ボイス メッセージング

改訂日：2019 年 2 月 19 日

この章では、エンタープライズ コラボレーションのプリファード アーキテクチャに含まれるボイス メッセージング サービスについて説明します。この章では Cisco Unity Connection によるユニファイド メッセージング の実装方法について説明します。コア アーキテクチャの説明に加えて、展開プロセスの詳細も含まれています。

この章の新規情報とは

C：表 5-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

C：表 5-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
コラボレーションシステム リリース（CSR）12.5 の一部の内容のマイナー 修正およびアップデート。	この章の各項で説明	2019 年 1 月 23 日
Cisco Smart Software Manager を介した Unity Connection ライセンス供与	ライセンスの要件（C：5-6 ページ）	2017 年 8 月 30 日
更新トークンを使用した OAuth サポートの有効化	3. ユニティコネクションの基本設定（C：5-17 ページ）	2017 年 8 月 30 日

前提条件

コア アプリケーションをプリファード アーキテクチャに導入する前に、以下の点を確認してください。

- Cisco Unified Communications Manager（Unified CM）が導入されており、機能している。
- Microsoft Active Directory がインストールされており、各アプリケーションの統合について理解している。
- このマニュアルのコール制御の章の内容を理解しており、この機能を実装している。

Cisco Unity Connection によるユニファイド メッセージング

Cisco Unity Connection により、エンタープライズ コラボレーション向けシスコ プリファード アーキテクチャのユニファイド メッセージングが有効になります。この項では、ボイス メッセージングとユニファイド メッセージングのための Unity Connection と、シングル インボックスおよびビジュアル ボイスメールなどの機能の導入に関する情報と手順を説明します。この項では、2 つの Unity Connection クラスタ間のネットワークについても説明します。

コア コンポーネント

コア アーキテクチャに含まれている要素を次に示します。

- Cisco Unified Communications Manager（Unified CM）
- Cisco Unity Connection
- Microsoft Exchange
- Microsoft Active Directory

主なメリット

- ユーザは次のいずれかを使用してボイスメール システムにアクセスし、ボイス メッセージを取得できます。
  - Cisco Unified IP Phone、TelePresence エンドポイント、Jabber、およびモバイル デバイス
  - PC または Mac の Web インターフェイス
  - 電子メール クライアント アプリケーション（Microsoft Outlook など）
- ビジュアル ボイスメールにより、Jabber クライアントのボイス メッセージのビジュアル表示にアクセスできます。この表示には、送信者の名前、日付、メッセージの長さも示されます。

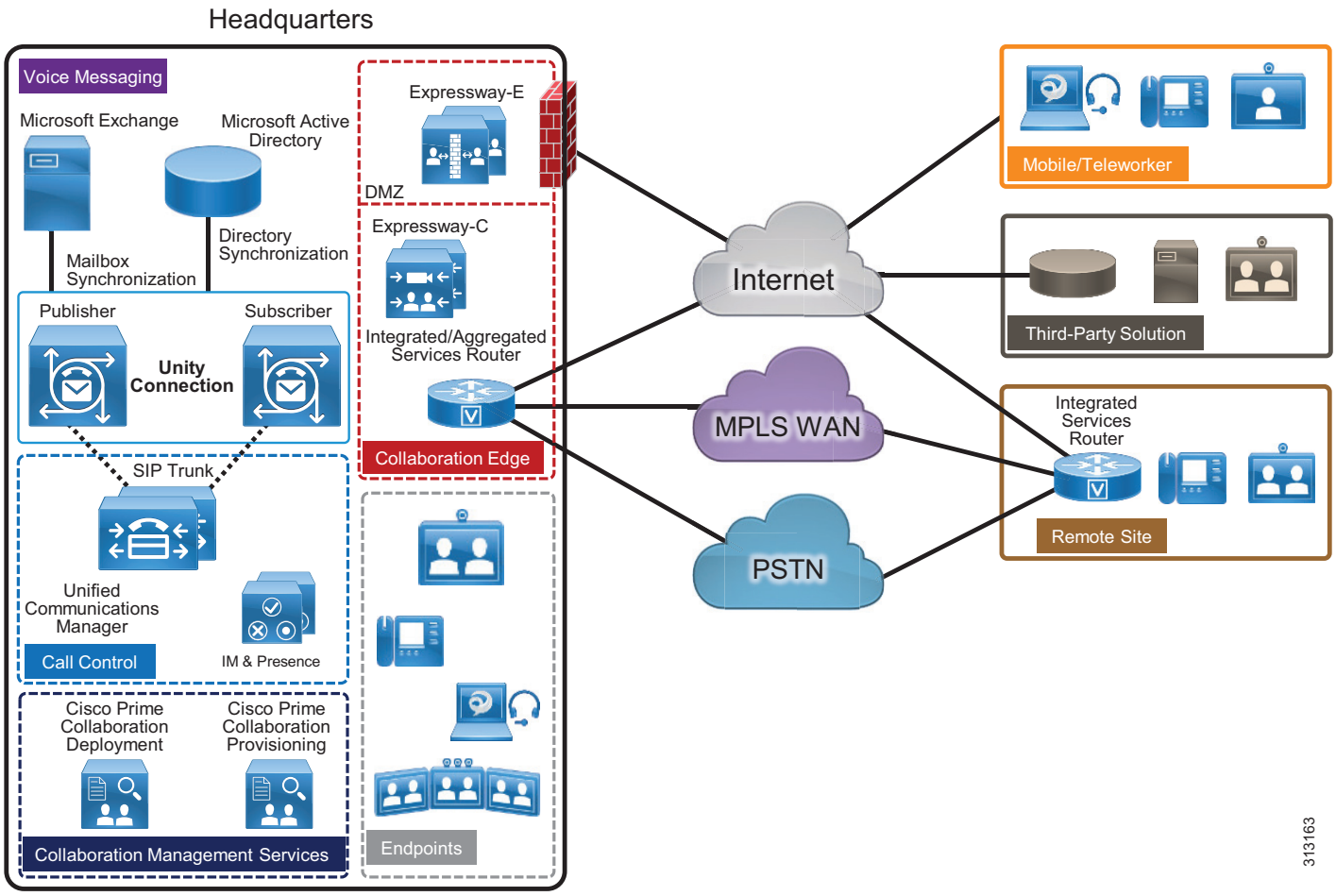
アーキテクチャー

プリファード アーキテクチャでは、このセクションで説明する、ボイス メッセージング用および呼処理用の集中型展開モデルが使用されます。

集中型メッセージングと集中型コール プロセッシング

C：図 5-1 に示すように、集中型メッセージングでは、Unity Connection が Unified Communications Manager（Unified CM）クラスタと同じサイトに配置されます。中央サイトから WAN 経由で接続しているリモート ブランチ サイトは、ユニファイド メッセージング サービスについて集中型 Unity Connection に依存しています。Unity Connection は、コール制御に SIP を使用し、メディア パスに RTP を使用して、Unified CM と統合しています。各 Unity Connection クラスタは 2 つのサーバ ノードで構成されており、高可用性と冗長性を備えています。

C：図 5-1　　アーキテクチャの概要



リモート ブランチ サイトでは、Cisco Unified Survivable Remote Site Telephony（SRST）がバックアップ コール エージェントとしてインストールされており、これは中央の Unity Connection サーバと統合しています。IP WAN の停止時には、リモート ブランチのすべての電話が SRST に登録されます。SRST は、無応答コールと話中コールを PSTN 経由で中央の Unity Connection サーバに送信するように事前に設定されています。

