Cisco Intercompany Media Engine

Cisco Intercompany Media Engine（Cisco IME）は、ピアツーピア技術を既存の公衆電話交換網（PSTN）インフラストラクチャと結合することで、企業間に直接 IP 接続を確立できる技術です。 Cisco IME を使用すると、Cisco Unified Communications Manager をすでに導入している企業は、エンタープライズ間にダイナミックな Session Initiation Protocol（SIP）トランクを作成し、PSTN ではなくインターネット経由でセキュアに通信を行うことができるようになります。インターネットを経由するエンタープライズ外のトラフィックを有効にすることで、Cisco IME はビデオ可能なコール、ワイドバンド オーディオのサポート、リッチ発信者 ID、プレゼンスといった、これまではエンタープライズ内でだけ動作していた機能を外部コールにも拡張します。

Cisco IME によって、コンサルタント、製造業者、供給業者、外部委託業者、販売業者、サプライ チェーン パートナーといったビジネスに欠かせない外部パートナーとの、もっと効果的な通信が実現します。

- 機能と利点，1 ページ
- IME の動作，2 ページ
- コンポーネント，6 ページ
- 配置モデル，8 ページ

機能と利点

Cisco Intercompany Media Engine（Cisco IME）は、事業者間にダイナミック SIP トランクを徐々に作成して、協働する一群のエンタープライズを、エンタープライズ間にクラスタ間トランクを持つ 1 つの大きな事業者と見なせるようにします。 Cisco IME によって、必要に応じて会社間でインターネットを介して相互接続できるようになります。 この機能は、お客様にとって重要な特徴を数多く有しています。

- 電話番号で使用可能：Cisco IME は、お客様がお持ちの電話番号で使用できます。 Cisco IME では、お客様が新しい番号を覚える必要も、プロバイダーを変更する必要もありません。

- 既存の電話機と使用可能：Cisco IME は、エンタープライズ内の既存の電話機とともに使用できます。 さらに機能が豊富な電話機を必要としないのであれば、電話機の変更は必要ありません。
- 新規サービスの購入が不要：Cisco IME なら、サービス プロバイダーから新しいサービスを購入する必要は何もありません。 現在の PSTN とインターネット接続を継続使用できます。 Cisco IME は、コールを徐々に PSTN からインターネットに移していきます。
- ユニファイド コミュニケーションを全面体験：Cisco IME は事業者間にクラスタ間 SIP トランクを作成するため、SIP トランク経由で動作し SIP トランクだけを必要とする機能であれば、すべて事業者間でも動作するようになります。
- インターネットで動作：Cisco IME では、インターネットや管理対象の外部ネットを介してコールを送信できます。
- 世界中に到達可能：Cisco IME なら、Cisco IME テクノロジーが運用されているエンタープライズであれば、世界のどのエンタープライズにも接続できます。
- 高い拡張性：Cisco IME では、連繋できるエンタープライズの数に制限がありません。
- 自己学習性：ご自分のネットワークの情報を設定した後は、他の事業者への IP ルートを Cisco IME が自動的に学習します。 他の事業者の電話プレフィックス、IP アドレス、ポート、ドメイン名、証明書といった情報を入力する必要はまったくありません。
- QoS 管理：Cisco IME には、インターネット接続のサービス品質（QoS）管理に役立つ機能が準備されています。 Cisco IME はリアルタイム転送プロトコル（RTP）トラフィックの QoS をリアルタイムに監視し、問題が発生すると自動的に PSTN にフォールバックします。

