CHAPTER 18

Cisco Mobility Advantage の設定

この章では、Cisco Unified Communications Mobility Advantage Proxy 機能向けに ASA を設定する方法について説明します。

この章の内容は、次のとおりです。

Cisco Mobility Advantage Proxy 機能に関する情報

ここでは、次の内容について説明します。

Cisco Mobility Advantage Proxy 機能

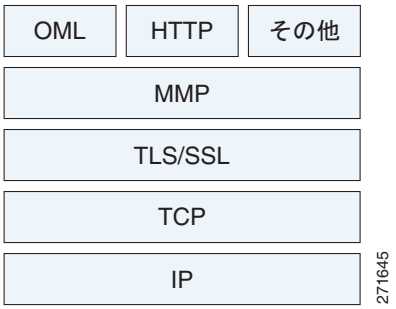
Cisco Mobility Advantage ソリューション向けの Cisco UMA をサポートするため、Mobility Advantage Proxy（TLS プロキシとして実装）には次の機能が含まれます。

- クライアントとのハンドシェイク中にクライアントの認証を許可しない機能
- サーバにインポートされた PKCS-12 証明書をプロキシの証明書として許可する機能

ASA には、Cisco UMA Mobile Multiplexing Protocol（MMP; モバイル多重化プロトコル）を検証するためのインスペクション エンジンが含まれます。

MMP は、Cisco UMA クライアントとサーバとの間でデータ エントリを送信するための転送プロトコルです。図 18-1 に示すように、MMP はコネクション型プロトコル（基礎となる転送）の上で実行する必要があり、TLS などのセキュアな転送プロトコルの上で実行することを意図しています。Orative Markup Language（OML）プロトコルは、データの同期を目的とした MMP に加えて、大規模なファイルのアップロードとダウンロードのための HTTP プロトコルの上で実行することを意図しています。

図 18-1　MMP スタック



TCP/TLS のデフォルト ポートは 5443 です。埋め込まれた NAT やセカンダリ接続はありません。

Cisco UMA クライアントおよびサーバ通信は TLS を通じてプロキシ処理ができます。ここで、データを復号化してインスペクション MMP モジュールに渡し、エンドポイントに転送する前にデータを再暗号化します。インスペクション MMP モジュールは MMP ヘッダーの整合性を確認し、OML/HTTP を適切なハンドラに渡します。ASA は、MMP ヘッダーおよびデータで次のアクションを実行します。

- クライアント MMP ヘッダーの形式が適切であることを確認します。間違った形式のヘッダーを検出すると、TCP セッションは終了します。
- クライアントからサーバへの MMP ヘッダーの長さを超えていないことを確認します。MMP ヘッダーの長さを超えている場合は（4096）、TCP セッションは終了します。
- クライアントからサーバへの MMP コンテンツの長さを超えていないことを確認します。エンティティのコンテンツの長さを超えている場合は（4096）、TCP セッションは終了します。

（注）　4096 は、MMP の実装で現在使用されている値です。

MMP ヘッダーとエンティティはパケット間で分割できるため、ASA はデータをバッファリングして、インスペクションの一貫性を確保します。Stream API（SAPI; ストリーム API）は、保留中のインスペクションを実行できるようにデータのバッファリングを処理します。MMP ヘッダー テキストは大文字と小文字を区別しないものとして処理されます。ヘッダー テキストと値の間にスペースが入ります。MMP の状態の再要求は、TCP 接続の状態をモニタすることによって実行されます。

Mobility Advantage Proxy の導入シナリオ

図 18-2 と図 18-3 に、Cisco Mobility Advantage ソリューションによって使用される TLS プロキシの 2 つの導入シナリオを示します。シナリオ 1（推奨される導入アーキテクチャ）では、ASA はファイアウォールと TLS プロキシの両方として機能します。シナリオ 2 では、ASA は TLS プロキシとしてだけ機能し、既存のファイアウォールを使用します。いずれのシナリオでも、クライアントはインターネットから接続します。

シナリオ 1 の導入では、ASA は Cisco UMA クライアントと Cisco UMA サーバの間にあります。Cisco UMA クライアントは、個々のスマートフォンにダウンロードされる実行可能ファイルです。Cisco UMA クライアント アプリケーションは、企業の Cisco UMA サーバに対するデータ接続（TLS 接続）を確立します。ASA は通信を代行受信し、クライアントが Cisco UMA サーバに送信するデータを検査します。

