Cisco Unified Communications Manager SIP トランク統合を設定する

この章では、Cisco Unified Communications Manager SIP トランクと Cisco Unity Connection の統合を設定する手順について説明します。このドキュメントは、Unity Connection が Cisco Unified CM と同じサーバー上に Cisco Business Edition としてインストールされている設定には適用されません。

（注） 分散型電話システムのトランク間で MWI リレーを設定する場合は、Cisco Unified CM のマニュアルで要件と手順を確認する必要があります。トランク間での MWI リレーの設定には、Unity Connection の設定は含まれません。

Cisco Unified CM SIP トランク統合の監視転送中は、Cisco Unified CM 保留音（MOH）機能を使用できません。

• Next Generation Security Over SIP 統合を有効にする （31 ページ）

前提条件

Cisco Unified CM と Unity Connection 間の SIP 統合を開始する前に、実行するタスクと統合に必要なコンポーネントを理解する必要があります。次の表に、統合を成功させるために考慮する必要がある前提条件のリストを示します。

前提条件	特記事項
該当するバージョンの Cisco Unified CM をインストールします。	• Cisco Unified CM の互換性のあるバージョンについては、 http://www.cisco.com/c/en/u unified-communications/unity-connection/products-device-support-tables-list.html にある『 リクス：*Cisco Unity Connection*』 を参照してください。
該当する数のボイスメッセージングポートを有効にするライセンスを使用して、該当するバージョンの Unity Connection をインストールします。	• Unit Connection の互換性のあるバージョンの詳細については、 http://www.cisco.com/c/e unified-communications/unity-connection/products-device-support-tables-list.html にある『 Connection の互換性マトリクス』 を参照してください。 • インストールタスクの詳細については、 https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15 にある『*Cisco Unity Connection* のインストール、アップグレード、およびメンテナン リリース *15*』の「Cisco Unity Connection をインストールする」の章を参照してくだ

SCCP 統合でサポートされている電話システムは次のとおりです。 • Cisco Unified CM 拡張の IP 電話のみ。 • Cisco Unified CM の内線番号用の IP 電話と SIP 電話の両方（Cisco Unified CM サーバーにメディア ターミネーション ポイント（MTP）はなし）。	• 該当する電話機をネットワークに接続する各場所の LAN 接続が必要です。 • Cisco Unified CM クラスタが複数ある場合に、ユーザーがトランクアクセスコーフィックスをダイヤルすることなく、別の Cisco Unified CM クラスタの内線番号きる機能。

	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/os_administration/guide/b_15c にある『Cisco Unity Connection の Cisco Unified Communications オペレーティング システ ストレーション ガイド、リリース 15』の「設定」の章の「イーサネット IPv6 の構成設 してください。

Unity Connection が IPv6 またはデュアルモード（IPv4 および IPv6）を使用して Cisco Unified CM と通信する場合は、次のサブタスクを実行します。 **1.** Unity Connection サーバーで IPv6 を有効にします。 **2.** Cisco Unity Connection Administration の **[システム設定（System Settings）] > [一般設定（General Configuration）]** ページで、Unity Connection が着信トラフィックをリッスンする場所を制御する IP アドレッシングモードのオプションを選択します。[IPv4]、[IPv6]、または [IPv4 および IPv6（IPv4 and IPv6）] を

選択できます。設定のデフォルトは [IPv4] です。	

セキュア SIP コールで Tomcat 証明書を使用する

Cisco Unity Connection は、SIP 証明書の代わりにセキュアコールを設定するために、RSA キーベースの Tomcat 証明書の使用をサポートしています。これにより、SIP セキュアコールに自己署名証明書とサードパーティ CA 署名証明書の両方を使用できます。

統合タスク

SIP トランクを介してスタンドアロンモードまたはクラスタモードで Cisco Unified CM と Unity Connection を統合するには、次の表に示すタスクを実行します。

表 *1:* 統合タスク

統合のシナリオ	統合タスク

Cisco Unified CM と Unity Connection との統合（スタンドアロン）	• Cisco Unity Connection でボイスメッセージングポートを計画する
	• 統合に向けて Cisco Unified CM を設定する
	  • SIP トランク セキュリティ プロファイルを作成する
	  • SIP プロファイルを作成する
	  • SIP トランクを作成する
	  • ルートパターンを作成する
	  • ボイスメールパイロットを作成する
	  • ボイスメールプロファイルを設定する
	  • ボイスメールサーバーのサービスパラメータを設定する
	• Cisco Unity Connection の統合を設定する
	• 統合をテストする
	• オプションタスク
	  • （オプション）SIP ダイジェスト認証を設定する
	  • （オプション）アプリケーションユーザーを作成する

統合のシナリオ	統合タスク

Cisco Unified CM と Unity Connection との統合（クラスタモード）	• Cisco Unity Connection でボイスメッセージングポートを計画する
	• 統合に向けて Cisco Unified CM を設定する
	  • SIP トランク セキュリティ プロファイルを作成する
	  • SIP プロファイルを作成する
	  • SIP トランクを作成する
	  • ルートパターンを作成する
	  • ルートリストを作成する
	  • ルートパターンを作成する
	  • ボイスメールパイロットを作成する
	  • ボイスメールプロファイルを設定する
	  • ボイスメールサーバーのサービスパラメータを設定する
	• Cisco Unity Connection の統合を設定する
	• 統合をテストする
	• オプション タスク
	  • （オプション）SIP ダイジェスト認証を設定する
	  • （オプション）アプリケーションユーザーを作成する
	  • （オプション）AXL サーバーを設定する （20 ページ）

（注） これが最初の連動の場合、最初の電話システムがデフォルト ユーザー テンプレートで自動的に選択されます。電話システム連動の作成後に追加したユーザーは、デフォルトでこの電話システムに割り当てられます。ただし、後続の統合ごとに、新しい電話システムに適用可能な新しいユーザーテンプレートを追加します。新しいユーザーテンプレートの追加、または新しいユーザーを追加する際のユーザ テンプレートの選択の詳細については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/administration/guide/b_15cucsag.html にある『Cisco Unity Connection システム アドミニストレーション ガイド』の「ユーザー属性」の章の「ユーザーテンプレート」セクションを参照してください。

SIP トランク セキュリティ プロファイルを作成する

すべてのユーザー電話（電話番号）によって使用されている1つのコーリングサーチスペース（CSS）が存在している必要があります。それぞれのポート数が適切でない場合、連動が正常

に機能しません。コーリングサーチスペースを設定し、ユーザーの電話を割り当てる手順については、Cisco Unified CM のヘルプを参照してください。

ステップ 1 Cisco Unified CM Administration の [システム（System）] メニューで、**[セキュリティ（Security）]** > に移動し、> **[SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）]** を選択します。

ステップ 2 [SIP トランク セキュリティ プロファイルの検索と一覧表示（Find and List SIP Trunk Security Profiles）] ページで、**[新規追加（Add New）]** を選択します。

ステップ 3 [SIP トランク セキュリティ プロファイルの設定（SIP Trunk Security Profile Configuration）] ページの [SIP トランク セキュリティ プロファイル情報（SIP Trunk Security Profile Information）] で、次の設定を入力します。

表 *2: SIP* トランク セキュリティ プロファイル設定ページの設定

フィールド	設定
名前（Name）	**[Unity Connection SIP トランク セキュリティ プロファイル（Unity Connection SIP Trunk Security Profile）]** または別の名前を入力します。
説明（Description）	**[Cisco Unity Connection の SIP トランク セキュリティ プロファイル（SIP trunk security profile for Cisco Unity Connection）]** または別の説明を入力します。

フィールド	設定
デバイスセキュリティモード（Device Security Mode）	Cisco Unified CM の認証と暗号化を有効にできない場合は、デフォルトの **[非セキュア（Non Secure）]** を受け入れます。 Cisco Unified CM の認証または暗号化を有効にする場合は、**[認証済み（Authenticated）]** または **[暗号化（Encrypted）]** を選択します。Cisco Unified CM サーバーの次の要件に注意してください。 • TFTPサーバーを設定する必要があります。 • Cisco Unified CM サーバーは、セキュアなシグナリングとメディア用に設定する必要があります。詳細については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/12_5_1/cucm_b_security-guide-1251.html にある『*Cisco Unified Communications Manager* セキュリティガイド、リリース *12.*』の「デフォルトのセキュリティ設定」の章の「デフォルトのセキュリティ機能」の項を参照してください。 • Cisco Unified CM サーバーの [デバイスセキュリティモード（Device Security Mode）] 設定は、Unity Connection サーバーの [セキュリティモード（Security Mode）] 設定（[認証済み（Authenticated）] または [暗号化（Encrypted）]）と一致している必要があります。 （注） Cisco Unity Connection で Next Generation Encryption が有効になっている場合は、Cisco Unified CM サーバーで**[暗号化（Encrypted）]** を選択する必要があります。
X.509 のサブジェクト名（X.509 Subject Name）	Cisco Unified CM の認証と暗号化を有効にできない場合は、このフィールドを空のままにします。 Cisco Unified CM の認証と暗号化を有効にする場合は、 **[接続（Connection）]** または別の名前を入力します。この名前は、Unity Connection サーバーの SIP 証明書の [サブジェクト名（Subject Name）] フィールドと一致する必要があります。 （注） X.509 サブジェクト名は Unity Connection サーバーの FQDN と一致する必要があります。
ダイアログ外 EFER要求の受け入れ（Accept Out-of-Dialog REFER）	このチェックボックスをオンにします。
Unsolicited NOTIFY の許可（Accept Unsolicited Notification）	このチェックボックスをオンにします。

