cisco UCM	5061	セキュア SIP の着信を許可する

ステップ 1　[Server Type] フィールドで、ドロップダウン リストからサーバを選択します（[Unified CM]、[TFTP]、または [Unified CM + TFTP]）。Cisco UCM および TFTP サーバが同じデバイス上に存在する場合は、[Unified CM + TFTP] を選択します。

（注） 選択するサーバのタイプ（[Unified CM] または [TFTP]）に応じて、このダイアログボックスの必要なフィールドのみが使用できるようになります。具体的には、サーバ タイプが [Unified CM] の場合、ダイアログの [TFTP] セクションは使用できません。サーバ タイプが [TFTP] の場合は [Voice] セクションが使用できません。

ステップ 2　[Private Address] フィールドで、サーバの実際の内部 IP アドレスを指定します。

ステップ 3　[FQDN] フィールドで、サーバの完全修飾ドメイン名を入力します。この名前には、`ucm.cisco.com` などのようにホスト名とドメイン名が含まれます（ここで、`ucm` はホスト名、`cisco.com` はドメイン名です）。

Unified CM サーバを設定している場合は、Cisco UCM に設定した完全修飾ドメイン名を入力します。

TFTP サーバを設定している場合は、そのサーバが FQDN を使用して設定されていれば TFTP サーバの完全修飾ドメイン名のみを指定します。TFTP サーバが FQDN を使用して設定されていない場合は、フィールドを空白のままにしておくことができます。

（注） 完全修飾ドメイン名を入力すると、ASA に DNS ルックアップが設定されていない場合や、設定された DNS サーバが使用できない場合に ASA でホスト名解決を実行できます。**dns domain-lookup** コマンドの詳細については、コマンド リファレンスを参照してください。

ステップ 4　[Address Translation] セクションで、インターフェイス IP アドレスを使用するか、または別の IP アドレスを入力するかを選択します。

[Use interface IP] オプション ボタンを選択すると、パブリック インターフェイスの IP アドレスを使用するようにサーバが設定されます。電話プロキシのパブリック ネットワークを設定する場合は、ウィザードのステップ 4 でパブリック インターフェイスを選択します。

[Use interface IP] オプション ボタンを選択した場合は、[Voice] と [TFTP] のセクションでポート変換設定を指定する必要があります。アドレスのみの変換を使用できるのは、パブリック インターフェイスの IP アドレス以外の IP アドレスを指定した場合のみです。

[Address only] オプション ボタンを選択すると、ASA はサーバと IP 電話間のすべてのトラフィックに対してアドレス変換を実行します。[Address and ports] オプション ボタンを選択すると、アドレス変換は指定されたポートに制限されます。

ステップ 5　（Unified CM または Unified CM + TFTP サーバのみ）[Voice] セクションで、次のフィールドに入力して SIP または SCCP プロトコル トラフィック、あるいは SIP および SCCP プロトコル トラフィックの両方のインスペクションを設定します。

a. [Translation Type] フィールドで、[Address only] を使用するか [Address and ports] を使用するかを指定します。

冗長化された Cisco UCM サーバや、TFTP と CAPF サービスの専用サーバが配置に含まれる場合は、音声のアドレス変換に [Address only] を選択します。

指定したポートにアドレス変換を制限する場合は、[Address and ports] オプションを選択します。

b. [Voice Protocols] フィールドで、企業に配置された IP 電話でサポートされるインスペクション プロトコルを選択します。選択したインスペクション プロトコル（[SCCP]、[SIP]、または [SCCP and SIP]）に応じて、選択した音声プロトコルのポート フィールドのみが使用できるようになります。

c. [Port Translation] セクションで、音声プロトコルのプライベート ポートおよびパブリック ポートを入力します。

音声ポートのデフォルト値はテキストのフィールドに表示されます。Cisco UCM の設定に一致するように、必要に応じてプライベート ポートを変更します。パブリック ポートに設定した値は、ASA を通過して Cisco UCM と通信するために IP 電話で使用されます。

セキュア SCCP のプライベート ポートとパブリック ポートは自動的に設定されます。これらのポート番号は、ノンセキュアのポート番号に 443 を加えた値に自動的に設定されます。

ステップ 6　（TFTP または Unified CM + TFTP サーバのみ）[TFTP] セクションで、アドレス変換に [Address only] または [Address and port] のいずれかを選択できます。セキュリティを強化するために、[Address and port] を指定することを推奨します。[Address and port] を指定すると、ポート 69 で TFTP 要求をリッスンするように TFTP サーバが設定されます。

サーバ タイプが [Unified CM + TFTP] の場合、ウィザードでは [Voice] および [TFTP] に同じタイプのアドレス変換が設定されます。たとえば、サーバ タイプが [Unified CM + TFTP] で [Address only] オプションが選択されている場合は、ウィザードによって、サーバとの間のすべてのトラフィックに対してグローバル アドレス変換ルールが作成されます。この場合は、TFTP サーバのポート変換を設定すると冗長になります。

ステップ 7　[OK] をクリックして、電話プロキシ設定にサーバを追加し、ウィザードのステップ 2 に戻ります。

IP 電話に対する Certificate Authority Proxy Function（CAPF）のイネーブル化

TLS ハンドシェイクによるリモート IP 電話の認証の代わりに、ローカルで有効な証明書（LSC）のプロビジョニングによる認証を設定できます。LSC プロビジョニングでは、リモート IP フォン ユーザごとにパスワードを作成し、各ユーザはリモート IP 電話でパスワードを入力して LSC を取得します。

リモート IP 電話の認証に LSC プロビジョニングを使用するには、IP 電話をまずノンセキュア モードで登録する必要があります。このため、IP 電話をエンドユーザに渡す前に、企業ネットワーク内で LSC プロビジョニングを実行することを推奨します。そうしない場合、IP 電話をノンセキュア モードで登録するには、SIP および SCCP 用のノンセキュア シグナリング ポートを ASA 上で管理者が開く必要があります。

認証局プロキシ関数（Certificate Authority Proxy Function）を使用した、ローカルで有効な証明書（LSC）のインストールについては、『Cisco Unified Communications Manager Security Guide』も参照してください。

ネットワークに Cisco IP Communicators（CIPC）が含まれている場合や、LSC 対応の IP 電話がある場合は、Cisco UCM から CAPF 証明書をインポートする必要があります。この証明書を使用して、IP 電話に LSC が生成されます。

Cisco UCM に CAPF 証明書が複数ある場合は、それらのすべてを ASA にインポートする必要があります。ただし、ウィザードでは 1 つの CAPF 証明書の設定のみをサポートします。この証明書がデフォルトになります。複数の CAPF 証明書をインポートするには、[Configuration] > [Device Management] > [Certificate Management] > [Identity Certificates] に移動してください。

LSC プロビジョニングを設定すると、エンドユーザ認証を追加できます。詳細については、Cisco Unified Communications Manager のコンフィギュレーション ガイドを参照してください。

ステップ 1　[Enable Certificate Authority Proxy Function] チェックボックスをオンにします。ページ内の残りのフィールドが使用可能になります。

ステップ 2　LSC プロバイダーのプライベート IP アドレスを入力します。

ステップ 3　[Public Address] フィールドで、ASA のパブリック インターフェイスの IP アドレスを使用するか、IP アドレスを入力するかを指定します。

