Cisco Unity Connection 向け SIP インテグレーション ガイド

リリース 11.x

2015 年 5 月発行

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
所在地、電話番号、FAX 番号
は以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices.

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

『SIP Integration Guide for Cisco Unity Connection Release 11.x』

はじめに

ここでは、次の内容について説明します。

対象読者および使用

このマニュアルでは、Cisco Unity Connection とサポート対象バージョンの Cisco Unified Communications Manager との連動を設定する手順について説明します。SIP トランクを介した Cisco Unity Connection との連動がサポートされている Cisco Unified CM のバージョンのリストについては、『*Cisco Unity Connection の互換性マトリクス*』（http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html）を参照してください。

表記法

『SIP Integration Guide for Cisco Unity Connection Release 11.x』では、次の表記法を使用しています。

表 1　　『SIP Integration Guide for Cisco Unity Connection Release 11.x』の表記法

表記法	説明
太字	次の場合は太字を使用します。 • キーおよびボタン名（例：[OK] を選択します）。 • ユーザが入力する情報（例：[ユーザ名（User Name）] ボックスに **Administrator** と入力します）。
< > （山カッコ）	ユーザが値を指定するパラメータを囲むために使用します（例：[コマンド プロンプト（Command Prompt）] ウィンドウで **ping <IP アドレス>** と入力します）。

表 1　『SIP Integration Guide for Cisco Unity Connection Release 11.x』の表記法（続き）

表記法	説明
- （ハイフン）	同時に押す必要があるキーを表します（例：**Ctrl-Alt-Delete** を押します）。
> （右向きの山カッコ）	メニュー上の選択項目を区切るために使用します（例：Windows の [スタート] メニューから [プログラム] > [Cisco Unified Serviceability] > [Real-Time Monitoring Tool] の順に選択します）。 Cisco Unity Connection Administration のナビゲーション バー（例：Cisco Unity Connection Administration で、[システム設定] > [詳細設定] と展開します）。

『SIP Integration Guide for Cisco Unity Connection Release 11.x』では、次の表記法も使用します。

Cisco Unity Connection のマニュアル

Cisco.com にある Cisco Unity Connection のマニュアルの説明と URL については、『*Documentation Guide for Cisco Unity Connection*』を参照してください。このマニュアルは Unity Connection に同梱されており、次の URL からも入手できます。
http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/roadmap/11xcucdg.html

Cisco Business Editionに関するマニュアル リファレンス

Unity Connection 11.x マニュアル セットでは、Cisco Business Edition への参照は Business Edition 6000 および 7000 に適用されます。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は Really Simple Syndication（RSS）フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

シスコ製品のセキュリティ

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、http://www.access.gpo.gov/bis/ear/ear_data.html で参照できます。

連動の説明

はじめに

SIP トランク連動は、SIP プロトコルを使用して Unity Connection と Cisco Unified CM 間の通信を確立する方法です。

SIP トランクを介した Cisco Unity Connection との連動がサポートされている Cisco Unified CM のバージョンのリストについては、『*Cisco Unity Connection の互換性マトリクス*』（http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html）を参照してください。

連動の機能

Cisco Unity Connection との Cisco Unified CM SIP トランク連動には、次の機能が用意されています。

- パーソナル グリーティングへの自動転送
- 通話中グリーティングへの自動転送
- 発信者 ID
- 容易なメッセージ アクセス（ユーザは ID を入力しなくてもメッセージを取得できます。Cisco Unity Connection では、通話発信元の内線番号に基づいてユーザを識別します。パスワードが必要になる場合があります）。
- 識別されたユーザのメッセージ（Cisco Unity Connection では、転送された内線通話中にメッセージを残したユーザを、通話発信元の内線番号に基づいて自動的に識別します）。
- メッセージ待機インジケータ（MWI）

この連動の機能は、次に説明する問題の影響を受ける場合があります。

Cisco Unified Survivable Remote Site Telephony（SRST）ルータの使用

ネットワークに Cisco Unified Survivable Remote Site Telephony（SRST）ルータが含まれている状況で、Cisco Unified SRST ルータが Cisco Unified CM から通話処理機能を引き継いだ場合（WAN リンクのダウンなどの理由で）、支社の電話機は動作を続行できます。ただし、この場合は、連動機能に次の制約が加えられます。

- **通話中グリーティングへの通話転送**：Cisco Unified SRST ルータが PSTN に対して FXO/FXS 接続を使用している状況で、支社から Cisco Unity Connection に着信が転送された場合、通話中グリーティングを再生することはできません。

- **内線グリーティングへの通話転送**：Cisco Unified SRST ルータが PSTN に対して FXO/FXS 接続を使用している状況で、支社から Cisco Unity Connection に着信が転送された場合、内線グリーティングを再生することはできません。PSTN は FXO 回線の発番号を提供するため、発信者はユーザとして識別されません。
- **着信転送**：PSTN に到達するにはアクセス コードが必要であるため、Unity Connection から支社への着信転送は失敗します。
- **識別されているユーザのメッセージ**：Cisco Unified SRST ルータが PSTN に対して FXO/FXS 接続を使用し、支社のユーザがメッセージを残したり通話を転送したりする場合、そのユーザは識別されません。発信者は、身元不明発信者と表示されます。
- **メッセージ待機インジケータ**：MWI は支社の電話機では更新されません。そのため、新規メッセージが到着した場合や、すべてのメッセージを聞いた場合、MWI はその状況を正しく反映しません。WAN リンクが再確立された場合は、MWI を再同期化することを推奨します。
- **ルーティング規則**：Cisco Unified SRST ルータが PSTN に対して FXO/FXS 接続を使用している状況で、支社から Unity Connection に着信が到達した場合（一般の着信または転送呼）、ルーティング規則は失敗します。

Cisco Unified SRST ルータが PRI/BRI 接続を使用している場合、支社から Unity Connection への通話の発信者 ID は、PSTN によって提供される完全な番号（局番および内線番号）となる場合があるため、Unity Connection ユーザの内線番号と一致しないことがあります。このケースに該当する場合は、代行内線番号を使用して発信者 ID を認識するように Unity Connection を設定できます。

SRST を使用する場合は、Redirected Dialed Number Information Service（RDNIS）がサポートされている必要があります。

Cisco Unified SRST ルータの設定については、該当する『*Cisco Unified SRST System Administrator Guide*』の「Integrating Voice Mail with Cisco Unified SRST」の章を参照してください。このドキュメントは、http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html にあります。

AAR によって転送されるボイス メール通話に与える RDNIS の送信不能の影響

自動代替ルーティング（AAR）を使用する場合は、RDNIS がサポートされている必要があります。

AAR では、WAN が加入過多の状態になった場合に、PSTN を介して通話を転送できます。ただし、PSTN を介して再転送される場合は、RDNIS が影響を受けることがあります。Cisco Unity Connection がそのメッセージ クライアントに対してリモートである場合は、RDNIS 情報に誤りが生じることにより、AAR が PSTN を介して再転送するボイス メール通話が影響を受けることがあります。RDNIS 情報が誤っている場合、通話はダイヤル先のユーザのボイス メール ボックスに到達せず、代わりに自動応答プロンプトを受信します。その場合、発信者は、到達先の内線番号の再入力を要求されることがあります。この動作は主に、電話通信事業者がネットワークを介した RDNIS を保証できない場合の問題です。通信事業者が RDNIS の正常な送信を保証できない理由は数多くあります。通信事業者に問い合わせて、回線のエンドツーエンドで RDNIS の送信を保証しているかどうかを確認してください。オーバーサブスクリプションの状態になった WAN に対して AAR を使用する代わりの方法は、単に、オーバーサブスクリプションの状況で発信者にリオーダー トーンが聞こえるようにすることです。

複数の電話システムとの連動

Unity Connection は、複数の電話システムと同時に連動できます。サポートされる最大の組み合わせ数、および Unity Connection と複数の電話システムを連動させる手順については、『*Multiple Phone System Integration Guide for Cisco Unity Connection Release 11.x*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/integration/guide/multiple_integration/cuc11xintmultiple.html にあります。

集中型ボイス メッセージ

Unity Connection は、電話システムを使用した集中型ボイス メッセージをサポートしており、Avaya DCS、Nortel MCDN、Siemens CorNet などの専用プロトコルや、QSIG または DPNSS などの規格ベースのプロトコルなど、さまざまな電話システム間ネットワーキング プロトコルをサポートしています。集中型ボイス メッセージは電話システムとそのインターフォン システム ネットワークの機能であり、ボイス メールではないことに注意してください。Unity Connection では、電話システムとそのインターフォン システム ネットワーキングが正しく設定されている場合に、集中型ボイス メッセージをサポートします。詳細については、『*Design Guide for Cisco Unity Connection, Release 11.x*』の「Integrating Cisco Unity Connection with the Phone System」章の「Centralized Voice Messaging の項を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/design/guide/11xcucdgx.html にあります。

Cisco Unity Connection におけるボイス メッセージ ポートの使用方法の計画

ポート設定の計画

電話システムをプログラミングする前に、ボイス メッセージ ポートを Cisco Unity Connection でどのように使用するかを計画する必要があります。次の考慮事項は、電話システムのプログラミング（ハント グループの設定、ボイス メッセージ ポートへのコール転送など）に影響を与えます。

- インストール済みのボイス メッセージ ポートの数。

  Unity Connection クラスタでは、他のサーバが機能停止した場合に、すべてのボイス メッセージ トラフィックを処理するのに十分なポートが各 Unity Connection サーバに割り当てられている必要があります。

- 通話に応答するボイス メッセージ ポートの数。
- 発信専用ボイス メッセージ ポートの数。このポートは、たとえば、メッセージの到着通知の送信、メッセージ受信インジケータ（MWI）の設定、および電話での録音および再生（TRAP）接続の確立などを行います。

次の表は、Cisco Unity Connection Administration の [テレフォニー統合（Telephony Integration）] > [ポート（Port）] で設定できる、Unity Connection のボイス メッセージ ポートの設定を示しています。

表 2-1　ボイス メッセージ ポートの設定

フィールド	説明
有効化（Enabled）	このチェックボックスをオンにします。
サーバ（Server）	*（Unity Connection クラスタが構成されている場合）*このポートを処理する Unity Connection サーバの名前を選択します。 等しい数の応答ボイス メッセージ ポートと発信ボイス メッセージ ポートを Unity Connection サーバに割り当てて、これらのポートがボイス メッセージ トラフィックを等しく共有するようにします。