フィールド	設定
ヘッダー置き換えの許可（Accept Replaces Header）	このチェックボックスをオンにします。

ステップ 4 **[保存（Save）]** を選択します。

SIP プロファイルを作成する

ステップ 1 [デバイス（Device）] メニューから、**[デバイスの設定（Device Settings）]** > に移動し、 > **[SIP プロファイル（SIP Profile）]**を選択します。

ステップ 2 [SIP プロファイルの検索と一覧表示（Find and List SIP Profiles）] ページで、**[検索（Find）]** を選択します。

ステップ 3 コピーする SIP プロファイルの右側にある **[コピー（Copy）]** を選択します。

ステップ 4 [SIP プロファイルの設定（SIP Profile Configuration）] ページの [SIP プロファイル情報（SIP Profile Information）] で、次の設定を入力します。

表 *3 : SIP* プロファイル設定ページの設定

フィールド	設定
名前（Name）	**[Unity Connection SIP プロファイル（Unity Connection SIP Profile）]** または別の名前を入力します。
説明	**[Unity Connection の SIP プロファイル（SIP profile for Unity Connection）]** またはその他の説明を入力します。

ステップ 5 Unity Connection が Cisco Unified CM との通信に IPv6 または IPv4/IPv6 デュアルスタックを使用する場合は、[ANAT を有効化（Enable ANAT）] チェックボックスをオンにします。IPv6 またはデュアルスタック環境で発信者が正しく処理されるようにするには、この手順を実行する必要があります。

ステップ 6 **[保存（Save）]** を選択します。

SIP トランクを作成する

ステップ 1 [デバイス（Device）] メニューで、**[トランク（Trunk）]** を選択します。

ステップ 2 [トランクの検索と一覧表示（Find and List Trunks）] ページで、**[新規追加（Add New）]** を選択します。

ステップ 3 [トランクの設定（Trunk Configuration）] ページの [トランクタイプ（Trunk Type）] フィールドで、**[SIP トランク（SIP Trunk）]** を選択します。

ステップ 4 [デバイスプロトコル（Device Protocol）] フィールドで、**[SIP]** を選択し、**[次へ（Next）]** を選択します。

ステップ 5 [デバイス情報（Device Information）] で、次の情報を入力します。

表 *4*: トランク設定ページでのデバイス情報の設定

フィールド	設定
デバイス名（Device Name）	**Unity_Connection_SIP_Trunk** または別の名前を入力します。
説明（Description）	**Unity Connection の SIP トランク** または別の説明を入力します。
SRTP 許可（SRTP Allowed）	Cisco Unified CM の認証と暗号化を有効にする場合は、このチェックボックスをオンにします。

ステップ 6 ユーザーの電話がコーリングサーチスペースに含まれている場合は、[着信コール（Inbound Calls）] で次の設定を入力します。制限しない場合は、ステップ 7 に進みます。

表 *5*: トランク設定ページでの着信コールの設定

フィールド	設定
コーリングサーチスペース（Calling Search Space）	ユーザーの電話機を含むコーリングサーチスペースの名前を選択します。
Diversionヘッダー配信のリダイレクト - インバウンド（Redirecting Diversion Header Delivery - Inbound）	このチェックボックスをオンにします。

ステップ 7 ユーザーの電話がコーリングサーチスペースに含まれている場合は、[アウトバウンドコール（Outbound Calls）] で次の設定を入力します。

フィールド	設定
Diversionヘッダー配信のリダイレクト - アウトバウンド（Redirecting Diversion Header Delivery - Outbound）	このチェックボックスをオンにします。

フィールド	設定
接続されたパーティでのみ DN を配信（Deliver DN only in connected party）	発信 SIP メッセージでは、Unity Connection は SIP の連絡先のヘッダー情報に発信元の電話番号を挿入します。これがデフォルトの設定です。
接続されたパーティでのみ URI を配信（Deliver URI only in connected party）	発信 SIP メッセージでは、Unity Connection は SIP の連絡先のヘッダー情報に発信元の電話番号を挿入します。ディレクトリ URI が利用できない場合、Unity Connection は電話番号を挿入します。
接続されたパーティで URI と DN を配信（Deliver URI and DN in connected party）	発信 SIP メッセージでは、Unity Connection は SIP の連絡先ヘッダーに発信側のディレクトリ URI と電話番号を含む混合アドレスを挿入します。ディレクトリ URI が利用できない場合、Unity Connection は電話番号だけを含めます。

トランク設定ページでの発信コールの設定

ステップ 8 [SIP 情報（SIP Information）] で、次の設定を入力します。

表 *6*: トランク設定ページでの *SIP* 情報の設定

フィールド	設定
接続先アドレス（Destination Address）	Cisco Unified CM の接続先となる Unity Connection SIP ポートの IP アドレスを入力します。
宛先アドレス IPv6（Destination Address IPv6）	Cisco Unified CM の接続先となる Unity Connection SIP ポートの IP6 アドレスを入力します。 IPv6 アドレスは、IPv6 アドレス テキスト表現の「RFC 5952」標準で提案されている正規のテキスト表現形式である必要があります。 （注） IPv6 は、Unity Connection と Cisco Unified CM の間の SIP インテグレーションに対応しています。
接続先ポート（Destination Port）	デフォルト値の **5060** を使用することを推奨します。
SIPトランクセキュリティプロファイル（SIP Trunk Security Profile）	[SIP トランク セキュリティ プロファイルの検索と一覧表示（Find and List SIP Trunk Security Profiles）] ページで、SIP トランク セキュリティ プロファイルを作成するの手順で作成した SIP トランク セキュリティ プロファイルを選択します。例えば、「Unity Connection SIP トランク セキュリティ プロファイル」を選択します。

フィールド	設定
再ルーティング用コーリングサーチスペース（Rerouting Calling Search Space）	ユーザーの電話機で使用されるコーリングサーチスペースの名前を選択します。
アウトオブダイアログREFERコーリングサーチスペース（Out-of-Dialog Refer Calling Search Space）	ユーザーの電話機で使用されるコーリングサーチスペースの名前を選択します。
SIP プロファイル（SIP Profile）	SIP プロファイルを作成するの手順で作成した SIP プロファイルの名前を選択します。例えば、「Unity Connection SIP トランクプロファイル」を選択します。

ステップ 9 サイトに必要なその他の設定を調整します。

ステップ 10 **[保存（Save）]** を選択します。

ルートパターンを作成する

ステップ 1 [コールルーティング（Call Routing）] メニューで、**[ルート/ハント（Route/Hunt）]** > に移動し、 > **[ルートパターン（Route Pattern）]** を選択します。

ステップ 2 [ルートパターンの検索と一覧表示（Find and List Route Patterns）] ページで、**[新規追加（Add New）]** を選択します。

ステップ 3 [ルートパターンの設定（Route Pattern Configuration）] ページで、次の設定を入力します。

表 7: ルートパターンの設定ページの設定

フィールド	設定
ルートパターン（Route Pattern）	Unity Connection のボイスメールのパイロット番号を入力します。
ゲートウェイ/ルートリスト（Gateway/Route List）	SIP トランクを作成するで作成した SIP トランクの名前を選択します。例えば、「Unity_Connection_SIP_Trunk」を選択します。

ステップ 4 **[保存（Save）]** を選択します。

ルートグループを作成する

ステップ 1 [コールルーティング（Call Routing）] メニューで、**[ルート/ハント（Route/Hunt）]** > に移動し、 > **[ルートグループ（Route Group）]** を選択します。

ステップ 2 [ルートグループの検索と一覧表示（Find and List Route Groups）] ページで、**[新規追加（Add New）]** を選択します。

ステップ 3 [ルートグループの設定（Route Group Configuration）] ページで、次の設定を入力します。

表 *8:* ルートグループの設定ページの設定

フィールド	設定
ルートグループ名（Route Group Name）	**SIP_Trunk_Route_Group** または別の名前を入力します。
分配アルゴリズム（Distribution Algorithm）	**[トップダウン（Top Down）]** を選択します。

ステップ 4 両方の SIP トランクが [使用可能なデバイス（Available Devices）] フィールドに表示されることを確認します。それ以外の場合は、**[検索（Find）]** を選択します。

ステップ 5 **[ルートグループに追加（Add to Route Group）]** を選択します。

ステップ 6 [現在のルート グループ メンバー（Current Route Group Members）] で、サブスクライバサーバーに接続する SIP トランクがリストの最初に表示されることを確認します。

上向き矢印または下向き矢印をクリックして SIP トランクの順序を変更できます。

ステップ 7 **[保存（Save）]** を選択します。

ルートリストを作成する

ステップ 1 [コールルーティング（Call Routing）] メニューで、**[ルート/ハント（Route/Hunt）]** > に移動し、 > **[ルートリスト（Route List）]** を選択します。

ステップ 2 [ルートリストの検索と一覧表示（Find and List Route Lists）] ページで、**[新規追加（Add New）]** を選択します。