LSC プロバイダーのプライベート IP アドレスおよびパブリック IP アドレスを指定すると、LSC プロビジョニングの CAPF ポートを開いて IP 電話から Cisco UCM への接続を許可するアクセス リスト エントリが作成されます。

ステップ 4　[Translation Type] フィールドで、[Address only] または [Address and ports] オプション ボタンを選択します。

IP 電話は Cisco UCM 上の CAPF サービスに接続する必要があります。CAPF 用に選択するアドレス変換のタイプ（[Address only] と [Address and ports]）は、CAPF サービスが実行されている Cisco UCM のアドレス変換タイプと一致する必要があります。この Cisco UCM サーバのアドレス変換タイプは、このウィザードの前のステップで設定します（「電話プロキシのサーバの設定」（P.15-6）を参照）。

デフォルトでは、CAPF サービスはポート 3804 を使用します。Cisco UCM 上でこのデフォルト値を変更した場合にのみ、値を変更します。

ステップ 5　[Address and ports] オプション ボタンを選択した場合は、CAPF サービスのプライベート ポートおよびパブリック ポートを入力します。

ステップ 6　[Install CAPF Certificate] ボタンをクリックします。[Install Certificate] ダイアログボックスが表示されます。「証明書のインストール」（P.15-25）を参照してください。

ステップ 7　[Next] をクリックします。

パブリック IP 電話ネットワークの設定

このページで指定する値によって、IP フォンで使用するアドレス変換ルールが生成され、IP フォンの設定を ASA で処理する方法が設定されます。

ステップ 1　[Interface] ドロップダウン リストから、ASA が IP 電話からの接続をリッスンするインターフェイスを選択します。

ステップ 2　IP 電話上に Call Manager コンフィギュレーションを維持するには、[Preserve the Unified CM's configuration on the phone's service] チェックボックスをオンにします。このチェックボックスをオフにすると、次のサービス設定が IP 電話でディセーブルになります。

- Web Access
- PC Port
- Voice VLAN Access
- Gratuitous ARP
- Span to PC Port

ステップ 3　IP 電話のアドレス変換を設定するには、[Enable address translation for IP phones] チェックボックスをオンにします。（ウィザードのステップ 2 で選択した）ASA のプライベート インターフェイスの IP アドレスを使用するか、IP アドレスを入力するかを選択します。

IP フォンのアドレス変換を設定すると、IP フォンで使用するアドレスが設定されます。外部ネットワークからのすべてのトラフィックは 1 つの送信元 IP アドレスに収束します。このため、ネットワーク内に企業ファイアウォールがもう 1 つある場合でも、この IP アドレスのピンホールを開くだけで済み、すべてのトラフィックのピンホールを開く必要はありません。

ステップ 4　<proxyServerURL> タグの下の IP フォンのコンフィグレーション ファイルに書き込まれる Phone Proxy 機能の HTTP プロキシを設定するには、以下を実行します。

a.　[Configure an HTTP proxy to redirect phone URLs...] チェックボックスをオンにします。

b.　[IP Address] フィールドに、HTTP プロキシの IP アドレスを入力します。

c.　[Port] フィールドに、HTTP プロキシのリスニング ポートを入力します。

入力する IP アドレスは、IP フォンと HTTP プロキシが存在している場所に基づいたグローバル IP アドレスにします。[IP Address] フィールドにホスト名を入力できるのは、適応型セキュリティ アプライアンスがホスト名を IP アドレスに解決できる場合（DNS ルックアップが設定されている場合など）ですが、これは適応型セキュリティ アプライアンスによってホスト名が IP アドレスに解決されるからです。ポートが指定されていない場合、デフォルトで 8080 になります。

d.　[Interface] フィールドで、適応型セキュリティ アプライアンス上の、HTTP プロキシが常駐しているインターフェイスを選択します。

電話プロキシのプロキシ サーバ コンフィギュレーション オプションを設定すると、DMZ または外部ネットワークで HTTP プロキシを使用できます。これらのネットワークでは、電話機上のサービスについてすべての IP フォンの URL がこのプロキシ サーバに誘導されます。この設定では、非セキュアな HTTP トラフィックに対応します。このようなトラフィックは社内ネットワークに入ることはできません。

ステップ 5　[Next] をクリックします。

Unified Communication プロキシのメディア ターミネーション アドレスの設定

このステップからのデータによって、電話プロキシおよび UC-IME プロキシに MTA インスタンスが追加されます。

電話プロキシおよび UC-IME プロキシでは、Secure RTP（SRTP）と RTP のトラフィックにメディア ターミネーション アドレスを使用します。外部の IP フォンから内部ネットワークの IP フォンに ASA 経由で送信される SRTP トラフィックは、RTP トラフィックに変換されます。このトラフィックは適応型セキュリティ アプライアンスで終端されます。SRTP は、音声やビデオなどの Internet Media トラフィックに対し、メッセージ認証とリプレイ保護を提供します。RTP では、インターネット経由で音声とビデオを配信するための標準化されたパケット形式が定義されます。

UC-IME プロキシおよび電話プロキシが完全に機能するには、メディア ターミネーション アドレス（MTA）のパブリック IP アドレスがインターネットからアクセス可能であるようにする必要があります。Unified Communication Wizard の概要ページにこの要件が表示されます。

指定する MTA IP アドレスは、特定の要件を満たす必要があります。詳細については、「メディア ターミネーション インスタンスの前提条件」（P.16-7）を参照してください。

ステップ 1　プライベート IP アドレス用のフィールドに、プライベート メディア トラフィックが終端する IP アドレスを入力します。この IP アドレスは、プライベート インターフェイス IP アドレスと同じサブネット内になければなりません 正しいサブネット範囲は、プライベート IP アドレスのフィールドの右側に表示されます。

ステップ 2　パブリック IP アドレス用のフィールドに、パブリック メディア トラフィックが終端する IP アドレスを入力します。この IP アドレスは、パブリック インターフェイス IP アドレスと同じサブネット内になければなりません。正しいサブネット範囲は、パブリック IP アドレスのフィールドの右側に表示されます。

ステップ 3　メディア停止インスタンスの RTP ポート範囲の最小および最大値を指定します。

ポート値は 1024 ～ 65535 の範囲である必要があります。

ステップ 4　[Next] をクリックします。

このウィザードは、プロキシに対して作成される設定の概要を表示して完了します。

Unified Communication Wizard を使用した Mobility Advantage の設定

（注）　Unified Communication Wizard は、ASA バージョン 8.3(1) 以降でサポートされています。

Unified Communication Wizard では、Mobility Advantage Proxy を設定するための手順を示します。メニューから [Wizards] > [Unified Communication Wizard] を選択します。Unified Communications Wizard が開きます。[Remote Access] セクションの下にある [Cisco Mobility Advantage Proxy] オプション ボタンをクリックします。

ウィザードを使用して Mobility Advantage プロキシを作成すると、ASDM では必要な TLS プロキシの自動作成、Mobility Advantage トラフィックの MMP インスペクションのイネーブル化、アドレス変換（NAT）文の生成、および Cisco Mobility Advantage サーバとモビリティ クライアント間のトラフィックを許可するために必要なアクセス ルールの作成を行います。