表 2-1　ボイス メッセージ ポートの設定（続き）

フィールド	説明
コールへの応答（Answer Calls）	このチェックボックスをオンにします。 **注意**　Cisco Unified CM サーバに接続するすべてのボイス メッセージ ポートで、[コールへの応答（Answer Calls）] チェックボックスがオンになっている必要があります。オフになっていると、Unity Connection への通話が応答されない場合があります。
メッセージ通知を実行する（Perform Message Notification）	ポートをユーザ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。
MWI 要求を送信する（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。
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、ユーザは Unity Connection の Web アプリケーションで電話機を録音および再生デバイスとして使用することができます。

インストールするボイス メッセージ ポートの数の決定

インストールするボイス メッセージ ポートの数は、次のような数多くの要因によって決まります。

- コール トラフィックがピーク状態のときに Unity Connection が応答する通話の数。
- 発信者が録音してユーザが聞く個々のメッセージの想定される長さ。
- ユーザ数。
- 発信専用に設定されるポートの数。
- メッセージの到着通知のために発信する通話の数。
- コール トラフィックがピーク状態のときにアクティブにする MWI の数。
- コール トラフィックがピーク状態のときに必要になる TRAP 接続の数（TRAP 接続は、Unity Connection の Web アプリケーションが電話で再生および録音するときに使用します）。
- コール トラフィックがピーク状態のときに自動受付およびコール ハンドラを使用する通話の数。
- Unity Connection クラスタが設定されているかどうか。詳細については、「Unity Connection クラスタに関する考慮事項」セクション（2-3 ページ）を参照してください。

システム リソースが未使用ポートに割り当てられない範囲で、必要な数のボイス メッセージ ポートだけをインストールすることを推奨します。

通話に応答するボイス メッセージ ポートの数の決定

ボイス メッセージ ポートが応答する通話は、身元不明の発信者やユーザからの着信コールであることもあります。通常、通話に応答するボイス メッセージ ポートは、稼働率が最も高くなります。

ボイス メッセージ ポートは、通話への応答と発信（たとえば、メッセージの到着通知を送信する）の両方を行うように設定できます。ただし、ボイス メッセージ ポートが複数の機能を実行する場合、稼働率の高い状態にある（たとえば、多数の通話に応答している）ときは、残りの機能はボイス メッセージ ポートが開放されるまで遅延されることがあります（たとえば、応答する通話数が減るまでメッセージの到着通知を送信できない）。最高のパフォーマンスを得るには、ボイス メッセージ ポートを応答専用と発信専用に分けます。ポートの機能を分割することにより、コリジョンが発生する可能性を最小限に抑えることができます。このようにした場合、Unity Connection がポートをオフフックにして発信すると同時に、着信コールがポートに到着します。

システムが Unity Connection クラスタ用に設定されている場合は、「Unity Connection クラスタに関する考慮事項」セクション（2-3 ページ）を参照してください。

発信するボイス メッセージ ポートの数の決定

発信専用でコールに応答しないポートは、次に示す 1 つ以上の処理を実行できます。

- メッセージが到着したことを、電話、ポケットベル、または電子メールでユーザに通知する。
- ユーザの内線で MWI のオンとオフを切り替える。
- TRAP 接続を確立して、ユーザが Unity Connection の Web アプリケーションで電話機を録音および再生デバイスとして使用できるようにする。

通常、このようなボイス メッセージ ポートは最も稼働率が低いポートです。

システムが Cisco Unity Connection クラスタ用に設定されている場合は、「Unity Connection クラスタに関する考慮事項」セクション（2-3 ページ）を参照してください。

注意　電話システムをプログラムするときは、通話に応答できない Cisco Unity Connection のボイス メッセージ ポート（[コールに応答する（Answer Calls）] に設定されていないボイス メッセージ ポート）に通話を送信しないようにしてください。たとえば、ボイス メッセージ ポートを [MWI 要求を送信する（Send MWI Requests）] だけに設定した場合、そのポートに通話を送信しないでください。

Unity Connection クラスタに関する考慮事項

システムが Unity Connection クラスタ用に設定されている場合は、さまざまなシナリオでのボイス メッセージ ポートの使用方法について検討してください。

両方の Unity Connection サーバが機能している場合

- ハント グループは、着信を最初にサブスクライバ サーバに送信し、次に、サブスクライバ サーバで応答ポートを使用できない場合はパブリッシャ サーバに送信します。
- 両方の Unity Connection サーバがアクティブで、システムのボイス メッセージ トラフィックを処理します。

- Cisco Unity Connection Administrationでは、等しい数のボイス メッセージ ポートが各 Unity Connection サーバに割り当てられるようにボイス メッセージ ポートが設定されます。このマニュアルでは、適切な時期にボイス メッセージ ポートを特定のサーバに割り当てるよう推奨しています。
- 1 つの Unity Connection サーバに割り当てられるボイス メッセージ ポートの数は、他の Unity Connection サーバが機能停止したときにシステムのすべてのボイス メッセージ トラフィック（応答と発信）を処理するのに十分である必要があります。

  ボイス メッセージ トラフィックを処理するために両方の Unity Connection サーバが機能している必要がある場合は、いずれかのサーバが機能停止するとシステムの容量は十分ではなくなります。
- 各 Unity Connection サーバには、ボイス メッセージ ポート数の合計の半分が割り当てられます。

  すべてのボイス メッセージ ポートが 1 つの Unity Connection サーバに割り当てられると、もう 1 つの Unity Connection サーバは通話に応答したり、発信したりできなくなります。
- 各 Unity Connection サーバには、通話に応答し、（たとえば、MWI を設定するために）発信できるボイス メッセージ ポートが必要です。

1 つの Unity Connection サーバだけが機能している場合

- 電話システムのハント グループが、機能している Unity Connection サーバにすべての通話を送信します。
- 機能している Unity Connection サーバは、システムのすべてのボイス メッセージ トラフィックを受信します。
- 機能している Unity Connection サーバに割り当てられるボイス メッセージ ポートの数は、システムのすべてのボイス メッセージ トラフィック（応答と発信）を処理するのに十分である必要があります。
- 機能している Unity Connection サーバには、通話に応答し、（たとえば、MWI を設定するために）発信できるボイス メッセージ ポートが必要です。

  機能している Unity Connection サーバに通話応答用のボイス メッセージ ポートがない場合、システムは着信コールに応答できません。同様に、機能している Unity Connection サーバに発信用のボイス メッセージ ポートがない場合、システムは（たとえば、MWI を設定するために）発信できません。

Cisco Unified Communications Manager SIP トランク連動の設定

この章では、Cisco Unity Connection との Cisco Unified Communications Manager SIP トランク連動の設定方法について説明します。Unity Connection が Cisco Unified CM と同じサーバに Cisco Business Edition としてインストールされている構成の場合、このマニュアルは該当しません。

（注） 分散電話システムでトランク全体に MWI リレーを設定する場合は、Cisco Unified CM のマニュアルを参照して、要件や手順を確認する必要があります。トランク全体に MWI リレーを設定する場合、Unity Connection を設定する必要はありません。

Cisco Unified CM の保留音（MoH）機能は、Cisco Unified CM SIP トランク連動の監視転送が行われている間は利用できません。

連動のタスク

次のタスクを実行して SIP トランクにより Unity Connection と Cisco Unified CM を連動させるには、その前に、『*Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 11.x,*』の「Installing Cisco Unity Connection」の章の該当するタスクを実行し、連動に向けて Unity Connection サーバの準備をします。このドキュメントは、http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/11xcuciumgx.html から入手できます。

Cisco Unified CM SIP トランク連動を設定するには、次のタスク リストを使用します。

1. システムや機器の要件を確認して、すべての電話システムおよび Unity Connection サーバが要件を満たしていることを確認します。「要件」セクション（3-2 ページ）
2. Unity Connection によるボイス メッセージ ポートの使用方法を計画します。第 2 章「Cisco Unity Connection におけるボイス メッセージ ポートの使用方法の計画」を参照してください
3. Unity Connection が IPv6 またはデュアル モードの 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てください。
   a. Unity Connection サーバ上で IPv6 をイネーブルにします。『*Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 10.x*』の「Settings」章の「Ethernet IPv6 Configuration Settings」の項を参照してください。このドキュメントは http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html から入手できます。

b. Cisco Unity Connection Administrationの [システム設定(System Settings)] > [全般設定(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 と IPv6 の両方から選択できます。設定のデフォルトは IPv4 です。

4. Cisco Unified CM をプログラムします。「Cisco Unified CallManager電話システムのプログラミング」セクション(3-3 ページ)
5. 連動を作成します。「Cisco Unified CM との新しい連動の作成」セクション(3-22 ページ)

(注) 新しい電話システム、ポート グループ、およびポートを追加することで Cisco Unified CM クラスタをさらに追加できます。各 Cisco Unified CM クラスタは個別の電話システム連動です。

6. 連動をテストします。第 5 章「複数の連動用の新しいユーザ テンプレートの追加」を参照してください。
7. この連動が 2 番目以降の連動である場合は、新しい電話システムに適した新しいユーザ テンプレートを追加します。第 5 章「複数の連動用の新しいユーザ テンプレートの追加」を参照してください。

要件

Cisco Unified CM SIP 連動では、次のコンポーネントの構成がサポートされます。

- **[電話システム(Phone System)]**
  - Cisco Unified CM
  - Cisco Unified CM の互換バージョンの詳細については、*Cisco Unity Connection の互換性マトリクス* (http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html)を参照してください。
  - Cisco Unified CM 内線番号の場合は、次のいずれかの構成がサポートされます。
  - *(推奨)*RFC 2833 で規定された DTMF リレーをサポートしている SIP 電話機のみ。
  - SCCP 電話機と SIP 電話機の両方。
  - 比較的古い SCCP 電話モデルでは、正常な動作にメディア ターミネーション ポイント(MTP)が必要になる可能性があることに注意してください。
  - 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。
  - Cisco Unified CM クラスタが複数ある場合に、ユーザがトランク アクセス コードまたはプレ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をダイヤルできる機能。
- **Unity Connection サーバ**
  - 適切なバージョンの Unity Connection。Cisco Unity Connection の互換バージョンの詳細については、*Cisco Unity Connection の互換性マトリクス* (http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html)を参照してください。

- 『*Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 11.x,* 』の「Installing Cisco Unity Connection」の章の手順に従って、Unity Connection がインストールされ連動の準備が整っている。このドキュメントは http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/11xcuciumgx.html から入手できます。
- 適切な数のボイス メッセージ ポートを有効化するライセンス。

Cisco Unified CallManager電話システムのプログラミング

Cisco Unified CM ソフトウェアのインストール後、次の手順を実行して、Unity Connection との連動のために Cisco Unified CM 電話システムをプログラムします。