ステップ 3 [ルートリストの設定（Route List Configuration）] ページで、次の設定を入力します。

表 *9*: ルートリストの設定ページの設定

フィールド	設定
名前（Name）	**SIP_Trunk_Route_List** または別の名前を入力します。
説明（Description）	**[SIP トランクルートリスト（SIP Trunk Route List）]** または別の説明を入力します。
Cisco Unified Communications Manager グループ（Cisco Unified Communications Manager Group）	**[デフォルト（Default）]** を選択します。

ステップ 4 **[保存（Save）]** を選択します。

ステップ 5 **[このルートリストを有効にする（Enable This Route List）]** チェックボックスがオンになっていることを確認します。

ステップ 6 [ルートリストメンバー情報（Route List Member Information）] で、**[ルートグループの追加（Add Route Group）]** を選択します。

ステップ 7 [ルートリストの詳細設定（Route List Detail Configuration）] ページの [ルートグループ（Route Group）] フィールドで、Cisco Unity Connection の統合を設定するの手順で作成したルートグループを選択し、**[保存（Save）]** を選択します。

ステップ 8 ルートリスト設定が保存されることが示されたら、**[OK]** をクリックします。

ステップ 9 [ルートリストの設定（Route List Configuration）] ページで、**[リセット（ Reset）]** を選択します。

ステップ 10 ルートリストのリセットを確認するように求められた場合は、**[リセット（Reset）]** をクリックします。

ステップ 11 **[閉じる（Close）]** を選択します。

ボイスメールパイロットを作成する

ステップ 1 [高度な機能（Advanced Features）] メニューで、**[ボイスメール（Voice Mail）]** > に移動し 、 > **[ボイスメールパイロット（Voice Mail Pilot）]** を選択します。

ステップ 2 [ボイスメールパイロットの検索と一覧表示（Find and List Voice Mail Pilots）] ページで、**[新規追加（Add New）]** を選択します。

ステップ 3 [ボイスメールパイロットの設定（Voice Mail Pilot Configuration）] ページで、次のボイスメールパイロット番号の設定を入力します。

表 *10* : ボイスメール パイロット設定ページの設定

フィールド	設定
ボイスメールパイロット番号（Voice Mail Pilot Number）	ユーザーが自分のボイスメッセージを聞くためにダイヤルするボイスメールパイロット番号を入力します。この番号は、ルートパターンを作成するの手順で入力したルートパターンと一致している必要があります。
コーリングサーチスペース（Calling Search Space）	ユーザー電話を含むパーティションと、ボイスメールのパイロット番号用に設定したパーティションを含む通話検索スペースを選択します。
説明	**[Unity Connection パイロット（Unity Connection Pilot）]** またはその他の説明を入力します。
システムのデフォルトボイスメールパイロットに設定（Make This the Default Voice Mail Pilot for the System）	この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ンにすると、現在のデフォルトのパイロット番号がこのボイスメールパイロット番号に置き換えられます。

ステップ 4 **[保存（Save）]** を選択します。

ボイスメールプロファイルを設定する

ステップ 1 [高度な機能（Advanced Features）] メニューで、**[ボイスメール（Voice Mail）]** > に移動し 、 > **[ボイスメールプロファイル（Voice Mail Profile）]** を選択します。

ステップ 2 [ボイスメールプロファイルの検索と一覧表示（Find and List Voice Mail Profiles）] ページで、**[新規追加（Add New）]** を選択します。

ステップ 3 [ボイスメールプロファイルの設定（Voice Mail Profile Configuration）] ページで、次のボイスメールプロファイル設定を入力します。

表 *11* : ボイスメールパイロット設定ページの設定

フィールド	設定
ボイスメールプロファイル名（Voice Mail Profile Name）	**[Unity Connection プロファイル（Unity Connection Profile）]** またはボイスメールプロファイルを識別するための別の名前を入力します。
説明（Description）	**[Unity Connection のプロファイル（Profile for Unity Connection）]** またはその他の説明を入力します。

フィールド	設定
ボイスメールパイロット（Voice Mail Pilot）	ボイスメールパイロットを作成するで定義したボイスメールパイロットを選択します。
ボイスメールボックスのマスク（Voice Mail Box Mask）	Cisco Unified CM でマルチテナントサービスを有効にしていない場合は、このフィールドを空白のままにします。 マルチテナントサービスを有効にしている場合、各テナントは自身のボイスメール プロファイルを使用し、他のテナントと共有するパーティションごとに内線番号（電話番号）を識別するためのマスクを作成する必要があります。たとえば、あるテナントは972813XXXX というマスクを使用し、別のテナントは214333XXXX というマスクを使用することができます。また、それぞれのテナントは MWI 用に独自のトランスレーション パターンを使用します。
このボイスメールプロファイルをシステムのデフォルトにする（Make This the Default Voice Mail Profile for the System）	このボイスメールプロファイルをデフォルトにするには、この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ンにすると、現在のデフォルトのボイスメールプロファイルが、このボイスメールプロファイルに置き換えられます。

ステップ 4 **[保存（Save）]** を選択します。

ボイスメールサーバーのサービスパラメータを設定する

SIP ダイジェスト認証を設定しない場合は、 Cisco Unity Connection の統合を設定するに進みます。

ステップ 1 Cisco Unified CM Administration で、**[システム（System）]** > > **[サービス パラメータ（Service Parameters）]** の順に選択します。

ステップ 2 [サービスパラメータの設定（Service Parameters Configuration）] ページの [サーバー（Server）] フィールドで、Cisco Unified CM サーバーの名前を選択します。

ステップ 3 [サービス（Service）] リストから、**[Cisco CallManager]** を選択します。パラメータのリストが表示されます。

ステップ 4 [クラスタ全体のパラメータ（機能 - 全般）（Clusterwide Parameters (Feature - General)）] で、[マルチテナント MWI モード（Multiple Tenant MWI Modes）] パラメータを見つけます。

ステップ 5 複数のテナント MWI 通知を使用する場合は、**[はい（True）]** を選択します。

このパラメータを [はい（True）] に設定すると、Cisco Unified CM は、MWI がオンまたはオフにされたときに、任意の設定済みトランスレーションパターンを使用して、ボイスメールの内線番号を電話番号に変換します。

ステップ 6 いずれかの設定を変更した場合は、**[保存（Save）]** を選択します。次に、Cisco Unified CM サーバーをシャットダウンして再起動します。

（オプション）SIP ダイジェスト認証を設定する

ステップ 1 [システム（System）] メニューから、**[セキュリティ（Security）]** > に移動し、 > **[SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）]** を選択します。

ステップ 2 [SIP トランク セキュリティ プロファイルの検索と一覧表示（Find and List SIP Trunk Security Profiles）] ページで、 SIP トランク セキュリティ プロファイルを作成するの手順で作成した SIP トランク セキュリティ プロファイルを選択します。

ステップ 3 [SIPトランク セキュリティプロファイルの設定（SIP Trunk Security Profile Configuration）] ページで、**[ダイジェスト認証を有効化（Enable Digest Authentication）]** チェック ボックスをオンにします。

ステップ 4 **[保存（Save）]** を選択します。

（オプション）アプリケーションユーザーを作成する

ステップ 1 [ユーザー管理（User Management）] メニューで、**[アプリケーションユーザー（Application User）]** を選択します。

ステップ 2 [アプリケーションユーザーの検索/一覧表示（Find and List Application Users）] ページで、**[新規追加（Add New）]** を選択します。

ステップ 3 [アプリケーションユーザーの設定（Application User Configuration）] ページで、次の設定を入力します。

表 *12*：アプリケーションユーザーの設定ページの設定

フィールド	設定
ユーザーID（User ID）	アプリケーションユーザーの識別名を入力します。Cisco Unified CM では、ユーザー ID の作成後の変更はできません。使用できる特殊文字は、=、+、<、>、#、;、\、,、“”、および空白です。
パスワード（Password）	ダイジェスト信用証明書に使用するものと同じパスワードを入力します。
パスワードの確認（Confirm Password）	パスワードを再度入力します。

フィールド	設定
ダイジェストクレデンシャル（Digest Credentials）	ダイジェスト信用証明書の名前を入力します。
ヘッダー置き換えの許可（Accept Replaces Header）	このチェックボックスはオフのままにします。
使用可能なデバイス（Available Devices）	このリストボックスには、このアプリケーションユーザーに関連付けることのできるデバイスが表示されます。 デバイスをこのアプリケーションユーザーに関連付けるには、デバイスを選択し、リストボックスの下にある下矢印を選択します。 このアプリケーションユーザーに関連付けようとするデバイスがこのペインに表示されない場合は、次のいずれかのボタンを選択して、他のデバイスを検索します。 • **さらに電話を検索（Find more Phones）**：このアプリケーションユーザーに関連付ける電話機をさらに検索するには、このボタンを選択します。[電話の検索と一覧表示（Find and List Phones）] ウィンドウが表示され、電話機を検索できます。 • **さらにルートポイントを検索（Find More Route Points）**：このアプリケーションユーザーに関連付ける電話機をさらに検索するには、このボタンを選択します。[CTI ルートポイントの検索と一覧表示（Find and List CTI Route Points）] ウィンドウが表示され、CTIルートポイントを検索できます。
割り当てられているCAPFプロファイル（Associated CAPF Profiles）	[割り当てられている CAPF プロファイル（Associated CAPF Profiles）] ペインには、そのユーザー用にアプリケーションユーザー CAPF プロファイルを設定した場合は、アプリケーションユーザー CAPF プロファイルのインスタンス ID が表示されます。プロファイルを編集するには、[インスタンス ID（Instance ID）] を選択し、[プロファイルの編集（Edit Profile）] を選択します。[アプリケーション ユーザー CAPF プロファイルの設定（Application User CAPF Profile Configuration）] ウィンドウが表示されます。
グループ（Groups）	このリスト ボックスには、アプリケーション ユーザの所属先となるグループが表示されます。
ロール（Roles）	このリスト ボックスには、アプリケーション ユーザに割り当てられる権限が表示されます。