次の手順では、Mobility Advantage Proxy の設定の概要について説明します。

ステップ 1　パブリック ネットワークとプライベート ネットワークのインターフェイス、Cisco Mobility Advantage サーバの IP アドレスなど、プライベート ネットワークとパブリック ネットワークのトポロジを定義する設定を指定します。「Cisco Mobility Advantage Proxy のトポロジの設定」（P.15-12）を参照してください。

ステップ 2　Cisco Mobility Advantage サーバと ASA の間で交換される証明書を設定します。「Cisco Mobility Advantage Proxy のサーバ側証明書の設定」（P.15-13）を参照してください。

ステップ 3　クライアント側の証明書管理を設定します。つまり、Unified Mobile Communicator クライアントと ASA の間で交換される証明書を設定します。「Cisco Mobility Advantage Proxy のクライアント側証明書の設定」（P.15-14）を参照してください。

ウィザードは、Mobility Advantage Proxy に対して作成される設定のサマリーを表示して完了します。

Cisco Mobility Advantage Proxy のトポロジの設定

Mobility Advantage Proxy を設定する場合は、プライベート ネットワークとパブリック ネットワークのインターフェイス、Cisco Mobility Advantage サーバのプライベート IP アドレスやパブリック IP アドレスなど、プライベート ネットワークとパブリック ネットワークのトポロジを定義する設定を指定します。

このページで指定する値によって、Mobility Advantage Proxy の次のコンフィギュレーション設定が生成されます。

- Cisco Mobility Advantage サーバのスタティック PAT
- Cisco Unified Mobile Communicator クライアントのスタティック NAT（[Enable address translation for Mobility clients] チェックボックスがオンになっている場合）
- Cisco Unified Mobile Communicator クライアントの Cisco Mobility Advantage サーバへのアクセスを許可するアクセス リスト

ステップ 1　[Private Network] 領域で、ドロップダウン リストからインターフェイスを選択します。

ステップ 2　[Unified MA Server] 領域に、Cisco Mobility Advantage サーバのプライベート IP アドレスとパブリック IP アドレスを入力します。これらの IP アドレスに対するポートの入力はオプションです。デフォルトではポート番号 5443 が入力されています。この番号は、MMP インスペクションのデフォルト TCP ポートです。

ステップ 3　[FQDN] フィールドに、Cisco Mobility Advantage サーバのドメイン名を入力します。このドメイン名は、このウィザードで後で生成する証明書署名要求に含まれます。

ステップ 4　[Public Network] 領域で、ドロップダウン リストからインターフェイスを選択します。

プロキシでは、このインターフェイスを使用して、Cisco Mobility Advantage サーバのスタティック PAT の設定と、Cisco Unified Mobile Communicator クライアントによる Cisco Mobility Advantage サーバへのアクセスを許可するアクセス リストの設定を行います。

ステップ 5　**Cisco Unified Mobile Communicator クライアントでアドレス変換（NAT）を**使用するかを設定するには、[Enable address translation for Mobility clients] チェックボックスをオンにして、パブリック インターフェイスの IP アドレスを使用するか、IP アドレスを入力するかを選択します。

ステップ 6　[Next] をクリックします。

Cisco Mobility Advantage Proxy のサーバ側証明書の設定

ASA と Cisco UMA サーバの間の信頼関係は、自己署名証明書を使用して確立できます。ASA の ID 証明書はエクスポートされ、Cisco UMA サーバのトラストストアにアップロードされます。Cisco UMA サーバの証明書はダウンロードされ、ASA のトラストストアにアップロードされます。

自己署名証明書の使用はこの手順でのみサポートされます。

ステップ 1　[ASA's Identity Certificate] 領域で、[Generate and Export ASA's Identity Certificate] をクリックします。

登録が成功したことを示すダイアログボックスが表示されます。[Enrollment Status] ダイアログ ボックスで、[OK] をクリックします。[Export Certificate] ダイアログボックスが表示されます。

（注）

- ASA のアイデンティティ証明書がすでに作成されている場合、この領域のボタンは [Export ASA's Identity Certificate] として表示され、[Export Certificate] ダイアログボックスがすぐに表示されます。
- ウィザードを使用して Cisco Mobility Advantage Proxy を設定する場合、ウィザードでは自己署名証明書のインストールだけがサポートされています。

ステップ 2　ASA のウィザードで生成されたアイデンティティ証明書をエクスポートします。「ID 証明書のエクスポート」（P.15-24）を参照してください。

ステップ 3　[Unified MA Server's Certificate] 領域で、[Install Unified MA Server's Certificate] をクリックします。[Install Certificate] ダイアログが表示されます。

ステップ 4　Cisco Mobility Advantage サーバの証明書を含むファイルを検索するか、またはダイアログボックスに証明書の詳細を貼り付けます。「証明書のインストール」（P.15-25）を参照してください。

ステップ 5　[Next] をクリックします。

（注）　このサーバの証明書をエクスポートする方法の詳細については、Cisco Mobility Advantage サーバのマニュアルを参照してください。

Cisco Mobility Advantage Proxy のクライアント側証明書の設定

Cisco Unified Mobile Communicator（UMC）クライアントと ASA の間に信頼関係を確立するために、ASA は Cisco Mobility Advantage サーバの FQDN を使用して設定された CA 署名付き証明書を使用します（証明書偽装とも呼ばれます）。

[Client-Side Certificate Management] ページに、中間 CA 証明書（該当する場合、VeriSign の場合と同様）と ASA の署名付きの ID 証明書の両方を入力します。

（注）　署名付きの ID 証明書が ASA にすでにある場合は、この手順のステップ 1 をスキップしてステップ 2 に直接進むことができます。

ステップ 1　[ASA's Identity Certificate] 領域で、[Generate CSR] をクリックします。[CSR parameters] ダイアログボックスが表示されます。

証明書署名要求（CSR）に対する追加パラメータの指定に関する詳細ついては、「Unified Communications Proxy の証明書署名要求（CSR）の生成」（P.15-25）を参照してください。

ウィザードが ASA に設定を配信し、証明書キー ペア情報が取得されたことを示すダイアログボックスが表示されます。[Identity Certificate Request] ダイアログボックスが表示されます。

生成された CSR の保存と CA への送信に関する詳細については、「ID 証明書要求の保存」（P.15-26）を参照してください。

ステップ 2　[Install ASA's Identity Certificate] をクリックします。証明書をインストールします。「Mobility Advantage サーバへの ASA ID 証明書のインストール」（P.15-27）を参照してください。

ステップ 3　[Install Root CA's Certificate] をクリックします。[Install Certificate] ダイアログボックスが表示されます。証明書をインストールします。「証明書のインストール」（P.15-25）を参照してください。

ステップ 4　[Next] をクリックします。

ウィザードは、Mobility Advantage Proxy に対して作成される設定のサマリーを表示して完了します。

Unified Communication Wizard を使用したプレゼンス フェデレーション プロキシの設定

（注）　Unified Communication Wizard は、ASA バージョン 8.3(1) 以降でサポートされています。

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] の順に選択します。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。

ウィザードを使用して Cisco Presence Federation Proxy を作成すると、ASDM では必要な TLS プロキシの自動作成、Presence Federation トラフィックの SIP インスペクションのイネーブル化、ローカルの Cisco Unified Presence サーバのアドレス変換（スタティック PAT）文の生成、およびローカルの Cisco Unified Presence サーバとリモート サーバ間のトラフィックを許可するためのアクセス リストの作成を行います。