Unified CM の役割

Unified CM は、コール制御機能を備えており、着信側電話が話中または無応答の場合にコールを Unity Connection に転送します。ユーザが電話のメッセージ ボタンを押すか、または外部ネットワークからボイスメール パイロット番号にダイヤルすると、Unified CM はそのコールを Unity Connection にルーティングします。

Unity Connection の役割

集中型メッセージング環境では、Unity Connection によりユーザがボイスメールを保存および取得できます。一般に、Unity Connection に転送されるコールは直接コールであるか、または話中または無応答であった内線コールによるものです。ユーザに対し新しいメッセージが保存されている場合は、エンドポイントにメッセージ受信インジケータ（MWI）が表示されます。通常、電話システムと Unity Connection の間でコールごとに次のコール情報が渡されます。

- 着信側の内線番号
- 発信側の内線番号（内線の場合）、または発信側の電話番号（外線であり、電話システムが発信者 ID をサポートしている場合）
- 転送の理由（内線が通話中である、応答しない、またはすべてのコールを転送するように設定されている）

着信側が応答しないためにコールが転送された場合、Unity Connection は着信側ユーザの標準グリーティングを再生します。着信側電話が通話中であるためにコールが転送された場合、Unity Connection は着信側ユーザの通話中グリーティングを再生します。

Unity Connection は、直接コールと転送コールを異なる方法で処理します。Unity Connection は、コールを受信すると最初に発信者がユーザであるかどうかを判別します。このために、発信者 ID がユーザのプライマリ内線番号または代行内線番号に一致するかどうかを特定します。Unity Connection は一致を検出すると、ユーザが発信していると想定し、そのユーザのボイスメール PIN を入力するよう求めます。発信者 ID がユーザに関連付けられていないと Unity Connection が判断した場合、コールはガイダンスに送信されます。ガイダンスとは、外部の発信者が Unity Connection 自動応答に接続すると再生されるメイン グリーティングです。

Microsoft Exchange の役割

シングル インボックス機能を有効にするため、Unity Connection は Microsoft Exchange と統合されています。Unity Connection のシングル インボックスは、ユニファイド メッセージングを可能にし、Unity Connection と Microsoft Exchange の間でボイス メッセージを同期します。これにより、ユーザは電子メール クライアントを使用してボイスメールを受け取ることができます。

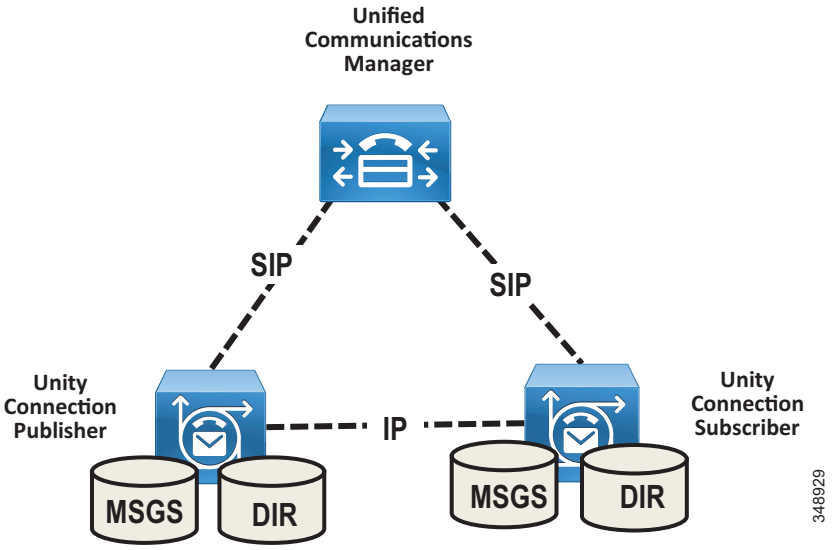
この章では、Microsoft Exchange が統合されている Unified Messaging を中心に説明します。Unity Connection は IBM Lotus Sametime インスタント メッセージング アプリケーションとも統合できます。この統合では、ユーザが Lotus Sametime を使用してボイス メッセージを再生できます。このトピックの詳細については、次の URL から入手可能な Unity Connection のマニュアルを参照してください。

https://www.cisco.com/en/US/products/ps6509/index.html

ユニファイド メッセージングの高適用性

C：図 5-2 に、アクティブ / アクティブ ペアの Unity Connection を示します。この場合、Unity Connection サーバを同じ建物または異なる建物に設置でき、高可用性と冗長性が実現します。アクティブ / アクティブ ペアの両方のサーバで Unity Connection が稼働しており、この両方のサーバでコールと HTTPS 要求が受け入れられ、ユーザ情報とメッセージが保存されます。クラスタ ペアの 1 つのサーバだけがアクティブな場合、Unity Connection は完全なエンドユーザ機能（ボイス コールと HTTPS 要求を含む）を維持します。ただし、コールに対する Unity Connection ポート キャパシティは半減し、単一サーバのキャパシティと同様になります。