ステップ 4 **[保存（Save）]** を選択します。

（オプション）AXL サーバーを設定する

Unity Connection が AXL サーバーに接続する場合は、次の設定を行います。

ステップ 1 **[テレフォニー統合（Telephony Integrations）]** を展開し、[電話システム（Phone System）] を選択します。

ステップ 2 [電話システムの検索（Search Phone Systems）] ページで、作成した電話システムの表示名を選択します。

ステップ 3 [電話システムの基本（Phone System Basics）] ページの [編集（Edit）] メニューで、[Cisco Unified Communications Manager AXL サーバー（**Cisco Unified Communications Manager AXL Servers**）] を選択します。

AXL サーバーへの接続は、Cisco Unified CM ユーザーのインポートや、Cisco Unity Connection の個人的なコール転送ルールのユーザーの特定の電話設定を変更するために、Unity Connection が Cisco Unified CM データベースにアクセスする必要がある場合に必要です。

（注） Cisco Unified CM ユーザーのインポートを計画している場合は、各ユーザーのエンドユーザー設定ページのプライマリ内線フィールドが入力されていることを確認してください。入力されていないと、検索でインポートするユーザーが見つかりません。

ステップ 4 **[AXL サーバーの編集（Edit AXL Servers）]** ページの [AXL サーバー（AXL Servers）] で、**[新規追加（Add New）]** を選択します。

ステップ 5 AXL サーバーの次の設定を入力し、[保存（Save）] を選択します。

表 *13 : AXL* サーバーの設定

フィールド	設定
順序（Order）	AXL サーバーの優先順位を入力します。最も小さい数字はプライマリ AXL サーバーで、それよりも大きい数字はセカンダリサーバーを表します。
IP アドレス（IP Address）	AXL サーバーの IP アドレスを入力します。
ポート（Port）	Unity Connection で接続する AXL サーバーのポートを入力します。この設定は、AXL サーバーが使用するポートと同じにする必要があります。

ステップ 6 他のすべての AXL サーバーに対して、ステップ 4 とステップ 5 を繰り返します。

ステップ 7 [AXL サーバー設定（AXL Server Settings）] で、次の設定を入力し、[保存（Save）] を選択します。

表 *14 : AXL* サーバーの設定

フィールド	設定
ユーザー名（Username）	Unity Connection で AXL サーバーにサインインするために使用するユーザー名を入力します。 （注） このユーザーは、「標準 AXL API アクセス」ロールに割り当てられた Cisco Unified CM アプリケーションユーザーの名前と一致する必要があります。
パスワード（Password）	Unity Connection で AXL サーバーにサインインするために使用するユーザーのパスワードを入力します。 （注） このパスワードは、[ユーザー名（User Name）] フィールドに入力した Cisco Unified CM アプリケーションユーザーのパスワードと一致する必要があります。
Cisco Unified Communications Manager のバージョン（Cisco Unified Communications Manager Version）	以下を正確に説明する適切な設定を選択します。 • Unity Connection と統合する Cisco Unified CM のバージョン。 • AXL ポートで SSL を有効にするかどうか。 非 SSL バージョンを選択する場合、AXL ポートは非 SSL ポート（通常はポート 80）である必要があります。SSL 対応バージョンを選択する場合、AXL ポートは SSL 対応ポート（通常はポート 443 またはポート 8443）である必要があります。
プライマリ AXL サーバのエンドユーザ暗証番号同期を有効にする（Enable End User PIN Synchronization for Primary AXL Server）	同じユーザー ID（Unity Connection のエイリアス）を持つユーザーに対して、Unity Connection と Cisco Unified CM 間の PIN 同期を有効にするには、このチェックボックスをオンにします。 この機能を有効にすると、ユーザーが Cisco Unity Connection で PIN を更新するたびに、PIN は Cisco Unified CM と同期され、その逆も同様です。 デフォルト設定：チェックボックスはオフです。 PIN 同期の詳細については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/design/b_15cucsag/b_12xcucsag_appendix_010011.html にある『*Cisco Unity Connection* システム アドミニストレーション ガイド、リリース*15*』の「ユーザー設定」の章にある「Unity Connection と Cisco Unified CM 間の PIN 生成」の項を参照してください。

フィールド	設定
証明書エラーを無視する（Ignore Certificate Errors）	AXL サーバーの証明書検証エラーを無視する場合は、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、Unity Connection は AXL サーバーの証明書を検証します。ただし、チェックボックスをオンにする前に、Cisco Unified CM の tomcat ルート証明書を Unity Connection サーバーの tomcat trust にアップロードする必要があることを確認してください。 デフォルト設定：チェックボックスはオンです。 証明書の詳細については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/os_administration/guide/b_15cucosagx.html にある『*Cisco Unified Communications* オペレーティング システム アドミニストレーション ガイド、リリース *15*』の「セキュリティ」の章を参照してください。

ステップ 8 対応するアプリケーションサーバーを Cisco Unified CM に追加するには、Cisco Unified CM Administration にログインします。

ステップ 9 Cisco Unified CM Administration で、**[システム（System）] > [アプリケーションサーバー（Application Server）]** ページに移動します。

ステップ 10 [アプリケーションサーバーの検索と一覧表示（Find and List Application Servers）] ページで、[検索（Find）] を選択してすべてのアプリケーションサーバーを表示します。

ステップ 11 [名前（Name）] 列で、Cisco Unity Connection サーバーの名前を選択します。

ステップ 12 [アプリケーションサーバーの設定（Application Server Configuration）] ページの [使用可能なアプリケーションユーザー（Available Application User）] フィールドで、ステップ 7 で使用した Cisco Unified CM アプリケーションユーザーを選択し、下矢印を選択してそれを [選択されたアプリケーションユーザー（Selected Application User）] フィールドに移動します。

ステップ 13 [保存（Save）] を選択します。

Cisco Unity Connection の統合を設定する

Unity Connection は、Cisco Unified Communications Manager との SIP トランク統合によるボイスメッセージポートの認証と暗号化に、証明書とセキュリティプロファイルを使用します。

前提条件

統合プロセスを開始する前に、セキュア SIP 設定を成功させるために、次の点を考慮する必要があります。

- Cisco Unity Connection は、輸出規制機能が許可されているスマートライセンスに登録する必要があります。シスコ スマート ソフトウェア ライセンシングの詳細は、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_0_1/systemConfig/cucm_b_system-configuration-guide-1201.html にある『*Cisco Unified Communications Manager* シス

テム設定ガイド、リリース *12*』の「スマート ソフトウェア ライセンシング」の章の「スマート ソフトウェア ライセンシングの概要」の項を参照してください。

- Cisco Unity Connection は制限付きバージョンを実行している必要があります。Cisco Unity Connection の制限版と無制限版の詳細については、 https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/security/b_12xcucsecx.html にある『Cisco Unity Connection セキュリティガイド、リリース 12』の「Cisco Unity Connection：制限版と無制限版」の章にある「Cisco Unity Connection：制限版と無制限版」の項を参照してください。
- Cisco Unity Connection は、CLI コマンド**「utils cuc encryption enable」**を使用して暗号化を有効にする必要があります。CLI コマンドの詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『Cisco Unified Solutions コマンド ライン インターフェイス リファレンス ガイド』を参照してください。

Cisco Unified Communications Manager と Unity Connection が統合できる状態になっていることを確認したら、次の手順で統合を設定し、ポート設定を入力します。

統合を作成する

ステップ 1 Cisco Unity Connection Administration にサインインします。

ステップ 2 Cisco Unity Connection Administration で、**[テレフォニー統合（Telephony Integrations）]** を展開し、**[電話システム（Phone System）]** を選択します。

ステップ 3 [電話システムの検索（Search Phone Systems）] ページの [表示名（Display Name）] で、デフォルトの電話システム名をクリックします。

ステップ 4 [電話システムの基本設定（Phone System Basics）] ページの [電話システム名（Phone System Name）] フィールドで、電話システムの説明的な名前を入力します。

ステップ 5 この電話システムを TRaP 接続のデフォルトとして使用し、ボイスメールボックスを持たない管理者やユーザーが Unity Connection Web アプリケーションで電話を通じて録音および再生できるようにする場合は、**[デフォルト TRAP スイッチ（Default TRAP Switch）]** チェックボックスをオンにします。別の電話システムを TRaP 接続のデフォルトとして使用する場合は、このチェックボックスをオフにします。