次の手順では、プレゼンス フェデレーション プロキシの設定の概要について説明します。

ステップ 1　Presence Federation サーバのプライベート IP アドレスやパブリック IP アドレスなど、プライベート ネットワークとパブリック ネットワークのトポロジを定義する設定を指定します。「Cisco Presence Federation Proxy のトポロジの設定」（P.15-15）を参照してください。

ステップ 2　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。「Cisco Presence Federation Proxy のローカル側証明書の設定」（P.15-16）を参照してください。

ステップ 3　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。「Cisco Presence Federation Proxy のリモート側証明書の設定」（P.15-16）を参照してください。

ウィザードは、Presence Federation プロキシに対して作成される設定のサマリーを表示して完了します。

Cisco Presence Federation Proxy のトポロジの設定

プレゼンス フェデレーション プロキシを設定する場合は、プライベート ネットワークとパブリック ネットワークのインターフェイス、Cisco Unified Presence サーバのプライベート IP アドレスやパブリック IP アドレスなど、プライベート ネットワークとパブリック ネットワークのトポロジを定義する設定を指定します。

このページで指定する値によって、プレゼンス フェデレーション プロキシの次のコンフィギュレーション設定が生成されます。

- ローカルの Cisco Unified Presence サーバのスタティック PAT
- ローカルの Cisco Unified Presence サーバとリモート サーバ間のトラフィックのアクセス リスト

ステップ 1　[Private Network] 領域で、ドロップダウン リストからインターフェイスを選択します。

ステップ 2　[Unified Presence Server] 領域に、Unified Presence サーバのプライベート IP アドレスとパブリック IP アドレスを入力します。これらの IP アドレスに対するポートの入力はオプションです。デフォルトではポート番号 5061 が入力されています。この番号は、SIP インスペクションのデフォルト TCP ポートです。

ステップ 3　[FQDN] フィールドに、Unified Presence サーバのドメイン名を入力します。このドメイン名は、このウィザードで後で生成する証明書署名要求に含まれます。

ステップ 4　[Public Network] 領域で、ドロップダウン リストからパブリック ネットワークのインターフェイスを選択します。プロキシでは、このインターフェイスを使用して、ローカルの Cisco Unified Presence サーバのスタティック PAT の設定と、リモート サーバによる Cisco Unified Presence サーバへのアクセスを許可するアクセス リストの設定を行います。

ステップ 5　[Next] をクリックします。

Cisco Presence Federation Proxy のローカル側証明書の設定

企業内では、自己署名証明書を使用して信頼関係を設定します。自己署名証明書の使用はこの手順でのみサポートされます。

ステップ 1　[ASA's Identity Certificate] 領域で、[Generate and Export ASA's Identity Certificate] をクリックします。

登録が成功したことを示す情報ダイアログボックスが表示されます。[Enrollment Status] ダイアログボックスで、[OK] をクリックします。[Export Certificate] ダイアログボックスが表示されます。

（注）
- ASA のアイデンティティ証明書がすでに作成されている場合、この領域のボタンは [Export ASA's Identity Certificate] として表示され、[Export Certificate] ダイアログボックスがすぐに表示されます。
- ウィザードを使用して Cisco Presence Federation Proxy を設定する場合、ウィザードでは自己署名証明書のインストールだけがサポートされています。

ステップ 2　ASA のウィザードで生成されたアイデンティティ証明書をエクスポートします。「ID 証明書のエクスポート」（P.15-24）を参照してください。

ステップ 3　[Local Unified Presence Server's Certificate] 領域で、[Install Server's Certificate] をクリックします。[Install Certificate] ダイアログが表示されます。

ステップ 4　Cisco Unified Presence サーバの証明書を含むファイルを検索するか、またはダイアログボックスに証明書の詳細を貼り付けます。「証明書のインストール」（P.15-25）を参照してください。

ステップ 5　[Next] をクリックします。

（注）　このサーバの証明書をエクスポートする方法の詳細については、Cisco Unified Presence サーバのマニュアルを参照してください。

Cisco Presence Federation Proxy のリモート側証明書の設定

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。セキュリティ アプライアンスは、Cisco Unified Presence サーバの FQDN 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（つまり、ローカル エンティティとリモート 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。ローカル エンティティとリモート 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、ローカルとリモートの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。セキュリティ アプライアンスは、企業のいずれかに常に関連付けられています。その企業内では、エンティティとセキュリティ アプライアンスは自己署名証明書を使用して相互に認証を行います。

セキュリティ アプライアンスとリモート エンティティ間で信頼関係を確立するために、セキュリティ アプライアンスはローカル エンティティの Cisco Unified Presence サーバの代わりに CA に登録できます。登録要求で、ローカル エンティティの ID（ドメイン名）が使用されます。

信頼関係を確立するため、セキュリティ アプライアンスは自分が Cisco Unified Presence サーバであるかのように、Cisco Unified Presence サーバの FQDN を使用してサードパーティ CA に登録します。

（注）　署名付きの ID 証明書が ASA にすでにある場合は、この手順のステップ 1 をスキップしてステップ 2 に直接進むことができます。

ステップ 1　[ASA's Identity Certificate] 領域で、[Generate CSR] をクリックします。[CSR Parameters] ダイアログボックスが表示されます。

証明書署名要求（CSR）に対する追加パラメータの指定については、「Unified Communications Proxy の証明書署名要求（CSR）の生成」（P.15-25）を参照してください。

ウィザードが ASA に設定を配信し、証明書キー ペア情報が取得されたことを示すダイアログボックスが表示されます。[Identity Certificate Request] ダイアログボックスが表示されます。

生成された CSR の保存と CA への送信に関する詳細については、「ID 証明書要求の保存」（P.15-26）を参照してください。

ステップ 2　[Install ASA's Identity Certificate] をクリックします。「Presence Federation および Cisco Intercompany Media Engine サーバへの ASA ID 証明書のインストール」（P.15-28）を参照してください。

ステップ 3　[Remote Server's CA's Certificate] をクリックします。[Install Certificate] ダイアログボックスが表示されます。証明書をインストールします。「証明書のインストール」（P.15-25）を参照してください。

（注）　異なる組織では異なる CA を使用している可能性があるため、ASA と通信するリモート エンティティごとにルート CA 証明書をインストールする必要があります。

ステップ 4　[Next] をクリックします。

ウィザードは、Presence Federation プロキシに対して作成される設定のサマリーを表示して完了します。

Unified Communication Wizard を使用した UC-IME の設定

（注）　Unified Communication Wizard は、ASA バージョン 8.3(1) 以降でサポートされています。

ASDM を使用して Cisco Intercompany Media Engine Proxy 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] セクションの下にある [Cisco Intercompany Media Engine Proxy] オプションを選択し、[Next] をクリックします。

（注）　Cisco Intercompany Media Engine Proxy は、このプロキシに必要なライセンスが ASA にインストールされていなければ、Unified Communication Wizard にオプションとして表示されません。