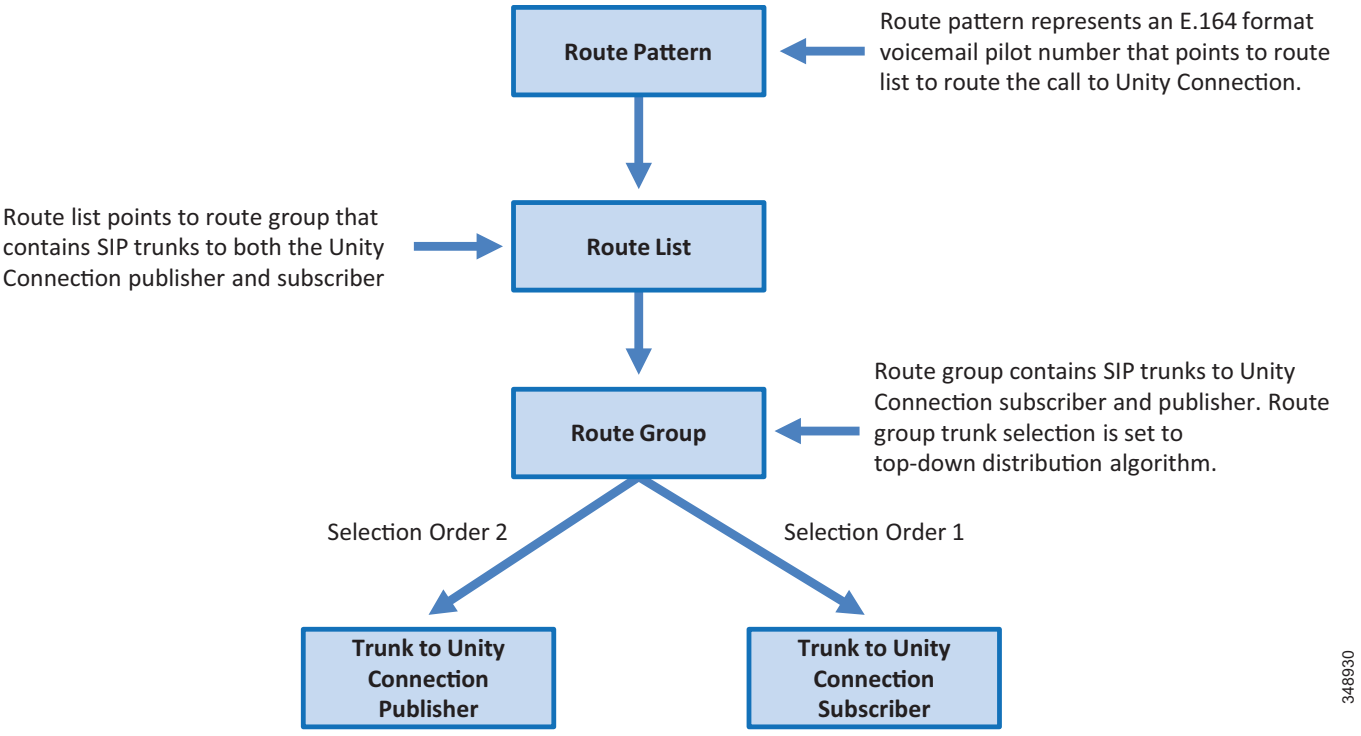
C：図 5-2　Unity Connection クラスタ



すべてのユーザ クライアント セッションおよび管理者セッション（IMAP および Cisco Personal Communications Assistant など）と管理トラフィック（Cisco Unity Connection の管理、一括管理ツール、バックアップ操作など）は、Unity Connection パブリッシャ サーバに接続します。パブリッシャ サーバが機能しなくなった場合、ユーザ クライアント セッションと管理者セッションは、Unity Connection サブスクライバ サーバに接続できます。

このトポロジでは、クラスタ内の各 Unity Connection サーバ ノードを指し示す 2 つの個別の Unified CM SIP トランクが必要です。この構成では、高可用性と冗長性の両方が実現します。すべてのコールを最初に Unity Connection サブスクライバ ノードにルーティングするように Unified CM を設定する必要があります。サブスクライバ サーバが使用不可であるか、またはサブスクライバのすべてのポートが使用中の場合、コールはパブリッシャ ノードにルーティングされます。Unified CM と Unity Connection 間で SIP が統合されている場合、トランクの選択は Unified CM ルート パターン、ルート リスト、およびルート グループ構成によって決まります。（C：図 5-3 を参照）。両方のトランクは同じルート グループに属し、同じルート リストに割り当てられています。ルート グループ内のトランクは、優先度順のトランク分配アルゴリズムを使用して並べ替えられます。この方法では、通常の運用時とフェールオーバー時の Unity Connection サーバ ノードの選択設定を Unified CM が制御できます。

C：図 5-3 Unity Connection SIP トランクの選択



Unity Connection では、高可用性のために Microsoft Exchange Database Availability Group（DAG）でのシングル インボックスの使用がサポートされています。DAG は、Microsoft の推奨事項に基づいて導入されます。高可用性を実現するため、Unity Connection ではクライアント アクセス サーバ（CAS）アレイへの接続もサポートされています。この項では、Microsoft Exchange の高可用性展開については説明しません。Exchange の高可用性展開の詳細については、http://www.microsoft.com/ で入手可能な Microsoft Exchange 製品情報を参照してください。

ライセンスの要件

Unity Connection のライセンスは Cisco Smart Software Manager によって管理されます。ライセンスされた機能を Unity Connection で使用するには、有効な機能ライセンスがお客様の Cisco Smart Software Manager ライセンス アカウントで使用可能になっている必要があり、Unity Connection はライセンスにアクセスして使用する目的で Cisco Smart Software Manager サービスと通信する必要があります。Cisco Smart Software Manager は、ユーザ ベースでライセンスを管理するための、Web に基づく集中型で全社規模のシンプルな管理機能を提供します。

ユニファイド メッセージングの要件

- Unity Connection は、Microsoft Exchange、Microsoft Business Productivity Online Suite（BPOS）専用サービス、および Microsoft Office 365 クラウドベース Exchange for Single Inbox をサポートします。
- Exchange サーバと Active Directory ドメイン コントローラ / グローバル カタログ サーバ（DC/GC）は、Microsoft がサポートする任意のハードウェア仮想環境にインストールできます。サポートされているハードウェア プラットフォームの詳細については、http://www.microsoft.com/ で入手可能な Microsoft Exchange の製品情報を参照してください。
- Microsoft Exchange メッセージ ストアは、Microsoft がサポートする任意のストレージ エリア ネットワーク コンフィギュレーションに格納できます。サポートされているストレージ エリア ネットワークの詳細については、http://www.microsoft.com/ で入手可能な Microsoft Exchange の製品情報を参照してください。
- 各サーバで 50 個のボイス メッセージング ポートごとに、Unity Connection と Microsoft Exchange の間でメッセージ同期のために 7 Mbps の帯域幅が必要となります。
- Unity Connection のデフォルト設定は、最大 2,000 ユーザと、Unity Connection と Microsoft Exchange サーバの間での最大 80 ミリ秒のラウンドトリップ遅延に十分に対応できます。2,000 を超えるユーザや 80 ミリ秒を超える遅延に対応する場合は、デフォルト設定を変更できます。詳細については、次の場所にある最新版『*Design Guide for Cisco Unity Connection*』で遅延に関する情報を参照してください。

  https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-implementation-design-guides-list.html

Unity Connection のスケーリング

Unity Connection クラスタは、最大 2 つのノード（アクティブ / アクティブ展開の 1 つのパブリッシャと 1 つのサブスクライバ）で構成されます。通常の運用時には、アクティブ / アクティブ展開では呼処理負荷分散は発生しません。Unified CM は、すべてのコールを最初に Unity Connection サブスクライバ サーバにルーティングするように設定されています。すべてのポートが使用中であるか、またはサブスクライバ サーバが使用不可の場合、コールはパブリッシャにルーティングされます。Unity Connection のサイジングでは、次の点を考慮してください。

- 現在と将来のユーザの総数
- ボイス メッセージングに必要なストレージ容量
- 各プラットフォームでサポートされるボイスメール ポートの数
- 暗号化が有効化されるかどうか

Unity Connection のスケーリングの詳細については、サイジング の章を参照してください。

Cisco Unity Connection 導入プロセス

このセクションでは、プリファード アーキテクチャでの Cisco Unity Connection の展開方法について説明します。

前提条件

ユニファイド メッセージング アーキテクチャを導入する前に、次の点を確認してください。

- Cisco Unified CM がインストールされ、コール制御用に設定されている（コール制御 の章を参照）。
- Microsoft Exchange がインストールされており、電子メール サーバとして設定されている。

展開の概要

このプリファード アーキテクチャの目的上、米国内の 3 か所のサイト（SJC、RCD、RTP）に対応する集中型メッセージング導入モデルを想定します。集中型メッセージングの導入では最初に、Unity Connection クラスタをインストールし、続いてプロビジョニングと設定を行います。Cisco Unity Connection で集中型メッセージングを導入するには、次のタスクを記載の順に行います。

1. Unity Connection クラスターのプロビジョニング
2. Unity Connection 統合のための Unified CM の設定
3. ユニティコネクションの基本設定
4. シングル インボックスの有効化
5. ビジュアル ボイスメールの有効化
6. SRST モードでのボイスメール
7. 2 つのユニティコネクションクラスタの HTTPS インターネットワーキング