ステップ 6 **[保存（Save）]** を選択します。

ステップ 7 [電話システムの基本設定（Phone System Basics）] ページの [関連リンク（Related Links）] ドロップダウンボックスで、**[ポートグループの追加（Add Port Group）]** を選択して、**[移動（Go）]** を選択します。

ステップ 8 [新しいポートグループ（New Port Group）] ページで、該当する設定を入力し、**[保存（Save）]** を選択します。

表 *15* : 新しいポートグループページの設定

フィールド	設定
電話システム（Phone System）	ドロップダウンリストから、ステップ 5 で入力した電話システムの名前を選択します。

フィールド	設定
作成元（Create From）	**[ポートグループテンプレート（Port Group Template）]** を選択し、ドロップダウンボックスで **[SIP]** を選択します。
表示名（Display Name）	ポート グループの説明的な名前を入力します。デフォルト名をそのまま使用することも、任意の名前を入力することもできます。
SIP サーバーで認証する（Authenticate with SIP Server）	Unity Connection で Cisco Unified CM サーバーを認証する場合は、このチェックボックスをオンにします。
認証ユーザー名（Authentication User Name）	Unity Connection が Cisco Unified CM サーバーとの認証に使用する名前を入力します。
認証パスワード（Authentication Password）	Unity Connection が Cisco Unified CM サーバーでの認証に使用するパスワードを入力します。
連絡先回線名（Contact Line Name）	ユーザーが Unity Connection に連絡するために使用し、Unity Connection が Cisco Unified CM サーバーに登録するために使用する音声メッセージング回線名（またはパイロット番号）を入力します。
SIP セキュリティ プロファイル（SIP Security Profile）	Unity Connection が使用する SIP セキュリティプロファイルを選択します。
次世代暗号化の有効化（Enable Next Generation Encryption）	（注） （セキュアな *TLS* ポートが使用されている場合のみ）Unity Connection で RSA キーベースまたは EC キーベースの証明書（自己署名証明書およびサードパーティ証明書）を使用して SIP インターフェイスで次世代暗号化サポートを提供する場合は、このチェックボックスをオンにします。詳細については、Next Generation Security Over SIP 統合を有効にするを参照してください。

フィールド	設定
セキュリティモード（Security Mode）	（セキュアな *TLS* ポートが使用され、*[*次世代暗号化を有効にする（*Enable Next Generation Encryption*）*]* チェックボックスがオフの場合のみ） 該当するセキュリティモードを選択します。 • **認証済み（Authenticated）**：コールシグナリング メッセージは、認証済み TLS ポートを使用して Cisco Unified CM に接続されるため、完全性が保証されます。ただし、クリア（暗号化されていない）テキストで送信されるため、コールシグナリング メッセージのプライバシーは保証されません。 • **暗号化（Encrypted）**：コールシグナリング メッセージは、セキュアな TLS ポートを使用して Cisco Unified CM に接続され、暗号化されるため、完全性とプライバシーが保証されます。 Unity Connection サーバーの [セキュリティモード（Security Mode）] 設定は、Cisco Unified CM サーバーの [デバイスセキュリティモード（Device Security Mode）] 設定と一致している必要があります。
セキュア RTP（Secure RTP）	（セキュアな *TLS* ポートを使用する場合のみ）メディアストリーム（RTP）が暗号化されるように、このチェックボックスをオンにします。メディアストリームを暗号化しない場合は、チェックボックスをオフにします。
SIP転送プロトコル（SIP Transport Protocol）	Unity Connection によって使用される SIP 転送プロトコルを選択します。
IPv4 アドレス/ホスト名（IPv4 Address or Host Name）	Unity Connection と統合しているプライマリ Cisco Unified CM サーバーの IPv4 アドレス（または、ホスト名）を入力します。 このフィールドに IP アドレスまたはホスト名を入力するか、[IPv6 アドレス/ホスト名（IPv6 Address or Host Name）] フィールドに IP アドレスまたはホスト名を入力する必要があります（また、該当する場合は、両方のフィールドに情報を入力します）。両方のフィールドを空白のままにすることはできません。

フィールド	設定
IPv6 アドレス/ホスト名（IPv6 Address or Host Name）	Unity Connection と統合しているプライマリ Cisco Unified CM サーバーの IPv6 アドレス（または、ホスト名）を入力します。 IPv6 アドレスは、IPv6 アドレステキスト表現の「RFC 5952」標準で提案されている正規のテキスト表現形式である必要があります。 このフィールドに IP アドレスまたはホスト名を入力するか、[IPv4 アドレス/ホスト名（IPv6 Address or Host Name）] フィールドに IP アドレスまたはホスト名を入力する必要があります（また、該当する場合は、両方のフィールドに情報を入力します）。両方のフィールドを空白のままにすることはできません。 （注） IPv6 は、Cisco Unified CM 10.0 との SIP 統合向けにサポートされています。
IPアドレスまたはホスト名	Cisco Unity Connection と統合しているプライマリ Cisco Unified CM サーバーの IP アドレス（または、ホスト名）を入力します。
ポート	Unity Connection と統合しているプライマリ Cisco Unified CM サーバーの TCP ポートを入力します。デフォルト設定を使用することを推奨します。

ステップ 9 Cisco Unified CM クラスタにセカンダリサーバーがある場合、または TFTP サーバーを追加する場合（Cisco Unified CM の認証と暗号化に必要）、[ポートグループの基本設定（Port Group Basics）] ページで、次のサブステップを実行します。それ以外の場合は、ステップ 11 に進みます。

a) [編集（Edit）] メニューで、**[サーバー（Servers）]** を選択します。

b) セカンダリ Cisco Unified CM サーバーを追加する場合、[サーバーの編集（Edit Servers）] ページの [SIP サーバー（SIP Servers）] で、**[追加（Add）]** を選択します。それ以外の場合は、ステップ 10e. に進みます。

c) セカンダリ Cisco Unified CM サーバーの次の設定を入力し、**[保存（Save）]** を選択します。

表 *16 : SIP* サーバーの設定

フィールド	設定
順位（Order）	Cisco Unified CM サーバーの優先順位を入力します。最も小さい数字はプライマリ Cisco Unified CM サーバーで、それよりも大きい数字はセカンダリサーバーを表します。

フィールド	設定
IPv4 アドレス/ホスト名（IPv4 Address or Host Name）	セカンダリ Cisco Unified CM サーバーの IPv4 アドレス（またはホスト名）を入力します。 このフィールドに IP アドレスまたはホスト名を入力するか、[IPv6 アドレス/ホスト名（IPv6 Address or Host Name）] フィールドに IP アドレスまたはホスト名を入力する必要があります（また、該当する場合は、両方のフィールドに情報を入力します）。両方のフィールドを空白のままにすることはできません。
IPv6 アドレス/ホスト名（IPv6 Address or Host Name）	セカンダリ Cisco Unified CM サーバーの IPv6 アドレス（またはホスト名）を入力します。 IPv6 アドレスは、IPv6 アドレステキスト表現の「RFC 5952」標準で提案されている正規のテキスト表現形式である必要があります。 このフィールドに IP アドレスまたはホスト名を入力するか、[IPv4 アドレス/ホスト名（IPv6 Address or Host Name）] フィールドに IP アドレスまたはホスト名を入力する必要があります（また、該当する場合は、両方のフィールドに情報を入力します）。両方のフィールドを空白のままにすることはできません。 （注） IPv6 は、Cisco Unified CM 10.0 との SIP 統合向けにサポートされています。
IPアドレスまたはホスト名（IP Address or Host Name）	セカンダリ Cisco Unified CM サーバーの IP アドレス（またはホスト名）を入力します。
ポート（Port）	Unity Connection と統合する Cisco Unified CM サーバーの IP ポートを入力します。デフォルト設定を使用することを推奨します。
TLS ポート（TLS Port）	Unity Connection と統合する Cisco Unified CM サーバーの TLS ポートを入力します。デフォルト設定を使用することを推奨します。

d) 必要に応じて、Cisco Unified CM クラスタ内の追加の Cisco Unified CM サーバーについてステップ 10b. とステップ 10c. を繰り返します。

e) TFTP サーバー（Cisco Unified CM の認証と暗号化に必要）を追加する場合は、[TFTP サーバー（TFTP Servers）] で **[追加（Add）]** を選択します。それ以外の場合は、ステップ 10h. に進みます。

f) セカンダリ Cisco Unified CM サーバーの次の設定を入力し、**[保存（Save）]** を選択します。

表 *17 : TFTP* サーバーの設定

フィールド	設定
順序（Order）	TFTP サーバーの優先順位を入力します。数値の最も小さいサーバーがプライマリ TFTP サーバーで、数値がプライマリよりも大きい場合はセカンダリ サーバーです。