- **クラスタがない Unity Connection**：「クラスタがない Unity Connection の場合」セクション（3-3 ページ）の手順を実行してください。
- **クラスタが設定されている Unity Connection**：「Unity Connection にクラスタが設定されている場合」セクション（3-12 ページ）の手順を実行してください。

クラスタがない Unity Connection の場合

すべてのユーザ電話機（電話番号）で使用されるコーリング サーチ スペースが存在している必要があります。そうしないと、連動が正常に機能しません。コーリング サーチ スペースを設定してユーザの電話機を割り当てる方法については、Cisco Unified CM の [ヘルプ（Help）] 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

ステップ 1　Cisco Unified CM Administration で、[システム（System）] メニューの [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 3-1　[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）] ページの設定

フィールド	設定
[名前（Name）]	**Unity Connection SIP Trunk Security Profile**、または別の名前を入力します。
説明	**SIP trunk security profile for Cisco Unity Connection**、または別の説明を入力します。

表 3-1　[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)] ページの設定(続き)

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 の認証や暗号化を有効化できない場合は、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(Authenticated)] または [暗号化(Encrypted)] を選択します。次の Cisco Unified CM サーバの要件に注意してください。 • TFTP サーバを設定する必要があります。 • セキュリティのために、Cisco Unified CM サーバは Cisco CTL クライアントを使用して設定する必要があります。詳細については、『*Cisco Unified Communications ManagerSecurity Guide*』の「Configuring the Cisco CTL Client」の章の「Configuring the Cisco CTL Client」を参照してください。このドキュメントは http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/8_5_1/secugd/secuauth.html から入手できます。 • Cisco Unified CM サーバの [デバイス セキュリティ モード(Device Security Mode)] 設定は、Unity Connection サーバの [セキュリティ モード(Security Mode)] 設定(認証または暗号化)と一致している必要があります。
X.509 のサブジェクト名(X.509 Subject Name)	Cisco Unified CM の認証や暗号化を有効化できない場合は、このフィールドを空白のままにします。 Cisco Unified CM の認証と暗号化を有効にする場合は、**Connection** または別の名前を入力します。この名前は、Unity Connection サーバの SIP 証明書の [件名(Subject Name)] フィールドと一致している必要があります。
[Out-of-Dialog REFERの許可(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。
[Replacesヘッダーの許可(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)] メニューで、[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で [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）] の下で、次の設定を入力します。

表 3-2　[SIP プロファイルの設定（SIP Profile Configuration）] ページの設定

フィールド	設定
[名前（Name）]	**Unity Connection SIP Profile**、または別の名前を入力します。
[説明（Description）]	**SIP profile for Unity Connection**、または別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 またはデュアル スタック IPv4 と IPv6 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。この手順は、IPv6 またはデュアル スタック環境の発信者の適切な処理のために必要です。

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、次の設定を入力します。

表 3-3　[トランクの設定（Trunk Configuration）] ページの [デバイス情報（Device Information）] 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）]	**SIP trunk for Unity Connection**、または別の説明を入力します。
SRTP を許可（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　ユーザの電話機がコーリング サーチ スペースに含まれている場合は、[インバウンド コール（Inbound Calls）] に次の設定を入力します。それ以外の場合は、ステップ 7 に進みます。

表 3-4　[トランクの設定(Trunk Configuration)] ページの [インバウンド コール(Inbound Calls)] 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)]	ユーザの電話機を含んでいるコーリング 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　ユーザの電話機がコーリング サーチ スペースに含まれている場合は、[Outbound Calls(アウトバウンド コール)] に次の設定を入力します。

表 3-5　[トランクの設定(Trunk Configuration)] ページの [アウトバウンド コール(Outbound Calls)] の設定

フィールド	設定
[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。
接続側にのみ DN を配信(Deliver DN only in connected party)	発信 SIP メッセージで、Unity Connection は SIP コンタクト ヘッダー情報に発信側の電話番号を挿入します。これがデフォルトの設定です。
接続側にのみ URI を配信(Deliver URI only in connected party)	発信 SIP メッセージで、Unity Connection は SIP コンタクト ヘッダーに送信側のディレクトリ URI を挿入します。ディレクトリ URI が使用可能でない場合、Unity Connection は電話番号を挿入します。
接続先側にのみ URI および DN を配信(Deliver URI and DN in connected party)	発信 SIP メッセージで、Unity Connection は、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 SIP コンタクト ヘッダーに挿入します。ディレクトリ URI が使用可能でない場合、Unity Connection は電話番号だけを含めます。

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

表 3-6　[トランクの設定（Trunk Configuration）] ページの [SIP 情報（SIP Information）] の設定

フィールド	設定
[宛先アドレス（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 IPv6 アドレスを入力します。 IPv6 アドレスは、「RFC 5952」が推奨する IPv6 Address Text Representation（IPv6 アドレス表記）に準拠したテキスト表記にする必要があります。 **（注）**　IPv6 は、Unity Connection と Cisco Unified CM 間の SIP 連動でサポートされます。
宛先ポート（Destination Port）	**5060** のデフォルト値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 プロファイルを作成する」の手順（3-3 ページ）で作成した SIP トランク セキュリティ プロファイルの名前を選択します。たとえば、[Unity Connection SIP トランク セキュリティ プロファイル（Cisco Unity Connection SIP Trunk Security Profile）] を選択します。
再ルーティング用コーリング サーチ スペース（Rerouting Calling Search Space）	ユーザの電話機で使用するコーリング 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）	ユーザの電話機で使用するコーリング 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（3-4 ページ）で作成した SIP プロファイルの名前を選択します。たとえば、[Unity Connection SIP プロファイル（Cisco Unity Connection SIP Profile）] を選択します。

ステップ 9　その他の設定をサイトに合せて調整します。

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/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 3-7　[ルート パターンの設定(Route Pattern Configuration)] 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 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」の手順(3-5 ページ)で作成した SIP トランクの名前を選択します。たとえば、[Unity_Connection_SIP_Trunk] を選択します。

ステップ 4　[保存(Save)] を選択します。

ボイス メール パイロットを作成する

ステップ 1　[拡張機能(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 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、次のようにボイス メール パイロット番号の設定を入力します。

表 3-8　[ボイス メール パイロットの設定(Voice Mail Pilot Configuration)] 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(3-7 ページ)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)]	ユーザの電話機を割り当てたパーティションとボイス メール パイロット番号用に設定したパーティションを含むコーリング サーチスペースを選択します。
[説明(Description)]	「**Unity Connection のパイロット**」と入力するか、別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 パイロットを設定する

ステップ 1　[拡張機能（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、次のようにボイス メール プロファイルの設定を入力します。

表 3-9　[ボイス メール プロファイルの設定（Voice Mail Profile Configuration）] 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 ConnectionProfile**、または別の名前を入力して、ボイス メール プロファイルを識別できるようにします。
説明	**Enter Profile for Unity Connection**、または別の説明を入力します。
[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」の手順（3-8 ページ）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 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。
これをシステムのデフォルト ボイス メール プロファイルに設定（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 サーバのサービス パラメータを設定する

ステップ 1　Cisco Unified CM Administration で、[システム（System）] に移動し、[サービス パラメータ（Service Parameters）] を選択します。

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

ステップ 3　[サービス（Service）] リストで [Cisco CallManager（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　Clusterwide パラメータ（[機能（Feature）] - [一般（General）]）で、Multiple Tenant MWI Modes パラメータを検索します。

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

このパラメータを [True（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 サーバをシャットダウンしてから再起動します。

SIP ダイジェスト認証を設定しない場合は、「Cisco Unified CM との新しい連動の作成」セクション（3-22 ページ）に進みます。

（任意）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、「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（3-3 ページ）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。

（任意）アプリケーション ユーザを作成する

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

ステップ 2　[アプリケーション ユーザの検索と一覧表示（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 ユーザの設定（Application User Configuration）] ページで、次の設定を入力します。

表 3-10　[アプリケーション ユーザの設定（Application User Configuration）] ページの設定

フィールド	設定
ユーザ ID（User ID）	アプリケーション ユーザの識別名を入力します。Cisco Unified CM では、ユーザ 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。

表 3-10　[アプリケーション ユーザの設定(Application User Configuration)] ページの設定(続き)

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。
[Replacesヘッダーの許可(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 ユーザに関連付けるには、デバイスを選択し、このリスト 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。 • [別の電話を検索(Find More Phones)]: このアプリケーション ユーザに関連付ける別の電話機を検索するには、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。 • [別のルート ポイントを検索(Find More Route Points)]: このアプリケーション ユーザに関連付ける別のルート ポイントを検索するには、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)	ユーザの [アプリケーション ユーザ CAPF プロファイル(Application User CAPF Profile)] を設定した場合は、[割り当てられている CAPF プロファイル(Associated CAPF Profiles)] ペインに、アプリケーション ユーザ 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 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	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。

Unity Connection にクラスタが設定されている場合

すべてのユーザ電話機（電話番号）で使用されるコーリング サーチ スペースが存在している必要があります。そうしないと、連動が正常に機能しません。コーリング サーチ スペースを設定してユーザの電話機を割り当てる方法については、Cisco Unified CM の [ヘルプ（Help）] 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（Unity Connection クラスタ用）

ステップ 1　Cisco Unified CM Administration で、[システム（System）] メニューの [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 3-11　[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）] ページの設定

フィールド	設定
[名前（Name）]	**Unity Connection SIP Trunk Security Profile**、または別の名前を入力します。
説明	**SIP trunk security profile for Cisco Unity Connection**、または別の説明を入力します。
[デバイスセキュリティ モード（Device Security Mode）]	Cisco Unified CM の認証や暗号化を有効化できない場合は、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（Authenticated）] または [暗号化（Encrypted）] を選択します。次の Cisco Unified CM サーバの要件に注意してください。 • TFTP サーバを設定する必要があります。 • セキュリティのために、Cisco Unified CM サーバは Cisco CTL クライアントを使用して設定する必要があります。詳細については、『*Cisco Unified Communications ManagerSecurity Guide*』の「Configuring the Cisco CTL Client」の章の「Configuring the Cisco CTL Client」を参照してください。このドキュメントは http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html から入手できます。 • Cisco Unified CM サーバの [デバイス セキュリティ モード（Device Security Mode）] 設定は、Unity Connection サーバの [セキュリティ モード（Security Mode）] 設定（認証または暗号化）と一致している必要があります。
X.509 のサブジェクト名（X.509 Subject Name）	Cisco Unified CM の認証や暗号化を有効化できない場合は、このフィールドを空白のままにします。 Cisco Unified CM の認証と暗号化を有効にする場合は、**Connection** または別の名前を入力します。この名前は、Unity Connection サーバの SIP 証明書の [件名（Subject Name）] フィールドと一致している必要があります。