注 このマニュアルでは、非デフォルト値およびその他の設定フィールド値だけが示されています。フィールド設定値が示されていない場合は、デフォルト値が想定されます。

1. Unity Connection クラスターのプロビジョニング

Unity Connection サーバ ノードをクラスタリングする場合、サーバ ペアの 1 方がパブリッシャ サーバ、もう 1 方がサブスクライバ サーバとして指定されます。

パブリッシャー

Unity Connection では、アクティブ / アクティブの高可用性を実現するために 2 つのサーバのみがクラスタでサポートされています。パブリッシャ サーバは最初にインストールするサーバであり、データベースとメッセージ ストアをパブリッシュし、クラスタ内のもう一方のサブスクライバ サーバにこの情報をレプリケートします。

サブスクライバー

ソフトウェアをインストールしたら、サブスクライバ サーバ ノードをパブリッシャに登録して、データベースとメッセージ ストアのコピーを取得します。

Unity Connection メールボックス ストア

インストール時に、Unity Connection により次のものが自動的に作成されます。

- ディレクトリ データベース：システム設定情報（ユーザ データ、テンプレート、サービス クラスなど）に使用されます。
- メールボックス ストア データベース：ボイス メッセージに関する情報（メッセージの送信先、送信時刻、ハードディスク上の WAV ファイルの場所など）に使用されます。
- オペレーティング システム ディレクトリ：ボイス メッセージの WAV ファイルに使用されます。

サーバを同じ建物に設置する場合の Unity Connection クラスタ導入の前提条件

- Unity Connection に対する着信コールと発信コールのためには、次の場所にある『*Security Guide for Cisco Unity Connection*』の最新版の「*IP Communications Required by Cisco Unity Connection*」に関する章に記載されているように、ファイアウォールの TCP ポートと UDP ポートが開いている必要があります。

  https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html
- 2 つの仮想マシンが含まれているクラスタでは、この両方のマシンが同一の仮想プラットフォーム オーバーレイに属している必要があります。
- サーバはファイアウォールによって隔離されてはなりません。
- 両方の Unity Connection サーバが同一のタイム ゾーンに位置している必要があります。
- 両方の Unity Connection サーバ ノードは同一の電話システムに統合されている必要があります。
- 両方の Unity Connection サーバで、同じ機能と構成が有効である必要があります。

サーバを異なる建物に設置する場合の Unity Connection クラスタ導入の前提条件

- Unity Connection に対する着信コールと発信コールのためには、次の場所にある『*Security Guide for Cisco Unity Connection*』の最新版の「*IP Communications Required by Cisco Unity Connection*」に関する章に記載されているように、ファイアウォールの TCP ポートと UDP ポートが開いている必要があります。

  https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html
- 2 つの仮想マシンが含まれているクラスタでは、この両方のマシンが同一の仮想プラットフォーム オーバーレイに属している必要があります。
- 両方の Unity Connection サーバ ノードは同一の電話システムに統合されている必要があります。
- 両方の Unity Connection サーバで、同じ機能と構成が有効である必要があります。
- 各 Unity Connection サーバ ノードのボイス メッセージング ポートの数に応じて、サーバ ノード間の接続に、次に示す定常輻輳のない保証帯域幅が必要です。
  - 各サーバで 50 個のボイス メッセージング ポートごとに、7 Mbps の帯域幅が必要となります。
  - 最大往復遅延は、150 ミリ秒（ms）以下でなければなりません。

Unity Connection クラスターを導入する

- ポートの最大数とユーザの最大数に基づいて、Unity Connection ノードに導入する VMware Open Virtual Archive（OVA）テンプレートを決定します。Unity Connection のスケーリングの項を参照してください。
- 両方の Unity Connection ノードをホスト A レコードとして企業のドメイン ネーム サービス（DNS）サーバに追加します。たとえば、パブリッシャ Unity Connection ホスト名を US-CUC1.ent-pa.com と設定し、サブスクライバ ホスト名を US-CUC2.ent-pa.com と設定します。
- インストールに必要なネットワーク パラメータを判別します。
  - サーバのタイム ゾーン
  - ホスト名、IP アドレス、ネットワーク マスク、およびデフォルト ゲートウェイ。ホスト名と IP アドレスが前の DNS 設定に一致していることを確認します。
  - DNS IP アドレス
  - ネットワーク タイム プロトコル（NTP）サーバの IP アドレス
- 該当する OVA ファイルを Cisco Web サイトからダウンロードします。
- VMware vSphere Client を使用して Unity Connection のパブリッシャ サーバ ノードとサブスクライバ サーバ ノードを展開します。
- Cisco Prime Collaboration Deployment を使用して、Unity Connection のパブリッシャ ノードとサブスクライバ ノードをインストールします。

詳細については、コラボレーション管理サービスの章の Cisco Prime Collaboration Deployment に関するセクションを参照してください。

注 必要に応じて、Unity Connection クラスタを手動で展開することもできます。その場合は、まず、VMWare ホスト上で推奨される OVA を使って Unity Connection パブリッシャ ノードを展開した後、そのパブリッシャ ノードに Unity Connection パッケージを手動でインストールします。パブリッシャ ノードのインストールが完了したら、サブスクライバ ノード向けのプロセスを繰り返します (VMWare ホスト上で OVA を展開し、Unity Connection パッケージを手動でインストールします)。

2. Unity Connection 統合のための Unified CM の設定

Unity Connection が Unified CM と通信する前に、Unified CM で実行する必要があるタスクがあります。Unity Connection は SIP トランクを介して Unified CM と通信します。この項では、Unified CM を Unity Connection と統合するために必要なタスクの概要を説明します。

エンドユーザ PIN 同期のための Unity Connection アプリケーションのユーザー名とサーバー

エンドユーザ PIN 管理を簡略化するには、Unified CM と Unity Connection の間の PIN 同期を有効にします。PIN 同期を使用すれば、エンドユーザは、ボイス メール アクセス、Extension Mobility、および Conference Now などの複数の目的に同じ PIN を使用できます。ユーザが PIN 番号を変更するのに Unified CM セルフケア ポータルを使用するか、それとも Cisco Unity Connection Personal Communications Assistant (PCA) を使用するかに関係なく、PIN が同期されます。

最初に、Unity Connection システム管理者アカウントのユーザ名とパスワードに一致する 1 人のアプリケーション ユーザが設定されていることを確認します（たとえば **administrator**）。Unified CM と Unity Connection でシステム管理者アカウントの名前とパスワードが同じであれば、このアカウントはすでに設定済みです。

次に、C：表 5-2 に示すように、パブリッシャ ノードとサブスクライバ ノードの両方の新しい Unity Connection アプリケーション サーバを追加します。

C：表 5-2　Unity Connection アプリケーション サーバの定義

パラメータ	値	注
[名前（Name）]	**US-CUC1**	Unity Connection サーバの名前を入力します。
[IP アドレス（IP Address）]	*<IP_Address_US-CUC1>*	Unity Connection サーバの IP アドレスを入力します。
選択されたアプリケーション ユーザ	**管理者**	Unity Connection システム管理者アカウントに一致するアプリケーション ユーザを選択します。
エンド ユーザ PIN 同期を有効化	オン	Unified CM（Extension Mobility 用など）と Unity Connection（ボイス メッセージ アクセス用）の間のエンド ユーザ PIN 同期を有効にするには、オンにします。