IME の動作

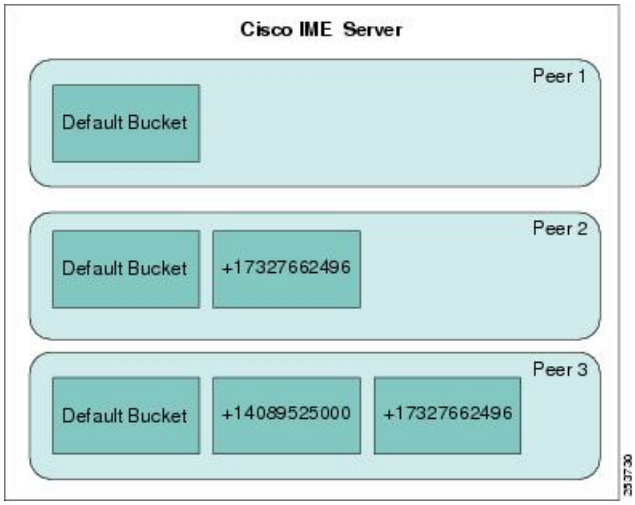
Cisco Intercompany Media Engine（Cisco IME）を使用すると、Cisco Unified Communications Manager をすでに配置している企業は、エンタープライズ間にダイナミック SIP トランクを作成し、PSTN ではなくインターネット経由で通信を行えるようになります。

Cisco IME を使用するには、Cisco IME ソリューションを導入する必要があります。これには、Cisco IME に参加させる Cisco Unified Communications Manager でダイヤル イン（DID）番号を設定することが含まれます。 Cisco Unified Communications Manager はこれらの番号を Cisco IME サーバにパブリッシュし、このサーバが今度は番号を IME 分散キャッシュ リング内のサーバにパブリッシュします。 Cisco IME（ピア）サーバはすべて、暗号化形式で IME 分散キャッシュ リングに参加し、データを保存します。

（注） Cisco IME では、ユーザのダイヤルする番号を、システムが国際番号の + プレフィックスを含む E.164 形式の番号（+14085551212 など）に変更することが要求されています。 この形式のことを、本マニュアル中では E.164 形式と呼びます。

以下の図は IME 分散キャッシュ リングを説明しています。

図 *1*：*IME* 分散キャッシュ リング



IME 分散キャッシュ リングに格納された番号を持つ別のエンタープライズとインターネットを介して通信するには、最初に公衆電話交換網（PSTN）コールの設定可能な番号を、そのエンタープライズ内の番号として完成させる必要があります。 PSTN コールの終了後、コール当事者のエンタープライズは、コールについての情報を音声コール レコード（VCR）で Cisco IME サーバに送ります。 VCR では、コールについて、開始時間、停止時間、着信側番号、発呼側番号といった情報が示されます。 検証プロセスが始まります。 発信側の Cisco IME サーバは、ダイヤルされた番号の所有者とされるエンタープライズの特定を試み、着信側エンタープライズが実際にその電話番号を所有しているどうかを検証するプロセスを開始します。 着信側では、このドメイン名がブラックリスト ドメインのセットに含まれていないことを検証します。

検証が完了すると、発信側 Cisco IME サーバは Cisco Unified Communications Manager サーバにメッセージを送信し、この番号の VoIP ルートを提供します。 発信側 Cisco Unified Communications Manager はルートを学習し、今後の使用のためデータベース内にルートと検証チケットを保存します。 このチケットは、宛先エンタープライズの特定の電話番号へのコールの権限がエンタープライズに与えられていることを示します。 ルートとチケットの有効期限は 1 年間です。 ユーザが次に発信側エンタープライズのいずれかの番号から同じ番号へコールを発信するときには、コールはダイナミック SIP トランクによりインターネットを介して送信されます。 このコールが着信側エンタープライズの Cisco Intercompany Media Engine 有効 ASA に到達すると、Cisco Intercompany Media Engine 有効 ASA は SIP メッセージに含まれるチケットを検証します。 チケット内のドメインは発信側エンタープライズのドメインと、着信者番号はチケットが許可した番号とそれぞれ一致している必要があります。

Cisco IME は、有効なルートだけが Cisco Unified Communications Manager に送られるようにするためのセキュリティと、インターネット接続の品質低下時に QoS を維持するための手段を備えています。 これらの機能の詳細については、次の項を参照してください。

- 検証ルール，（4 ページ）
- PSTN フォールバック，（5 ページ）

検証ルール

Cisco Unified Communications Manager サーバのセキュリティを確保するため、Cisco Intercompany Media Engine（Cisco IME）機能は検証ルールのセットを適用し、有効なルートだけが Cisco Unified Communications Manager に送られるようにします。