表 3-11　[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)] ページの設定(続き)

フィールド	設定
[Out-of-Dialog REFERの許可(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。
[Replacesヘッダーの許可(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(Unity Connection クラスタ用)

ステップ 1　[デバイス(Device)] メニューで、[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で [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)] の下で、次の設定を入力します。

表 3-12　[SIP プロファイルの設定(SIP Profile Configuration)] ページの設定

フィールド	設定
[名前(Name)]	**Unity Connection SIP Profile**、または別の名前を入力します。
[説明(Description)]	**SIP profile for Unity Connection**、または別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 またはデュアル スタック IPv4 と IPv6 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。この手順は、IPv6 またはデュアル スタック環境の発信者の適切な処理のために必要です。

ステップ 6　[電話機で使用されるパラメータ(Parameters Used in Phone)] の下の [再試行回数(Retry INVITE)] フィールドで、5 以下の値を入力します。

ステップ 7　[保存(Save)] を選択します。

SIP トランクを作成する（Unity Connection クラスタ用）

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、次の設定を入力します。

表 3-13　[トランクの設定（Trunk Configuration）] ページの [デバイス情報（Device Information）] の設定

フィールド	設定
デバイス名（Device Name）	**Unity_Connection_SIP_Trunk_1** または別の名前を入力します。
説明	**SIP trunk 1 for Cisco Unity Connection** または別の説明を入力します。
SRTP を許可（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　ユーザの電話機がコーリング サーチ スペースに含まれている場合は、[インバウンド コール（Inbound Calls）] に次の設定を入力します。それ以外の場合は、ステップ 7 に進みます。

表 3-14　[トランクの設定（Trunk Configuration）] ページの [インバウンド コール（Inbound Calls）] 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）]	ユーザの電話機を含んでいるコーリング 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　[アウトバウンド コール（Outbound Calls）] で、[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）] チェックボックスをオンにします。

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

表 3-15　[トランクの設定（Trunk Configuration）] ページの [SIP 情報（SIP Information）] の設定

フィールド	設定
[宛先アドレス（Destination Address）]	パブリッシャ サーバの IP アドレスを入力します。
宛先アドレス IPv6（Destination Address IPv6）	パブリッシャ サーバの IPv6 アドレスを入力します。 IPv6 アドレスは、「RFC 5952」が推奨する IPv6 Address Text Representation（IPv6 アドレス表記）に準拠したテキスト表記にする必要があります。 **（注）**　IPv6 は、Unity Connection と Cisco Unified CM 間の SIP 連動でサポートされます。
宛先ポート（Destination Port）	**5060** のデフォルト値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 プロファイルを作成する（Unity Connection クラスタ用）」の手順（3-12 ページ）で作成した SIP トランク セキュリティ プロファイルの名前を選択します。たとえば、[Unity Connection SIP トランク セキュリティ プロファイル（Cisco Unity Connection SIP Trunk Security Profile）] を選択します。
再ルーティング用コーリング サーチ スペース（Rerouting Calling Search Space）	ユーザの電話機で使用するコーリング 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）	ユーザの電話機で使用するコーリング 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（Unity Connection クラスタ用）」の手順（3-13 ページ）で作成した SIP プロファイルの名前を選択します。たとえば、[Unity Connection SIP プロファイル（Cisco Unity Connection SIP Profile）] を選択します。

ステップ 9　その他の設定をサイトに合せて調整します。

ステップ 10　[保存（Save）] を選択します。

ステップ 11　[新規追加（Add New）] を選択します。

ステップ 12　[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 13　[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 14　[デバイス情報（Device Information）] で、次の設定を入力します。

表 3-16　[トランクの設定（Trunk Configuration）] ページの [デバイス情報（Device Information）] の設定

フィールド	設定
デバイス名（Device Name）	**Unity_Connection_SIP_Trunk_2** または別の名前を入力します。
説明	**SIP trunk 2 for Cisco Unity Connection** または別の説明を入力します。
SRTP を許可（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 15　ユーザの電話機がコーリング サーチ スペースに含まれている場合は、[インバウンド コール（Inbound Calls）] に次の設定を入力します。それ以外の場合は、ステップ 16 に進みます。

表 3-17　[トランクの設定（Trunk Configuration）] ページの [インバウンド コール（Inbound Calls）] 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）]	ユーザの電話機を含んでいるコーリング 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 16　[アウトバウンド コール（Outbound Calls）] で、[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）] チェックボックスをオンにします。

ステップ 17　[SIP 情報（SIP Information）] で、次の設定を入力します。

表 3-18　[トランクの設定（Trunk Configuration）] ページの [SIP 情報（SIP Information）] の設定

フィールド	設定
[宛先アドレス（Destination Address）]	サブスクライバ サーバの IP アドレスを入力します。
宛先アドレス IPv6（Destination Address IPv6）	サブスクライバ サーバの IPv6 アドレスを入力します。 IPv6 アドレスは、「RFC 5952」が推奨する IPv6 Address Text Representation（IPv6 アドレス表記）に準拠したテキスト表記にする必要があります。 **（注）**　IPv6 は、Unity Connection と Cisco Unified CM 間の SIP 連動でサポートされます。
宛先ポート（Destination Port）	**5060** のデフォルト値を使用することを推奨します。

表 3-18　[トランクの設定(Trunk Configuration)] ページの [SIP 情報(SIP Information)] の設定(続き)

フィールド	設定
[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 プロファイルを作成する(Unity Connection クラスタ用)」の手順(3-12 ページ)で作成した SIP トランク セキュリティ プロファイルの名前を選択します。たとえば、[Unity Connection SIP トランク セキュリティ プロファイル(Cisco Unity Connection SIP Trunk Security Profile)] を選択します。
再ルーティング用コーリング サーチ スペース(Rerouting Calling Search Space)	ユーザの電話機で使用するコーリング 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)	ユーザの電話機で使用するコーリング 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(Unity Connection クラスタ用)」の手順(3-13 ページ)で作成した SIP プロファイルの名前を選択します。たとえば、[Unity Connection SIP プロファイル(Cisco Unity Connection SIP Profile)] を選択します。

ステップ 18　その他の設定をサイトに合せて調整します。

ステップ 19　[保存(Save)] を選択します。

ルート グループを作成する(Unity Connection クラスタの場合)

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 3-19　[ルート グループの設定(Route Group Configuration)] 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)]	[上から下(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。

上向きまたは下向き矢印を選択して 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(Cisco Unity Connection クラスタの場合)

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 3-20　[ルート リストの設定(Route List Configuration)] 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	**SIP Trunk Route List** または別の説明を入力します。
[Cisco Unified CM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選択され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 リスト詳細の設定(Route List Detail Configuration)] ページの [ルート グループ(Route Group)] フィールドで、「ルート グループを作成する(Unity Connection クラスタの場合)」の手順(3-17 ページ) 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(OK)] を選択します。

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)] を選択します。

ステップ 11　[閉じる(Close)] を選択します。

ルート パターンを作成する(Unity Connection クラスタの場合)

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/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 3-21　[ルート パターンの設定(Route Pattern Configuration)] 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 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)]	「ルート リストを作成する(Cisco Unity Connection クラスタの場合)」の手順(3-18 ページ)で作成したルート リストの名前を選択します。たとえば、[SIP_Trunk_Route_List] を選択します。

ステップ 4　[保存(Save)] を選択します。

ボイス メール パイロットを作成する(Unity Connection クラスタの場合)

ステップ 1　[拡張機能(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 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、次のようにボイス メール パイロット番号の設定を入力します。

表 3-22　[ボイス メール パイロットの設定(Voice Mail Pilot Configuration)] 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(Unity Connection クラスタの場合)」の手順(3-18 ページ)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)]	ユーザの電話機を割り当てたパーティションとボイス メール パイロット番号用に設定したパーティションを含むコーリング サーチスペースを選択します。
説明	「**Unity Connection のパイロット**」と入力するか、別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（Unity Connection クラスタの場合）

ステップ 1　[拡張機能（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、次のようにボイス メール プロファイルの設定を入力します。

表 3-23　[ボイス メール プロファイルの設定（Voice Mail Profile Configuration）] 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 ConnectionProfile**、または別の名前を入力して、ボイス メール プロファイルを識別できるようにします。
説明	**Enter Profile for Unity Connection**、または別の説明を入力します。
[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（Unity Connection クラスタの場合）」の手順（3-19 ページ）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 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。
これをシステムのデフォルト ボイス メール プロファイルに設定（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。

SIP ダイジェスト認証を設定しない場合は、「Cisco Unified CM との新しい連動の作成」セクション（3-22 ページ）に進みます。

（任意）SIP ダイジェスト認証を設定する（Unity Connection クラスタの場合）

ステップ 1　[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、「SIP トランク セキュリティ プロファイルを作成する（Unity Connection クラスタ用）」の手順（3-12 ページ）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。

（任意）アプリケーション ユーザを作成する（Unity Connection クラスタの場合）

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

ステップ 2　[アプリケーション ユーザの検索と一覧表示（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 ユーザの設定（Application User Configuration）] ページで、次の設定を入力します。

表 3-24　[アプリケーション ユーザの設定（Application User Configuration）] ページの設定

フィールド	設定
ユーザ ID（User ID）	アプリケーション ユーザの識別名を入力します。Cisco Unified CM では、ユーザ 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。
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。
プレゼンス グループ（Presence Group）	アプリケーション ユーザ（IPMASysUser など）は、プレゼンス機能で使用される場合はプレゼンス エンティティに関するステータスを要求するため、ウォッチャとして機能します。 プレゼンス エンティティのステータスをアプリケーション ユーザが受信できるようにするには、その**アプリケーション ユーザ プレゼンス** グループに対して、電話番号に適用される**プレゼンス** グループのステータスの閲覧が許可されていることを確認します。この項目は、[プレゼンス グループの設定（Presence Group Configuration）] ウィンドウで指定されています。
[プレゼンスのSUBSCRIBEの許可（Accept Presence Subscription）]	このチェックボックスはオフのままにします。
[Out-of-Dialog REFERの許可（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。
[Replacesヘッダーの許可（Accept replaces header）]	このチェックボックスはオフのままにします。

表 3-24　[アプリケーション ユーザの設定(Application User Configuration)] ページの設定(続き)

