CHAPTER 4

Cisco ASA 設定

Cisco Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）ファイアウォールは、Cisco Intercompany Media Engine ソリューションのセキュリティにおいて、重要な役割を果たします。この項では、コマンド ライン インターフェイスを使用した ASA の設定についてと、Web ベースの GUI アプリケーションの ASDM について説明します。

プロキシ設定のガイドラインと制限事項

コンテキスト モード ガイドライン

シングル コンテキスト モードのみがサポートされています。

ファイアウォール モード ガイドライン

ルーティング ファイアウォール モードのみがサポートされています。

IPv6 ガイドライン

IPv6 アドレスはサポートされていません。

その他のガイドラインおよび制限事項

Cisco Intercompany Media Engine には、以下の制限があります。

- ファクスはサポートされていません。ファクス機能を SIP トランクで無効にする必要があります。
- Cisco Unified Intercompany Media Engine のステートフル フェールオーバーはサポートされていません。フェールオーバーの間は、Cisco Intercompany Media Engine プロキシを通過中の既存のコールは切断されますが、フェールオーバーが終了した後、新規のコールはこのプロキシを正常に通過します。
- Cisco Intercompany Media Engine プロキシでは、複数の適応型セキュリティ アプライアンスのインターフェイス上での Cisco UCM の使用はサポートされていません。適応型セキュリティ アプライアンスで、マッピング サービスのリスニング インターフェイスを指定し、Cisco UCM を 1 つの信頼できるインターフェイスに接続する必要があるため、特に、オフパス配置では、1 つの信頼できるインターフェイスで Cisco UCM を使用する必要があります。
- 複数 MIME はサポートされていません。
- 既存の SIP の機能およびメッセージのみがサポートされています。

- H.264 はサポートされていません。
- RTCP はサポートされていません。適応型セキュリティ アプライアンスは、内部インターフェイスから外部インターフェイスに送信されるすべての RTCP トラフィックをドロップします。適応型セキュリティ アプライアンスは、内部インターフェイスからの RTCP トラフィックを SRTP トラフィックに変換しません。
- 適応型セキュリティ アプライアンスで設定された Cisco Intercompany Media Engine プロキシは、リモート環境への各接続のダイナミック SIP トランクを作成します。ただし、SIP トランクごとに一意な件名を設定できません。Cisco Intercompany Media Engine プロキシは、プロキシに設定された件名を 1 つだけ設定できます。

  また、Cisco Intercompany Media Engine プロキシに設定した件名 DN は、ローカル Cisco UCM に設定したドメイン名と一致します。
- Cisco Intercompany Media Engine プロキシのサービス ポリシー ルールが（サービス ポリシー コマンドを使用せずに）削除されたり、再設定されたりした場合、適応型セキュリティ アプライアンスを通過する最初のコールは失敗します。Cisco UCM は接続がクリアされたことを認識せず、シグナリングのためにそのクリアされた IME SIP トランクの使用を試行するため、コールは PSTN にフェールオーバーします。

  この問題を解決するには、**clear connection all** コマンドを追加で入力し、適応型セキュリティ アプライアンスを再起動する必要があります。フェールオーバーのために失敗する場合、プライマリ適応型セキュリティ アプライアンスからの接続はスタンバイ適応型セキュリティ アプライアンスに同期されません。
- UC-IME プロキシが有効な適応型セキュリティ アプライアンスで **clear connection all** コマンドが発行されます。IME コールが PSTN にフェールオーバーされた後、SCCP IP Phone の発信側と着信側の間の次の IME コールは完了しますが、音声がなく、シグナリング セッションが確立するとドロップされます。

  SCCP IP Phone 間の IME コールは、両方向の IME SIP トランクを使用します。つまり、発信側から着信側へのシグナリングは IME SIP トランクを使用します。次に着信側は、リターン シグナリングおよびメディア変換のためにリバース IME SIP トランクを使用します。ただし、この接続が適応型セキュリティ アプライアンスですでにクリアされている場合、IME コールが失敗する原因となります。

  次の IME コール（**clear connection all** コマンドが発行されてから 3 番目のコール）は正常に完了します。

  （注）　この制限は、発信側および着信側の IP Phone が SIP で設定されている場合、適用されません。

- 適応型セキュリティ アプライアンスでは、ライセンスが取得されている必要があります。また、IME コール ボリュームを処理するために十分な TLS プロキシ セッションが設定されている必要もあります。TLS プロキシ セッションに関するライセンス要件については、Licensing for Cisco Intercompany Media Engine を参照してください。

  この制限は、IME コールを完了するために必要な TLS プロキシ セッションが十分に残されていないと、IME コールが PSTN にフェールバックできないために発生します。2 つの SCCP IP Phone 間の IME コールでは、適応型セキュリティ アプライアンスが 2 つの TLS プロキシ セッションを使用して TLS ハンドシェイクを正常に完了する必要があります。

  たとえば、適応型セキュリティ アプライアンスが最大 100 の TLS プロキシ セッションを使用できるように設定されていて、SCCP IP Phone 間の IME コールがすでに 101 TLS プロキシ セッションを確立しているとします。この例では、次の IME コールは発信側の SCCP IP Phone によって正常

に開始されますが、着信側 SCCP IP Phone によって受け取られると失敗します。着信側 IP Phone の呼び出し音は鳴りますが、コールに応答すると、TLS ハンドシェイクが完了していないために、そのコールは切断します。コールは PSTN にフォールバックされません。

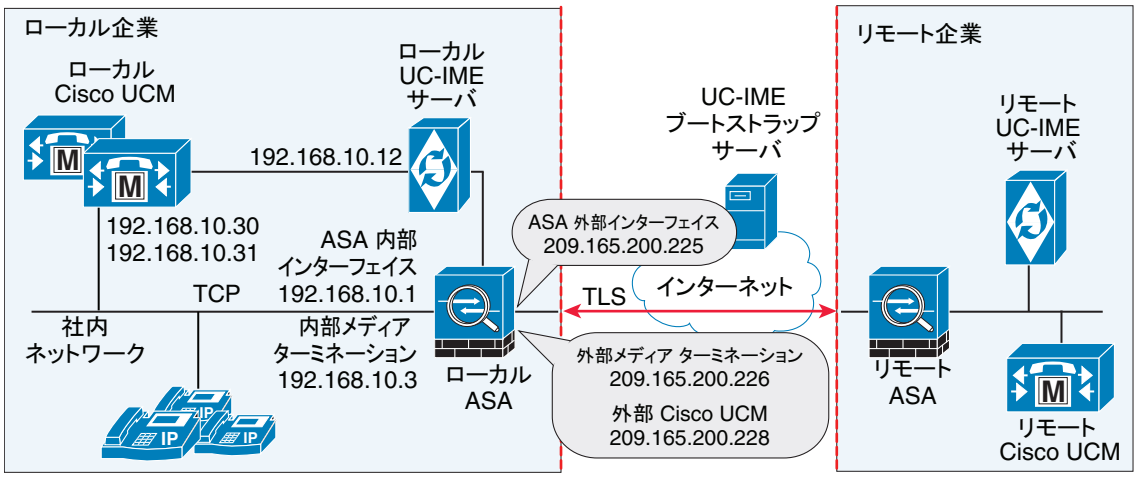
プロキシ CLI 設定

この項では、次のトピックについて取り上げます。

Cisco Intercompany Media Engine の設定のタスク フロー

図 4-1 では、Cisco Intercompany Media Engine の基本配置の例が示されています。以下のタスクには、図 4-1 に基づくコマンド ラインの例が含まれています。

図 4-1　　基本（インライン）配置タスクの例



（注）　ステップ 1 からステップ 8 は、基本（インライン）配置およびオフパス配置の両方に適用され、ステップ 9 は、オフパス配置にのみ適用されます。

基本配置で Cisco Intercompany Media Engine を構成する場合、以下のタスクを実行します。

ステップ 1　Cisco UCM のスタティック NAT を設定します。「Cisco Intercompany Media Engine プロキシの NAT 設定」（P.4-4）を参照してください。

または

UCM サーバの PAT を設定します。「Cisco UCM サーバの PAT 設定」（P.4-6）を参照してください。

ステップ 2　Cisco Intercompany Media Engine プロキシのアクセス リストを作成します。「Cisco Intercompany Media Engine プロキシのアクセス リストの作成」（P.4-8）を参照してください。

ステップ 3　Cisco Intercompany Media Engine プロキシのメディア ターミネーション アドレス インスタンスを作成します。「メディア ターミネーション インスタンスの作成」（P.4-9）を参照してください。

ステップ 4　Cisco Intercompany Media Engine プロキシを作成します。「Cisco Intercompany Media Engine プロキシの作成」（P.4-11）を参照してください。

ステップ 5　トラストポイントを作成し、Cisco Intercompany Media Engine プロキシの証明書を生成します。「トラストポイントの作成および証明書の生成」（P.4-14）を参照してください。

ステップ 6　TLS プロキシを作成します。「TLS プロキシの作成」（P.4-17）を参照してください。

ステップ 7　Cisco Intercompany Media Engine プロキシの SIP インスペクションを設定します。「Cisco Intercompany Media Engine プロキシの SIP インスペクションの有効化」（P.4-18）を参照してください。