注　Unified CM と Unity Connection の間のエンドユーザ PIN 同期を有効にする際には、Unified CM で割り当てられる PIN 認証ルールと Unity Connection で割り当てられるボイスメール認証ルールが、最小クレデンシャル長および有効期限の点で必ず一致することが重要です。これらの認証ルールが一致するよう調整しない場合、PIN 同期エラーやログイン障害が発生する可能性があり、管理者の介入が必要になることもあります。

注　PIN 同期が機能するためには、Unity Connection と Unified CM の両方に、**tomcat-trust** に読み込まれる遠端サーバまたはルート CA 証明書が含まれている必要があります。証明書管理の詳細については、セキュリティーの章を参照してください。

SIP トランク セキュリティー プロファイル

メディアおよびシグナリングの暗号化に関して、このマニュアルではこれらの暗号化は使用されず、代わりに Unified CM と Unity Connection サーバ ノードの間には非セキュアな SIP トランクが実装されていることを前提としています。デバイス セキュリティ モードが [非セキュア（Non Secure）] に設定された状態で、Unity Connection に新規 SIP トランク セキュリティ プロファイルを作成します。C：表 5-3 に、SIP トランク セキュリティ プロファイルの設定を示します。

C：表 5-3　SIP トランク セキュリティ プロファイルの設定

パラメータ	値	注
[名前（Name）]	Unit Connection SIP トランク セキュリティ プロファイル	セキュリティ プロファイルの名前を入力します。
[説明（Description）]	Unit Connection SIP トランク セキュリティ プロファイル	プロファイル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）]	非セキュア（Non Secure）	SIP トランクのセキュリティ モード。
[ダイアログ外 REFER の許可（Accept Out-of-Dialog refer）]	オン	Unified CM が、SIP トランク経由で着信する非インバイトの ダイアログ外 REFER メッセージを受け入れることを指定します。
[未承諾 NOTIFY の許可（Accept unsolicited notification）]	オン	Unified CM が、SIP トランク経由で着信する非インバイトの未承諾 NOTIFY メッセージを受け入れることを指定します。Unity Connection から MWI メッセージを受け入れるには、このパラメータをオンにする必要があります。
[REPLACE ヘッダの許可（Accept replaces header）]	オン	Unified CM が、既存の SIP ダイアログを置き換える新しい SIP ダイアログを受け入れることを指定します。これにより、Cisco Unity Connection が開始する監視転送に使用される "REFER w/replaces" を渡すことができるようになります。

SIP プロファイル

Unity Connection への SIP トランクの SIP プロファイルを設定します。標準 SIP プロファイルをコピーし、その名前を **Unity Connection SIP Profile** に変更します。Unified CM サーバの IP アドレスが、Unified CM により送信される SIP 発呼側情報に含まれないようにするには、[SIP 要求で完全修飾ドメイン名を使用（Use Fully Qualified Domain Name in SIP Requests）] チェックボックスをオンにします。[サービスタイプ " なし (デフォルト)" のトランクの接続先ステータスをモニタするために OPTIONS Ping を有効にする（Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"）] 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。これにより、システムが Unity Connection ノードへの接続の状況を追跡できます。

OPTIONS Ping が有効な場合、トランクの SIP デーモンを実行する各ノードは、トランクの各宛先 IP アドレスに対して OPTIONS 要求を定期的に送信して到達可能性を判断し、到達可能なノードにのみコールを送信します。宛先アドレスが OPTIONS 要求に応答しない場合、Service Unavailable（503）応答または Request Timeout（408）応答を送信する場合、または TCP 接続を確立できない場合、そのアドレスは「アウト オブ サービス」と見なされます。1 つ以上のノードが、1 つ以上の宛先アドレスから（408 または 503 以外の）応答を受信した場合、トランク全体の状態は「イン サービス」と見なされます。SIP トランク ノードは、トランクの設定済み宛先 IP アドレス、またはトランクの DNS SRV エントリの解決済み IP アドレスに対して OPTIONS 要求を送信できます。すべての SIP トランクで SIP OPTIONS Ping を有効にすることを推奨します。有効にすることで、Unified CM は、コールごとの状態、ノードごとの状態、およびタイムアウトに基づいて判別するのではなく、動的にトランクの状態を追跡することができるためです。

SIP トランク

クラスタ内の Unity Connection サーバ ノードごとに 1 つずつ、合計で 2 つの個別 SIP トランクを作成します。C：表 5-4 に SIP トランクの設定を示します。

C：表 5-4　Unity Connection サーバへの SIP トランクのパラメータ設定

パラメータ	値	説明
名前（Name）	US_CUC1_SIP_Trunk	Unity Connection への SIP トランクの固有名を入力します。
[説明（Description）]	Unity Connection パブリッシャ	SIP トランクの説明を入力します。
[デバイスプール（Device Pool）]	Trunks_and_Apps	Unity Connection のデバイス プールを入力します。（コール制御の章を参照。）
[すべてのアクティブな Unified CM ノードで実行（Run on All Active Unified CM Nodes）]	オン	SIP トランクを使用した発信コールでは、Unified CM 呼処理サブスクライバ間のクラスタ内制御シグナリングが必要ではないことを指定します。
[コールルーティング情報 - インバウンドコール（Call Routing Information - Inbound Calls）]		
[コーリングサーチスペース（CSS）（Calling Search Space (CSS)）]	ボイスメール（CSS 設定の詳細については、コール制御の章を参照してください。）	割り当てられる CSS には、DID、DID 以外の番号、URI パーティションなどのすべてのネットワーク上の宛先が含まれています。CSS にこれらのすべてのパーティションが含まれていないと、Unity Connection からの MWI 未承認 NOTIFY メッセージがユーザの電話に到達しません。
[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）]	オン	リダイレクト情報要素、最初のリダイレクト番号、およびコール転送理由が着信メッセージの一部として送信され、受け入れられることを指定します。Unity Connection は最初のリダイレクト番号を使用してコールに応答します。

C：表 5-4　Unity Connection サーバへの SIP トランクのパラメータ設定（続き）

パラメータ	値	説明
[コールルーティング情報 - アウトバウンドコール（Call Routing Information - Outbound Calls）]		
[発呼側および接続側情報形式（Calling and Connected Party Info Format）]	[接続側にのみ URI および DN を配信 (使用可能な場合) （Deliver URI and DN in connected party, if available）]	このオプションは、Unified CM がディレクトリ番号、ディレクトリ URI、またはディレクトリ番号とディレクトリ URI の両方を含むアドレスを、発信 SIP メッセージの SIP ID ヘッダーに挿入するかどうかを決定します。
[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）]	オン	リダイレクト情報要素、最初のリダイレクト番号、およびコール転送理由が発信メッセージの一部として送信され、受け入れられることを指定します。Unity Connection は最初のリダイレクト番号を使用してコールに応答します。
[SIP 宛先情報（SIP Destination Information）]		
[宛先アドレス（Destination Address）]	us-cuc1.ent-pa.com	Unity Connection サーバの完全修飾ドメイン名（FQDN）を入力します。
[SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）]	Unit Connection SIP トランク セキュリティ プロファイル	C：表 5-3 を参照してください。
[SIP プロファイル（SIP Profile）]	Unity Connection SIP プロファイル	SIP プロファイルを参照してください。