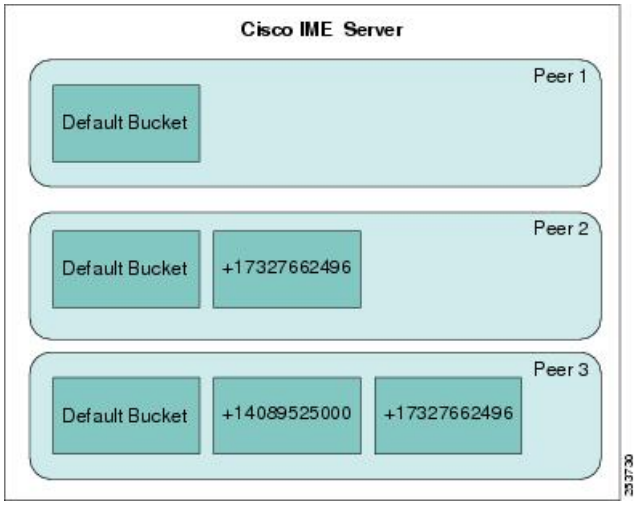
次のリストに、検証基準の要約を示します。

- Cisco Unified Communications Manager が、学習したルートを Cisco IME サーバから受信する前に満たす必要がある、指定のエンタープライズ（または Cisco IME サーバ）の所有する DID に対する検証の連続成功回数。 デフォルトでは、Cisco Intercompany Media Engine は 3 回の検証を要求します。 検証は、異なる接続先番号に対するものでもかまいません。 検証に 3 回連続して成功すると、Cisco IME サーバは学習した 3 ルートすべてを Cisco Unified Communications Manager に送ります。 セキュリティ要求事項に応じて、Cisco Unified Communications Manager がルートを学習するまでに必要な検証成功回数を増減できます。
- 特定の番号に対する検証が失敗した場合、システムでは、Cisco IME が学習したルートを Cisco Unified Communications Manager に送る前に、当該番号に対する検証が連続して成功することが要求されます。
- 音声コール レコード（VCR）が相関しないようにするため、Cisco Unified Communications Manager が 1 時間以内に発生した 2 つの同一番号の VCR を検証することはありません。 セキュリティ要求事項に応じ、同一番号への検証試行の最小間隔を設定できます。

検証結果を追跡するために、Cisco IME サーバはプールを使用します。プールは特定の Cisco IME（またはピア）と関連付けられたバケットの集合です。 デフォルト バケットは Cisco IME サーバに対する検証成功を追跡し、番号特定バケットは同一 DID に対する検証成功を追跡します。

以下の図に、3 つの異なるピアのプールを持つ Cisco IME サーバの例を示します。

図 *2*：プールとバケット



この例では、各プールにデフォルト バケットが含まれています。 ピア 2 には、+17327662496 の番号特定バケットも含まれています。 ピア 3 には、+1408952500 および +17327662496 という 2 つの番号特定バケットが含まれています。 番号 +17327662496 が 2 つの異なる Cisco IME サーバ（またはピア）に存在するため、この番号の番号特定バケットが2つの異なるプールに存在しますが、これらのバケットは相関していません。

それぞれのバケットに、検証成功の結果が保持されています。 特定のピアに対する検証が成功すると、Cisco IME は、検証された番号に一致する番号特定バケットが存在する場合そのバケットに、存在しない場合はデフォルトバケットに検証結果を置きます。 各検証結果はまた、Cisco IME サーバがコールの検証に使用した方法に応じて、特定の値と関連付けられます。 検証結果がバケットに入れられると、バケットの値が検証結果の値（8 または 12）だけ増加します。

各バケットにはしきい値が設定されています。 設定されたしきい値は、デフォルトバケットと番号特定バケットの両方に適用されます。 バケットの検証結果の値がしきい値を超えると、バケット内の検証結果は削除され（空にされ）、結果は Cisco Unified Communications Manager に送られます。

（注） Cisco IME サーバ上のバケットのしきい値は、set ime validator local bucketentropy CLI コマンドで変更できます。