図 18-2　Cisco Mobility Advantage ソリューションの TLS プロキシは、Cisco UMA クライアントが証明書を提供できないため、クライアント認証をサポートしません。Mobility Advantage Proxy と MMP インスペクションを使用したファイアウォールとして機能するセキュリティ アプライアンス

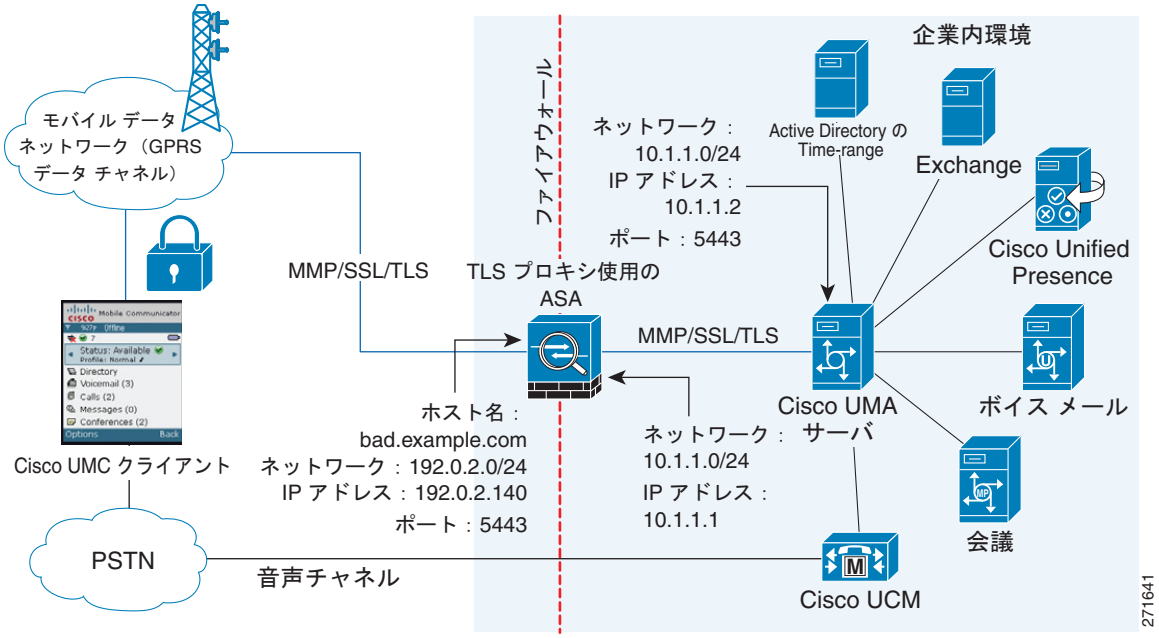


図 18-2 では、ASA は Cisco UMA サーバの 10.1.1.2 IP アドレスを 192.0.2.140 に変換することで、スタティック NAT を実行しています。