ルート グループ

Unity Connection クラスタに対し、別のルート グループ RG_CUC を作成します。このルート グループには、Unity Connection サブスクライバ ノードとパブリッシャ ノードへの SIP トランクが含まれています。リストに、サブスクライバ ノードに接続する SIP トランク（US_CUC2_SIP_Trunk）が最初に示され、続いてパブリッシャ ノードに接続する SIP トランク（US_CUC1_SIP_Trunk）が示されていることを確認してください。ルート グループ分配アルゴリズムとして、[優先度順（Top Down）] トランク選択方式を設定する必要があります。[優先度順（Top Down）] 分配アルゴリズムが設定されているルート グループでは常に、コールが最初に Unity Connection サブスクライバ サーバ ノード（US-CUC2）に送信されます。Unity Connection サブスクライバ サーバ ノードがビジーまたは使用不可の場合、コールはパブリッシャ サーバ ノード（US-CUC1）に送信されます。

ルート リスト

Unity Connection クラスタに対し、別のルート リスト RL_CUC を作成します。このルート リストには、前述の説明で作成した Unity Connection ルート グループ（RG_CUC）だけが含まれている必要があります。[このルートリストを有効にする（Enable this Route List）] と [すべてのアクティブな Unified CM ノードで実行（Run on all Active Unified CM Nodes）] オプションが選択されていることを確認してください。

ルート パターン

前述の説明で作成した Unity Connection ルート リストを指し示すボイスメール パイロット番号の別のルート パターンを作成します。この番号はボイスメール パイロット番号に一致している必要があります。C：表 5-5 に、ルート パターンの設定例を示します。

C：表 5-5　Unity Connection パイロット番号：ルート パターンの例

パラメータ	値
[ルートパターン（Route Pattern）]	+14085554999
[ルートパーティション（Route Partition）]	DN
[ゲートウェイ / ルートリスト（Gateway/Route List）]	RL_CUC
[コールの分類（Call Classification）]	オンネット（OnNet）
[外部ダイヤルトーンの提供（Provide Outside Dial Tone）]	オフ

ボイスメールパイロット

ボイスメール パイロット番号は、ユーザがボイス メッセージにアクセスするための電話番号を指定します。Unified CM は、ユーザが IP エンドポイントの [メッセージ（Messages）] ボタンを押すと、自動的にボイスメール パイロット番号にダイヤルします。3 つのサイトすべてに対して 1 つのボイスメール パイロット番号が作成されます。C：表 5-6 に、ボイスメール パイロットの設定例を示します。

C：表 5-6　ボイスメール パイロットの例

パラメータ	値
[ボイスメールパイロット番号（Voice Mail Pilot Number）]	+14085554999
[コーリングサーチスペース（Calling Search Space）]	DN
[説明（Description）]	VM Pilot
[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）]	オン

リモート サイトのボイスメール ユーザは、各自の DID 範囲からボイスメール アクセス番号にダイヤルして、PSTN からメッセージを確認できます。ボイスメール PSTN アクセス番号をボイスメール パイロット番号に変換するためのトランスレーション パターンが個別に作成されます。表 6 に、ボイスメール パイロットのトランスレーション パターンの設定を示します。

C：表 5-7　ボイスメール パイロットのトランスレーション パターンの例

パラメータ	値
[トランスレーションパターン（Translation Pattern）]	+19195551999
[パーティション（Partition）]	DN
[発信側コーリングサーチスペースを使用（Use Originators Calling Search Space）]	オン
[ルートオプション（Route Option）]	[このパターンをルーティング（Route this pattern）]
[着信側トランスフォーメーション（Called Party Transformations）]	
[着信側トランスフォーメーションマスク（Called Party Transform Mask）]	+14085554999

他のリモート サイト向けに追加のトランスレーション パターンが作成されます。

ボイスメール プロファイル

すべてのエンドポイント デバイスとエクステンション モビリティ プロファイルで、各ユーザの電話回線に対してボイスメール プロファイルが割り当てられます。このプロファイルにより、ユーザはエンドポイントの [メッセージ（Messages）] ボタンを押すだけで、ボイスメール システムにワンタッチでアクセスできます。Unity Connection が単一電話システムに統合されている場合は、デフォルトのボイスメール プロフィルを使用することを推奨します。エンドポイント デバイスでの回線の初期プロビジョニング時に、デフォルトのボイスメール プロファイル（[なし（None）]）が電話番号に割り当てられます。ボイスメールにアクセスする必要がないユーザの場合、そのエンドポイント回線にボイスメール プロファイルが割り当てられません。C：表 5-8 に、ボイスメール プロファイルの設定例を示します。

C：表 5-8　ボイスメール プロファイルの例

パラメータ	値
[ボイスメールプロファイル名（Voice Mail Profile Name）]	デフォルト
説明	VM プロファイル
[ボイスメールパイロット（Voice Mail Pilot）]	+14085554999/DN
[ボイスメールマスク（Voice Mail Mask）]	空欄
[システムのデフォルトボイスメール プロファイルとして使用する（Make this the default Voice Mail Profile for the System）]	オン

3. ユニティコネクションの基本設定

サービスのアクティベーション

- Unity Connection のインストールが完了したら、Cisco Unified Serviceability にログインし、パブリッシャ サーバ ノードの **DirSync** サービスをアクティブにします。
- [ユニファイドサービスアビリティ（Unified Serviceability）] 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。パブリッシャ サーバ ノードで Cisco DirSync サービスが開始していることを確認します。
- [Unity Connection のサービスアビリティ（Unity Connection Serviceability）] で [ツール（Tools）] –> [サービス管理（Service Management）] に移動します。パブリッシャおよびサブスクライバ Unity Connection サーバ ノードでサービスのステータスを確認します。C：表 5-9 に、この導入環境のサービス ステータスを示します。

C：表 5-9　Unity Connection サービス ステータス

サービス	Unity Connection パブリッシャ（プライマリ）	Unity Connection サブスクライバ (セカンダリ)
ステータスのみのサービス（OS コマンド ライン インターフェイスから非アクティブにできます）		
このカテゴリのすべてのサービス	はい	はい
重要なサービス		
接続会話マネージャ	はい	はい
接続メールボックスの同期	はい	いいえ（No）
接続メッセージ転送エージェント	はい	いいえ（No）
接続ミキサー	はい	はい
接続通知	はい	いいえ（No）
基本サービス		
このカテゴリのすべてのサービス	はい	はい
オプション サービス		
接続ブランチ同期サービス	いいえ（No）	いいえ（No）
コネクション デジタル ネットワーク レプリケーションエージェント	いいえ（No）	いいえ（No）
このカテゴリに含まれるその他の残りのすべてのサービス (Connection Jetty と Connection REST サービスを含む)	はい	はい

データベースのリプリケーション

パブリッシャとサブスクライバの両方の Unity Connection サーバ ノードでサービスをアクティブにした後、サブスクライバ ノードからパブリッシャ ノードに接続できることを確認します。また、両方のノードで OS コマンド ライン インターフェイス（CLI）のコマンド **show perf query class "Number of Replicates Created and State of Replication"** を使用して、データベース レプリケーションのステータスを確認します。

Unified CM の統合

各 Unity Connection クラスタは、同じ場所に配置されている Unified CM クラスタと統合されます。これにより、Unified CM クラスタ専用の各 Unity Connection クラスタによる単純な統合モデルが実現します。Unified CM では Unity Connection クラスタとの相互接続のために SIP トランクが設定されますが、Unity Connection システムではキャパシティとライセンスの目的で、ボイスメール ポートが使用されます。この項では、設計時の考慮事項、キャパシティ プランニング、ボイスメール ポートの設定について説明します。