ステップ 8　（オプション）環境内の TLS を設定します。「（オプション）ローカル環境内での TLS の設定」（P.4-20）を参照してください。

ステップ 9　（オプション）オフパス シグナリングを設定します。「（オプション）オフパス シグナリングの設定」（P.4-24）を参照してください。

（注）　オフパス配置で Cisco Intercompany Media Engine プロキシを設定しているときのみ、ステップ 9 を実行できます。

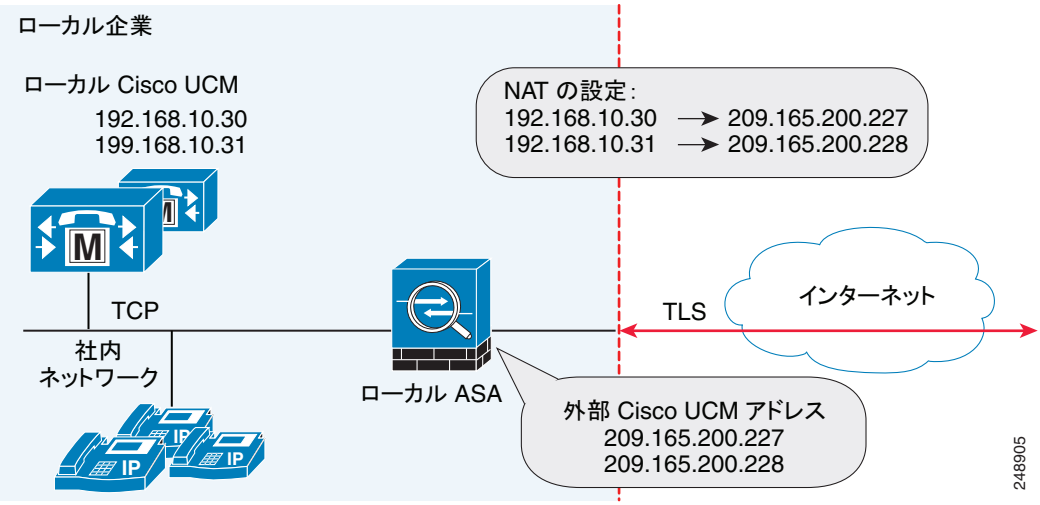
Cisco Intercompany Media Engine プロキシの NAT 設定

自動 NAT を設定するには、まずオブジェクトを設定し、そのオブジェクト コンフィギュレーション モードで **nat** コマンドを使用します。

このタスクのコマンド ラインの例は、基本（インライン）配置に基づいています。このタスクのコマンド ラインの例を説明する図については、図 4-1（P.4-3）を参照してください。

また、Cisco Intercompany Media Engine プロキシの PAT を設定することもできます。「Cisco UCM サーバの PAT 設定」（P.4-6）を参照してください。

図 4-2　配置に関する NAT の設定例



Cisco UCM サーバの自動 NAT ルールを設定するには、以下の手順を実行します。

	コマンド	目的
ステップ 1	hostname(config)# **object network** *name* **例：** hostname(config)# object network ucm_real_192.168.10.30 hostname(config)# object network ucm_real_192.168.10.31	変換する Cisco UCM の実際のアドレスのネットワーク オブジェクトを設定します。
ステップ 2	hostname(config-network-object)# **host** *ip_address* **例：** hostname(config-network-object)# host 192.168.10.30 hostname(config-network-object)# host 192.168.10.31	ネットワーク オブジェクトの Cisco UCM ホストの実際の IP アドレスを指定します。
ステップ 3	（オプション） hostname(config-network-object)# **description** *string* **例：** hostname(config-network-object)# description "Cisco UCM Real Address"	ネットワーク オブジェクトの説明を示します。
ステップ 4	hostname(config-network-object)# **exit**	オブジェクト コンフィギュレーション モードを終了します。
ステップ 5	hostname(config)# **object network** *name* **例：** hostname(config)# object network ucm_map_209.165.200.228	Cisco UCM のマップされたアドレスのネットワーク オブジェクトを設定します。
ステップ 6	hostname(config-network-object)# **host** *ip_address* **例：** hostname(config-network-object)# host 209.165.200.228	ネットワーク オブジェクトの Cisco UCM ホストのマップされた IP アドレスを指定します。
ステップ 7	（オプション） hostname(config-network-object)# **description** *string* **例：** hostname(config-network-object)# description "Cisco UCM Mapped Address"	ネットワーク オブジェクトの説明を示します。

	コマンド	目的
ステップ 8	`hostname(config-network-object)# exit`	オブジェクト コンフィギュレーション モードを終了します。

ステップ 9	`hostname(config)# nat (inside,outside) source static real_obj mapped_obj`
	例：
	`hostname(config)# nat (inside,outside) source static ucm_real_192.168.10.30 ucm_209.165.200.228`
	`hostname(config)# nat (inside,outside) source static ucm_real_192.168.10.31 ucm_209.165.200.228`
		この手順で作成されたネットワーク オブジェクトでのアドレス変換を指定します。
		ここで、*real_obj* は、このタスクのステップ 1 で作成した *name* です。
		ここで、*mapped_obj* は、このタスクのステップ 5 で作成した *name* です。

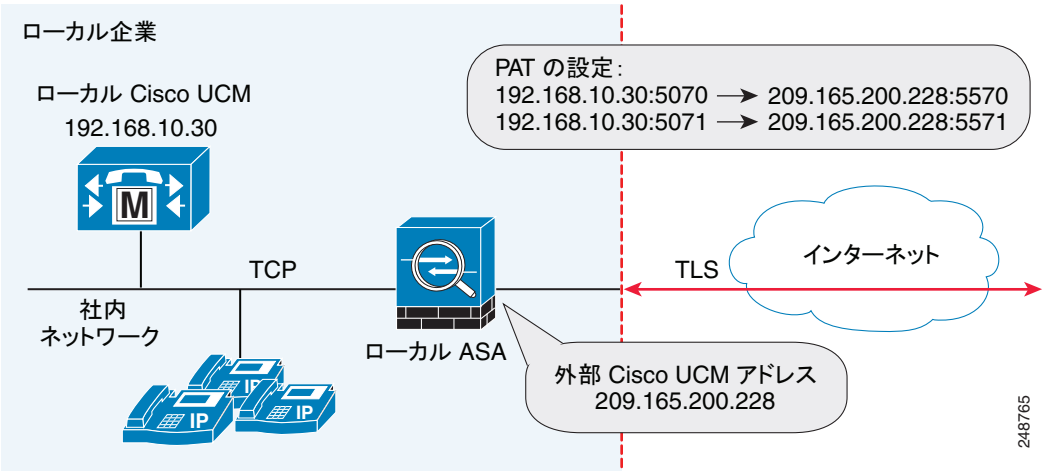
次のタスクの内容

Cisco Intercompany Media Engine プロキシのアクセス リストを作成します。「Cisco Intercompany Media Engine プロキシのアクセス リストの作成」（P.4-8）を参照してください。

Cisco UCM サーバの PAT 設定

Cisco Intercompany Media Engine プロキシの NAT を設定する別の方法としてこのタスクを実行します。

図 4-3　　配置に関する PAT の設定例



（注）　Cisco UCM サーバに対して NAT を設定していないときのみ、この手順を実行できます。

Cisco UCM サーバの PAT を設定するには、以下の手順を実行します。

	コマンド	目的
ステップ1	hostname(config)# **object network** *name* 例： hostname(config)# object network ucm-pat-209.165.200.228	変換する Cisco UCM の外部 IP アドレスについてネットワーク オブジェクトを設定します。
ステップ2	hostname(config-network-object)# **host** *ip_address* 例： hostname(config-network-object)# host 209.165.200.228	ネットワーク オブジェクトの Cisco UCM ホストの実際の IP アドレスを指定します。
ステップ3	hostname(config-network-object)# **exit**	オブジェクト コンフィギュレーション モードを終了します。
ステップ4	hostname(config)# **object service** *name* 例： hostname(config)# object service tcp_5070 hostname(config)# object service tcp_5071	外部 Cisco Intercompany Media Engine ポートのサービス オブジェクトを作成します。
ステップ5	hostname(config-service-object)# **tcp source eq** *port* 例： hostname(config-service-object)# tcp source eq 5070 hostname(config-service-object)# tcp source eq 5071	ポート番号を指定します。
ステップ6	hostname(config-service-object)# **exit**	オブジェクト コンフィギュレーション モードを終了します。
ステップ7	hostname(config)# **object network** *name* 例： hostname(config)# object network ucm-real-192.168.10.30 hostname(config)# object network ucm-real-192.168.10.31	Cisco UCM の実際の IP アドレスを表すネットワーク オブジェクトを設定します。
ステップ8	hostname(config-network-object)# **host** *ip_address* 例： hostname(config-network-object)# host 192.168.10.30 hostname(config-network-object)# host 192.168.10.31	ネットワーク オブジェクトの Cisco UCM ホストの実際の IP アドレスを指定します。
ステップ9	hostname(config-network-object)# **exit**	オブジェクト コンフィギュレーション モードを終了します。
ステップ10	hostname(config)# **object service** *name* 例： hostname(config)# object service tcp_5570 hostname(config)# object service tcp_5571	Cisco UCM SIP ポートのサービス オブジェクトを作成します。
ステップ11	hostname(config-service-object)# **tcp source eq** *port* 例： hostname(config-service-object)# tcp source eq 5570 hostname(config-service-object)# tcp source eq 5571	ポート番号を指定します。