あるピアへの検証が失敗すると、Cisco IME はそのピアに対応するプール内のバケットすべてを空にし、プールに宛先番号の番号特定バケットを作成します（存在しない場合）。 検証失敗後にピアがルート学習を行うためには、同一番号への検証実行が連続して成功する必要があります。

番号特定バケットは、ペナルティ ボックスを表します。いつでも検証結果が成功するピアには番号特定バケットが作成されず、ピアは異なる番号に対する検証が設定された回数連続して成功した後にルートを学習します。 検証に失敗したピアは番号特定バケットを持つようになり、同一番号に対する検証が設定された回数連続して成功する必要があります。

PSTN フォールバック

Cisco IME 機能は、許容レベルを下回るほどサービス品質（QoS）が低下した場合に、コールを PSTN にフォールバックするメカニズムを提供します。 発信側と着信側の Cisco Intercompany Media Engine 有効 ASA は、トラフィックの品質を監視します。 見つかったロスとジッターのプロパティをもとに、Cisco Intercompany Media Engine 有効 ASA はコールを PSTN にフォールバックさせる必要があるかを判定します。 音声コールは PSTN 上で継続され、コールへの影響やユーザへのアラートは発生しません。

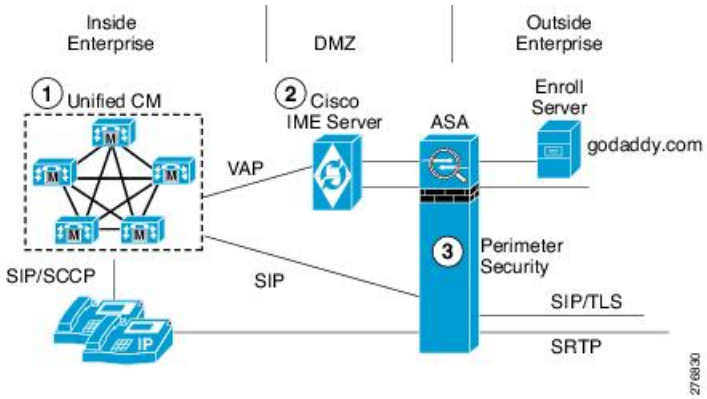
PSTN にフォールバックが必要なコールについては、発信側 Cisco Unified Communications Manager が Cisco IME コールが有効なうちに PSTN コールをセットアップします。 Cisco Unified Communications Manager が PSTN コールを確立すると、Cisco Unified Communications Manager は Internet/RTP ストリームをインターネットから PSTN にシームレスに切り替えます。 ビデオなどの拡張機能はすべて失われますが、コールの音声部分はそのまま残ります。

コンポーネント

Cisco Intercompany Media Engine（Cisco IME）ソリューションは、IME ルートの動的学習と、組織間でのコール シグナリングおよびメディアの安全な暗号化を実現する複数のコンポーネントで構成されています。 コンポーネントには Cisco IME サーバ、Cisco Unified Communications Manager サーバ、Cisco Intercompany Media Engine 有効 ASA、GoDaddy.com Web サイトからの証明書などがあります。 Cisco IME サーバは加入者宅内の非武装地帯（DMZ）に存在し、自動化されたプロビジョニング サービスとして機能します。 サーバは特定の電話番号への VoIP（または Cisco IME）ルートを学習し、ルートを Cisco Unified Communications Manager にプッシュします。 Cisco Unified Communications Manager サーバは Validation Access Protocol（VAP）という独自のプロトコルによって Cisco IME サーバに接続します。 Cisco Unified Communications Manager は、コール処理機能すべてを標準の Cisco Unified Communications Manager 導入として実行します。 Cisco Intercompany Media Engine 有効 ASA は、Cisco Intercompany Media Engine ソリューションに周辺のセキュリティを提供します。 GoDaddy.com Web サイトでは、Cisco IME サーバのリングが作成するピアツーピア ネットワークへの参加に必要な証明書を取得できます。