ボイスメール ポートのオーディオ コーデック設定

Unity Connection では、Unity Connection SIP シグナリングでサポートされるオーディオ コーデック形式のコールは常に PCM リニアにトランスコードされます。PCM リニアから、Unity Connection Administration のシステムレベル録音オーディオ コーデック システム全体設定で録音がエンコードされます。デフォルトは G.711 mu-law です。

この項では、発信側デバイスと Unity Connection の間でネゴシエートされるオーディオ コーデックを*回線コーデック*と呼び、システムレベルの録音用オーディオ コーデックとして設定されたオーディオ コーデックを*録音コーデック*と呼びます。

サポートされる回線コーデック（公表コーデック）

- G.711 mu-law
- G.711 a-law
- G.722
- G.729
- iLBC

サポートされる録音コーデック（システムレベルの録音オーディオ コーデック）

- PCM リニア
- G.711 mu-law（デフォルト）
- G.711 a-law
- G.729a
- G.726
- GSM 6.10

トランスコーディングは、本来すべての接続で発生するので、ライン コーデックと録音コーデックが違っても、システムへの影響にほとんど違いはありません。たとえば、G.729a を回線コーデックとして、G.711 mu-law を録音コーデックとして使用しても、Unity Connection サーバにはトランスコーディングに伴う大きな追加負荷はかかりません。しかし、iLBC コーデックまたは G.722 コーデックはトランスコーディングにより多くの計算を必要とするので、Unity Connection サーバに大きな追加負荷がかかります。そのため、Unity Connection サーバがサポートできる G.722 または iLBC 接続の数は、G.711 mu-law 接続の数の半分のみです。

このトポロジの例では、システム録音コーデックはデフォルト（G.711 mu-law）のままです。サポートされる回線コーデックは G.729 および G.711 mu-law に設定されます。このデフォルト設定を使用する場合、同一の Unity Connection サイトのユーザは G711 mu-law を使用します。中央の Unity Connection サーバに WAN 経由で接続するユーザの場合、選択される回線コーデックは G.729 です。

G.722 コーデックまたは iLBC コーデックを回線コーデック（アドバタイズされているコーデック）として使用すると、Cisco Unity Connection サーバでプロビジョニング可能なボイス ポートの数が減少します。G.722 または iLBC コーデックを使用する場合に各プラットフォーム オーバレイでサポートされるボイス ポートの数の詳細については、『Virtualization for Cisco Unity Connection』を参照してください。

システム設定（System Settings）

Unified CM コール制御システムの場合と同様に、Unity Connection ボイスメール システムでは更新トークンを使用した OAuth が必要です。更新トークンを使用した OAuth をシステムで有効にして、Unified CM パブリッシャ ノードを承認 (Authz) サーバとして設定する必要があります。

[Cisco Unity Connection Administration] > [システム設定（System Settings）] > [エンタープライズ パラメータ（Enterprise Parameters）] に移動して、[SSO と OAuth の設定（SSO and OAuth Configuration）] セクションで、[更新ログイン フローを使用した OAuth（OAuth with Refresh Login Flow）] を [有効（Enabled）] に設定します。

次に、[システム設定（System Settings）] > [Authz サーバ（Authz Servers）] に移動して、[新規追加（Add New）] ボタンをクリックし、Authz サーバを追加します。C：表 5-10 に、Unified CM パブリッシャを追加して AuthZ サーバとして設定するための Authz サーバ設定を示します。

C：表 5-10　Authz サーバ設定

パラメータ	値	説明
Display Name	Authz サーバ（us-cm-pub）	この設定は、Authz サーバの表示名を定義します。
[認証サーバ（Authz Server）]	us-cm-pub.ent-pa.com	この設定は、Unified CM パブリッシャ ノードである Authz サーバの FQDN を指定します。
[ポート（Port）]	8443（デフォルト）	この設定は、Authz サーバとの通信に使われるポートを決定します。
[ユーザ名（Username）]	管理者	これは、Unity Connection が Authz サーバへのサインインに使用するユーザ名です。
[パスワード（Password）]	*<password>*	これは、Unity Connection が Authz サーバへのサインインに使用するパスワードです。
[証明書エラーを無視する（Ignore Certificate Errors）]	オフ（デフォルト）	この設定は、Unity Connection が Authz サーバから受信した証明書を検証するかどうかを決定します。

[保存（Save）] をクリックして、Authz サーバを作成し、キーを同期します。

電話システムの設定

電話システムの統合により、Unity Connection と Unified CM の間の通信が実現します。Unity Connection が 1 つの Unified CM クラスタと統合している場合は、デフォルトの **PhoneSystem** を使用することを推奨します。C：表 5-11 に、電話システムの設定を示します。

C：表 5-11　電話システムの設定

パラメータ	値	説明
[電話システムの名前（Phone System Name）]	PhoneSystem	電話システム
[デフォルト TRAP 電話システム（Default TRAP Phone System）]	オン	電話システムにより TRAP 接続が有効になるので、ボイス メール ボックスを使用していない管理者とユーザが、Unity Connection Web アプリケーションで電話から録音、再生できます。
[内線番号を使用したコールループの検出（Call Loop Detection by Using Extension）]		
[転送メッセージ通知コールに対して有効にする (内線番号を使用)（Enable for Forwarded Message Notification Calls (by Using Extension)）]	オン	（携帯電話などの）デバイスに送信される新規メッセージ通知、およびデバイスが応答しなかったために Unity Connection にデバイスが再転送した新規メッセージ通知を Unity Connection で内線番号を使用し検出して拒否します。コールループが検出されず拒否されない場合、コールによってユーザ宛ての新しいボイス メッセージが作成され、Unity Connection が新規メッセージ通知のコールをデバイスに送信します。
[発信コール規制（Outgoing Call Restrictions）]		
[発信コールを有効にする（Enable outgoing calls）]	オン	Unity Connection は、必要に応じて電話システムを通じて発信コール（MWI の設定など）をかけます。
[AXL サーバ（AXL Servers）]（[編集（Edit）] > [Cisco Unified Communications Manager AXL サーバ（Cisco Unified Communications Manager AXL Servers）] の下)		
[順序 0（Order 0）]	*<IP_Address_US-CM-PUB>*	Unified CM AXL サーバ ノード（パブリッシャ）の IP アドレスを入力します。
[ポート（Port）]	8443	Unity Connection が AXL 通信に使用する Unified CM サーバの TCP ポートを入力します。
[ユーザ名 / パスワード（Username/Password）]	管理者	「標準 AXL API アクセス」の役割を持つ Unified CM アプリケーション ユーザのユーザ名とパスワードを入力します。
[Cisco Unified Communications Manager のバージョン（Cisco Unified Communications Manager Version）]	5.0 以降（SSL 対応）	Unified CM 5.0 以降のバージョンの SSL を指定します。
[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）]	オン	Unity Connection（ボイス メッセージ アクセス用）と Unified CM（Extension Mobility 用など）の間でエンドユーザ PIN 同期を有効にするには、オンにします。
[証明書エラーを無視する（Ignore Certificate Errors）]	オフ	Unity Connection が Unified CM Tomcat 証明書を必ず検証するようにするには、オフにします。

注　Unified CM と Unity Connection の間のエンドユーザ PIN 同期を有効にする際には、Unified CM で割り当てられる PIN 認証ルールと Unity Connection で割り当てられるボイスメール認証ルールが、最小クレデンシャル長および有効期限の点で必ず一致することが重要です。これらの認証ルールが一致するよう調整しない場合、PIN 同期エラーやログイン障害が発生する可能性があり、管理者の介入が必要になることもあります。