ウィザードを使用して Cisco Intercompany Media Engine Proxy を作成すると、ASDM では必要な TLS プロキシの自動作成、Cisco Intercompany Media Engine トラフィックの SIP インスペクションのイネーブル化、ローカルの Cisco Unified Communications Manager サーバのアドレス変換（スタティック PAT）文の生成、およびローカルの Cisco Unified Communications Manager サーバとリモート サーバ間のトラフィックを許可するためのアクセス リストの作成を行います。

次の手順では、Cisco Intercompany Media Engine Proxy の設定の概要について説明します。

ステップ 1　Cisco Intercompany Media Engine Proxy のトポロジを選択します。つまり、セキュリティ アプライアンスはすべてのインターネット トラフィックが通過するエッジ ファイアウォールなのか、セキュリティ アプライアンスは主要なインターネット トラフィックのパスから外れているのか（パス外配置と呼びます）を選択します。「Cisco Intercompany Media Engine Proxy のトポロジの設定」（P.15-18）を参照してください。

ステップ 2　Cisco UCM IP アドレスなどのプライベート ネットワーク設定とチケット設定を指定します。「Cisco Intercompany Media Engine Proxy のプライベート ネットワーク設定の実行」（P.15-19）を参照してください。

ステップ 3　パブリック ネットワーク設定を指定します。「Cisco Intercompany Media Engine Proxy のパブリック ネットワーク設定の実行」（P.15-21）を参照してください。

ステップ 4　Cisco UMC のメディア ターミネーション アドレス設定を指定します。「Unified Communication プロキシのメディア ターミネーション アドレスの設定」（P.15-11）を参照してください。

ステップ 5　ローカル側の証明書管理を設定します。つまり、ローカルの Cisco Unified Communications Manager サーバとセキュリティ アプライアンスの間で交換される証明書を設定します。「Cisco Intercompany Media Engine Proxy のローカル側証明書の設定」（P.15-22）を参照してください。

ステップ 6　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。この証明書がリモート サーバに提示されることにより、リモート サーバは ASA を信頼できるサーバとして認証できるようになります。「Cisco Intercompany Media Engine Proxy のリモート側証明書の設定」（P.15-23）を参照してください。

このウィザードは、Cisco Intercompany Media Engine に対して作成される設定のサマリーを表示して完了します。

Cisco Intercompany Media Engine Proxy のトポロジの設定

ステップ 1　次のいずれかのオプションをクリックして、ICME 配置のトポロジを選択します。

- [All Internet traffic flows through the ASA] オプション ボタン。このオプションは基本配置とも呼ばれます。
- [This ASA is off the path of the regular Internet traffic]。このオプションはパス外配置とも呼ばれます。

ステップ 2　[Next] をクリックします。

基本配置

基本配置では、Cisco Intercompany Media Engine Proxy は、インターネット ファイアウォールとともにインラインに配置され、すべてのインターネット トラフィックが ASA を経由します。この配置では、単一の Cisco UCM または Cisco UCM クラスタが、Cisco Intercompany Media Engine サーバ（場合によってはバックアップも）とともに企業内の中央に配置されます。単一のインターネット接続が ASA を通過します。これは、Cisco Intercompany Media Engine Proxy でイネーブルにされています。

ASA は企業のエッジに位置し、企業間のダイナミック SIP トランクを作成することにより、SIP シグナリングを検査します。

パス外配置

パス外配置では、インバウンドとアウトバウンドの Cisco Intercompany Media Engine コールは、Cisco Intercompany Media Engine Proxy でイネーブルにされた ASA を通過します。ASA は DMZ にあり、主に Cisco Intercompany Media Engine をサポートするように設定されています。通常のインターネットに向かうトラフィックは、この ASA を通過しません。

すべてのインバウンド コールのシグナリングは、宛先の Cisco UCM のグローバル IP アドレスが ASA 上に設定されているため、ASA に誘導されます。アウトバウンド コールの場合、着信側はインターネット上の任意の IP アドレスになる可能性があります。そのため、ASA には、インターネット上の着信側のグローバル IP アドレスごとに ASA 上で内部 IP アドレスを動的に提供するマッピング サービスが設定されます。

Cisco UCM は、すべてのアウトバウンド コールを、インターネット上の着信側のグローバル IP アドレスではなく、ASA 上のマッピング内部 IP アドレスに直接送信します。その後、ASA によって、それらのコールは着信側のグローバル IP アドレスに転送されます。

（注） Cisco Intercompany Media Engine をパス外配置に設定する場合は、Cisco Unified Communications Manager サーバのパブリック IP アドレスとポートおよびメディア ターミネーション アドレス用のパブリック IP アドレスが、インターネットからアクセス可能になっている必要があります。Unified Communication Wizard のサマリー ページに要件が記載されています。

Cisco Intercompany Media Engine Proxy のプライベート ネットワーク設定の実行

Cisco Intercompany Media Engine Proxy を設定する場合は、プライベート ネットワーク インターフェイス、Cisco Unified Communications サーバの IP アドレス、チケットの検証など、プライベート ネットワークのトポロジを定義する設定を指定します。また、Cisco Unified Communications サーバがセキュア モードで動作している場合は、Cisco Intercompany Media Engine Proxy の X.509 サブジェクト名を指定します。

このページで指定する値は、次に示す Cisco Intercompany Media Engine Proxy のコンフィグレーション設定を生成します。

- Cisco Unified Communications サーバのリスト
- Cisco Intercompany Media Engine Proxy で使用されるチケット エポックおよびパスワード
- パス外配置の場合のみ、Cisco Unified Communications サーバと同じインターフェイス上のマッピング サービス

ステップ 1　基本配置の一部として Cisco Intercompany Media Engine Proxy を設定するには、ローカルの Cisco Unified Communications サーバに接続するインターフェイスを選択します。

または

パス外配置の一部として Cisco Intercompany Media Engine Proxy を設定するには、次の手順を実行します。

a. [Listening Interface] ドロップダウン リストから、ASA がマッピング要求をリッスンするインターフェイスを選択します。

b. [Port] フィールドに、ASA がマッピング要求をリスンする TCP ポートとして 1024 ～ 65535 の数値を入力します。このポート番号は、デバイス上の他のサービス（Telnet や SSH など）との競合を避けるために、1024 以上にする必要があります。デフォルトでは、このポート番号は TCP 8060 です。

c. [UC-IME Interface] ドロップダウン リストから、Cisco Intercompany Media Engine Proxy でイネーブルにされたリモート ASA への接続に ASA が使用するインターフェイスを選択します。

（注） 基本配置でもパス外配置でも、すべての Cisco Unified Communications サーバが同じインターフェイス上にある必要があります。

ステップ 2　ウィザードの [Unified CM Servers] 領域には、ASA に設定されたすべての Cisco Unified Communications サーバのプライベート IP アドレス、パブリック IP アドレス、およびセキュリティ モードが表示されます。必要に応じて [Add] をクリックし、Cisco Unified Communications サーバを追加します。Cisco Intercompany Media Engine の SIP トランクがイネーブルになっているクラスタ内の各 Cisco UCM に対してエントリを追加する必要があります。

ステップ 3　[Ticket Epoch] フィールドに、1 ～ 255 の整数を 1 つ入力します。

エポックは、パスワードが変更された回数を表します。プロキシを初めて設定し、パスワードを初めて入力したとき、エポックの整数として 1 を入力します。このパスワードを変更するたびに、エポックを増やして新しいパスワードを示します。パスワードを変更するたびに、エポックの値を増やす必要があります。通常、エポックは連続的に増やします。しかし、セキュリティ アプライアンスでは、エポックを更新するときに任意の値を選択できます。