フィールド	設定
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 ユーザに関連付けるには、デバイスを選択し、このリスト 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。 • [別の電話を検索(Find More Phones)]: このアプリケーション ユーザに関連付ける別の電話機を検索するには、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。 • [別のルート ポイントを検索(Find More Route Points)]: このアプリケーション ユーザに関連付ける別のルート ポイントを検索するには、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)	ユーザの [アプリケーション ユーザ CAPF プロファイル(Application User CAPF Profile)] を設定した場合は、[割り当てられている CAPF プロファイル(Associated CAPF Profiles)] ペインに、アプリケーション ユーザ 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 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	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。

Cisco Unified CM との新しい連動の作成

- 連動を作成する
- SIP 連動による次世代セキュリティの有効化

Cisco Unified Communications Manager と Unity Connection が連動可能な状態にあることを確認したら、次の手順を実行して、連動を設定し、ポート設定を入力します。

連動を作成する

ステップ 1　Cisco Unity Connection Administration にログインします。

ステップ 2　Cisco Unified CM の認証と暗号化を使用する場合は、次のサブステップを実行します。そうでない場合は、ステップ 3 に進みます。

a. Cisco Unity Connection Administration で、[テレフォニー統合（Telephony Integrations）] > [セキュリティ（Security）] を展開し、[SIP 証明書（SIP Certificate）] を選択します。

b. [SIP 証明書（SIP Certificates）] ページで、[新規追加（Add New）] を選択します。

c. [新規 SIP 証明書（New SIP Certificate）] ページで、SIP 証明書に関する次の設定を入力し、[保存（Save）] を選択します。

表 3-25　[新規 SIP 証明書（New SIP Certificate）] ページの設定

フィールド	設定
[表示名（Display Name）]	SIP 証明書の表示名を入力します。
件名（Subject Name）	Cisco Unified CM Administration の SIP トランクに対する SIP セキュリティ プロファイルの X.509 の件名と一致する件名を入力します。 この件名は、Cisco Unified CM で使用される SIP セキュリティ プロファイルの X.509 のサブジェクト名と一致している必要があります。一致していない場合、Cisco Unified CM の認証と暗号化は失敗します。

ステップ 3　Cisco Unity Connection Administrationで、[テレフォニー（Telephony Integrations）] を展開し、[電話システム（Phone System）] を選択します。

ステップ 4　[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の名前を選択します。

ステップ 5　[電話システムの基本設定（Phone System Basics）] ページの [電話システムの名前（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 6　（ボイス メール ボックスの無い管理者やユーザが Unity Connection の Web アプリケーションで電話から録音および再生を行うときに）TRaP 接続にこの電話システムをデフォルトとして使用する場合は、[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。TRaP 接続に別の電話システムを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 7　[保存（Save）] を選択します。

ステップ 8　[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 9　[ポート グループの新規作成（New Port Group）] ページで適切な設定を入力して、[保存（Save）] を選択します。

表 3-26　[ポート グループの新規作成(New Port Group)] ページの設定

フィールド	設定
[電話システム(Phone System)]	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。
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(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 サーバで認証する(Authenticate with SIP Server)	Unity Connection が Cisco Unified CM サーバによる認証を受ける場合は、このチェックボックスをオンにします。
認証ユーザ名(Authentication User Name)	Cisco Unified CM サーバによる認証で Unity Connection が使用する名前を入力します。
認証パスワード(Authentication Password)	Cisco Unified CM サーバによる認証で Unity Connection が使用するパスワードを入力します。
連絡先回線名(Contact Line Name)	ユーザが Unity Connection への接続に使用し、Unity Connection が Cisco Unified CM サーバへの登録に使用するボイス メッセージ回線名(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 によって使用される 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)* SIP インターフェイスで次世代暗号化をサポートできるように、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、「SIP 連動による次世代セキュリティの有効化」セクション(3-30 ページ)を参照してください。
SIP 証明書	*(セキュアな TLS ポートが使用され、[次世代暗号化の有効化(Enable Next Generation Encryption)] チェックボックスがオフになっている場合のみ)* 適切な SIP 証明書が選択されていることを確認します。

表 3-26　[ポート グループの新規作成(New Port Group)] ページの設定(続き)

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、[次世代暗号化の有効化(Enable Next Generation Encryption)] チェックボックスがオフになっている場合のみ)*適切なセキュリティ モードを選択します。 • [認証(Authenticated)]: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 サーバの [セキュリティ モード(Security Mode)] 設定は、Cisco Unified CM サーバの [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 ポートが使用されている場合のみ)*このチェックボックスをオンにすると、メディア ストリーム(RTP)が暗号化されます。メディア ストリームを暗号化しない場合は、この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 と連動させるプライマリ Cisco Unified CM サーバの 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)	Unity Connection と連動させるプライマリ Cisco Unified CM サーバの IPv6 アドレス(またはホスト名)を入力します。 IPv6 アドレスは、「RFC 5952」が推奨する IPv6 Address Text Representation(IPv6 アドレス表記)に準拠したテキスト表記にする必要があります。 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(IPv4 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 連動でサポートされます。

表 3-26　[ポート グループの新規作成(New Port Group)] ページの設定(続き)

フィールド	設定
IP アドレス/ホスト名(IPv6 Address or Host Name)	Cisco Unity Connection と連動させるプライマリ Cisco Unified CM サーバの IP アドレス(またはホスト名)を入力します。
[ポート(Port)]	Unity Connection と連動させるプライマリ Cisco Unified CM サーバの 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 10　Cisco Unified CM クラスタにセカンダリ サーバがある場合、または(Cisco Unified CM の認証と暗号化に必要な)TFTP サーバを追加する場合は、[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。そうでない場合は、ステップ 11 に進みます。

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

b. セカンダリ Cisco Unified CM サーバを追加する場合は、[サーバの編集(Edit Servers)] ページの [SIP サーバ(SIP Servers)] で、[追加(Add)] を選択します。そうでない場合は、ステップ 10e. に進みます。

c. セカンダリ Cisco Unified CM サーバについて次の設定を入力し、[保存(Save)] を選択します。

表 3-27　SIP サーバの設定

フィールド	設定
順序	Cisco Unified CM サーバ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 サーバを表し、それよりも大きい数字はセカンダリ サーバを表します。
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、「RFC 5952」が推奨する IPv6 Address Text Representation(IPv6 アドレス表記)に準拠したテキスト表記にする必要があります。 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(IPv4 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 連動でサポートされます。
IP アドレス/ホスト名(IPv6 Address or Host Name)	セカンダリ Cisco Unified CM サーバの IP アドレス(またはホスト名)を入力します。

表 3-27　SIP サーバの設定（続き）

フィールド	設定
[ポート（Port）]	Unity Connection と連動させる Cisco Unified CM サーバの 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 と連動させる Cisco Unified CM サーバの 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 クラスタ内の他の Cisco Unified CM サーバに対して、ステップ 10b. および ステップ 10c. を繰り返します。

e. TFTP サーバ（Cisco Unified CM の認証および暗号化で必要）を追加する場合は、[TFTP サーバ（TFTP Servers）] で [追加（Add）] を選択します。そうでない場合は、ステップ 10h. に進みます。

f. TFTP サーバについて次の設定を入力し、[保存（Save）] を選択します。

表 3-28　TFTP サーバの設定

フィールド	設定
順序	TFTP サーバの優先順位を入力します。数値の最も小さいサーバがプライマリ TFTP サーバで、数値がプライマリよりも大きい場合はセカンダリ サーバです。
IPv4 アドレス/ホスト名（IPv4 Address or Host Name）	TFTP サーバの 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、「RFC 5952」が推奨する IPv6 Address Text Representation（IPv6 アドレス表記）に準拠したテキスト表記にする必要があります。 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（IPv4 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 連動でサポートされます。
IP アドレス/ホスト名（IPv6 Address or Host Name）	TFTP サーバの 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、他の TFTP サーバに対して、ステップ 10e. および 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 11　[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 12　[ポートの新規作成(New Port)] ページで次の設定を入力して、[保存(Save)] を選択します。

表 3-29　[ポートの新規作成(New Port)] 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。
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 クラスタの場合は、すべての Unity Connection サーバで使用されるボイス メッセージ ポート数の合計を入力する必要があります。各ポートは後で特定の Unity Connection サーバに割り当てられます。
[電話システム(Phone System)]	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	Unity Connection サーバの名前を選択します。

ステップ 13　[ポートの検索(Search Ports)] ページで、この電話システム連動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 14　[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 ポートの設定を入力します。次の表のフィールドは、変更可能なものを示しています。

表 3-30　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、このチェックボックスをオンにします。ポートは通常の動作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。ポートが無効になっている場合にポートを呼び出すと、呼び出し音は鳴りますが、応答はありません。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ります。
サーバ	*(Unity Connection クラスタの場合に限る)*このポートを処理する Unity Connection サーバの名前を選択します。 等しい数の応答ボイス メッセージ ポートと発信ボイス メッセージ ポートを Cisco Unity Connection サーバに割り当てて、これらのポートがボイス メッセージ トラフィックを等しく共有するようにします。
コールへの応答	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す。これらの通話は、識別できない発信者またはユーザからの着信です。

表 3-30　ボイス メッセージ ポートの設定（続き）

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要求を送信する（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 要求を送信する（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、ユーザは 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 15　[保存（Save）] を選択します。

ステップ 16　[次へ（Next）] を選択します。

ステップ 17　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 ～ステップ 16 を繰り返します。

ステップ 18　Cisco Unified CM の認証と暗号化を使用する場合は、次のサブステップを実行します。そうでない場合は、ステップ 20 に進みます。

a. Cisco Unity Connection Administrationで [テレフォニー統合（Telephony Integrations）] > [セキュリティ（Security）] を展開し、[ルート証明書（Root Certificate）] を選択します。

b. [ルート証明書の表示（View Root Certificate）] ページで、[右クリックして証明書をファイルとして保存（Right-Click to Save the Certificate as a File）] のリンク部分を右クリックして、[名前を付けて保存（Save Target As）] を選択します。

c. [名前を付けて保存（Save As）] ダイアログボックスで、Unity Connection ルート証明書をファイルとして保存する場所を参照します。

d. [ファイル名（File Name）] フィールドで、拡張子が .pem である（.htm ではない）ことを確認し、[保存（Save）] を選択します。

注意　証明書は、拡張子 .pem（.htm ではなく）付きのファイルとして保存する必要があります。そうしないと、Cisco Unified CM で証明書が認識されません。

e. [ダウンロードの完了（Download Complete）] ダイアログボックスで、[閉じる（Close）] を選択します。

ステップ 19　次の手順に従って、この Cisco Unified CM システム統合にあるすべての Cisco Unified CM サーバに Unity Connection ルート証明書ファイルをコピーします。