	コマンド	目的
ステップ 21	hostname(config-service-object)# **exit**	オブジェクト コンフィギュレーション モードを終了します。
ステップ 31	hostname(config)# **nat (inside,outside) source static** *real_obj mapped_obj* **service** *real_port mapped_port* **例：** hostname(config)# nat (inside,outside) source static ucm-real-192.168.10.30 ucm-pat-209.165.200.228 service tcp_5070 tcp_5570 hostname(config)# nat (inside,outside) source static ucm-real-192.168.10.31 ucm-pat-128.106.254.5 service tcp_5071 tcp_5571	Cisco UCM のスタティック マッピングを作成します。 *ここで、real_obj は、このタスクのステップ 1 で作成した名前です。* *ここで、mapped_obj は、このタスクのステップ 7 で作成した名前です。* *ここで、real_port は、このタスクのステップ 4 で作成した名前です。* *ここで、mapped_obj は、このタスクのステップ 10 で作成した名前です。*

Cisco Intercompany Media Engine プロキシのアクセス リストの作成

Cisco UCM サーバに到達するように Cisco Intercompany Media Engine プロキシのアクセス リストを設定するには、以下の手順を実行します。

このタスクのコマンド ラインの例は、基本（インライン）配置に基づいています。このタスクのコマンド ラインの例を説明する図については、図 4-1（P.4-3）を参照してください。

	コマンド	目的
ステップ 1	hostname(config)# **access-list** *id* **extended permit tcp any host** *ip_address* **eq** *port* **例：** hostname(config)# access-list incoming extended permit tcp any host 192.168.10.30 eq 5070	Access Control Entry（ACE; アクセス コントロール エントリ）を追加します。アクセス リストは、同じアクセス リスト ID を使用する 1 つ以上の ACE によって構成されます。この ACE は、指定されたポートでの Cisco Intercompany Media Engine 接続の着信アクセスを許可して、アクセス コントロールを提供します。 *ip_address* 引数に、Cisco UCM の実際の IP アドレスを指定します。
ステップ 2	hostname(config)# **access-group** *access-list* **in interface** *interface_name* **例：** hostname(config)# access-group incoming in interface outside	アクセス リストをインターフェイスにバインドします。
ステップ 3	hostname(config)# **access-list** *id* **extended permit tcp any host** *ip_address* **eq** *port* **例：** hostname(config)# access-list ime-inbound-sip extended permit tcp any host 192.168.10.30 eq 5070	ACE を追加します。この ACE によって、適応型セキュリティ アプライアンスは Cisco Intercompany Media Engine のインバウンド SIP トラフィックを許可できます。このエントリは、クラス マップおよびポリシー マップのトラフィックを分類するために使用されます。 **（注）**　ここで設定するポートは、Cisco UCM で設定されるトランクの設定に一致します。この設定に関する詳細については、Cisco Unified Communications Manager の関連資料を参照してください。

	コマンド	目的
ステップ 4	hostname(config)# **access-list** *id* **extended permit tcp** *ip_address mask* **any range** *range* **例：** hostname(config)# access-list ime-outbound-sip extended permit tcp 192.168.10.30 255.255.255.255 any range 5000 6000	ACE を追加します。この ACE によって、適応型セキュリティ アプライアンスは Cisco Intercompany Media Engine のアウトバウンド SIP トラフィックを許可できます（例では、ソースが 192.168.10.30 で、宛先ポートの範囲が 5000 ～ 6000 のすべての TCP トラフィックが許可されます）。このエントリは、クラス マップおよびポリシー マップのトラフィックを分類するために使用されます。 **（注）** Cisco UCM と Cisco Intercompany Media Engine サーバとの間の TCP トラフィックには、このポート範囲を使用しないでください（その接続が適応型セキュリティ アプライアンスを経由する場合）。
ステップ 5	hostname(config)# **access-list** *id* **permit tcp any host** *ip_address* **eq 6084** **例：** hostname(config)# access-list ime-traffic permit tcp any host 192.168.10.12 eq 6084	ACE を追加します。この ACE によって、適応型セキュリティ アプライアンスは Cisco Intercompany Media Engine サーバからリモート Cisco Intercompany Media Engine サーバへのトラフィックを許可できます。
ステップ 6	hostname(config)# **access-list** *id* **permit tcp any host** *ip_address* **eq 8470** **例：** hostname(config)# access-list ime-bootserver-traffic permit tcp any host 192.168.10.12 eq 8470	ACE を追加します。この ACE によって、適応型セキュリティ アプライアンスは Cisco Intercompany Media Engine サーバから Cisco Intercompany Media Engine のブートストラップ サーバへのトラフィックを許可できます。

次のタスクの内容

Cisco Intercompany Media Engine プロキシの適応型セキュリティ アプライアンス上にメディア ターミネーション インスタンスを作成します。「メディア ターミネーション インスタンスの作成」（P.4-9）を参照してください。

メディア ターミネーション インスタンスの作成

ガイドライン

設定するメディア ターミネーション アドレスは、以下の要件を満たしている必要があります。

- グローバル インターフェイスを使用せずに、インターフェイスで、メディア ターミネーション アドレスを設定する場合、Cisco Intercompany Media Engine プロキシのサービス ポリシーを適用する前に、少なくとも 2 つのインターフェイス（内部インターフェイスと外部インターフェイス）に 1 つのメディア ターミネーション アドレスを設定する必要があります。設定しない場合、プロキシで SIP インスペクションを有効にしていると、エラー メッセージを受け取ります。

（注） Cisco は、グローバル メディア ターミネーション アドレスを設定せずに、インターフェイスで Cisco Intercompany Media Engine プロキシのメディア ターミネーション アドレスを設定することをお勧めします。

- Cisco Intercompany Media Engine プロキシは、一度に 1 つのタイプのメディア ターミネーション インスタンスを使用できます。たとえば、すべてのインターフェイス用の 1 つのグローバル メディア ターミネーション アドレスを設定するか、または異なるインターフェイス用の 1 つのメ

ディア ターミネーション アドレスを設定できます。しかし、同時にグローバル メディア ターミネーション アドレスとインターフェイスごとに設定されたメディア ターミネーション アドレスを使用できません。

（注）　プロキシのメディア ターミネーション アドレスを作成した後に、Cisco Intercompany Media Engine プロキシ設定に何らかの変更を加えた場合、**no media-termination** コマンドを使用してメディア ターミネーション アドレスを再設定する必要があります。その際、以下の手順のように再設定します。

手順

Cisco Intercompany Media Engine プロキシとともに使用するメディア ターミネーション インスタンスを作成します。

このタスクのコマンド ラインの例は、基本（インライン）配置に基づいています。このタスクのコマンド ラインの例を説明する図については、図 4-1（P.4-3）を参照してください。

Cisco Intercompany Media Engine プロキシ用にメディア ターミネーション インスタンスを作成するには、以下の手順を実行します。

	コマンド	目的
ステップ 1	hostname(config)# **media-termination** *instance_name* **例：** hostname(config)# **media-termination** *uc-ime-media-term*	Cisco Intercompany Media Engine プロキシに接続するメディア ターミネーション インスタンスを作成します。
ステップ 2	hostname(config-media-termination)# **address** *ip_address* **interface** *intf_name* **例：** hostname(config-media-termination)# address 209.165.200.228 interface outside	適応型セキュリティ アプライアンスの外部インターフェイスによって使用されるメディア ターミネーション アドレスを設定します。 外部 IP アドレスは、パブリックにルーティング可能なアドレスで、そのインターフェイスのアドレス範囲内で未使用の IP アドレスである必要があります。 UC-IME プロキシ設定については、「Cisco Intercompany Media Engine プロキシの作成」（P.4-11）を参照してください。**no service-policy** コマンドについては、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

	コマンド	目的
ステップ 3	hostname(config-media-termination)# **address** *ip_address* **interface** *intf_name* **例：** hostname(config-media-termination)# address 192.168.10.3 interface inside	適応型セキュリティ アプライアンスの内部インターフェイスによって使用されるメディア ターミネーション アドレスを設定します。 **（注）** この IP アドレスは、そのインターフェイスの同じサブネット内で未使用の IP アドレスである必要があります。
ステップ 4	ÅiÉIÉvÉVÉáÉìÅj hostname(config-media-termination)# ***rtp-min-port*** *port1* **rtp-maxport** *port2* **例：** hostname(config-media-termination)# rtp-min-port 1000 rtp-maxport 2000	Cisco Intercompany Media Engine プロキシの RTP 最小ポートおよび RTP 最大ポート制限を設定します。Cisco Intercompany Media Engine をサポートするコール数を増やす必要があるときに、メディア ターミネーション ポイントの RTP ポート範囲を設定します。 ここで、*port1* には、メディア ターミネーション ポイントの RTP ポート範囲の最小値を指定します。port1 には、1024 ～ 65535 までの値を指定できます。デフォルトでは、*port1* の値は 16384 です。 ここで、*port2* には、メディア ターミネーション ポイントの RTP ポート範囲の最大値を指定します。port2 には、1024 ～ 65535 までの値を指定できます。デフォルトでは、*port2* の値は 32767 です。

次のタスクの内容

メディア ターミネーション インスタンスを作成したら、Cisco Intercompany Media Engine プロキシを作成します。「Cisco Intercompany Media Engine プロキシの作成」（P.4-11）を参照してください。

Cisco Intercompany Media Engine プロキシの作成

Cisco Intercompany Media Engine プロキシを作成するには、以下の手順を実行します。

このタスクのコマンド ラインの例は、基本（インライン）配置に基づいています。このタスクのコマンド ラインの例を説明する図については、図 4-1（P.4-3）を参照してください。

（注） プロキシが SIP インスペクションに対して有効なときに、以下の手順で示されている Cisco Intercompany Media Engine プロキシのいかなる設定も変更できません。この手順で説明されている設定のいずれかを変更するには、SIP インスペクションから Cisco Intercompany Media Engine プロキシを削除します。