エポック値を変更すると、現在のパスワードは無効になり、新しいパスワードを入力する必要があります。

ステップ 4　[Ticket Password] フィールドに、US-ASCII 文字セットから印刷可能な文字を 10 文字以上 64 文字以下で入力します。使用可能な文字は 0x21 ～ 0x73 であり、空白文字は除外されます。チケット パスワードはフラッシュ上に保存されます。

（注） 20 文字以上のパスワードを推奨します。パスワードは一度に 1 つしか設定できません。

ASA 上で設定するエポックおよびパスワードは、Cisco Intercompany Media Engine サーバ上で設定されたエポックおよびパスワードと一致する必要があります。詳細については、Cisco Intercompany Media Engine サーバのマニュアルを参照してください。

ステップ 5　[Confirm Password] フィールドにパスワードを再入力します。

ステップ 6　[X.509 Subject Name] フィールドに、ローカルの企業の識別名（DN）を入力します。入力する名前は、クラスタ内の Cisco Unified Communications サーバに設定した名前と一致する必要があります。詳細については、Cisco Unified Communications サーバのマニュアルを参照してください。

ステップ 7　[Next] をクリックします。

UC-IME Proxy 用の Cisco Unified Communications Manager サーバの追加

Cisco Intercompany Media Engine Proxy の SIP トランクがイネーブルになっているクラスタ内の各 Cisco UCM に対してエントリを追加する必要があります。

ステップ 1　Cisco UCM サーバのプライベート IP アドレスおよび（5000 ～ 6000 の範囲で）ポート番号を入力します。

ステップ 2　[Address Translation] 領域に、Cisco UCM サーバのパブリック IP アドレスを入力します。

ステップ 3　必要に応じて、[Translate address and port] オプション ボタンをクリックして [Port] フィールドに（5000 ～ 6000 の範囲で）番号を入力し、パブリック IP アドレスのポート番号を入力します。

ステップ 4　[Security Mode] 領域で、[Secure] または [Non-secure] オプション ボタンをクリックします。Cisco UCM または Cisco UCM クラスタに [secure] を指定すると、Cisco UCM または Cisco UCM クラスタで TLS を開始することが指定されます。

Cisco UCM サーバのいくつかがセキュア モードで動作すると指定した場合は、Unified Communications Wizard に、ASA とその Cisco UCM サーバ間のローカル側通信のための証明書を生成するプロキシ コンフィギュレーションのステップが追加されます。「Cisco Intercompany Media Engine Proxy のローカル側証明書の設定」（P.15-22）を参照してください。

ステップ 5　[OK] をクリックします。

Cisco Intercompany Media Engine Proxy のパブリック ネットワーク設定の実行

パブリック ネットワークの設定は、このウィザードのトポロジに関するステップで選択した導入シナリオによって異なります。具体的には、パス外配置の一部として UC-IME プロキシを設定している場合、ウィザードのこのステップにはアドレス変換に関するフィールドが表示されるので、UC-IME プロキシのプライベート IP アドレスを指定する必要があります。このプライベート IP アドレスを指定すると、着信トラフィックの IP アドレスに変換されます。

パス外配置では、使用環境内に配置済みの既存の ASA は、Cisco Intercompany Media Engine トラフィックを伝送できません。したがって、パス外シグナリングでは、外部アドレスが内部（プライベート）IP アドレスに変換される必要があります。このマッピング サービス設定には、内部インターフェイス アドレスを使用できます。Cisco Intercompany Media Engine Proxy の場合、外部アドレスから内部 IP アドレスへの動的なマッピングが ASA によって作成されます。

このページで指定する値は、次に示す Cisco Intercompany Media Engine Proxy のコンフィグレーション設定を生成します。

- Cisco Unified Communications サーバのスタティック PAT
- ローカル サーバとリモート サーバ間のトラフィックのアクセス リスト

ステップ 1　[Configure public network] 領域で、[Interface] ドロップダウン リストからインターフェイスを選択します。

ステップ 2　パス外配置を設定する場合は、[Address Translation] 領域で、パブリック ネットワークに対してプライベート IP アドレスを使用するかを指定します。

または

[Specify IP address] オプション ボタンをクリックして、フィールドに IP アドレスを入力します。

ステップ 3　[Next] をクリックします。

Cisco Intercompany Media Engine Proxy のローカル側証明書の設定

ウィザードのこのステップを完了すると、ASA の自己署名証明書が生成されます。サーバ プロキシ証明書は、このウィザードの前のステップで指定したサブジェクト名を使用して自動的に生成されます。

自己署名証明書の使用は、ウィザードのみでサポートされています。

ASA と Cisco UMA サーバの間の信頼関係は、自己署名証明書を使用して確立できます。これらの証明書は、TLS ハンドシェイク時にセキュリティ アプライアンスと Cisco UCM が互いをそれぞれ認証するために使用されます。

ASA の ID 証明書はエクスポート後、プロキシを持つクラスタ内の各 Cisco Unified Communications Manager（UCM）サーバにインストールする必要があります。Cisco UCM の各 ID 証明書は、セキュリティ アプライアンスにインストールする必要があります。

Unified Communications Wizard のこのステップが表示されるのは、作成中の UC-IME プロキシに少なくとも 1 つのセキュアな Cisco Unified Communications Manager サーバが定義されている場合のみです。詳細については、「Cisco Intercompany Media Engine Proxy のトポロジの設定」（P.15-18）を参照してください。

ステップ 1　[ASA's Identity Certificate] 領域で、[Generate and Export ASA's Identity Certificate] をクリックします。

登録が成功したことを示すダイアログボックスが表示されます。[Enrollment Status] ダイアログ ボックスで、[OK] をクリックします。[Export Certificate] ダイアログボックスが表示されます。

（注）

- ASA のアイデンティティ証明書がすでに作成されている場合、この領域のボタンは [Export ASA's Identity Certificate] として表示され、[Export Certificate] ダイアログボックスがすぐに表示されます。
- ウィザードを使用して Cisco Intercompany Media Engine Proxy を設定する場合、ウィザードでは自己署名証明書のインストールだけがサポートされています。

ステップ 2　ASA のウィザードで生成されたアイデンティティ証明書をエクスポートします。「ID 証明書のエクスポート」（P.15-24）を参照してください。

ステップ 3　[Local Unified CM's Certificate] 領域で、[Install Local Unified CM's Certificate] をクリックします。[Install Certificate] ダイアログが表示されます。

ステップ 4　Cisco Unified Communications Manager サーバの証明書を含むファイルを検索するか、またはダイアログボックスに証明書の詳細を貼り付けます。「証明書のインストール」（P.15-25）を参照してください。クラスタ内の各 Cisco Unified Communications Manager サーバから証明書をインストールする必要があります。

ステップ 5　[Next] をクリックします。

（注）　このサーバの証明書をエクスポートする方法の詳細については、Cisco Intercompany Media Engine サーバのマニュアルを参照してください。

Cisco Intercompany Media Engine Proxy のリモート側証明書の設定

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 Unified Communications Manager サーバの FQDN 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。その企業内では、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 エンティティ間で信頼関係を確立するために、ASA はローカルの企業の代わりに CA に登録できます。登録要求で、ローカルの Cisco UCM の ID（ドメイン名）が使用されます。