次の図に、Cisco Intercompany Media Engine ネットワークのコンポーネントを示します。

図 *3*：*Cisco Intercompany Media Engine* コンポーネント



以降の項で、Cisco IME の各コンポーネントについて詳しく説明します。

Cisco Intercompany Media Engine（ピア）サーバ

DMZ 内に位置する Cisco IME サーバは、Validation Access Protocol（VAP）によって Cisco Unified Communications Manager サーバと通信し、他の Cisco IME サーバとはインターネットを介して通信します。 Cisco IME サーバは協働して、公衆インターネット経由の IME 分散キャッシュ リングを作成するピアツーピア ネットワークを形成します。

IME 分散キャッシュ リング内の各 Cisco IME サーバは、リングが所有するデータの一部を格納します。 データは暗号化され、データを格納する Cisco IME サーバが内容を読み取れないようになっています。 リング上の各 Cisco IME が、データをリングに格納し、リングからデータを取得することが可能です。 リングに格納されるダイヤルイン（DID）番号は、DHT に格納される前に一方向ハッシュされます。 Cisco IME サーバはコール制御を行いません。 Cisco IME サーバはダイヤ

ルイン（DID）番号を IME 分散キャッシュ リングに格納し、リングから Cisco Intercompany Media Engine に提供されるリモート DID へのルートを学習します。

Cisco IME のローカル管理とメンテナンスは、コマンド ライン インターフェイス（CLI）を通じて行います。

Cisco Intercompany Media Engine（ブートストラップ）サーバ

Cisco IME の動作は、シスコが管理する一群のブートストラップ サーバに依存します。 ブートストラップ サーバは、どのピア サーバが IME 分散キャッシュ リングに加われるかを決定します。 ブートストラップ サーバは設定情報を配布します。 シスコがブートストラップ サーバ上で設定変更を行うと、変更はリング全体に伝搬され、他のすべてのノードの設定が更新されます。

Cisco Unified Communications Manager

Cisco Unified Communications Manager は Cisco IME サーバから学習した VoIP ルートを格納し、Cisco IME ソリューションのコール処理機能すべてを提供します。 Cisco Unified Communications Manager の管理ページは Cisco Unified Communications Manager で Cisco IME 機能を使用するためのプロビジョニングを助けます。 Cisco Unified Communications Manager の管理ページでは、Cisco IME サーバ、Cisco IME の使用を許可する電話番号、信頼するドメインなどを指定します。 パラメータを指定して、コール品質が許容レベル以下になった場合に Cisco IME コールを公衆電話交換網（PSTN）にフォールバックさせることも可能です。

ASA

Cisco Intercompany Media Engine 対応の適応型セキュリティ アプライアンス（ASA）は Cisco IME ソリューションのセキュリティの中核を担います。 Cisco Intercompany Media Engine 有効 ASA は、コール制御とメディアのインターフェイスをセキュアにします。 Cisco Intercompany Media Engine プロキシと同時に使用することで、ASA は周辺のセキュリティ機能を提供し、SIP トランク間の SIP シグナリングを検査します。 Cisco Intercompany Media Engine 有効 ASA は、具体的には次の機能を実行します。

- SIP アプリケーション レベル ゲートウェイ（ALG）：Cisco Intercompany Media Engine 有効 ASA を通過する SIP シグナリング メッセージを検査します。 Cisco Intercompany Media Engine 有効 ASA は、SDP とさまざまな SIP ヘッダー フィールドを適用して、ネットワーク アドレス変換（NAT）が有効なケースを扱います。 SIP ALG はまた、メディア ストリームのためのピンホールを空けて（またはバインドを作成して）、メディアのフローの Cisco Intercompany Media Engine 対応 ASA への出入りを可能にします。
- SIP メッセージ検証：SIP メッセージが Cisco Unified Communications Manager やネットワーク内の他のコンポーネントをクラッシュさせないようにします。 Cisco Intercompany Media Engine 有効 ASA は、Uniform Resource Identifier（URI）を許可するキー ヘッダー フィールドを解析し、検証します。 Cisco Intercompany Media Engine 有効 ASA は、SIP ステート ダイアグラムに準拠していないメッセージをブロックします。
- SIP から SIP/TLS へ：Cisco Unified Communications Manager がセキュア モードでない場合に、インターネットへの SIP/TLS 接続を終了し、Cisco Unified Communications Manager への TCP だけの接続を再度開始します。 Cisco Unified Communications Manager がセキュア モードの場合、Cisco Intercompany Media Engine 有効 ASA は Cisco Unified Communications Manager への TLS 接続を開始します。 Cisco Intercompany Media Engine 有効 ASA は TLS プロキシとして動作するようになり、Cisco Unified Communications Manager で SIP メッセージの参照や処理が