ステップ 20　別の電話システム連動が存在する場合は、Cisco 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 21　電話システムのトランクの検索（Search Phone System Trunks）] ページで、[電話システムのトランク（Phone System Trunk）] メニューの [電話システム トランクの新規作成（New Phone System Trunk）] を選択します。

ステップ 22　電話システム トランクの新規作成（New Phone System Trunk）] ページで、次に示す電話システム トランクの設定を入力して [保存（Save）] を選択します。

表 3-31　電話システム トランクの設定

フィールド	設定
発信側電話システム（From Phone System）	トランクの作成対象となる電話システムの表示名を選択します。
受信側電話システム（To Phone System）	トランクの接続先とな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）	Unity Connection が既存の電話システムの内線番号にゲートウェイ経由で通話を転送するときにダイヤルする追加ダイヤル番号を入力します。

ステップ 23　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 21 とステップ 22 を繰り返します。

SIP 連動による次世代セキュリティの有効化

Unity Connection は、暗号化アルゴリズムによって機密性、整合性、認証を提供する、次世代セキュリティを SIP インターフェイスを介してサポートします。次世代暗号化では、TLS 1.2、SHA-2、AES256 プロトコルに基づいて Suite B 暗号化を使用するように SIP インターフェイスが制限されるため、セキュリティが向上します。暗号化に加えて、次世代暗号化には、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 パーティの証明書が含まれています。Unity Connection と Cisco Unified CM 間の通信時、暗号化とサードパーティ証明書の両方が両端で確認されます。次世代暗号化サポートの設定は次のとおりです。

セキュリティ モードの設定

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（Next Generation Encryption）] チェックボックスをオンにします。

ステップ 5　Cisco Unified CM Administration にログインします。

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（3-3 ページ）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 のサブジェクト名（X.509 Subject Name）] がそれぞれの Unity Connection サーバの FQDN になっている必要があります。

ステップ 9　「TLS 暗号の設定」の項の説明に従って、TLS 暗号化を設定します。

TLS 暗号の設定

Unity Connection および Cisco Unified CM で TLS 暗号オプションを設定する手順は以下のとおりです。

ステップ 1　Cisco Unified CM Administration ページにサインインして、[システム（Systems）] > [エンタープライズ パラメータ（Enterprise Parameters）] > [セキュリティ パラメータ（Security Parameters）] > [TLS 暗号（TLS Ciphers）] の順に移動します。

ステップ 2　ドロップダウン リストから適切な TLS 暗号オプションを選択します。

ステップ 3　画面の右上隅の [ナビゲーション（Navigation）] ペインで、Cisco Unified Serviceability を選択し、[移動（Go）] を選択します。

ステップ 4　Cisco Unified Serviceability ページで、[ツール（Tools）] > [コントロール センターの機能サービス（Control Centre-Feature Services）] に移動します。リストから [Cisco Call Manager] を選択し、[リスタート（Restart）] を選択します。

（注）　Cisco Unified CM クラスタの場合は、パブリッシャとサブスクライバの両方を再起動する必要があります。

ステップ 5　Cisco Unity Connection Administration ページにサインインして、[システム設定（System Settings）] > [全般設定（General Configurations）] の順に展開し、[TLS 暗号（TLS Ciphers）] を選択します。

ステップ 6　ドロップダウン リストから適切な TLS 暗号オプションを選択します。

ステップ 7　画面の右上隅の [ナビゲーション（Navigation）] ペインで、Cisco Unity Connection Serviceability を選択し、[移動（Go）] を選択します。

ステップ 8　[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 が停止したら、それを再起動します。

（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に対して Connection Conversation Manager を再起動する必要があります。

ステップ 9　「証明書の作成とアップロード」の項の説明に従って、RSA と EC キー ベースの証明書を作成してアップロードします。

以下のリストは、ドロップダウン メニューの TLS 暗号オプションおよび対応する優先順位を示しています。

表 3-32　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）
AES-256 SHA384 暗号化のみの RSA を優先（AES-256 SHA384 ciphers only RSA preferred）	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384
AES-128 SHA256 暗号化のみの RSA を優先（AES-128 SHA256 ciphers only RSA preferred）	ECDHE--RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256

表 3-32　TLS 暗号オプションと優先順位（続き）

AES-256、AES-128 暗号化 ECDSA を優先（AES-256, AES-128 ciphers ECDSA preferred）	ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 AES-128-SHA
AES-256、AES-128 暗号化 ECDSA のみ（AES-256, AES-128 ciphers ECDSA only）	ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256
AES-256、AES-128 暗号化 RSA を優先（AES-256, AES-128 ciphers RSA preferred）（デフォルト）	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 AES-128-SHA
AES-128 SHA1 暗号化のみ	AES-128-SHA

Unity Connection と Cisco Unified Communications Manager (CM) Express (formerly known as Cisco Unified CallManager Express) 間のネゴシエーションは、次の条件による TLS 暗号の設定に応じて異なります。

- Unity Connection がサーバとして動作する場合、TLS 暗号ネゴシエーションは Cisco Unified CM で選択されたプリファレンスに基づきます。
  - ECDSA ベースの暗号（AES-256、AES-128 暗号化 ECDSA のみ）がネゴシエートされる場合は、SSL ハンドシェイクで EC キー ベースの Call Manager-ECDSA 証明書が使用されます。
  - RSA ベースの暗号がネゴシエートされる場合は、SSL ハンドシェイクで RSA キー ベースの Tomcat 証明書が使用されます。
- Unity Connection がクライアントとして動作する場合、TLS 暗号ネゴシエーションは Unity Connection で選択されたプリファレンスに基づきます。
- クライアント モードでは、TLS 暗号オプションとして [AES-256、AES-128 暗号化 ECDSA のみ（AES-256, AES-128 ciphers ECDSA only）] が選択されている場合にのみ、Unity Connection と Cisco Unified CM の両方が EC キー ベースの証明書を送信します。それ以外の場合は、SSL ハンドシェイクで常に RSA ベースの証明書が送信されます。

RTP インターフェイスを介した次世代セキュリティを有効にする場合は、次のように SRTP 暗号を設定します。

SRTP 暗号の設定

ステップ 1　Cisco Unified CM Administration ページにサインインして、[システム（Systems）] > [エンタープライズ パラメータ（Enterprise Parameters）] > [セキュリティ パラメータ（Security Parameters）] > [SRTP 暗号（SRTP Ciphers）] の順に移動します。

ステップ 2　ドロップダウン リストから適切な SRTP 暗号オプションを選択します。

ステップ 3　画面の右上隅の [ナビゲーション（Navigation）] ペインで、Cisco Unified Serviceability を選択し、[移動（Go）] を選択します。

ステップ 4　Cisco Unified Serviceability ページで、[ツール（Tools）] > [コントロール センターの機能サービス（Control Centre-Feature Services）] に移動します。リストから [Cisco Call Manager] を選択し、[リスタート（Restart）] を選択します。

（注）　Cisco Unified CM クラスタの場合は、パブリッシャとサブスクライバの両方を再起動する必要があります。

ステップ 5　Cisco Unity Connection Administration ページにサインインして、[システム設定（System Settings）] > [全般設定（General Configurations）] の順に展開し、[SRTP 暗号（SRTP Ciphers）] を選択します。

ステップ 6　ドロップダウン リストから適切な SRTP 暗号オプションを選択します。

ステップ 7　画面の右上隅の [ナビゲーション（Navigation）] ペインで、Cisco Unity Connection Serviceability を選択し、[移動（Go）] を選択します。

ステップ 8　[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 が停止したら、それを再起動します。

（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に対して Connection Conversation Manager を再起動する必要があります。

以下のリストは、ドロップダウン メニューの SRTP 暗号オプションおよび対応する優先順位を示しています。

表 3-33　SRTP 暗号オプションと優先順位

SRTP 暗号オプション	SRTP 暗号（優先順）
すべてのサポートされる AES-256、AES-128 暗号（All supported AES-256,AES-128 ciphers）	AEAD_AES_256_GCM AEAD_AES_128_GCM AES-128 SHA1
AEAD AES256 GCM ベースの暗号のみ（AEAD AES256 GCM-based ciphers only）	AEAD AES256 GCM
AEAD AES128 GCM ベースの暗号のみ（AEAD AES128 GCM-based ciphers only）	AEAD AES128 GCM
AES-128 SHA1 暗号化のみ	AES128-SHA

Unity Connection と Cisco Unified CM 間のネゴシエーションは、次の条件による SRTP 暗号の設定に応じて異なります。

- Unity Connection がサーバとして動作する場合、SRTP 暗号ネゴシエーションは Cisco Unified Communications Manager で選択されたプリファレンスに基づきます。
- Unity Connection がクライアントとして動作する場合、SRTP 暗号ネゴシエーションは Unity Connection で選択されたプリファレンスに基づきます。

証明書の作成とアップロード

Unity Connection では、RSA キー ベースの Tomcat 証明書と EC キー ベースの Call Manager-ECDSA 証明書（自己署名およびサードパーティ）が使用されます。それらの設定は次のとおりです。

- RSA キー ベースの証明書用の設定
- EC キー ベースの証明書用の設定

RSA キー ベースの証明書用の設定

Unity Connection の RSA キー ベースの証明書を作成して Cisco Unified CM にアップロードする手順は以下のとおりです。

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作成する場合は、ステップ 4 から ステップ 6 を実行します。そうでない場合は、ステップ 7 に進みます。

ステップ 4　[証明書の管理（Certificate Management）] ページで、[自己署名証明書の作成（Generate Self Signed）] を選択します。

ステップ 5　[自己署名証明書の作成（Generate Self Signed）] ウィンドウの [証明書の用途（Certificate Purpose）] で、[tomcat] を選択します。

ステップ 6　[生成（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作成するには、[証明書の管理（Certificate Management）] ページで [CSR の作成（Generate CSR）] を選択します。

ステップ 8　[証明書署名要求の作成（Generate Certificate Signing Request）] ウィンドウの [証明書の用途（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）] フィールドで、Unity Connection の完全な FQDN を入力します。

ステップ 10　[生成（Generate）] を選択します。

ステップ 11　[証明書の一覧（Certificate List）] ページで、[CSR のダウンロード（Download CSR）] を選択します。これによって、Microsoft CA または VeriSign であるサードパーティから Unity Connection 証明書が作成されます。

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）] ウィンドウの [証明書の用途（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）] に移動して [参照（Browse）] を選択し、サードパーティ CSR によって作成された（ステップ 12 で保存した）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　[証明書の一覧（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）] ウィンドウの [証明書の用途（Certificate Purpose）] フィールドで、[CallManager の信頼性（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）] に移動して [参照（Browse）] を選択し、ステップ 6 で作成した Unity Connection 自己署名証明書をアップロードします。Unity Connection 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 の信頼性（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作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 ベースの証明書を作成して Unity Connection にアップロードする手順は以下のとおりです。