	コマンド	目的
ステップ1	hostname(config)# **uc-ime** *uc_ime_name* **例：** hostname(config)# uc-ime local-ent-ime	Cisco Intercompany Media Engine プロキシを設定します。 ここで、*uc_ime_name* は、Cisco Intercompany Media Engine プロキシの名前です。この名前は、64 文字までに制限されています。 適応型セキュリティ アプライアンスでは、Cisco Intercompany Media Engine プロキシを 1 つだけ設定できます。
ステップ2	hostname(config-uc-ime)# **media-termination** *mta_instance_name* **例：** hostname(config-uc-ime)# media-termination ime-media-term	Cisco Intercompany Media Engine プロキシによって使用されるメディア ターミネーション インスタンスを指定します。 **（注）** Cisco Intercompany Media Engine プロキシでメディア ターミネーション インスタンスを指定する前に、このインスタンスを作成する必要があります。 ここで、*mta_instance_name* は、メディア ターミネーション インスタンスの作成のステップ 1 で作成した *instance_name* です。 メディア ターミネーション インスタンスを作成する手順については、「メディア ターミネーション インスタンスの作成」（P.4-9）を参照してください。
ステップ3	hostname(config-uc-ime)# **ucm address** *ip_address* **trunk-security-mode** [**nonsecure** | **secure**] **例：** hostname(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure	環境内の Cisco UCM サーバを指定します。Cisco UCM サーバの実際の IP アドレスを指定する必要があります。サーバのマップされた IP アドレスを指定しないでください。 **（注）** SIP トランクが有効な Cisco Intercompany Media Engine を使用するクラスタ内の各 Cisco UCM にエントリを含める必要があります。 ここで、**nonsecure** および **secure** オプションは、Cisco UCM または Cisco UCM のクラスタのセキュリティ モードを指定します。 **（注）** Cisco UCM または Cisco UCM クラスタに対して **secure** を指定すると、Cisco UCM または Cisco UCM クラスタは TLS を開始します。そのため、コンポーネントの TLS を設定する必要があります。「（オプション）ローカル環境内での TLS の設定」（P.4-20）を参照してください。 このタスクで **secure** オプションを指定できます。または、後で環境の TLS を設定する際に、このオプションを更新できます。「（オプション）ローカル環境内での TLS の設定」（P.4-20）のステップ 11 を参照してください。

	コマンド	目的
ステップ 4	hostname(config-uc-ime)# **ticket epoch** *n* **password** *password* **例：** hostname(config-uc-ime)# ticket epoch 1 password password1234	Cisco Intercompany Media Engine のチケット エポックおよびパスワードを設定します。 ここで、*n* は 1 ～ 255 までの整数です。エポックには、パスワードが変更されるたびに更新される整数が入ります。プロキシを初めて設定し、パスワードを初めて入力するときに、エポックの整数として 1 を入力します。パスワードを変更するたびに、新しいパスワードを示すためにエポックを増やします。ユーザは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。 通常は、順番にエポックを増やしますが、適応型セキュリティ アプライアンスを使用すると、エポックを更新する際に任意の値を選択できます。 エポック値を変更する場合、現在のパスワードは無効となり、新規パスワードを入力する必要があります。 ここで、*password* には、US-ASCII 文字セットから印刷可能な 10 ～ 64 文字が入ります。使用可能な文字には、0x21 ～ 0x73 までが含まれ、スペース文字は除外されます。 少なくとも 20 文字以上のパスワードが推奨されています。同時に設定できるパスワードは 1 つだけです。 チケット パスワードは、フラッシュに格納されます。**show running-config uc-ime** コマンドの出力には、パスワード文字列の代わりに「*****」が表示されます。 **（注）** 適応型セキュリティ アプライアンスで設定するエポックおよびパスワードは、Cisco Intercompany Media Engine サーバで設定する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 サーバの関連資料を参照してください。

	コマンド	目的

ステップ 5	（オプション）
	`hostname(config-uc-ime)# fallback monitoring timer timer_millisec | hold-down timer timer_sec`
	例：
	`hostname(config-uc-ime)# fallback monitoring timer 120`
	`hostname(config-uc-ime)# fallback hold-down timer 30`
		Cisco Intercompany Media Engine のフォールバック タイマーを指定します。
		monitoring timer を指定すると、適応型セキュリティ アプライアンスがインターネットから受信する RTP パケットをサンプリングする時間間隔が設定されます。適応型セキュリティ アプライアンスは、このデータ サンプルを使用して、コールに対して PSTN へのフォールバックが必要であるかを判別します。
		ここで、*timer_millisec* には、モニタリング タイマーの長さを指定します。デフォルトでは、モニタリング タイマーの長さは 100 ミリ秒です。使用可能な範囲は、10 ～ 600 ミリ秒です。
		hold-down timer を指定すると、PSTN にフォールバックするかどうかを Cisco UCM に通知するまで適応型セキュリティ アプライアンスが待機する時間が設定されます。
		ここで、*timer_sec* には、ホールドダウン タイマーの長さを指定します。デフォルトでは、ホールドダウン タイマーの長さは 20 秒です。使用可能な範囲は、10 ～ 360 秒です。
		このコマンドを使用してフォールバック タイマーを指定しない場合、適応型セキュリティ アプライアンスはフォールバック タイマーのデフォルト設定を使用します。

ステップ 6	（オプション）
	`hostname(config-uc-ime)# fallback sensitivity-file file_name`
	例：
	`hostname(config-uc-ime)# fallback sensitivity-file ime-fallback-sensitvity.fbs`
		通話中 PSTN フォールバックに使用するファイルを指定します。
		ここで、*file_name* は、.fbs ファイル拡張子を含むディスク上のファイルの名前である必要があります。
		フォールバック ファイルは、Cisco Intercompany Media Engine がコールを PSTN に転送するほどコールの QoS が低下しているかを識別するために使用されます。

次のタスクの内容

ローカル エンティティ信頼ストアに証明書をインストールします。ローカル エンティティによって信頼されたローカル CA で証明書を登録することもできます。

トラストポイントの作成および証明書の生成

適応型セキュリティ アプライアンスによって使用される証明書のキー ペアを生成する必要があります。また、TLS ハンドシェイクで適応型セキュリティ アプライアンスによって送信される証明書を識別するようにトラストポイントを設定する必要があります。

このタスクのコマンド ラインの例は、基本（インライン）配置に基づいています。このタスクのコマンド ラインの例を説明する図については、図 4-1（P.4-3）を参照してください。

（注）　このタスクは、ローカル環境とリモート環境のトラストポイントを作成する方法、およびこれらの環境の間での証明書の交換方法を説明します。このタスクでは、ローカル Cisco UCM とローカル適応型セキュリティ アプライアンスとの間でのトラストポイントの作成および証明書の交換に関する手順は扱われません。ただし、ローカル環境内での追加のセキュリティが必要な場合、「（オプション）ローカル環境内での TLS の設定」（P.4-20）で示されるオプションのタスクを実行する必要があります。そのタスクを実行することにより、ローカル Cisco UCM とローカル適応型セキュリティ アプライアンスとの間でのセキュア TLS 接続が可能となります。そのタスクでは、ローカル Cisco UCM とローカル適応型セキュリティ アプライアンスとの間のトラストポイントを作成する方法が説明されます。

証明書のインストールに関する前提条件

リモート エンティティによって信頼された適応型セキュリティ アプライアンスでプロキシ証明書を作成するには、信頼できる CA から証明書を取得する、またはリモート環境の適応型セキュリティ アプライアンスから証明書をエクスポートします。

リモート環境から証明書をエクスポートするには、リモートの適応型セキュリティ アプライアンスで以下のコマンドを入力します。

hostname(config)# **crypto ca export trustpoint identity-certificate**

適応型セキュリティ アプライアンスは、ターミナルの画面に証明書を表示します。ターミナルの画面から証明書をコピーします。このタスクのステップ 5 で、この証明書のテキストが必要になります。

手順

トラストポイントを作成し、証明書を生成するには、以下の手順を実行します。

	コマンド	目的
ステップ 1	hostname(config)# **crypto key generate rsa label** *key-pair-label* **modulus** *size* **例：** hostname(config)# crypto key generate rsa label local-ent-key modulus 2048	ローカルの適応型セキュリティ アプライアンスで、トラストポイントで使用される RSA キー ペアを作成します。これは、ローカル エンティティの署名付き証明書に関するキー ペアおよびトラストポイントです。 選択するモジュール キー サイズは、設定するセキュリティのレベル、および証明書を取得する CA によって課される制約によって異なります。選択する数が増えれば増えるほど、証明書のセキュリティ レベルは高くなります。ほとんどの CA では、キー モジュール サイズとして 2048 が推奨されています。ただし、 （注）　GoDaddy では、キー モジュール サイズは 2048 である必要があります。
ステップ 2	hostname(config)# **crypto ca trustpoint** *trustpoint_name* **例：** hostname(config)# crypto ca trustpoint local_ent	ローカル エンティティのトラストポイントが作成できるように、指定したトラストポイントのトラストポイント コンフィギュレーション モードを入力します。 トラストポイントは、CA によって発行された証明書に基づく CA ID、場合によってはデバイス ID を表します。名前の最大長は、128 文字です。