信頼関係を確立するため、ASA は自分が Cisco UCM であるかのように、Cisco Unified Communications Manager サーバの FQDN を使用してサードパーティ CA に登録します。

（注）　署名付きの ID 証明書が ASA にすでにある場合は、この手順のステップ 1 をスキップしてステップ 3 に直接進むことができます。

ステップ 1　[ASA's Identity Certificate] 領域で、[Generate CSR] をクリックします。[CSR Parameters] ダイアログボックスが表示されます。

証明書署名要求（CSR）に対する追加パラメータの指定については、「Unified Communications Proxy の証明書署名要求（CSR）の生成」（P.15-25）を参照してください。

ウィザードが ASA に設定を配信し、証明書キー ペア情報が取得されたことを示すダイアログボックスが表示されます。[Identity Certificate Request] ダイアログボックスが表示されます。

生成された CSR の保存と CA への送信に関する詳細については、「ID 証明書要求の保存」（P.15-26）を参照してください。

ステップ 2　[ASA's Identity Certificate] 領域で、[Install ASA's Identity Certificate] をクリックします。「Presence Federation および Cisco Intercompany Media Engine サーバへの ASA ID 証明書のインストール」（P.15-28）。

ステップ 3　[Remote Server's CA's Certificate] 領域で、[Install Remote Server's CA's Certificate] をクリックします。ASA でリモート サーバが信頼できると判断できるように、リモート サーバの CA のルート証明書をインストールする必要があります。

[Install Certificate] ダイアログボックスが表示されます。証明書をインストールします。「証明書のインストール」（P.15-25）を参照してください。

（注）　ルート証明書をインストールする必要があるのは、ASA の ID 証明書を提供した CA 以外の CA からリモート サーバのルート証明書を受信した場合のみです。

ステップ 4　[Next] をクリックします。

このウィザードは、Cisco Intercompany Media Engine に対して作成される設定のサマリーを表示して完了します。

Unified Communication Wizard での証明書に関する作業

この項では、次のトピックについて取り上げます。

ID 証明書のエクスポート

Cisco Mobility Advantage Proxy、Cisco Presence Federation Proxy、または Cisco Intercompany Media Engine Proxy では、ASA の ID 証明書をエクスポートして、それぞれ Cisco Mobility Advantage サーバ、Cisco Presence Federation サーバ、および Cisco Unified Communications サーバにインストールする必要があります。

自己署名した ID 証明書のエクスポートにはウィザードを使用します。ID 証明書には関連するキーがすべて含まれ、公開キー暗号化標準である PKCS12 形式を取っています。ウィザードを使用して Unified Communications プロキシを設定する場合は、ウィザードのローカル側またはサーバ側証明書管理ステップで [Generate and Export ASA's Identify Certificate] ボタンをクリックします。[Export Certificate] ダイアログボックスが表示されます。

[Export certificate] ダイアログボックスから、次の手順を実行します。

ステップ 1　証明書コンフィギュレーションをエクスポートするときに使用する PKCS12 形式ファイルの名前を入力します。または、[Browse] をクリックして [Export ID Certificate File] ダイアログボックスを表示し、証明書コンフィギュレーションをエクスポートするファイルを探します。

ステップ 2　[Export Certificate] をクリックして、証明書コンフィギュレーションをエクスポートします。

証明書コンフィギュレーション ファイルが指定した場所に正しくエクスポートされたことを示す情報ダイアログボックスが表示されます。

Cisco Mobility Advantage Proxy、Cisco Presence Federation Proxy、または Cisco Intercompany Media Engine Proxy の設定を完了するには、設定するプロキシに応じて Cisco Mobility Advantage サーバ、Cisco Presence Federation サーバ、および Cisco Unified Communications サーバのそれぞれに、生成された ASA の ID 証明書をインポートする必要があります。

それぞれに ID 証明書をインポートする方法の詳細については、これらの各製品のマニュアルを参照してください。

証明書のインストール

電話プロキシ、Cisco Mobility Advantage Proxy、Cisco Presence Federation Proxy、および Cisco Intercompany Media Engine Proxy の証明書を設定する場合は、ASA 上の Cisco Unified Communications Manager サーバ、Cisco Mobility Advantage サーバ、Cisco Presence Federation サーバ、および Cisco Unified Communications Manager サーバからそれぞれ証明書をインストールする必要があります。それぞれから ID 証明書を取得する方法の詳細については、これらの各製品のマニュアルを参照してください。

Cisco 電話プロキシの設定時、LSC プロビジョニングが必要な場合、または LSC 対応の IP 電話がある場合は、ASA 上の Cisco UCM から CAPF 証明書をインストールする必要があります。Cisco UCM に CAPF 証明書が複数ある場合は、それらのすべてを ASA にインポートする必要があります。「IP 電話に対する Certificate Authority Proxy Function（CAPF）のイネーブル化」（P.15-9）を参照してください。

また、Cisco Mobility Advantage Proxy の設定時は、[Install Certificate] ダイアログボックスを使用して、認証局から受信したルート証明書をインストールします。認証局からのルート証明書が他の証明書に署名するために使用されます。ルート証明書は、認証局から受信した署名付きの ID 証明書を認証するために ASA によって使用されます。

（注）　ウィザードを使用して Unified Communications プロキシを設定する場合、ウィザードでは自己署名証明書のインストールだけがサポートされています。

[Install Certificate] ダイアログボックスから、次の手順を実行します。

ステップ 1　次のいずれかの操作を実行します。

- 既存のファイルから証明書コンフィギュレーションを追加するには、[Install from a file] オプション ボタンをクリックします（これがデフォルトの設定です）。パスおよびファイル名を入力するか、または [Browse] をクリックしてファイルを検索します。次に、[Install Certificate] をクリックします。
- 手動で登録するには、[Paste certificate in PEM format] オプション ボタンをクリックします。表示された領域に PEM 形式（base64 または 16 進数値）証明書をコピー アンド ペーストします。

ステップ 2　[Install Certificate] をクリックします。

ASA に証明書が正しくインストールされたことを示す情報ダイアログボックスが表示されます。

Unified Communications Proxy の証明書署名要求（CSR）の生成

Cisco Mobility Advantage Proxy、Cisco Presence Federation Proxy、または Cisco Intercompany Media Engine Proxy の証明書を設定する場合は、ASA の ID 証明書要求を生成する必要があります。

（注）　署名付きの ID 証明書が ASA にすでにある場合は CSR を生成する必要はなく、この証明書の ASA へのインストールに直接進むことができます。アイデンティティ証明書をインストールする手順については、「Mobility Advantage サーバへの ASA ID 証明書のインストール」（P.15-27）および「Presence Federation および Cisco Intercompany Media Engine サーバへの ASA ID 証明書のインストール」（P.15-28）を参照してください。

受信した ID 証明書は、次のような Unified Communication プロキシのそれぞれのエンティティに対して提示されます。

- Cisco Mobility Advantage Proxy の Unified Mobile Communicator クライアント
- Cisco Presence Federation Proxy の Remote Presence Federation サーバ
- Cisco Intercompany Media Engine Proxy のリモート ASA