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作成する場合は、ステップ 4 から ステップ 6 を実行します。そうでない場合は、ステップ 7 に進みます。

ステップ 4　[証明書の管理（Certificate Management）] ページで、[自己署名証明書の作成（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作成（Generate New Self Signed Certificate）] ウィンドウの [証明書の用途（Certificate Purpose）] フィールドで、[CallManager] を選択します。

ステップ 6　[生成（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作成するには、[証明書の管理（Certificate Management）] ページで [CSR の作成（Generate CSR）] を選択します。

ステップ 8　[証明書署名要求の作成（Generate Certificate Signing Request）] ウィンドウの [証明書の用途（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）] フィールドで、Cisco Unified CM の完全な FQDN を入力します。

ステップ 10　[生成（Generate）] を選択します。

ステップ 11　[証明書の一覧（Certificate List）] ページで、[CSR のダウンロード（Download CSR）] を選択します。これによって、Microsoft CA または VeriSign であるサードパーティから Cisco Unified CM 証明書が作成されます。

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　[証明書の一覧（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）] ウィンドウの [証明書の用途（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）] に移動して [参照（Browse）] を選択し、サードパーティ CSR によって作成された（ステップ 12 で保存した）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。

ステップ 17　Unity Connection 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　[証明書の一覧（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）] ウィンドウの [証明書の用途（Certificate Purpose）] フィールドで、[Tomcat の信頼性（Tomcat-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）] に移動して [参照（Browse）] を選択し、ステップ 6 で作成した Cisco Unified CM 自己署名証明書をアップロードします。Cisco Unified CM 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）　Cisco Unified CM クラスタの場合は、Unity Connection の [Tomcat の信頼性（Tomcat-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作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。

EC キー ベースの証明書用の設定

Unity Connection の EC キー ベースの証明書を作成して Cisco Unified CM にアップロードする手順は以下のとおりです。

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作成する場合は、ステップ 4 から ステップ 6 を実行します。そうでない場合は、ステップ 7 に進みます。

ステップ 4　[証明書の管理（Certificate Management）] ページで、[自己署名証明書の作成（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作成（Generate New Self Signed Certificate）] ウィンドウの [証明書の用途（Certificate Purpose）] フィールドで、[CallManager-ECDSA] を選択します。

ステップ 6　[生成（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作成するには、[証明書の管理（Certificate Management）] ページで [CSR の作成（Generate CSR）] を選択します。

ステップ 8　[証明書署名要求の作成（Generate Certificate Signing Request）] ウィンドウの [証明書の用途（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）] フィールドで、Unity Connection の完全な FQDN を入力します。

ステップ 10　[生成（Generate）] を選択します。

ステップ 11　[証明書の一覧（Certificate List）] ページで、[CSR のダウンロード（Download CSR）] を選択します。これによって、Microsoft CA または VeriSign であるサードパーティから Unity Connection ECDSA 証明書が作成されます。

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）] ウィンドウの [証明書の用途（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）] に移動して [参照（Browse）] を選択し、サードパーティ CSR によって作成された（ステップ 12 で保存した）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　[証明書の一覧（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）] ウィンドウの [証明書の用途（Certificate Purpose）] フィールドで、[CallManager の信頼性（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）] に移動して [参照（Browse）] を選択し、ステップ 6 で作成した Unity Connection 自己署名証明書をアップロードします。Unity Connection 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 の信頼性（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作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 ベースの証明書を作成して Unity Connection にアップロードする手順は以下のとおりです。

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作成する場合は、ステップ 4 から ステップ 6 を実行します。そうでない場合は、ステップ 7 に進みます。

ステップ 4　[証明書の管理（Certificate Management）] ページで、[自己署名証明書の作成（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作成（Generate New Self Signed Certificate）] ウィンドウの [証明書の用途（Certificate Purpose）] フィールドで、[CallManager-ECDSA] を選択します。

ステップ 6　[生成（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作成するには、[証明書の管理（Certificate Management）] ページで [CSR の作成（Generate CSR）] を選択します。

ステップ 8　[証明書署名要求の作成（Generate Certificate Signing Request）] ウィンドウの [証明書の用途（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）] フィールドで、Cisco Unified CM の完全な FQDN を入力します。

ステップ 10　[生成（Generate）] を選択します。

ステップ 11　[証明書の一覧（Certificate List）] ページで、[CSR のダウンロード（Download CSR）] を選択します。これによって、Microsoft CA または VeriSign であるサードパーティから Cisco Unified CM 証明書が作成されます。

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　[証明書の一覧（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）] ウィンドウの [証明書の用途（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）] に移動して [参照（Browse）] を選択し、サードパーティ CSR によって作成された（ステップ 12 で保存した）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。

ステップ 17　Unity Connection 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　[証明書の一覧（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）] ウィンドウの [証明書の用途（Certificate Purpose）] フィールドで、[CallManager の信頼性（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）] に移動して [参照（Browse）] を選択し、ステップ 6 で作成した Cisco Unified CM 自己署名証明書をアップロードします。Cisco Unified CM 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）　Cisco Unified CM クラスタの場合は、Unity Connection の [CallManager の信頼性（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作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。

RSA および ECDSA ベースの証明書の詳細については、『*Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 11.x*』の「Security」の章の「Manage Certificates and Certificate Trust Lists」を参照してください。このドキュメントは次の URL から入手できます。

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/os_administration/guide/11xcucosagx.html。

連動のテスト

Cisco Unity Connection と電話システムが適切に連動されているかどうかをテストするには、次の手順を実行します。

いずれかのステップで失敗が示された場合は、次の資料のうち該当するものを参照してください。

- 『*Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 11.x,* 』の「Installing Cisco Unity Connection」の章（http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/11xcuciumgx.html から入手可能）。
- 『*Troubleshooting Guide for Cisco Unity Connection Release 11.x*』（http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/troubleshooting/guide/11xcuctsgx.html から入手可能）。
- このマニュアルでこれまでに示した設定情報

テレフォニー統合をテストする

ステップ 1 Cisco Unity Connection Administration で、[テレフォニー統合（Telephony Integrations）] に移動し、[電話システム（Phone System）] を選択します。

ステップ 2 設定をテストする必要がある電話システムをリストから選択します。

ステップ 3 [関連リンク（Related Links）] ドロップダウン リストから [テレフォニーの設定の確認（Check Telephony Configuration）] を選択し、[移動（Go）] を選択して電話システム連動の設定を確認します。

テストに失敗した場合は、[タスクの実行結果（Task Execution Results）] に 1 つ以上のメッセージがトラブルシューティング手順と共に表示されます。問題を解決した後に、もう一度接続をテストしてください。

ステップ 4 [タスクの実行結果（Task Execution Results）] ウィンドウで [閉じる（Close）] を選択します。

テスト用の環境を設定する

ステップ 1 Unity Connection が接続されている 1 つの電話システム上に、テスト用の 2 つの内線電話（電話機 1 および電話機 2）を設定します。

ステップ 2 通話に対する応答がない場合に通話を Cisco Unity Connection パイロット番号に転送するように、電話機 1 を設定します。

注意　呼び出し音が 4 回以上鳴ってから Unity Connection パイロット番号に通話を転送するよう電話システムを設定することが必要です。そのように設定しないと、テストが失敗する場合があります。

ステップ 3　Cisco Unity Connection Administration で、[ユーザ（Users）] を展開し、[ユーザ（Users）] を選択します。

ステップ 4　[ユーザの検索（Search Users）] ページで、テストに使用するユーザの表示名を選択します。このユーザの内線番号は電話機 1 の内線を設定する必要があります。

ステップ 5　[ユーザの基本設定の編集（Edit User Basics）] ページで、[次回ログイン時の自己登録を設定する（Set for Self-enrollment at Next Login）] チェックボックスをオフにします。

ステップ 6　[音声名（Voice Name）] フィールドで、テスト ユーザの音声名を録音します。

ステップ 7　[保存（Save）] を選択します。

ステップ 8　[編集（Edit）] メニューで、[メッセージ受信インジケータ（Message Waiting Indicators）] を選択します。

ステップ 9　[メッセージ受信インジケータ（Message Waiting Indicators）] ページで、メッセージ受信インジケータを選択します。表内にメッセージ受信インジケータがない場合は、[新規追加（Add New）] を選択します。

ステップ 10　[メッセージ受信インジケータの編集（Edit Message Waiting Indicator）] ページで、次の設定を入力します。

表 4-1　[メッセージ受信インジケータの編集（Edit Message Waiting Indicator）] 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すると、テスト ユーザの MWI が有効になります。
[表示名（Display Name）]	デフォルトをそのまま使用するか、別の名前を入力します。
Inherit User's Extension（ユーザの内線番号を継承）	このチェックボックスをオンにすると、電話機 1 の MWI が有効になります。

ステップ 11　[保存（Save）] を選択します。

ステップ 12　[編集（Edit）] メニューの [転送オプション（Transfer Options）] を選択します。

ステップ 13　[転送オプション（Transfer Options）] ページで、アクティブなオプションを選択します。

ステップ 14　[転送オプションの編集（Edit Transfer Option）] ページの [転送操作（Transfer Action）] の [内線（Extension）] オプションを選択し、電話機 1 の内線番号を入力します。

ステップ 15　[転送タイプ（Transfer Type）] フィールドで、[スイッチへリリースする（Release to Switch）] を選択します。

ステップ 16　[保存（Save）] を選択します。

ステップ 17　[Cisco Unity Connection Administration（Cisco Unity Connection Administration）] ウィンドウを最小化します。

[Cisco Unity Connection Administration] ウィンドウは、後の手順で再び使用するので閉じないでください。

ステップ 18　Real-Time Monitoring Tool（RTMT）にログインします。

ステップ 19　[Unity Connection] メニューの [Port Monitor] を選択します。右側のペインに [ポート モニタ（Port Monitor）] ツールが表示されます。

ステップ 20　右側のペインで [ポーリングの開始（Start Polling）] を選択します。発信を処理するポートが [ポート モニタ（Port Monitor）] に表示されます。

リリース転送を使用して外線通話をテストする

ステップ 1　電話機 2 で、外線に接続するために必要なアクセス コードを入力し、外部発信者が Unity Connection に直接ダイヤルするために使用する番号を入力します。

ステップ 2　Port Monitor で、どのポートがこの通話を処理するかを確認します。

ステップ 3　オープニング グリーティングが再生されたら、電話機 1 の内線番号を入力します。オープニング グリーティングが再生された場合、そのポートは正しく設定されています。