	コマンド	目的
ステップ 3	hostname(config-ca-trustpoint)# **subject-name** *X.500_name* **例：** hostname(config-ca-trustpoint)# subject-name cn=Ent-local-domain-name**	登録時に、証明書に示された件名 DN を指定します。 **（注）** ここで入力するドメイン名は、ローカル Cisco UCM で設定したドメイン名と一致する必要があります。Cisco UCM のドメイン名の設定方法については、Cisco Unified Communications Manager の関連資料を参照してください。
ステップ 4	hostname(config-ca-trustpoint)# **keypair** *keyname* **例：** hostname(config-ca-trustpoint)# keypair local-ent-key	認証される公開鍵のキー ペアを指定します。
ステップ 5	hostname(config-ca-trustpoint)# **enroll terminal**	このトラストポイントを登録する方法として、「コピー アンド ペースト」（手動登録）の使用を指定します。
ステップ 6	hostname(config-ca-trustpoint)# **exit**	CA トラストポイント コンフィギュレーション モードを終了します。
ステップ 7	hostname(config)# **crypto ca enroll** *trustpoint* **例：** hostname(config)# crypto ca enroll remote-ent % % Start certificate enrollment ... % The subject name in the certificate will be: % cn=enterpriseA % The fully-qualified domain name in the certificate will @ be: ciscoasa % Include the device serial number in the subject name?[yes/no]: no Display Certificate Request to terminal?[yes/no]: yes	CA での登録プロセスを開始します。 ここで、*trustpoint* は、ステップ 2 で入力した *trustpoint_name* と同じ値です。 手動登録（**enroll terminal** コマンド）でトラストポイントを設定していると、適応型セキュリティ アプライアンスは Base 64 エンコード PKCS10 の証明書要求をコンソールに書き込み、CLI プロンプトを表示します。プロンプトからテキストをコピーします。 証明書要求を CA に送信します。たとえば、プロンプトに表示されたテキストを CA Web サイトの証明書署名要求登録ページに貼り付けます。 CA から署名付き ID 証明書が送られてきたら、この手順のステップ 8 に進みます。
ステップ 8	hostname(config)# **crypto ca import** *trustpoint* **certificate** **例：** hostname(config)# crypto ca import remote-ent certificate	手動登録要求の返信として CA から受け取った署名付き証明書をインポートします。 ここで、*trustpoint* には、ステップ 2 で作成したトラストポイントを指定します。 適応型セキュリティ アプライアンスは、Base 64 形式の署名付き証明書をターミナルに貼り付けるよう求めるプロンプトを表示します。
ステップ 9	hostname(config)# **crypto ca authenticate** *trustpoint* **例：** hostname(config)# crypto ca authenticate remote-ent	CA から受け取ったサードパーティ ID 証明書を認証します。この ID 証明書は、リモート環境用に作成したトラストポイントに関連付けられます。 適応型セキュリティ アプライアンスは、CA からの Base 64 形式の ID 証明書をターミナルに貼り付けるよう求めるプロンプトを表示します。

次のタスクの内容

Cisco Intercompany Media Engine の TLS プロキシを作成します。「TLS プロキシの作成」（P.4-17）を参照してください。

TLS プロキシの作成

ローカル Cisco UCM サーバ、リモート Cisco UCM サーバのどちらの環境でも、TLS ハンドシェイクを開始できるので（クライアントのみが 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 Mobility Advantage とは異なります）、双方向 TLS プロキシのルールを設定する必要があります。各環境で、TLS プロキシとして適応型セキュリティ アプライアンスを使用できます。

個別に接続が開始されたローカルおよびリモート エンティティの TLS プロキシ インスタンスを作成します。TLS 接続を開始するエンティティは、「TLS クライアント」のロールになります。TLS プロキシには、「クライアント」と「サーバ」の厳密な定義があるため、2 つの TLS プロキシ インスタンスは、いずれのエンティティで接続を開始できるか定義する必要があります。

このタスクのコマンド ラインの例は、基本（インライン）配置に基づいています。このタスクのコマンド ラインの例を説明する図については、図 4-1（P.4-3）を参照してください。

TLS プロキシを作成するには、次の手順を実行します。

	コマンド	目的

ステップ 1	`hostname(config)# tls-proxy proxy_name`
	例：
	`hostname(config)# tls-proxy local_to_remote-ent`
		アウトバウンド接続用の TLS プロキシを作成します。

ステップ 2	`hostname(config-tlsp)# client trust-point proxy_trustpoint`
	例：
	`hostname(config-tlsp)# client trust-point local-ent`
		アウトバウンド接続では、適応型セキュリティ アプライアンスが TLS クライアントのロールを担っているときに、TLS ハンドシェイクで使用するトラストポイントおよび関連する証明書を指定します。適応型セキュリティ アプライアンスが証明書（ID 証明書）を所有する必要があります。
		ここで、*proxy_trustpoint* には、「トラストポイントの作成および証明書の生成」（P.4-14）のステップ 2 で **crypto ca trustpoint** コマンドによって定義されたトラストポイントを指定します。

ステップ 3	`hostname(config-tlsp)# client cipher-suite cipher_suite`
	例：
	`hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`
		アウトバウンド接続に対して、暗号スイートの TLS ハンドシェイク パラメータを制御します。
		ここで、*cipher_suite* には、des-sha1、3des-sha1、aes128-sha1、aes256-sha1、または null-sha1 が入ります。
		クライアント プロキシ（このプロキシはサーバに対して TLS クライアントとして機能します）では、ユーザ定義の暗号スイートによって、デフォルトの暗号スイートまたは **ssl encryption** コマンドによって定義された暗号スイートが置き換えられます。このコマンドを使用して、2 つの TLS セッション間で異なる暗号化を実現します。AES 暗号を Cisco UCM サーバで使用する必要があります。

ステップ 4	`hostname(config-tlsp)# exit`	TLS プロキシ コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ5	hostname(config)# **tls-proxy** *proxy_name* **例：** hostname(config)# tls-proxy remote_to_local-ent	インバウンド接続用の TLS プロキシを作成します。
ステップ6	hostname(config-tlsp)# **server trust-point** *proxy_trustpoint* **例：** hostname(config-tlsp)# server trust-point local-ent	**インバウンド**接続では、TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定します。適応型セキュリティ アプライアンスが証明書（ID 証明書）を所有する必要があります。 ここで、*proxy_trustpoint* には、「トラストポイントの作成および証明書の生成」（P.4-14）のステップ 2 で **crypto ca trustpoint** コマンドによって定義されたトラストポイントを指定します。 TLS プロキシには、クライアント プロキシとサーバ プロキシの厳密な定義があるため、2 つの TLS プロキシ インスタンスは、いずれのエンティティで接続を開始できるか定義する必要があります。
ステップ7	hostname(config-tlsp)# **client cipher-suite** *cipher_suite* **例：** hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1	インバウンド接続に対して、暗号スイートの TLS ハンドシェイク パラメータを制御します。 ここで、*cipher_suite* には、des-sha1、3des-sha1、aes128-sha1、aes256-sha1、または null-sha1 が入ります。
ステップ8	hostname(config-tlsp)# **exit**	TSL プロキシ コンフィギュレーション モードを終了します。
ステップ9	hostname(config)# **ssl encryption 3des-sha1 aes128-sha1** [*algorithms*]	SSL/TLS プロトコルが使用する暗号化アルゴリズムを指定します。3des-sha1 と aes128-sha1 を指定する必要があります。その他のアルゴリズムの指定は、オプションです。 **（注）** Cisco Intercompany Media Engine プロキシでは、強度の高い暗号化を使用する必要があります。プロキシに K9 ライセンスを使用するライセンスがあるときは、このコマンドを指定する必要があります。

次のタスクの内容

TLS プロキシを作成したら、そのプロキシを SIP インスペクションに対して有効にします。

Cisco Intercompany Media Engine プロキシの SIP インスペクションの有効化

TLS プロキシを SIP インスペクションに対して有効にし、接続を開始できる両方のエンティティのポリシーを定義します。

このタスクのコマンド ラインの例は、基本（インライン）配置に基づいています。このタスクのコマンド ラインの例を説明する図については、図 4-1（P.4-3）を参照してください。

（注）　SIP インスペクションを有効にした後、Cisco Intercompany Media Engine プロキシの設定を変更する場合、**no service-policy** コマンドを入力し、以下の手順で示されているようにサービス ポリシーを再設定する必要があります。サービス ポリシーの削除および再設定は、既存のコールに影響しませんが、Cisco Intercompany Media Engine プロキシを通過する最初のコールは失敗します。**clear connection** コマンドを入力し、適応型セキュリティ アプライアンスを再起動します。