CSR を生成する前に、追加パラメータを入力できます。

ウィザードを使用して Unified Communications プロキシを設定する場合は、ウィザードのクライアント側またはリモート側証明書管理ステップで [Generate CSR] ボタンをクリックします。[CSR Parameters] ダイアログボックスが表示されます。

[CSR Parameters] ダイアログボックスで、次の手順を実行します。

ステップ 1　[Key Pair Size] ドロップダウン リストから、使用する証明書に必要なサイズを選択します。

選択するキー サイズは、設定するセキュリティのレベルおよび証明書の取得先の CA によって課せられる制限によって決まります。選択する数値を大きくすると、証明書のセキュリティ レベルが高くなります。ほとんどの CA では、キー係数サイズとして 2048 が推奨されます。ただし、GoDaddy では、2048 のキー係数サイズが必要です。

ステップ 2　（Cisco Intercompany Media Engine Proxy のみ）[CN] フィールドに、企業またはネットワークで使用するドメイン名を入力します。Cisco Intercompany Media Engine Proxy に対して設定するサブジェクト DN は、ローカルの Cisco Unified Communications Manager サーバに設定されているドメイン名と一致する必要があります。

（注）　Cisco Mobility Advantage Proxy および Cisco Presence Federation Proxy の場合、ウィザードには一般名（CN）が表示されます。これは、それぞれ Cisco Mobility Advantage サーバまたは Cisco Unified Presence サーバの FQDN です。

ステップ 3　[Additional DN Attributes] フィールドに、属性を入力します。

または

[Select] をクリックして、[Additional DN Attributes] ダイアログボックスを表示します。

a.　[Additional DN Attributes] ダイアログボックスで、ドロップダウン リストから属性を選択します。

b.　属性の値を入力します。

c.　[Add] をクリックします。リストに属性が表示されます。

d.　[OK] をクリックして [CSR Parameters] ダイアログボックスに戻ります。

[CSR Parameters] ダイアログボックスの [Additional DN Attributes] フィールドに、追加した値が表示されます。

ステップ 4　[OK] をクリックします。

ID 証明書要求の保存

いずれかの Unified Communications プロキシの ID 証明書要求の生成に成功すると、[Identity Certificate Request] ダイアログボックスが表示されて、要求を保存するように求められます。

ステップ 1　[Save CSR to File] フィールドに、CSR ファイルの名前とパスを入力します（c:\asa-csr.txt など）。

ステップ 2　[OK] をクリックします。CSR が正常に保存されたことを示す情報ダイアログボックスが表示されます。

ステップ 3　[OK] をクリックして、ダイアログボックスを閉じ、ウィザードに戻ります。

認証局（CA）に CSR を送信します。たとえば、CSR テキストを CA Web サイトの CSR 登録ページに貼り付けて送信します。

CA から署名付きの ID 証明書が返信されたら、Unified Communications Wizard に戻ります。ウィザードのクライアント側またはリモート側証明書管理ステップから、[Install ASA's Identity Certificate] をクリックします。アイデンティティ証明書をインストールする手順については、「Mobility Advantage サーバへの ASA ID 証明書のインストール」（P.15-27）および「Presence Federation および Cisco Intercompany Media Engine サーバへの ASA ID 証明書のインストール」（P.15-28）を参照してください。

Mobility Advantage サーバへの ASA ID 証明書のインストール

Cisco Mobility Advantage Proxy の証明書を設定する場合は、Cisco Mobility Advantage サーバに ASA の ID 証明書をインストールする必要があります。

通常、認証局は、署名付きのアイデンティティ証明書と認証局の証明書（ルート証明書と呼ばれます）の 2 種類の証明書を返します。ただし、（VeriSign など）認証局によっては中間証明書が送信される場合もあります。

認証局からのルート証明書が他の証明書に署名するために使用されます。ルート証明書は、認証局から受信した署名付きの ID 証明書を認証するために ASA によって使用されます。

認証局から中間証明書が提供された場合は、[Install ASA's Identity Certificate] ダイアログボックスの [Intermediate Certificate (If Applicable)] 領域に証明書テキストを入力する必要があります。

Cisco Mobility Advantage Proxy の場合は、別のダイアログボックスにルート証明書をインストールします。ルート証明書をインストールする手順については、「証明書のインストール」（P.15-25）を参照してください。

ステップ 1　[Intermediate Certificate (If Applicable)] 領域で、次のいずれかの操作を実行します。

- 既存のファイルから証明書コンフィギュレーションを追加するには、[Install from a file] オプション ボタンをクリックします（これがデフォルトの設定です）。パスおよびファイル名を入力するか、または [Browse] をクリックしてファイルを検索します。次に、[Install Certificate] をクリックします。
- 手動で登録するには、[Paste the certificate data in base-64 format] オプション ボタンをクリックします。表示された領域に PEM 形式（base64 または 16 進数値）証明書をコピー アンド ペーストします。

ステップ 2　[ASA's Identity Certificate] 領域で、次のいずれかの操作を実行します。

- 既存のファイルから証明書コンフィギュレーションを追加するには、[Install from a file] オプション ボタンをクリックします（これがデフォルトの設定です）。パスおよびファイル名を入力するか、または [Browse] をクリックしてファイルを検索します。次に、[Install Certificate] をクリックします。
- 手動で登録するには、[Paste the certificate data in base-64 format] オプション ボタンをクリックします。表示された領域に PEM 形式（base64 または 16 進数値）証明書をコピー アンド ペーストします。

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

Presence Federation および Cisco Intercompany Media Engine サーバへの ASA ID 証明書のインストール

Cisco Presence Federation Proxy および Cisco Intercompany Media Engine Proxy の証明書を設定する場合は、ASA の ID 証明書とルート証明書を Cisco Presence Federation サーバと Cisco Intercompany Media Engine サーバにそれぞれインストールする必要があります。

通常、認証局は、署名付きのアイデンティティ証明書と認証局の証明書（ルート証明書と呼ばれます）の 2 種類の証明書を返します。認証局からのルート証明書が他の証明書に署名するために使用されます。ルート証明書は、認証局から受信した署名付きの ID 証明書を認証するために ASA によって使用されます。

ステップ 1　[Root CA's Certificate] 領域で、次のいずれかの操作を実行します。

- 既存のファイルから証明書コンフィギュレーションを追加するには、[Install from a file] オプション ボタンをクリックします（これがデフォルトの設定です）。パスおよびファイル名を入力するか、または [Browse] をクリックしてファイルを検索します。次に、[Install Certificate] をクリックします。
- 手動で登録するには、[Paste the certificate data in base-64 format] オプション ボタンをクリックします。表示された領域に PEM 形式（base64 または 16 進数値）証明書をコピー アンド ペーストします。

ステップ 2　[ASA's Identity Certificate] 領域で、次のいずれかの操作を実行します。

- 既存のファイルから証明書コンフィギュレーションを追加するには、[Install from a file] オプション ボタンをクリックします（これがデフォルトの設定です）。パスおよびファイル名を入力するか、または [Browse] をクリックしてファイルを検索します。次に、[Install Certificate] をクリックします。
- 手動で登録するには、[Paste the certificate data in base-64 format] オプション ボタンをクリックします。表示された領域に PEM 形式（base64 または 16 進数値）証明書をコピー アンド ペーストします。

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