ステップ 4　電話機 1 の呼び出し音が鳴ることと、電話機 2 で呼び出している音が聞こえることを確認します。呼び出している音が聞こえた場合、Unity Connection が正しく通話をリリースし、電話機 1 に転送したと判断できます。

ステップ 5　電話機 1 を無応答のままにし、その通話を処理しているポートの状態が [アイドル（Idle）] に変化したことを確認します。この状態は、リリース転送が正常に行われたことを示しています。

ステップ 6　電話システムが待機するように設定されている呼び出し音の回数が経過した後に通話が Unity Connection に転送されること、およびテスト ユーザ用のグリーティングが再生されることを確認します。グリーティングが再生された場合、応答されなかった通話と通話転送情報を電話システムが Unity Connection に転送し、Cisco Unity Connection がその情報を正しく解釈したと判断できます。

ステップ 7　Port Monitor で、どのポートがこの通話を処理するかを確認します。

ステップ 8　テスト ユーザへのメッセージを残し、電話機 2 を切ります。

ステップ 9　[ポート モニタ（Port Monitor）] で、その通話を処理しているポートの状態が [アイドル（Idle）] に変化したことを確認します。この状態は、通話の終了時にポートが正常にリリースされたことを示しています。

ステップ 10　電話機 1 の MWI がアクティブになっていることを確認します。MWI がアクティブになっている場合、MWI をオンにすることに関して電話システムと Unity Connection が正常に連動していると判断できます。

メッセージ再生機能をテストする

ステップ 1　電話機 1 で、Unity Connection の内部パイロット番号を入力します。

ステップ 2　パスワードの入力を求められたら、テスト ユーザのパスワードを入力します。パスワードの入力を求める音声が再生された場合、必要な通話情報を電話システムが Unity Connection に送信し、Cisco Unity Connection がその情報を正しく解釈したと判断できます。

ステップ 3　録音したテスト ユーザの音声名が再生されることを確認します（テスト ユーザの名前を録音しなかった場合は、電話機 1 の内線番号が再生されます）。録音した名前が再生された場合、Unity Connection がユーザを内線番号で正しく識別したと判断できます。

ステップ 4　メッセージを聞きます。

ステップ 5　メッセージを聞いたら、メッセージを削除します。

ステップ 6　電話機 1 の MWI が非アクティブになっていることを確認します。MWI が非アクティブになっている場合、MWI をオフにすることに関して電話システムと Cisco Unity Connection が正常に連動していると判断できます。

ステップ 7　電話機 1 を切ります。

ステップ 8　[ポート モニタ（Port Monitor）] で、その通話を処理しているポートの状態が [アイドル（Idle）] に変化したことを確認します。この状態は、通話の終了時にポートが正常にリリースされたことを示しています。

Cisco Unity Connection で監視転送を設定する

ステップ 1　Cisco Unity Connection Administrationで、テスト ユーザの [転送オプションの編集（Edit Transfer Option）] ページの [転送タイプ（Transfer Type）] フィールドにある [転送を管理する（Supervise Transfer）] を選択します。

ステップ 2　[待機する呼び出し回数（Rings to Wait For）] フィールドに **3** と入力します。

ステップ 3　[保存（Save）] を選択します。

ステップ 4　[Cisco Unity Connection Administration（Cisco Unity Connection Administration）] ウィンドウを最小化します。

[Cisco Unity Connection の管理（Cisco Unity Connection Administration）] ウィンドウは、後の手順で再び使用するので閉じないでください。

監視転送をテストする

ステップ 1　電話機 2 で、外線に接続するために必要なアクセス コードを入力し、外部発信者が Unity Connection に直接ダイヤルするために使用する番号を入力します。

ステップ 2　Port Monitor で、どのポートがこの通話を処理するかを確認します。

ステップ 3　オープニング グリーティングが再生されたら、電話機 1 の内線番号を入力します。オープニング グリーティングが再生された場合、そのポートは正しく設定されています。

ステップ 4　電話機 1 の呼び出し音が鳴ることと、電話機 2 で呼び出している音が聞こえないことを確認します。その代わりに、通話が保留中であると判断できるように電話システムで使用する音（音楽など）を再生する必要があります。

ステップ 5　電話機 1 を無応答のままにし、その通話を処理しているポートの状態が [ビジー（Busy）] に変化したことを確認します。この状態になり、保留中であることを示す音が聞こえた場合、Unity Connection は転送を監視しています。

ステップ 6　呼び出し音が 3 回鳴ってから、テスト ユーザ用のグリーティングが再生されることを確認します。グリーティングが再生されるのは、Cisco Unity Connection が管理対象の転送通話を正常に再発信したことを意味します。

ステップ 7　グリーティングが再生されている間に電話機 2 を切ります。

ステップ 8　[ポート モニタ（Port Monitor）] で、その通話を処理しているポートの状態が [アイドル（Idle）] に変化したことを確認します。この状態は、通話の終了時にポートが正常にリリースされたことを示しています。

ステップ 9　[Stop Polling] を選択します。

ステップ 10　RTMT を終了します。

テスト ユーザを削除する

ステップ 1　Cisco Unity Connection Administration で、[ユーザ（Users）] を展開し、[ユーザ（Users）] を選択します。

ステップ 2　[ユーザの検索] ページで、テスト ユーザの左のチェックボックスをオンにします。

ステップ 3　[選択項目の削除（Delete Selected）] を選択します。

Unity Connection で Cisco Unified CM の認証と暗号化を設定している場合は、次の手順を実行します。

Cisco Unified CM の認証と暗号化をテストするには

ステップ 1　電話機 1 で、Unity Connection の内部パイロット番号をダイヤルします。

ステップ 2　電話機の LCD に認証アイコンと暗号化アイコンのいずれか（または両方）が表示されることを確認します。

ステップ 3　電話機 1 を切ります。

複数の連動用の新しいユーザ テンプレートの追加

最初の電話システム連動を作成すると、その電話システムが、デフォルトのユーザ テンプレートで自動的に選択されます。この電話システム連動を作成したあとで追加したユーザは、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、追加の電話システム連動を作成するたびに、ユーザを新しい電話システムに割り当てる適切なユーザ テンプレートを新たに追加する必要があります。新しい電話システムに割り当てる新しいユーザを追加する前に、新しいテンプレートを追加する必要があります。

新しいユーザ テンプレートの追加の詳細、または新規ユーザを追加する際のユーザ テンプレート選択の詳細については、『*System Administration Guide for Cisco Unity Connection Release 11.x*』の「User Attributes」の章に記載されている「User Templates」の項を参照してください。このガイドは、http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/11xcucsagx.html から入手可能です。

Cisco Unified Communications Manager との統合への Cisco Unified Communications Manager Express の追加

Cisco Unity Connection では、Cisco Unified CM サーバおよび Cisco Unified Communications Manager Express サーバのポート グループを持つ Cisco Unified Communications Manager 電話システム連動を統合できます。この設定は通常、WAN リンクがダウンした場合にブランチ オフィスで呼処理機能を維持するために使用されます。

ただし、次の考慮事項があります。

- Cisco Unified CM Express および Cisco Unity Connection のバージョンは、*Cisco Unity Connection の互換性マトリクス*（http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html）でサポートされる組み合わせである必要があります。
- Cisco Unified CM 電話システム連動は通常、Cisco Unified CM Express を追加する前にすでに作成されています。

Cisco Unified CM Express サーバを Cisco Unified CM に追加するには、次の手順を実行します。

Cisco Unified CM Express サーバを Cisco Unified CM 電話システム連動に追加する方法

ステップ 1 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 2 [ポート グループの検索（Search Port Groups）] ページで、Cisco Unified CM サーバのポート グループの名前を選択します。

ステップ 3 [ポート グループの基本設定（Port Group Basics）] ページの [編集（Edit）] メニューで、[サーバ（Servers）] を選択します。

ステップ 4 [サーバの編集（Edit Servers）] ページの [Cisco Unified Communications Manager（Cisco Unified Communications Manager）] で、[追加（Add）] を選択します。

ステップ 5 新しい行で、次の設定を入力します。

表 6-1　Cisco Unified CM Express サーバの設定

フィールド	設定
順序	Cisco Unified CM より大きい数を入力します。数値の最も小さいサーバがプライマリ Cisco Unified CM サーバで、数値がプライマリよりも大きい場合はセカンダリ サーバです。
IPv4 アドレス/ホスト名（IPv4 Address or Host Name）	Cisco Unified CM ポート グループに追加する Cisco Unified CM Express サーバの IPv4 アドレス（またはホスト名）を入力します。
IPv6 アドレス/ホスト名（IPv6 Address or Host Name）	このフィールドは、Cisco Unified CM Express 統合に使用しないでください。Cisco Unity Connection および Cisco Unified CM Express では、IPv6 がサポートされません。
IP アドレス/ホスト名（IP Address or Host Name）	Cisco Unified CM ポート グループに追加する Cisco Unified CM Express サーバの IP アドレス（またはホスト名）を入力します。
[ポート（Port）]	Cisco Unified CM ポート グループに追加する Cisco Unified CM Express サーバの 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。
TLS ポート（TLS Port）	Cisco Unified CM ポート グループに追加する Cisco Unified CM Express サーバの 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。

ステップ 6　[保存（Save）] を選択します。

ステップ 7　[編集（Edit）] メニューで、[詳細設定（Advanced Settings）] を選択します。

ステップ 8　[詳細設定の編集（Edit Advanced Settings）] ページの [応答後の待機時間（Delay After Answer）] フィールドで、**1000** と入力し、[保存（Save）] を選択します。

ステップ 9　[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。

ステップ 10　[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 11　リセットによってすべてのコール トラフィックが停止されることを示すメッセージが表示されたら、[OK] を選択します。

ステップ 12　[関連リンク（Related Links）] ドロップダウン リストで、[ポート グループのテスト（Test Port Group）] を選択し、[移動（Go）] を選択して Cisco Unified CM Express ポート グループ設定を確定します。

ステップ 13　テストによって進行中のコールが終了されるというプロンプトが表示されたら、[OK] を選択します。

テストに失敗した場合は、[タスクの実行結果（Task Execution Results）] に 1 つ以上のメッセージがトラブルシューティング手順と共に表示されます。問題を解決した後に、もう一度接続をテストしてください。

ステップ 14　[タスクの実行結果（Task Execution Results）] ウィンドウで [閉じる（Close）] を選択します。

ステップ 15　Cisco Unity Connection Administration からログアウトします。

M

T

こ

さ

て

ふ

ほ

め

ゆ