フィールド	設定
IPv4アドレス/ホスト名（IPv4 Address or Host Name）	TFTP サーバーの IPv4 アドレス（またはホスト名）を入力します。 このフィールドに IP アドレスまたはホスト名を入力するか、[IPv6 アドレス/ホスト名（IPv6 Address or Host Name）] フィールドに IP アドレスまたはホスト名を入力する必要があります（また、該当する場合は、両方のフィールドに情報を入力します）。両方のフィールドを空白のままにすることはできません。
IPv6アドレス/ホスト名（IPv6 Address or Host Name）	TFTP サーバーの IPv6 アドレス（またはホスト名）を入力します。 IPv6 アドレスは、IPv6 アドレステキスト表現の「RFC 5952」標準で提案されている正規のテキスト表現形式である必要があります。 このフィールドに IP アドレスまたはホスト名を入力するか、[IPv4 アドレス/ホスト名（IPv6 Address or Host Name）] フィールドに IP アドレスまたはホスト名を入力する必要があります（また、該当する場合は、両方のフィールドに情報を入力します）。両方のフィールドを空白のままにすることはできません。 （注） • IPv6 は、Cisco Unified CM 10.0 との SIP 統合向けにサポートされています。 • **[プライマリサーバー設定（Primary Server Settings）]** で [SIP セキュリティプロファイル（SIP security profile）] ドロップダウンメニューからセキュアな SIP プロファイルを選択する場合は、DNS サーバーが IPv6 アドレスとホスト名の両方を正しく解決できることを確認します。
IPアドレスまたはホスト名	TFTP サーバーの IP アドレス（またはホスト名）を入力します。

g) 必要に応じて、追加する TFTP サーバごとにステップ10e. とステップ10f. を繰り返します。
h) [編集（Edit）] メニューで、**[ポートグループの基本設定（Port Group Basics）]** を選択します。
i) [ポートグループの基本設定（Port Group Basics）] ページで、**[リセット（Reset）]** を選択します。

ステップ 10 [ポートグループの基本設定（Port Group Basics）] ページの [関連リンク（Related Links）] ドロップダウンボックスで、**[ポートの追加（Add Ports）]** を選択して、**[移動（Go）]** を選択します。

ステップ 11 [新しいポート（New Port）] ページで、次の設定を入力し、**[保存（Save）]** を選択します。

表 *18*：新しいポートページの設定

フィールド	設定
有効（Enabled）	このチェックボックスをオンにします。

フィールド	設定
ポート数（Number of Ports）	このポート グループ内に作成するボイス メッセージ ポートの数を入力します。 （注） Unity Connection クラスタでは、すべての Unity Connection サーバーで使用されるボイスメッセージポートの合計数を入力する必要があります。各ポートは特定の Unity Connection サーバーに割り当てられています。
電話システム（Phone System）	ドロップダウンリストから、ステップ 5 で入力した電話システムの名前を選択します。
ポートグループ（Port Group）	ステップ 9で追加したポートグループの名前を選択します。
サーバー（Server）	Unity Connection サーバーの名前を選択します。

ステップ 12 [ポートの検索（Search Ports）]ページで、この電話システム統合に対して作成した最初のボイスメッセージポートの表示名を選択します。

（注） デフォルトでは、ボイスメッセージポートの表示名は、ポートグループの表示名の後に増分番号が付加されたものになります。

ステップ 13 [ポートの基本設定（Port Basics）]ページで、必要に応じてボイスメッセージポートを設定します。以下の表のフィールドを変更できます。

表 *19*：個別のボイスメッセージポートの設定

フィールド	説明
有効（Enabled）	ポートを有効にするには、チェックボックスをオンにします。ポートは通常の中に有効になります。 ポートを無効にするには、このチェックボックスをオフにします。ポートが無なっている場合、そのポートへのコールに対して、呼び出し音は鳴りますが、はありません。通常、ポートは、テスト中インストーラによってだけ無効にな す。
サーバー（Server）	（*Unity Connection* クラスタのみ） このポートを処理する Unity Connection サーの名前を選択します。 ボイス メッセージング トラフィックを均等に共有するように、Cisco Unity Conn サーバーに同じ数の応答およびダイヤルアウト ボイス メッセージング ポートを当てます。
コールに応答（Answer Calls）	ポートを通話への応答用に指定するには、このチェックボックスをオンにしま これらのコールは、身元不明発信者またはユーザーからの着信コールである可 があります。

フィールド	説明
メッセージ通知を実行する（Perform Message Notification）	ポートをユーザーに対するメッセージ通知用に指定するには、このチェックボックスをオンにします。稼働率が最も低いポートに[メッセージ通知を実行する（Perform Message Notification）] を割り当てます。
MWIリクエストを送信する（Send MWI Requests）	ポートでの MWI のオン/オフを指定するには、このチェックボックスをオンにします。稼働率が最も低いポートに [MWI リクエストを送信する（Send MWI Requests）] を割り当てます。
TRAP接続を許可する（Allow TRAP Connections）	このチェックボックスをオンにすると、ユーザーは Cisco Unity Connection の web アプリケーションで電話から録音または再生用のポートを使用できます。稼働率が最も低いポートに [TRAP 接続を許可する（Allow TRAP Connections）] を割り当てます。

ステップ 14 **[保存（Save）]** を選択します。

ステップ 15 **[次へ（Next）]** を選択します。

ステップ 16 電話システムの残りすべてのボイスメッセージポートについて、 ステップ 14 からステップ 16 を繰り返します。

ステップ 17 Cisco Unified CM 認証と暗号化を使用する場合は、RSA キーベースの Tomcat 証明書を生成してアップロードします。詳細については、RSA キーベースの証明書を設定するの項を参照してください。

ステップ 18 別の電話システム統合が存在する場合は、Ciscon Unity Connection Administration で **[テレフォニー統合（Telephony Integrations）]** を展開し、**[トランク（Trunk）]** を選択します。

ステップ 19 [電話システムトランクの検索（Search Phone System Trunks）] ページの [電話システムトランク（Phone System Trunk）] メニューで、**[新しい電話システムトランク（New Phone System Trunk）]** を選択します。

ステップ 20 [新しい電話システムトランク（New Phone System Trunk）] ページで、電話システムトランクの次の設定を入力し、**[保存（Save）]** を選択します。

表 *20* : 電話システムトランクの設定

フィールド	設定
電話システム元（From Phone System）	トランクを作成する電話システムの表示名を選択します。
電話システム先（To Phone System）	トランクが接続する既存の電話システムの表示名を選択します。
トランクアクセスコード（Trunk Access Code）	以前の既存の電話システムでゲートウェイを使用してコールを内線に転送するために Unity Connection でダイヤルする必要がある追加コードを入力します。

ステップ 21 作成する残りすべての電話システムトランクについて、ステップ 18 とステップ 19 を繰り返します。

Next Generation Security Over SIP 統合を有効にする

Unity Connection では、暗号化アルゴリズムを使用して機密性、整合性、および認証を提供する Next Generation Security over SIP インターフェイスがサポートされています。次世代暗号化により、SIP インターフェイスは TLS 1.2、SHA-2、および AES256 プロトコルに基づいて Suite B暗号を使用するように制限されるため、より安全です。次世代暗号化には、暗号に加えて、Unity Connection と Cisco Unified CM の両方にアップロードする必要があるサードパーティ証明書も含まれています。Unity Connection と Cisco Unified CM 間の通信中に、暗号とサードパーティ証明書の両方が両端で検証されます。次に、次世代暗号化サポートの設定を示します。

証明書を生成、アップロードする

Unity Connection は、次世代のセキュリティのために、RSA キーベースの Tomcat 証明書と EC キーベースの Tomcat-ECDSA 証明書（自己署名およびサードパーティ）を使用します。各証明書の設定については、以降のセクションで説明します。

RSA キーベースの証明書を設定する

Unity Connection の RSA キーベースの証明書を生成する

次に、Unity Connection の RSA キーベースの証明書を生成し、Cisco Unified CM にアップロードする手順を示します。

ステップ 1 Unity Connection で、[Cisco Unified Operating System Administration] ページにサインインします。

ステップ 2 [セキュリティ（Security）] に移動し、**[証明書の管理（Certificate Management）]** を選択します。

ステップ 3 Unity Connection の自己署名証明書を生成する場合は、ステップ 4 からステップ 6 に従います。それ以外の場合は、 ステップ 7に進みます。

ステップ 4 [証明書管理（Certificate Management）] ページで、**[自己署名の生成（Generate Self Signed）]** を選択します。

ステップ 5 [自己署名の生成（Generate Self-Signed）] ウィンドウで、[証明書の目的（Certificate Purpose）] で **[Tomcat]** を選択します

ステップ 6 **[作成（Generate）]** を選択します。

ステップ 7 RSA キーベースのサードパーティ証明書を生成するには、[証明書管理（Certificate Management）] ページで **[CSR の生成（Generate CSR）]** を選択します。

ステップ 8 [証明書署名要求の生成（Generate Certificate Signing Request）] ウィンドウで、[証明書の目的（Certificate Purpose）] フィールドで **[tomcat]** を選択します。

ステップ 9 [親ドメイン（Parent Domain）] フィールドに、Unity Connection の完全な FQDN を入力します。

ステップ 10 **[作成（Generate）]** を選択します。

ステップ 11 [証明書リスト（Certificate List）] ページで、**[CSR のダウンロード（Download CSR）]** を選択します。これにより、Microsoft CA または Verisign であるサードパーティから Unity Connection 証明書が生成されます。

ステップ 12 Unity Connection のリーフ証明書と認証局のルート/チェーン証明書をシステムに保存します。

ステップ 13 [証明書一覧（Certificate List）] ページで、**[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）]** を選択します。

ステップ 14 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] ウィンドウで、[証明書の目的（Certificate Purpose）] フィールドで **[tomcat]** を選択します。