Cisco Intercompany Media Engine プロキシの SIP インスペクションを有効にするには、以下の手順を実行します。

	コマンド	目的
ステップ 1	hostname(config)# **class-map** *class_map_name* **例：** hostname(config)# class-map ime-inbound-sip	インバウンド Cisco Intercompany Media Engine SIP トラフィックのクラスを定義します。
ステップ 2	hostname(config-cmap)# **match access-list** *access_list_name* **例：** hostname(config-cmap)# match access-list ime-inbound-sip	検査する SIP トラフィックを指定します。 ここで、*access_list_name* は、タスク Cisco Intercompany Media Engine プロキシのアクセス リストの作成の「ÉXÉeÉbÉv 3」（P.4-8）で作成したアクセス リストです。
ステップ 3	hostname(config-cmap)# **exit**	クラス マップ コンフィギュレーション モードを終了します。
ステップ 4	hostname(config)# **class-map** *class_map_name* **例：** hostname(config)# class-map ime-outbound-sip	Cisco Intercompany Media Engine からのアウトバウンド SIP トラフィックのクラスを定義します。
ステップ 5	hostname(config)# **match access-list** *access_list_name* **例：** hostname(config-cmap)# match access-list ime-outbound-sip	検査するアウトバウンド SIP トラフィックを指定します。 ここで、*access_list_name* は、タスク Cisco Intercompany Media Engine プロキシのアクセス リストの作成の「ステップ 4」（P.4-9）で作成したアクセス リストです。
ステップ 6	hostname(config-cmap)# **exit**	クラス マップ コンフィギュレーション モードを終了します。
ステップ 7	hostname(config)# **policy-map** *name* **例：** hostname(config)# policy-map ime-policy	トラフィックのクラスのアクションに関連するポリシー マップを定義します。
ステップ 8	hostname(config-pmap)# **class** *classmap_name* **例：** hostname(config-pmap)# class ime-outbound-sip	アクションをクラス マップ トラフィックに割り当てることができるように、クラス マップをポリシー マップに割り当てます。 ここで、*classmap_name* は、このタスクのステップ 1 で作成した SIP クラス マップの名前です。
ステップ 9	hostname(config-pmap-c)# **inspect sip** [*sip_map*] **tls-proxy** *proxy_name* **uc-ime** *uc_ime_map* **例：** hostname(config-pmap-c)# inspect sip tls-proxy local_to_remote-ent uc-ime local-ent-ime	TLS プロキシおよび Cisco Intercompany Media Engine プロキシを指定した SIP インスペクション セッションに対して有効にします。
ステップ 10	hostname(config-cmap-c)# **exit**	ポリシー マップ クラス コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 11	hostname(config-pmap)# **class** *class_map_name* **例：** hostname(config-pmap)# class ime-inbound-sip	アクションをクラス マップ トラフィックに割り当てることができるように、クラス マップをポリシー マップに割り当てます。 ここで、*classmap_name* は、このタスクのステップ 4 で作成した SIP クラス マップの名前です。
ステップ 12	hostname(config-pmap-c)# **inspect sip** [*sip_map*] **tls-proxy** *proxy_name* **uc-ime** *uc_ime_map* **例：** hostname(config-pmap-c)# inspect sip tls-proxy remote-to-local-ent uc-ime local-ent-ime	TLS プロキシおよび Cisco Intercompany Media Engine プロキシを指定した SIP インスペクション セッションに対して有効にします。
ステップ 13	hostname(config-pmap-c)# **exit**	ポリシー マップ クラス コンフィギュレーション モードを終了します。
ステップ 14	hostname(config-pmap)# **exit**	ポリシー マップ コンフィギュレーション モードを終了します。
ステップ 15	hostname(config)# **service-policy** *policymap_name* **global** **例：** hostname(config)# service-policy ime-policy global	すべてのインターフェイスの SIP インスペクションのサービス ポリシーを有効にします。 ここで、*policymap_name* は、このタスクのステップ 7 で作成したポリシー マップの名前です。 UC-IME プロキシ設定については、「Cisco Intercompany Media Engine プロキシの作成」（P.4-11）を参照してください。**no service-policy** コマンドについては、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

次のタスクの内容

TLS プロキシを SIP インスペクションに対して有効にしたら、必要に応じて、環境内の TLS を設定します。「（オプション）ローカル環境内での TLS の設定」（P.4-20）を参照してください。

（オプション）ローカル環境内での TLS の設定

内部ネットワーク内で TCP が使用可能な場合、このタスクは必要ありません。

適応型セキュリティ アプライアンスが参照するように、環境内の TLS は Cisco Intercompany Media Engine トランクのセキュリティ ステータスを参照します。

（注）　Cisco UCM で Cisco Intercompany Media Engine トランクの転送セキュリティを変更した場合、同様に、適応型セキュリティ アプライアンスでも変更セキュリティを変更する必要があります。一致していないと、コール失敗が発生します。適応型セキュリティ アプライアンスは、SRTP を非セキュア IME トランクではサポートしません。適応型セキュリティ アプライアンスでは、SRTP がセキュア トランクで許可されていることが想定されています。そのため、TLS を使用する場合、IME トランクの [SRTP を許可(SRTP Allowed)] をオンにする必要があります。適応型セキュリティ アプライアンスは、セキュア IME トランク コールの RTP への SRTP フォールバックをサポートします。

ëOíÒèšåè

ローカル Cisco UCM で、Cisco UCM 証明書をダウンロードします。詳細については、Cisco Unified Communications Manager の関連資料を参照してください。以下の手順のステップ 6 を実行するときに、この証明書が必要になります。

手順

ローカル環境内で TLS を設定するには、ローカルの適応型セキュリティ アプライアンスで以下の手順を実行します。

	コマンド	目的
ステップ 1	hostname(config)# **crypto key generate rsa label** *key-pair-label* hostname(config)# **crypto ca trustpoint** *trustpoint_name* hostname(config-ca-trustpoint)# **enroll self** hostname(config-ca-trustpoint)# **keypair** *keyname* hostname(config-ca-trustpoint)# **subject-name** *x.500_name* **例：** hostname(config)# crypto key generate rsa label local-ent-key hostname(config)# crypto ca trustpoint local-asa hostname(config-ca-trustpoint)# enroll self hostname(config-ca-trustpoint)# keypair key-local-asa hostname(config-ca-trustpoint)# subject-name *cn=Ent-local-domain-name***., o="Example Corp"	自己署名証明書の RSA キーおよびトラストポイントを作成します。 ここで、*key-pair-label* は、ローカル適応型セキュリティ アプライアンスの RSA キーです。 ここで、*trustpoint_name* は、ローカル適応型セキュリティ アプライアンスのトラストポイントです。 ここで、*keyname* は、ローカル適応型セキュリティ アプライアンスのキー ペアです。 ここで、*x.500_name* には、ローカル適応型セキュリティ アプライアンスの X.500 識別名が入ります。たとえば、*cn=Ent-local-domain-name*** となります。 **（注）** ここで入力するドメイン名は、ローカル Cisco UCM で設定したドメイン名と一致する必要があります。Cisco UCM のドメイン名の設定方法については、Cisco Unified Communications Manager の関連資料を参照してください。
ステップ 2	hostname(config-ca-trustpoint)# **exit**	トラストポイント コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 3	hostname(config)# **crypto ca export** *trustpoint* **identity-certificate** **例：** hostname(config)# crypto ca export local-asa identity-certificate	ステップ 1 で作成した証明書をエクスポートします。証明書の内容は、ターミナルの画面に表示されます。 ターミナルの画面から証明書をコピーします。この証明書によって、Cisco UCM は、TLS ハンドシェイクで適応型セキュリティ アプライアンスが送信する証明書を検証できます。 ローカル Cisco UCM で、証明書を Cisco UCM トラスト ストアにアップロードします。詳細については、Cisco Unified Communications Manager の関連資料を参照してください。 **（注）** ローカル Cisco UCM に証明書をアップロードする際に入力した件名は、Cisco UCM 上の SIP トランク セキュリティ プロファイルで入力された [X.509 件名 (X.509 Subject Name)] フィールドと比較されます。たとえば、このタスクのステップ 1 で、「Ent-local-domain-name」と入力した場合、Cisco UCM 設定でも「Ent-local-domain-name」と入力する必要があります。
ステップ 4	hostname(config)# **crypto ca trustpoint** *trustpoint_name* hostname(config-ca-trustpoint)# **enroll terminal** **例：** hostname(config)# crypto ca trustpoint local-ent-ucm hostname(config-ca-trustpoint)# enroll terminal	ローカル Cisco UCM のトラストポイントを作成します。 ここで、*trustpoint_name* は、ローカル Cisco UCM のトラストポイントです。
ステップ 5	hostname(config-ca-trustpoint)# **exit**	トラストポイント コンフィギュレーション モードを終了します。
ステップ 6	hostname(config)# **crypto ca authenticate** *trustpoint* **例：** hostname(config)# crypto ca authenticate local-ent-ucm	ローカル Cisco UCM から証明書をインポートします。 ここで、*trustpoint* は、ローカル Cisco UCM のトラストポイントです。 ローカル Cisco UCM からダウンロードした証明書を貼り付けます。この証明書によって、適応型セキュリティ アプライアンスは、TLS ハンドシェイクで Cisco UCM が送信する証明書を検証できます。