行えるようになります。 Cisco Intercompany Media Engine 有効 ASA は、既知の認証局（CA）に対して遠端側エンタープライズから発行された証明書を検証します。

- NAT：ASA は、インターネットとの使用でしばしば必要となる NAT と SIP ALG の機能を提供します。
- RTP/SRTP：SRTP キーを作成し、コールの他端に送られる暗号化シグナリングを含めることで、Cisco Intercompany Media Engine 有効 ASA の内側の RTP を、Cisco Intercompany Media Engine 有効 ASA のインターネット側 SRTP に変換します。
- チケットの検証：Cisco IME チケットのヘッダーを検査し、Cisco Unified Communications Manager へのシグナリングすべてがチケット内の情報に基づいて許可されていることを確認します。 Cisco Intercompany Media Engine 有効 ASA は、有効なチケットのない要求すべてを拒否します。
- RTP のモニタリング：RTP ストリームのサービス品質（QoS）を監視します。

システムを設定することで、Cisco IME トラフィックは Cisco Intercompany Media Engine 有効 ASA を経由して送信し、他の企業トラフィックは既存の ASA を経由して送信するようにできます。詳細については、配置モデル, （8 ページ）を参照してください。

登録サーバ（GoDaddy.com）

GoDaddy.com は Cisco Intercompany Media Engine（Cisco IME）サーバが Cisco IME ピアツーピアネットワークに参加できるようにするための証明書を提供します。 ライセンスを購入して Cisco IME サーバにインストールした後、GoDaddy.com の Web サイトで Cisco IME 証明書を購入します。 証明書購入プロセスでは、GoDaddy で Cisco IME を一意で識別するために Cisco IME サーバ ID を提供する必要があります。 GoDaddy がサーバを有効と判定した場合、GoDaddy は Cisco IME サーバの証明書を返します。 証明書によって、分散キャッシュ リングを形成する Cisco IME サーバ間の TLS 接続が可能になります。

配置モデル

この項では、Cisco Intercompany Media Engine で利用可能な配置モデルについて説明します。

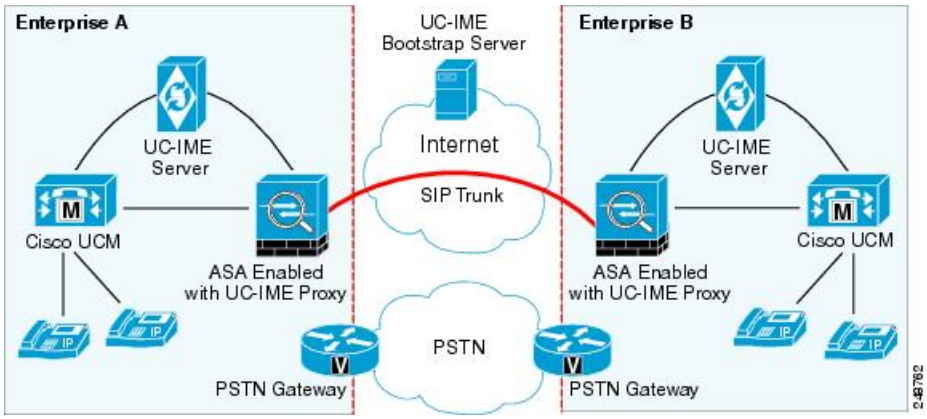
- 基本配置, （8 ページ）
- オフパス配置, （9 ページ）

基本配置

基本配置では、Cisco Intercompany Media Engine プロキシはインターネット ファイアウォールとインラインに存在するため、すべてのインターネット トラフィックが適応型セキュリティ アプライアンス（ASA）を通過します。 この配置では、Cisco Intercompany Media Engine（Cisco IME）サーバとともに、単一の Cisco Unified Communications Manager または Cisco Unified Communications Manager クラスタが、エンタープライズ内部の中心に配置されます。 単一のインターネット接続が、Cisco Intercompany Media Engine プロキシが有効な ASA を通過します。