ステップ 15 [ファイルのアップロード（Upload File）] に移動し、**[参照（Browse）]** を選択して、 ステップ 12で保存したサードパーティ CSR によって生成された Unity Connection リーフ証明書をアップロードします。

ステップ 16 **[アップロード（Upload）]** を選択します。

ステップ 17 Cisco Unified CM で、[Cisco Unified Operating System Administration] ページにサインインします。

ステップ 18 [セキュリティ（Security）] に移動し、**[証明書の管理（Certificate Management）]** を選択します。

ステップ 19 [証明書一覧（Certificate List）] ページで、**[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）]** を選択します。

ステップ 20 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] ウィンドウで、[証明書の目的（Certificate Purpose）] フィールドで **[CallManager-trust]** を選択します。

ステップ 21 [ファイルのアップロード（Upload File）] に移動し、[参照（Browse）] を選択して、ステップ 6 で生成した Unity Connection 自己署名証明書をアップロードします。Unity Connection のサードパーティ証明書をアップロードするには、ステップ 12 で保存したサードパーティ認証局のルート/チェーン証明書を参照します。

（注） Unity Connection クラスタの場合は、Cisco Unified CM の CallManager-trust でパブリッシャとサブスクライバの両方の自己署名証明書を生成してアップロードします。

ステップ 22 **[アップロード（Upload）]** を選択します。

Cisco Unified CM の RSA ベースの証明書を生成する

Cisco Unified CM の RSA ベースの証明書を生成し、Unity Connection にアップロードする手順は次のとおりです。

ステップ 1 Cisco Unified CM で、[Cisco Unified Operating System Administration] ページにサインインします。

ステップ 2 [セキュリティ（Security）] に移動し、**[証明書の管理（Certificate Management）]** を選択します。

ステップ 3 Cisco Unified CM の自己署名証明書を生成する場合は、 ステップ 4 ～ 6に従います。それ以外の場合は、ステップ 7に進みます。

ステップ 4 [証明書管理（Certificate Management）] ページで、**[自己署名の生成（Generate Self Signed）]** を選択します。

ステップ 5 [新しい自己署名証明書の生成（Generate New Self Signed Certificate）] ウィンドウで、**[証明書の目的（Certificate Purpose）]** フィールドで **[CallManager]** を選択します。

ステップ 6 **[作成（Generate）]** を選択します。

ステップ 7 RSA キーベースのサードパーティ証明書を生成するには、[証明書管理（Certificate Management）] ページで **[CSR の生成（Generate CSR）]** を選択します。

ステップ 8 [証明書署名要求の生成（Generate Certificate Signing Request）] ウィンドウで、[証明書の目的（Certificate Purpose）] フィールドで **[CallManager]** を選択します。

ステップ 9 [親ドメイン（Parent Domain）] フィールドに、Cisco Unified CM の完全な FQDN を入力します。

ステップ 10 **[作成（Generate）]** を選択します。

ステップ 11 [証明書リスト（Certificate List）] ページで、**[CSR のダウンロード（Download CSR）]** を選択します。これにより、Microsoft CA または Verisign であるサードパーティから Cisco Unified CM 証明書が生成されます。

ステップ 12 Cisco Unified CM のリーフ証明書と認証局のルート/チェーン証明書をシステムに保存します。

ステップ 13 [証明書一覧（Certificate List）] ページで、**[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）]** を選択します。

ステップ 14 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] ウィンドウで、[証明書の目的（Certificate Purpose）] フィールドで **[CallManager]** を選択します。

ステップ 15 [ファイルのアップロード（Upload File）] に移動し、[参照（Browse）] を選択して、 ステップ 12で保存したサードパーティ CSR によって生成された Cisco Unified CM リーフ証明書をアップロードします。

ステップ 16 **[アップロード（Upload）]** を選択します。

（注） 証明書はポートグループのリセット時に自動的にダウンロードされるため、Unity Connection で CallManager 証明書を手動でアップロードする必要はありません。ただし、サードパーティ証明書の場合は、Unity Connection の **CallManager-trust** にサードパーティ認証局のルート証明書をアップロードする必要があります。

EC キーベースの証明書を設定する

Unity Connection の EC キーベースの証明書を生成する

次に、Unity Connection の EC キーベースの証明書を生成し、Cisco Unified CM にアップロードする手順を示します。

ステップ 1 Unity Connection で、[Cisco Unified Operating System Administration] ページにサインインします。

ステップ 2 [セキュリティ（Security）] に移動し、[証明書の管理（Certificate Management）] を選択します。

ステップ 3 Unity Connection の自己署名証明書を生成する場合は、ステップ 4 からステップ 6 に従います。それ以外の場合は、ステップ 7 に進みます。

ステップ 4 [証明書管理（Certificate Management）] ページで、[自己署名の生成（Generate Self Signed）] を選択します。

ステップ 5 [新しい自己署名証明書の生成（Generate New Self Signed Certificate）] ウィンドウで、[証明書の目的（Certificate Purpose）] フィールドで [tomcat-ECDSA] を選択します。

ステップ 6 [作成（Generate）] を選択します。

ステップ 7 EC キーベースのサードパーティ証明書を生成するには、[証明書管理（Certificate Management）] ページで [CSR の生成（Generate CSR）] を選択します。

ステップ 8 [証明書署名要求の生成（Generate Certificate Signing Request）] ウィンドウで、[証明書の目的（Certificate Purpose）] フィールドで [tomcat-ECDSA] を選択します。

ステップ 9 [親ドメイン（Parent Domain）] フィールドに、Unity Connection の完全な FQDN を入力します。

ステップ 10 [作成（Generate）] を選択します。

ステップ 11 [証明書リスト（Certificate List）] ページで、[CSR のダウンロード（Download CSR）] を選択します。これにより、Microsoft CA または Verisign であるサードパーティから Unity Connection ECDSA 証明書が生成されます。

ステップ 12 Unity Connection のリーフ証明書と認証局のルート/チェーン証明書をシステムに保存します。

ステップ 13 [証明書の検索と一覧表示（Find and List Certificates）] ページで、[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] を選択します。

ステップ 14 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] ウィンドウで、[証明書の目的（Certificate Purpose）] フィールドで [tomcat-ECDSA] を選択します。

ステップ 15 [ファイルのアップロード（Upload File）] に移動し、[参照（Browse）] を選択して、ステップ 12 で保存したサードパーティ CSR によって生成された Unity Connection リーフ証明書をアップロードします。

ステップ 16 [アップロード（Upload）] を選択します。

ステップ 17 Cisco Unified CM で、[Cisco Unified Operating System Administration] ページにサインインします。

ステップ 18 [セキュリティ（Security）] に移動し、[証明書の管理（Certificate Management）] を選択します。

ステップ 19 [証明書一覧（Certificate List）] ページで、[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] を選択します。

ステップ 20 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] ウィンドウで、[証明書の目的（Certificate Purpose）] フィールドで [CallManager-trust] を選択します。

ステップ 21 [ファイルのアップロード（Upload File）] に移動し、[参照（Browse）] を選択して、ステップ 6 で生成した Unity Connection 自己署名証明書をアップロードします。Unity Connection のサードパーティ証明書をアップロードするには、ステップ 12 で保存したサードパーティ認証局のルート/チェーン証明書を参照します。

（注） Unity Connection クラスタの場合は、Cisco Unified CM の CallManager-trust でパブリッシャとサブスクライバの両方の自己署名証明書を生成してアップロードします。

ステップ 22 [アップロード（Upload）] を選択します。

Cisco Unified CM の EC キーベースの証明書を生成する

Cisco Unified CM の EC キーベースの証明書を生成し、Unity Connection にアップロードする手順は次のとおりです。

ステップ 1 Cisco Unified CM で、[Cisco Unified Operating System Administration] ページにサインインします。

ステップ 2 [セキュリティ（Security）] に移動し、[証明書の管理（Certificate Management）] を選択します。

ステップ 3 Cisco Unified CM の自己署名証明書を生成する場合は、ステップ 4 ～ 6 に従います。それ以外の場合は、ステップ 7 に進みます。

ステップ 4 [証明書管理（Certificate Management）] ページで、[自己署名の生成（Generate Self Signed）] を選択します。

ステップ 5 [新しい自己署名証明書の生成（Generate New Self Signed Certificate）] ウィンドウで、[証明書の目的（Certificate Purpose）] フィールドで [CallManager-ECDSA] を選択します。

ステップ 6 [作成（Generate）] を選択します。

ステップ 7 EC キーベースのサードパーティ証明書を生成するには、[証明書管理（Certificate Management）] ページで [CSR の生成（Generate CSR）] を選択します。

ステップ 8 [証明書署名要求の生成（Generate Certificate Signing Request）] ウィンドウで、[証明書の目的（Certificate Purpose）] フィールドで [CallManager-ECDSA] を選択します。

ステップ 9 [親ドメイン（Parent Domain）] フィールドに、Cisco Unified CM の完全な FQDN を入力します。

ステップ 10 [作成（Generate）] を選択します。

ステップ 11 [証明書リスト（Certificate List）] ページで、[CSR のダウンロード（Download CSR）] を選択します。これにより、Microsoft CA または Verisign であるサードパーティから Cisco Unified CM 証明書が生成されます。