	コマンド	目的
ステップ 7	hostname(config)# **tls-proxy** *proxy_name* hostname(config-tlsp)# **server trust-point** *proxy_trustpoint* hostname(config-tlsp)# **client trust-point** *proxy_trustpoint* hostname(config-tlsp)# **client cipher-suite** aes128-sha1 aes256-sha1 3des-sha1 null-sha1 **例：** hostname(config)# tls-proxy local_to_remote-ent hostname(config-tlsp)# server trust-point local-ent-ucm hostname(config-tlsp)# client trust-point local-ent hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1	**outbound** 接続の TLS プロキシを更新します。 ここで、*proxy_name* は、タスク TLS プロキシの作成のステップ 1 で入力した名前です。 ここで、**server trust-point** コマンドの *proxy_trustpoint* は、この手順のステップ 4 で入力した名前です。 ここで、**client trust-point** コマンドの *proxy_trustpoint* は、タスクトラストポイントの作成および証明書の生成のステップ 2 で入力した名前です。 **（注）** この手順では、クライアントとサーバの異なるトラストポイントを作成しています。
ステップ 8	hostname(config-tlsp)# **exit**	TLS プロキシ コンフィギュレーション モードを終了します。
ステップ 9	hostname(config)# **tls-proxy** proxy_name hostname(config-tlsp)# **server trust-point** *proxy_trustpoint* hostname(config-tlsp)# **client trust-point** *proxy_trustpoint* hostname(config-tlsp)# **client cipher-suite** aes128-sha1 aes256-sha1 3des-sha1 null-sha1 **例：** hostname(config)# tls-proxy remote_to_local-ent hostname(config-tlsp)# server trust-point local-ent hostname(config-tlsp)# client trust-point local-ent-ucm hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1	**インバウンド**接続用の TLS プロキシを更新します。 ここで、*proxy_name* は、タスク TLS プロキシの作成のステップ 5 で入力した名前です。 ここで、**server trust-point** コマンドの *proxy_trustpoint* は、タスクトラストポイントの作成および証明書の生成のステップ 2 で入力した名前です。 ここで、**client trust-point** コマンドの *proxy_trustpoint* は、この手順のステップ 4 で入力した名前です。
ステップ 10	hostname(config-tlsp)# **exit**	TLS プロキシ コンフィギュレーション モードを終了します。
ステップ 11	hostname(config)# **uc-ime** *uc_ime_name* hostname(config-uc-ime)# **ucm address** *ip_address* **trunk-security-mode secure** **例：** hostname(config)# uc-ime local-ent-ime hostname(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode secure	トランク セキュリティ モードの Cisco Intercompany Media Engine プロキシを更新します。 ここで、*uc_ime_name* は、タスク Cisco Intercompany Media Engine プロキシの作成のステップ 1 で入力した名前です。 タスク Cisco Intercompany Media Engine プロキシの作成のステップ 3 で非セキュアを入力した場合、この手順のみを実行します。

次のタスクの内容

環境内の TLS を設定したので、必要に応じて、オフパス配置のオフパス シグナリングを設定します。「（オプション）オフパス シグナリングの設定」（P.4-24）を参照してください。

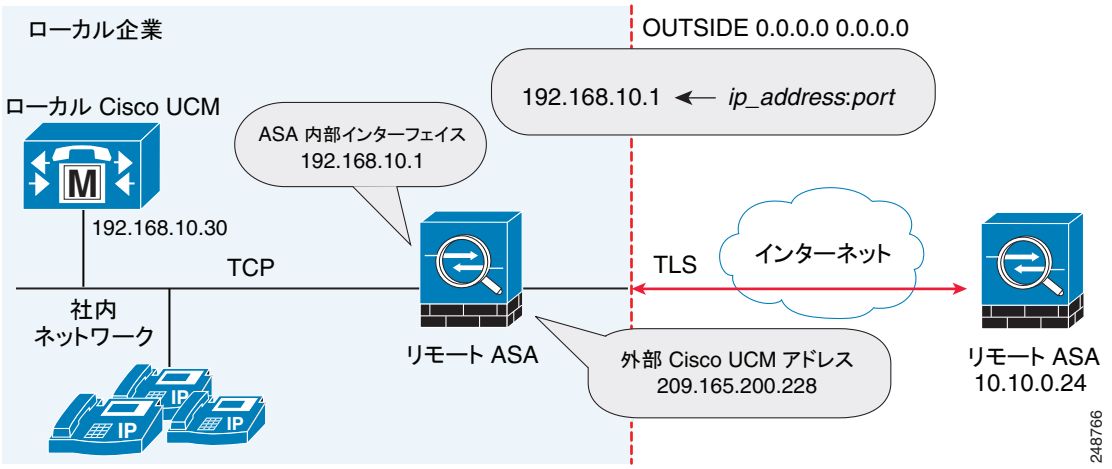
（オプション）オフパス シグナリングの設定

オフパス配置の一部として、Cisco Intercompany Media Engine プロキシを設定しているときのみ、このタスクを実行します。Cisco Intercompany Media Engine を使用したいものの、既存のインターネット ファイアウォールを Cisco Intercompany Media プロキシで有効化された適応型セキュリティ アプライアンス で置き換えたくないときに、オフパス配置を選択できます。

オフパス配置でご使用の環境に配置している既存のファイアウォールは、Cisco Intercompany Media Engine トラフィックを送信できません。

オフパス シグナリングでは、外部 IP アドレスを内部 IP アドレスに変換する必要があります。内部インターフェイス アドレスは、このマッピング サービス設定に使用されます。Cisco Intercompany Media Engine プロキシでは、適応型セキュリティ アプライアンスが、外部アドレスの内部 IP アドレスへのダイナミック マッピングを作成します。そのため、アウトバウンド コールでダイナミック NAT 設定を使用する際、Cisco UCM は SIP トラフィックをこの内部 IP アドレスに送信し、適応型セキュリティ アプライアンスがこのマッピングを使用して、インバウンド コールでの実際の宛先を識別します。オフパス設定のインバウンド コールでは、スタティック NAT または PAT マッピングが使用されます。

図 4-4　　オフパス配置でのオフパス シグナリングの設定例



オフパス シグナリングを設定した後、適応型セキュリティ アプライアンス マッピング サービスはインターフェイス「inside」で要求を受信します。このサービスが要求を受信すると、宛先インターフェイスとして「outside」のダイナミック マッピングを作成します。

Cisco Intercompany Media Engine プロキシのオフパス シグナリングを設定するには、以下の手順を実行します。

	コマンド	目的

ステップ 1	`hostname(config)# object network name`
	例：
	`hostname(config)# object network outside-any`
		オフパス適応型セキュリティ アプライアンスでは、すべての外部アドレスを表すネットワーク オブジェクトを作成します。

ステップ 2	`hostname(config-network-object)# subnet ip_address`
	例：
	`hostname(config-network-object)# subnet 0.0.0.0 0.0.0.0`
		サブネットの IP アドレスを指定します。

ステップ 3	`hostname(config-network-object)# nat (outside,inside) dynamic interface inside`	リモート環境の Cisco UCM のマッピングを作成します。

	コマンド	目的
ステップ 4	`hostname(config-network-object)# exit`	オブジェクト コンフィギュレーション モードを終了します。

ステップ 5	`hostname(config)# uc-ime uc_ime_name`
	例：
	`hostname(config)# uc-ime local-ent-ime`
		タスク「Cisco Intercompany Media Engine プロキシの作成」（P.4-11）で作成した Cisco Intercompany Media Engine プロキシを指定します。
		ここで、*uc_ime_name* は、「Cisco Intercompany Media Engine プロキシの作成」（P.4-11）のステップ 1 で指定した名前です。

ステップ 6	`hostname(config)# mapping-service listening-interface interface_name [listening-port port] uc-ime-interface uc-ime-interface_name`
	例：
	`hostname(config-uc-ime)# mapping-service listening-interface inside listening-port 8060 uc-ime-interface outside`
		オフパス適応型セキュリティ アプライアンスの場合、マッピング サービスを Cisco Intercompany Media Engine プロキシに追加します。
		適応型セキュリティ アプライアンス マッピング サービスのインターフェイスおよびリスニング ポートを指定します。
		Cisco Intercompany Media Engine プロキシのために設定できるマッピング サーバは 1 つだけです。
		ここで、*interface_name* は、適応型セキュリティ アプライアンスがマッピング要求を受信するインターフェイスの名前です。
		ここで、port は、適応型セキュリティ アプライアンスがマッピング要求を受信する TCP ポートです。デバイス上のその他のサービス（Telnet または SSH など）との競合を避けるため、1024 ～ 65535 の間のポート番号を指定する必要があります。デフォルトでは、ポート番号は TCP 8060 です。
		ここで、*uc-ime-interface_name* は、リモート Cisco UCM に接続するインターフェイスの名前です。

ASDM を使用したプロキシ設定

この項では、次の内容で構成されています。

- 「UC-IME プロキシ ペインを使用した Cisco UC-IMC プロキシの設定」（P.4-25）
- 「ユニファイド コミュニケーション ウィザードを使用した Cisco UC-IMC プロキシの設定」（P.4-28）

UC-IME プロキシ ペインを使用した Cisco UC-IMC プロキシの設定

[Cisco Intercompany Media Engine(UC-IME)プロキシの設定(Configure Cisco Intercompany Media Engine(UC-IME)proxy)] ペインを使用して、Cisco Intercompany Media Engine プロキシ インスタンスを追加または編集します。

（注）　Cisco Intercompany Media Engine プロキシは、このプロキシに必要なライセンスが適応型セキュリティ アプライアンスにインストールされていない場合、[ナビゲーション(Navigation)] ペインの [ユニファイドコミュニケーション(Unified Communications)] セクションの下にオプションとして表示されません。

このペインを使用してプロキシ インスタンスを作成しますが、UC-IME プロキシをフル機能で使用する場合、NAT ステートメント、アクセス リスト、および MTA の作成、証明書の設定、TLS プロキシの作成、SIP インスペクションの有効化など追加のタスクを完了する必要があります。

UC-IME プロキシがインターネット トラフィックのオフパスまたはインラインのどちらで配置されているかに応じて、Cisco UCM の組み込み NAT ステートメント、または PAT ステートメントを使用し、適切なネットワーク オブジェクトを作成する必要があります。

このペインは、[設定(Configuration)] > [ファイアウォール(Firewall)] > [ユニファイドコミュニケーション(Unified Communications)] > [UC-IMEプロキシ(UC-IME Proxy)] から使用できます。

ステップ 1　[設定(Configuration)] > [ファイアウォール(Firewall)] > [ユニファイドコミュニケーション(Unified Communications)] > [UC-IMEプロキシ(UC-IME Proxy)] からペインを開きます。

ステップ 2　[Cisco UC-IMEプロキシの有効化(Enable Cisco UC-IME proxy)] チェックボックスをオンにして、機能を有効にします。