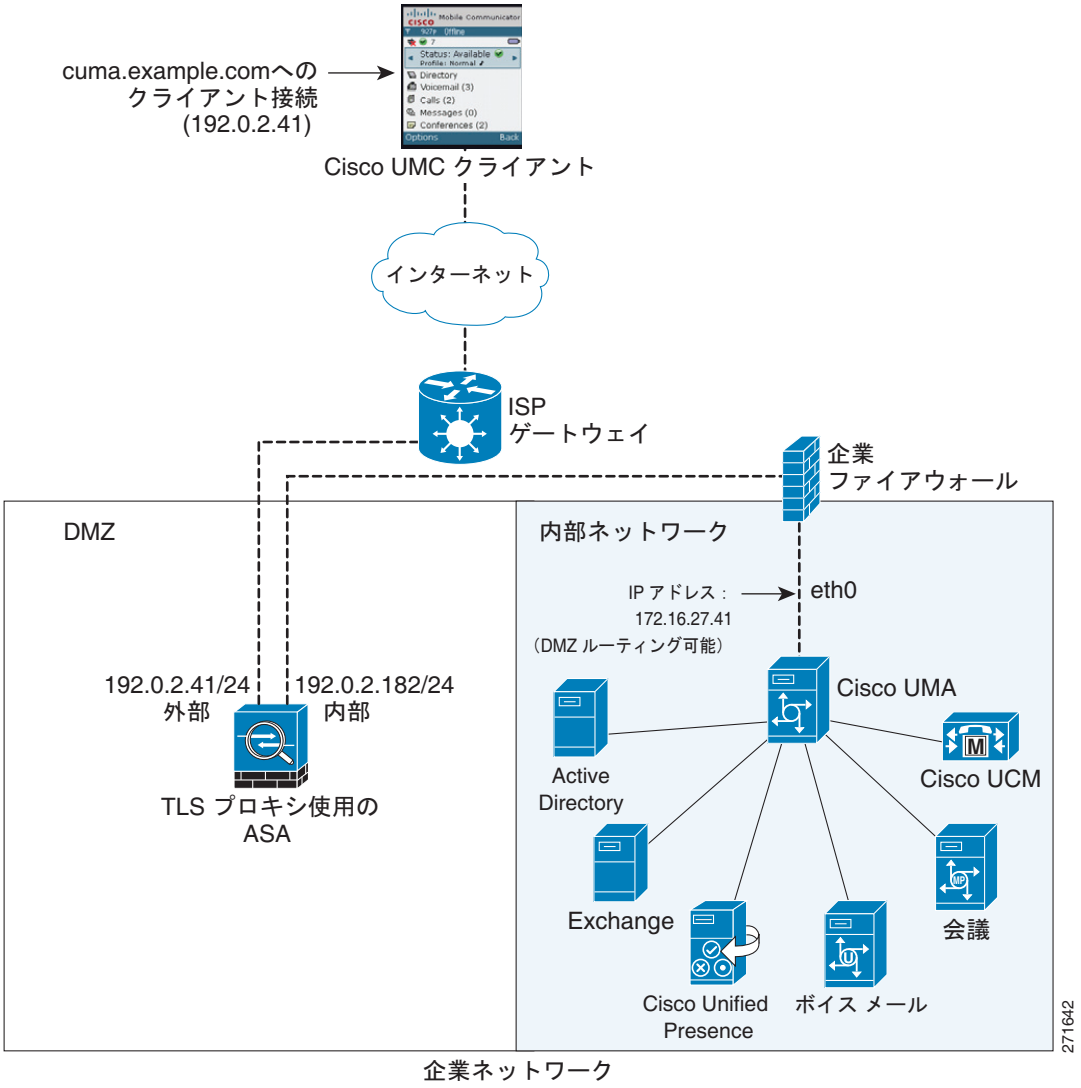
図 18-3 に導入シナリオ 2 を示します。ここでは、ASA が TLS プロキシとしてだけ機能し、企業ファイアウォールとしては機能しません。このシナリオでは、ASA と企業ファイアウォールは NAT を実行しています。企業ファイアウォールは、インターネットのどのクライアントを企業の Cisco UMA サーバに接続する必要があるのかを予測できません。したがって、この導入をサポートするために、次のアクションを実行することができます。

- 宛先 IP アドレス 192.0.2.41 を 172.16.27.41 に変換する着信トラフィックの NAT ルールを設定します。
- すべてのパケットの送信元 IP アドレスを変換する着信トラフィックのインターフェイス PAT ルールを設定し、企業ファイアウォールがワイルドカード ピンホールを開く必要がないようにします。Cisco UMA サーバは送信元 IP アドレスが 192.0.12.183 のパケットを受信します。

  詳細については、第 3 章「ネットワーク オブジェクト NAT の設定（ASA 8.3 以降）」と第 4 章「Twice NAT の設定（ASA 8.3 以降）」を参照してください。

（注） このインターフェイス PAT ルールでは、別の送信元ポートを使用して、ASA の外部インターフェイスの Cisco UMA クライアントの IP アドレスを、内部インターフェイスの 1 つの IP アドレスに収束します。このアクションは、多くの場合「外部 PAT」と呼ばれます。「外部 PAT」は、Cisco Mobility Advantage の TLS プロキシが、電話プロキシ、Cisco Unified Presence、またはアプリケーション インスペクションが必要なその他の機能を持つ ASA の同じインターフェイス上でイネーブルになっている場合には推奨しません。「外部 PAT」は、埋め込みアドレスの変換が必要な場合には、アプリケーション インスペクションによって完全にサポートされるわけではありません。

図 18-3　Cisco UMC/Cisco UMA のアーキテクチャ – シナリオ 2 : Mobility Advantage Proxy としてのみ機能するセキュリティ アプライアンス



NAT/PAT を使用した Mobility Advantage Proxy

いずれのシナリオ（図 18-2 および図 18-3）でも、NAT を使用して Cisco UMA サーバのプライベート アドレスを隠蔽できます。

シナリオ 2（図 18-3）では、PAT を使用して、すべてのクライアント トラフィックを 1 つの送信元 IP に収束し、ファイアウォールが着信トラフィックのためにワイルドカード ピンホールを開く必要がないようにします。