次の図に示すとおり、ASA はエンタープライズのエッジに位置し、エンタープライズ間にダイナミック SIP トランクを作成することで SIP シグナリングを検査します。

図 *4*：基本配置モデル



オフパス配置

企業ネットワーク間で 2 層のファイアウォールを使用する典型的な大規模ネットワークでは、既存のインターネット ファイアウォールを Cisco Intercompany Media Engine 有効 ASA に置き換える（またはアップグレードする）ことや、Cisco Intercompany Media Engine 有効 ASA をインターネットファイアウォールとインラインに追加するように既存のセキュリティアーキテクチャを変更することが難しい場合があります。 この問題を解決するため、シスコでは Cisco Intercompany Media Engine のオフパス ASA モデルを許容しています。

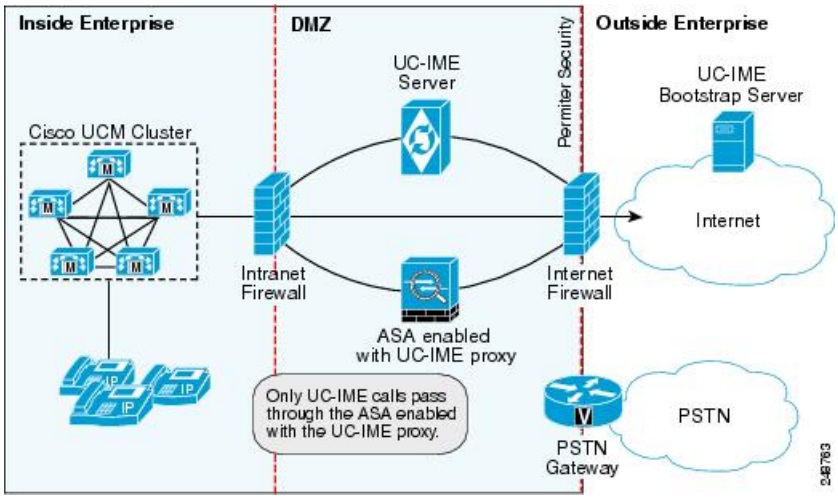
オフパス配置では、Cisco Intercompany Media Engine コールの発着信は、Cisco Intercompany Media Engine プロキシが有効な適応型セキュリティ アプライアンス（ASA）をパススルーします。 DMZ 内の ASA は、主に Cisco Intercompany Media Engine のサポート提供用として設定します。 通常のインターネット向けトラフィックがこの ASA を流れることはありません。

着信コールはすべて、シグナリングが直接 ASA に転送されます。宛先 Cisco Unified Communications Manager が ASA 上のグローバル IP アドレスに設定されているからです。 発信コールでは、着信側にインターネット上のどの IP アドレスでも指定できます。このため、ASA は、インターネット上の着信側の各グローバル IP アドレスに対し、ダイナミックに ASA 上の内部 IP アドレスを提供するマッピング サービスによって設定されます。

Cisco Unified Communications Manager は、発信コールすべてを、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、マッピングされた ASA 上の内部 IP アドレスに直接送ります。 その後、ASA がコールを着信側のグローバル IP アドレスに転送します。

次の図は、オフパス配置での Cisco Intercompany Media Engine のアーキテクチャを示しています。

図 *5* : オフパス配置モデル



オフパス配置では、Cisco IME トランクを持つ Cisco Unified Communications Manager サーバが、Cisco IME 配置をサポートする ASA への TCP 接続を開くことが必要です。 この接続は、1024 ～ 65535 からランダムに選択されるポートに存在します。 Cisco Unified Communications Manager サーバと、Cisco IME をサポートする ASA との間に何らかのファイアウォールが存在する場合、そのファイアウォールでこのポート範囲を開いておくことが必要です。

次の例に、サンプル ACL エントリを示します。

access-list SAMPLE extended permit tcp object-group CUCM object-group IME-ASA range 1024 65535