ステップ 3　[Unified CMサーバ(Unified CM Servers)] 領域で、Cisco Unified Communications Manager（Cisco UCM）の IP アドレスまたはホスト名を入力するか、省略記号をクリックしてダイアログを開き、IP アドレスまたはホスト名を参照します。

ステップ 4　[トランクセキュリティモード(Trunk Security Mode)] フィールドで、セキュリティ オプショ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 クラスタは TLS を開始します。

ステップ 5　[追加(Add)] をクリックして、Cisco Intercompany Media Engine プロキシの Cisco UCM を追加します。SIP トランクが有効な Cisco Intercompany Media Engine を使用するクラスタ内の各 Cisco UCM にエントリを含める必要があります。

ステップ 6　[チケットエポック(Ticket Epoch)] フィールドに、1 ～ 255 の整数を入力します。

エポックには、パスワードが変更されるたびに更新される整数が入ります。プロキシを初めて設定し、パスワードを初めて入力するときに、エポックの整数として 1 を入力します。パスワードを変更するたびに、新しいパスワードを示すためにエポックを増やします。ユーザは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。

通常は、順番にエポックを増やしますが、適応型セキュリティ アプライアンスを使用すると、エポックを更新する際に任意の値を選択できます。

エポック値を変更する場合、現在のパスワードは無効となり、新規パスワードを入力する必要があります。

（注）　適応型セキュリティ アプライアンスのこのステップで設定するエポックおよびパスワードは、Cisco Intercompany Media Engine サーバで設定する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 サーバの関連資料を参照してください。

ステップ 7　[チケットパスワード(Ticket Password)] フィールドに、US-ASCII 文字セットから印刷可能な少なくとも 10 文字を入力します。使用可能な文字には、0x21 ～ 0x73 までが含まれ、スペース文字は除外されます。チケット パスワードには、最長 64 文字まで指定できます。入力したパスワードを確認します。同時に設定できるパスワードは 1 つだけです。

ステップ 8　[MTA を UC-IME Link プロキシに適用する (Apply MTA to UC-IME Link proxy)] チェックボックスをオンにし、メディア ターミネーション アドレスを Cisco Intercompany Media Engine プロキシと関連付けます。

（注）　このアドレスを Cisco Intercompany Media Engine プロキシと関連付ける前に、メディア ターミネーション インスタンスを作成する必要があります。必要に応じて、[MTA の構成 (Configure MTA)] ボタンをクリックして、メディア ターミネーション アドレス インスタンスを設定します。

ステップ 9　Cisco Intercompany Media Engine プロキシがオフパス配置の一部として設定されている場合、[オフパス アドレス マッピング サービスの有効化 (Enable off path address mapping service)] チェックボックスをオンにして、オフパス配置設定を行います。

a.　[リスニング インターフェイス (Listening Interface)] フィールドから適応型セキュリティ アプライアンスのインターフェイスを選択します。これは、適応型セキュリティ アプライアンスがマッピング要求を受信するインターフェイスです。

b.　[ポート (Port)] フィールドに、適応型セキュリティ アプライアンスがマッピング要求を受信する TCP ポートとして 1024 ～ 65535 までの間の数字を入力します。デバイス上のその他のサービス（Telnet または SSH など）との競合を避けるため、1024 以上のポート番号を指定する必要があります。デフォルトでは、ポート番号は TCP 8060 です。

c.　[UC-IME インターフェイス (UC-IME Interface)] フィールドで、リストからインターフェイスを選択します。これは、適応型セキュリティ アプライアンスがリモート Cisco UCM と接続するために使用するインターフェイスです。

（注）　オフパス配置で環境に配置している既存の適応型セキュリティ アプライアンスは、Cisco Intercompany Media Engine トラフィックを送信できません。オフパス シグナリングでは、外部アドレスを（NAT を使用して）内部 IP アドレスに変換する必要があります。内部インターフェイス アドレスは、このマッピング サービス設定に使用されます。Cisco Intercompany Media Engine プロキシでは、適応型セキュリティ アプライアンスが外部アドレスの内部 IP アドレスへのダイナミック マッピングを作成します。

ステップ 10　[フォールバック (Fallback)] 領域で、以下の設定を指定して、Cisco Intercompany Media Engine のフォールバック タイマーを設定します。

a.　[フォールバック重要度ファイル (Fallback Sensitivity File)] フィールドに、適応型セキュリティ アプライアンスが通話中 PSTN フォールバックに使用するフラッシュ メモリにあるファイルへのパスを入力します。入力するファイル名は .fbs ファイル拡張子を含むディスク上のファイルの名前である必要があります。または、[フラッシュの参照 (Browse Flash)] ボタンをクリックして、フラッシュ メモリからファイルを見つけて選択します。

b.　[コール音声品質評価の間隔 (Call Quality Evaluation Interval)] フィールドに、10 ～ 600 の間の数字（ミリ秒単位）を入力します。この数字は、適応型セキュリティ アプライアンスがインターネットから受信する RTP パケットをサンプリングする頻度を制御します。適応型セキュリティ アプライアンスは、このデータ サンプルを使用して、コールに対して PSTN へのフォールバックが必要であるかを判別します。デフォルトでは、タイマーの間隔は 100 ミリ秒です。

c.　[通知間隔 (Notification Interval)] フィールドに、10 ～ 360 の間の数字（秒単位）を入力します。この数字は、PSTN にフォールバックするかどうかを Cisco UCM に通知するまで、適応型セキュリティ アプライアンスが待機する時間を制御します。デフォルトでは、このタイマーの間隔は 20 秒です。

（注）　Cisco Intercompany Media Engine プロキシのフォールバック タイマーを変更すると、ASDM が自動で SIP インスペクションからプロキシを削除します。また、プロキシが再度有効化されるときに、SIP インスペクションが再適用されます。

ステップ 11　[適用(Apply)] をクリックして、Cisco Intercompany Media Engine プロキシの設定変更を保存します。

ユニファイド コミュニケーション ウィザードを使用した Cisco UC-IMC プロキシの設定

ASDM を使用して Cisco Intercompany Media Engine プロキシを設定するには、メニューから [ウィザード(Wizards)] > [ユニファイドコミュニケーションウィザード(Unified Communications Wizard)] を選択します。[ユニファイドコミュニケーションウィザード(Unified Communications Wizard)] が開きます。最初のページで、[企業間(Business-to-Business)] セクションの下の [Cisco Intercompany Media Engine プロキシ(Cisco Intercompany Media Engine Proxy)] オプションを選択します。

ウィザードにより必要な TLS プロキシが自動で作成されます。その後ウィザードに従って、Intercompany Media Engine プロキシを作成し、必要な証明書のインポートおよびインストールを行うと、Intercompany Media Engine トラフィックの SIP インスペクションが自動で有効になります。

ウィザードに従って以下のステップを実行し、Cisco Intercompany Media Engine プロキシを作成します。

ステップ 1　[Intercompany Media Engineプロキシ(Intercompany Media Engine Proxy)] オプションを選択します。

ステップ 2　Cisco Intercompany Media Engine プロキシのトポロジを選択します。つまり、適応型セキュリティ アプライアンスはエッジ ファイアウォールとなり、すべてのインターネット トラフィックを通過させるか、または適応型セキュリティ アプライアンスは主なインターネット トラフィックのオフパス（オフパス配置とも呼ばれます）となるかを選択します。

ステップ 3　Cisco UCM IP アドレスやチケット設定などプライベート ネットワーク設定を指定します。

ステップ 4　パブリック ネットワーク設定を指定します。

ステップ 5　Cisco UCM のメディア ターミネーション アドレスを指定します。

ステップ 6　ローカル側の証明書（つまり、ローカル Cisco Unified Communications Manager サーバと適応型セキュリティ アプライアンスとの間で交換される証明書）の管理を設定します。ウィザードがこのステップで生成する ID 証明書は、このプロキシを使用するクラスタ内の各 Cisco Unified Communications Manager（UCM）サーバにインストールする必要があります。また、Cisco UCM からの各 ID 証明書を適応型セキュリティ アプライアンスにインストールする必要があります。適応型セキュリティ アプライアンスおよび Cisco UCM は、TLS ハンドシェイク中にそれぞれが互いを認証するために、これらの証明書を使用します。ウィザードでは、このステップの自己署名証明書のみがサポートされています。

ステップ 7　リモート側の証明書（つまり、リモート サーバと適応型セキュリティ アプライアンスとの間で交換される証明書）の管理を設定します。このステップでは、ウィザードは Certificate Signing Request（CSR; 証明書署名要求）を生成します。プロキシの ID 証明書要求が正常に生成された後、ウィザードはファイルを保存するか確認するプロンプトを表示します。

CSR テキスト ファイルを Certificate Authority（CA; 認証局）に送信する（たとえば、テキスト ファイルを CA Web サイトの CSR 登録ページに貼り付ける）必要があります。CA から ID 証明書が送られてきたら、その証明書を適応型セキュリティ アプライアンスにインストールする必要があります。この証明書は、リモート サーバが適応型セキュリティ アプライアンスを信頼できるサーバとして認証で

きるように、リモート サーバに提示されます。

最後に、ウィザードのこのステップに従って、適応型セキュリティ アプライアンスが、信頼できるリモート サーバであると判別できるように、リモート サーバからの CA のルート証明書をインストールします。

ウィザードは、Cisco Intercompany Media Engine 用に作成された設定の概要を表示して完了します。詳細については、このマニュアルのユニファイド コミュニケーション ウィザードに関するセクションを参照してください。