ステップ 12 Cisco Unified CM のリーフ証明書と認証局のルート/チェーン証明書をシステムに保存します。

ステップ 13 [証明書一覧（Certificate List）] ページで、[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] を選択します。

ステップ 14 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] ウィンドウで、[証明書の目的（Certificate Purpose）] フィールドで [CallManager-ECDSA] を選択します。

ステップ 15 [ファイルのアップロード（Upload File）] に移動し、[参照（Browse）] を選択して、ステップ 12 で保存したサードパーティ CSR によって生成された Cisco Unified CM リーフ証明書をアップロードします。

ステップ 16 **[アップロード（Upload）]** を選択します。

（注） 証明書はポートグループのリセット時に自動的にダウンロードされるため、Unity Connection で CallManager 証明書を手動でアップロードする必要はありません。ただし、サードパーティ証明書の場合は、Unity Connection の **CallManager-trust** にサードパーティ認証局のルート証明書をアップロードする必要があります。

セキュリティモードを設定する

ステップ 1 Cisco Unity Connection Administration にサインインします。

ステップ 2 Cisco Unity Connection Administration で、**[テレフォニー統合（Telephony Integrations）]** を展開し、**[ポートグループ（Port Group）]** を選択します。

ステップ 3 [ポートグループの検索（Search Port Groups）] ページで、該当するポートグループを選択します。

ステップ 4 **[次世代暗号化の有効化（Enable Next Generation Encryption）]** チェックボックスがオンになっていることを確認します。

ステップ 5 Cisco Unified CM Administration にサインインします。

ステップ 6 **[システム（System）]** > **[セキュリティ（Security）]** に移動し、**[SIP トランクセキュリティプロファイル（SIP Trunk Security Profile）]** を選択します。

ステップ 7 [SIP トランク セキュリティ プロファイルの検索と一覧表示（Find and List SIP Trunk Security Profiles）] ページで、SIP トランク セキュリティ プロファイルを作成するの手順で作成した SIP トランク セキュリティ プロファイルを選択します。

ステップ 8 [SIP トランク セキュリティ プロファイルの設定（SIP Trunk Security Profile Configuration）] ページで、**[X.509 サブジェクト名（X.509 Subject Name）]** に入力した値が対応する Unity Connection サーバーの FQDN であることを確認します。

ステップ 9 TLS 暗号の設定の項の説明に従って、TLS 暗号を設定します。

TLS 暗号の設定

次に、Unity Connection および Cisco Unified CM で TLS 暗号オプションを設定する手順を示します。

ステップ 1 Cisco Unified CM Administration で、**[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]** の順に選択します。

ステップ 2 **[セキュリティパラメータ（Security Parameters）]** の **[TLS 暗号（TLS Ciphers）]** ドロップダウンリストから適切な暗号オプションを選択します。

ステップ 3 画面の右隅にあるナビゲーションウィンドウで、**[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）]** を選択し、**[移動（Go）]** を選択します。

ステップ 4 [Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] ページで、**[ツール（Tools）]** > **[コントロールセンター - 機能サービス（Control Centre-Feature Services）]** に移動し、[CMサービス（CM Services）] で **[Cisco Call Manager]** を選択します。

ステップ 5 **[再起動（Restart）]** を選択します。

（注） Cisco Unified CM クラスタの場合は、パブリッシャサーバーとサブスクライバサーバーの両方で Cisco Call Manager サービスを再起動する必要があります。

ステップ 6 [Cisco Unity Connection の管理（Cisco Unity Connection Administration）] ページにサインインし、**[システム設定（System Settings）]** を展開し、**[全般設定（General Configuration）]** を選択します。

ステップ 7 **[TLS 暗号（TLS Ciphers）]** ドロップダウンリストから適切な暗号を選択します。

ステップ 8 画面の右隅にあるナビゲーションウィンドウで、**[Cisco Connection Serviceability]** を選択し、**[移動（Go）]** を選択します。

ステップ 9 **[ツール（Tools）]** > **[サービス管理（Service Management）]** に移動し、**Connection Conversation Manager** を停止します。Connection Conversation Manager サービスが停止したら、再度開始します。

（注） Unity Connection クラスタの場合は、パブリッシャとサブスクライバの両方で **Connection Conversation Manager** を再起動する必要があります。

ステップ 10 証明書を生成、アップロードするのセクションの説明に従って、RSA および EC キーベースの証明書を生成してアップロードします。

次の表に、RSA または ECDSA 暗号の優先順に TLS 暗号オプションを示します。

表 *21 : TLS* 暗号オプションと優先順位

TLS 暗号オプション	TLS 暗号（優先順）
最も強力：AES-256 SHA-384 のみ：RSA 推奨	• TLS_ECDHE_RSA_WITH_A • TLS_ECDHE_ECDSA_WITH
強力：AES-256 SHA-384 のみ：ECDSA 推奨	• TLS_ECDHE_ECDSA_WITH • TLS_ECDHE_RSA_WITH_A
中：AES-256 AES-128のみ：RSA 推奨	• TLS_ECDHE_RSA_WITH_A • TLS_ECDHE_ECDSA_WITH • TLS_ECDHE_RSA_WITH_A • TLS_ECDHE_ECDSA_WITH
中：AES-256 AES-128 のみ：ECDSA 推奨	• TLS_ECDHE_ECDSA_WITH • TLS_ECDHE_RSA_WITH_A • TLS_ECDHE_ECDSA_WITH • TLS_ECDHE_RSA_WITH_A
すべての暗号方式：RSA 推奨（デフォルト）	• TLS_ECDHE_RSA_WITH_A • TLS_ECDHE_ECDSA_WITH • TLS_ECDHE_RSA_WITH_A • TLS_ECDHE_ECDSA_WITH • TLS_RSA_WITH_AES_128_C
すべての暗号方式: ECDSA優先	• TLS_ECDHE_ECDSA_WITH • TLS_ECDHE_RSA_WITH_A • TLS_ECDHE_ECDSA_WITH • TLS_ECDHE_RSA_WITH_A • TLS_RSA_WITH_AES_128_C

Unity Connection と Cisco Unified Communications Manager 間のネゴシエーションは、次の条件の TLS 暗号設定に依存します。

- Unity Connection がサーバーとして機能する場合、TLS 暗号ネゴシエーションは、Cisco Unified CM によって選択された設定に基づきます。
  - ECDSA ベースの暗号がネゴシエートされる場合、EC キーベースの tomcat-ECDSA 証明書が SSL ハンドシェイクで使用されます。
  - RSA ベースの暗号がネゴシエートされる場合、RSA キーベースの Tomcat 証明書が SSL ハンドシェイクで使用されます。

- Unity Connection がクライアントとして機能する場合、TLS 暗号ネゴシエーションは Unity Connection によって選択された設定に基づきます。

SRTP 暗号の設定

Next Generation Security over RTP インターフェイスを有効にするには、次のように SRTP 暗号を設定します。

ステップ 1 Cisco Unified CM Administration で、**[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]** の順に選択します。

ステップ 2 **[セキュリティパラメータ（Security Parameters）]** の **[SRTP 暗号（SRTP Ciphers）]** ドロップダウンリストから適切な暗号オプションを選択します。

ステップ 3 画面の右隅にあるナビゲーションウィンドウで、**[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）]** を選択し、**[移動（Go）]** を選択します。

ステップ 4 [Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] ページで、**[ツール（Tools）]** > **[コントロールセンター - 機能サービス（Control Centre-Feature Services）]** に移動し、[CMサービス（CM Services）] で **[Cisco Call Manager]** を選択します。

ステップ 5 **[再起動（Restart）]** を選択します。

（注） Cisco Unified CM クラスタの場合は、パブリッシャサーバーとサブスクライバサーバーの両方で Cisco Call Manager サービスを再起動する必要があります。

ステップ 6 [Cisco Unity Connection の管理（Cisco Unity Connection Administration）] ページにサインインし、**[システム設定（System Settings）]** を展開し、**[全般設定（General Configuration）]** を選択します。

ステップ 7 **[SRTP 暗号（SRTP Ciphers）]** ドロップダウンリストから適切な暗号を選択します。

ステップ 8 画面の右隅にあるナビゲーションウィンドウで、**[Cisco Connection Serviceability]** を選択し、**[移動（Go）]** を選択します。

ステップ 9 **[ツール（Tools）]** > **[サービス管理（Service Management）]** に移動し、**Connection Conversation Manager** を停止します。Connection Conversation Manager サービスが停止したら、再度開始します。

（注） Unity Connection クラスタの場合は、パブリッシャとサブスクライバの両方で **Connection Conversation Manager** を再起動する必要があります。

次の表に、RSA または ECDSA 暗号の優先順に SRTP 暗号オプションを示します。

表 *22 : SRTP* 暗号オプションと優先順位

SRTP 暗号オプション	優先順位の **SRTP**
すべてのサポートされているAES-256およびAES-128暗号方式	• AEAD_AES_256_GCM • AEAD_AES_128_GCM • AES_CM_128_HMAC_SHA1_32 • AES_CM_128_HMAC_SHA1_80
AEAD AES-256、AES-28 GCMベース暗号方式	• AEAD_AES_256_GCM • AEAD_AES_128_GCM
AEAD AES256 GCMベースの暗号方式のみ	AEAD_AES_256_GCM

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。