Cisco UMA の導入の信頼関係

Cisco UMC クライアントと ASA との間に信頼関係を確立するために、ASA は Cisco UMA サーバの証明書とキー ペアを使用します。または、ASA は Cisco UMA サーバ FQDN を使用して証明書を取得します（証明書偽装）。ASA と Cisco UMA サーバとの間では、ASA と Cisco UMA サーバは、自己署名証明書またはローカル認証局が発行した証明書を使用します。

図 18-4 に、Cisco UMA サーバの証明書を ASA にインポートする方法を示します。Cisco UMA サーバがサードパーティ CA にすでに登録している場合は、秘密キーを使用して ASA に証明書をインポートできます。これで、ASA は Cisco UMA サーバの完全なクレデンシャルを持つことになります。Cisco UMA クライアントが Cisco UMA サーバに接続すると、ASA はハンドシェイクを代理受信し、Cisco UMA サーバの証明書を使用して、クライアントとのハンドシェイクを実行します。ASA は、サーバとのハンドシェイクも行います。

図 18-4　セキュリティ アプライアンスが Cisco UMA を表す方法 – 秘密キーの共有

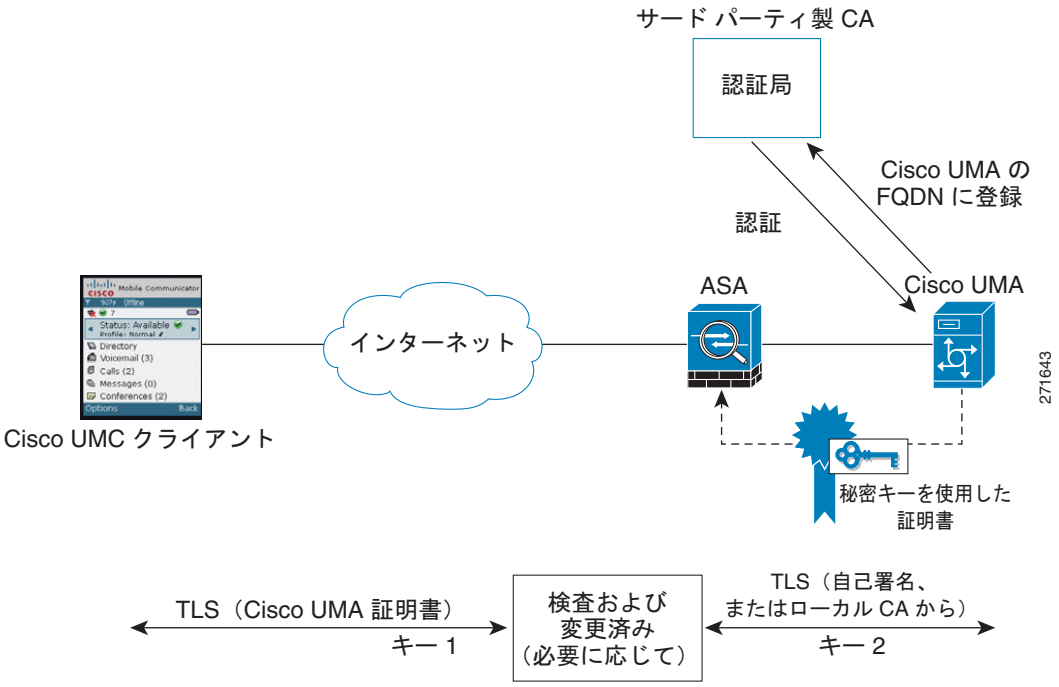
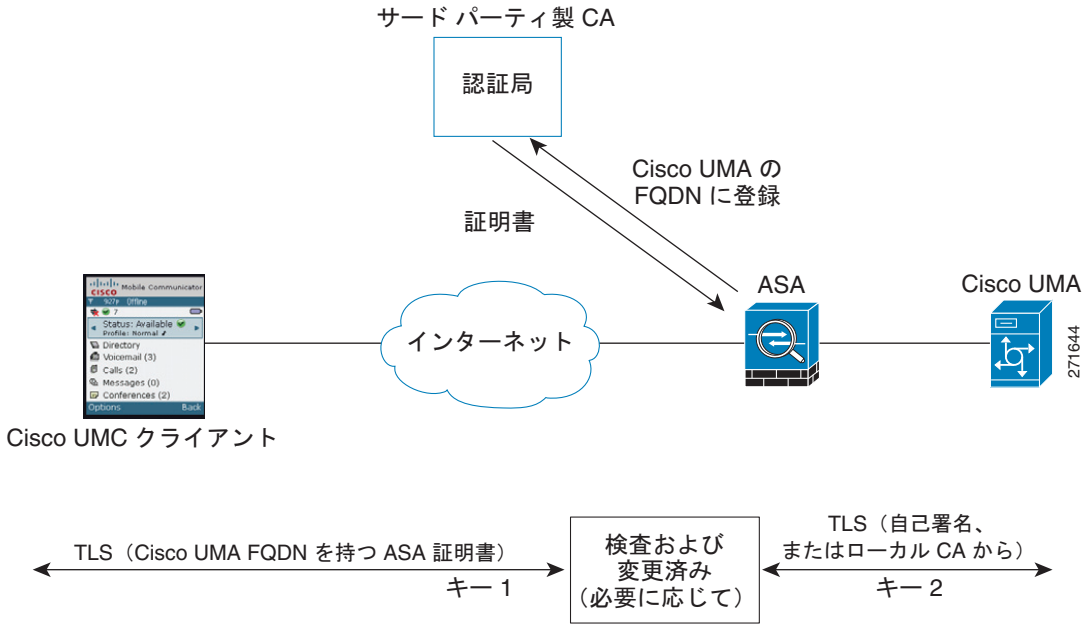


図 18-5 に、信頼関係を確立する別の方法を示します。導入に関わる各コンポーネントが新たにインストールされているため、図 18-5 は新しい場所への導入を示しています。ASA は、ASA が Cisco UMA サーバであるかのように、Cisco UMA サーバ FQDN を使用してサードパーティ CA に登録します。Cisco UMA クライアントが ASA に接続すると、ASA は、Cisco UMA サーバ FQDN を持つ証明書を示します。Cisco UMA クライアントは、通信相手が Cisco UMA サーバであるものと信じています。

図 18-5　セキュリティ アプライアンスが Cisco UMA を示す方法 – 証明書の偽装



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 サーバの証明書がダウンロードされて、トラストポイントを作成し、**crypto ca authenticate** コマンドを使用することにより、ASA のトラストストアにアップロードされます。

Cisco Mobility Advantage Proxy 機能のライセンス

ASA でサポートされる Cisco Unified Communications のプロキシ機能（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、および Cisco Presence Federation Proxy）には、Unified Communications Proxy ライセンスが必要です。ただし、バージョン 8.2(2) 以降では、Mobility Advantage Proxy に Unified Communications Proxy ライセンスは必要ありません。

次の表に、Mobility Advantage Proxy のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

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

Cisco Mobility Advantage の設定

この項では、次の内容について説明します。

- 「Cisco Mobility Advantage の設定のタスク フロー」（P.18-7）

Cisco Mobility Advantage の設定のタスク フロー

図 18-2 と図 18-3 に示すように、TLS プロキシと MMP インスペクションを実行するように ASA を設定するには、次のタスクを実行します。

ASA と Cisco UMA サーバの間で自己署名証明書を使用するものと仮定します。

ASDM を使用して Cisco Mobility Advantage Proxy を設定するには、メニューから [Wizards] > [Unified Communications Wizard] を選択します。Unified Communications Wizard が開きます。最初のページの [Remote Access] セクションで、[Cisco Mobility Advantage Proxy] オプションを選択します。

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

このウィザードでは、次の 4 つのステップで Mobility Advantage Proxy を作成します。

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

ステップ 2　プロキシ トポロジを定義するための設定（たとえば Mobility Advantage サーバの IP アドレス）を指定します。

ステップ 3　サーバ側の証明書管理を設定します。つまり、ローカルの Mobility Advantage サーバと ASA の間で交換される証明書を設定します。

ステップ 4　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 と ASA の間で交換される証明書を設定します。

ウィザードは、Mobility Advantage Proxy に対して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、「第 15 章「Cisco Unified Communication Wizard の使用」」を参照してください。

Cisco Mobility Advantage の機能履歴

表 18-1 に、この機能のリリース履歴を示します。

表 18-1　Cisco 電話プロキシの機能履歴

機能名	リリース	機能情報
Cisco Mobility Advantage Proxy	8.0(4)	Cisco Mobility Advantage Proxy 機能が導入されました。
Cisco Mobility Advantage Proxy	8.3(1)	Unified Communications Wizard が ASDM に追加されました。このウィザードを使用することにより、Cisco Mobility Advantage Proxy を設定できます。