ポート グループの設定

ポート グループを使用して、Unified CM クラスタと Unity Connection クラスタの間の SIP 通信を制御します。ポート グループを使用することで、システムは Unity Connection サーバが受け入れる SIP メッセージの送信元 Unified CM と、Unity Connection サーバが発信コールを Unified CM サーバにルーティングするときに使用する設定と順序を制限および指定できます。Unity Connection サーバは、Unity Connection 向けの Unified CM SIP ルーティング設計をミラーするように設定されているため、Unity Connection サーバで発信ルーティングが 1 番目に使用可能な Unified CM サブスクライバ ノードを選択するように設定する必要があります。C：表 5-12 に、ポート グループの設定を示します。

C：表 5-12　ポート グループの設定

パラメータ	値	説明
[表示名（Display Name）]	PhoneSystem-1	電話システムの記述名
[連動方法（Integration Method）]	SIP	Unity Connection と Unified CM の接続に使用する連動方法。
[セッション開始プロトコル (SIP) の設定（Session Initiation Protocol (SIP) Settings）]		
[SIP サーバで登録する（Register with SIP Server）]	オン	これにより、Cisco Unity Connection が SIP サーバに登録されます。
[SIP サーバ（SIP Servers）]（[編集（Edit）] > [サーバ（Servers）] の下）		
[順序 0（Order 0）]	*<IP_Address_US-CM-SUB1>*	順序 0 に設定されている SIP サーバには高い優先度が設定されます。プライマリ Unified CM 呼処理ノードの IP アドレスを入力します。
[順序 1（Order 1）]	*<IP_Address_US-CM-SUB2>*	順序 1 に設定されている SIP サーバには低い優先度が設定されます。セカンダリ Unified CM 呼処理ノードの IP アドレスを入力します。
[ポート（Port）]	5060	Unity Connection が SIP 通信に使用する Unified CM サーバの TCP ポートを入力します。
[TLS ポート（TLS Port）]	5061	Unity Connection がセキュア SIP 通信に使用する Unified CM サーバの TCP TLS ポートを入力します。
[TFTP サーバ（TFTP Servers）]（[編集（Edit）] > [サーバ（Servers）] の下）		

C：表 5-12　ポート グループの設定（続き）

パラメータ	値	説明
[順序 0（Order 0）]	*<IP_Address_US-CM-TFTP1>*	順序 0 に設定されている TFTP サーバには、より高い優先度が与えられます。プライマリ Unified CM TFTP ノードの IP アドレスを入力します。
[順序 1（Order 1）]	*<IP_Address_US-CM-TFTP2>*	順序 1 に設定されている TFTP サーバには、より低い優先度が与えられます。バックアップ Unified CM TFTP ノードの IP アドレスを入力します。

ボイス メッセージング ポートのサイジングに関する考慮事項

クラスタ内の各 Unity Connection サーバでは、いずれかのサーバが停止した場合のために、次のダイヤルイン機能用のボイス メッセージング ポートが指定されている必要があります。

- コールへの応答

各 Unity Connection サーバではさらに、次の発信機能用のボイス メッセージング ポートが指定されている必要があります。

- メッセージ受信インジケータ（MWI）の送信
- メッセージ到着通知の実行
- 電話での録音および再生（TRAP）接続の許可

システムのボイスメール ポートの合計数の 20% を、メッセージ通知、MWI の発信、および TRAP 用に確保しておくことを推奨します。これにより、コールへの応答とポートでの発信のためにポートでコール ブロッキングが発生する可能性が低減します。

ポート設定

前述の項で説明したように、ポートは着信ポートまたは発信ポートのいずれかになります。C：表 5-13 に、ボイスメール ポート割り当ての設定例を示し、C：表 5-14 に、応答ポートの設定のための設定テンプレートを示します。

C：表 5-13　ボイスメール ポート割り当ての設定例

Cisco Unity Connection のサーバ	ポート範囲	機能
US-CUC1	1 ～ 80	応答
US-CUC2	1 ～ 80	応答
US-CUC1	81 ～ 100	発信
US-CUC2	81 ～ 100	発信

C：表 5-14　ボイスメール応答ポートの設定例

パラメータ	値	説明
[有効（Enabled）]	オン	電話システム ポートを有効にするには、このボックスをオンにします。
[電話システムポート（Phone System Port）]		
[ポート名（Port Name）]	自動作成	Unity Connection によりポート名が自動的に作成されます。
[電話システム（Phone System）]	電話システム	適切な電話システムを選択します。
[ポートグループ（Port Group）]	PhoneSystem-1	適切なポート グループを選択します。
[サーバ（Server）]	US-CUC2/US-CUC1	最初に Cisco Unity Connection サブスクライバ ノードを選択し、同様に Unity Connection パブリッシャ ノードのポートを追加します。
[電話の動作（Phone behavior）]		
[呼び出しに応答（Answer Call）]	オン	この設定により、コールに応答するポートが指定されます。
[メッセージ通知を実行する（Perform Message Notification）]	オフ	この設定により、メッセージをユーザに通知するためのポートが指定されます。
[MWI 要求を送信する（Send MWI Requests）]	オフ	この設定により、MWI オン / オフ要求を送信するためのポートが指定されます。
[TRAP 接続を許可する（Allow TRAP Connections）]	オフ	この設定により、Telephony Recording and Playback（TRAP）接続のポートが指定されます。

C：表 5-14 に示す設定は、ボイスメールの発信ポートを作成するときにも使用する必要があります。ただし発信ポートの場合は、[呼び出しに応答（Answer Call）] パラメータをオフにし、[メッセージ通知を実行する（Perform Message Notification）]、[MWI 要求を送信する（Send MWI Requests）]、および [TRAP 接続を許可する（Allow TRAP Connections）] パラメータをオンにします。

アクティブ ディレクトリーの統合

Unity Connection は、Active Directory に対する認証を使用する Unity Connection Web アプリケーション（エンドユーザ向けの Cisco Personal Communications Assistant（PCA）など）の Microsoft Active Directory 同期および認証をサポートします。同様に、Unity Connection ボイス メッセージへにアクセスするために使用する IMAP 電子メール アプリケーションは、Active Directory に対して認証されます。電話ユーザ インターフェイスまたはボイス ユーザ インターフェイスによる Unity Connection ボイス メッセージへのアクセスでは、引き続き Unity Connection データベースに対して数値パスワード（PIN）による認証が行われます。Unity Connection と Unified CM の間で PIN 同期が有効になっている場合、これらの PIN は Unified CM システム PIN と同期されます。

Active Directory で、Unity Connection がユーザ検索ベースに指定されているサブツリーにアクセスするときに使用する管理者アカウントを作成する必要があります。検索ベースのすべてのユーザ オブジェクトを「読み取る」ための最小限の権限が設定されており、また、有効期限のないパスワードが設定されている Unity Connection 専用アカウントを使用することを推奨します。

Unified CM の [メール ID（Mail ID）] フィールドが、Active Directory のメール フィールドと同期されます。統合プロセスでは、これにより LDAP のメール フィールドが Unity Connection の [社内電子メールアドレス（Corporate Email Address）] フィールドに表示されます。Unity Connection は Unified Messaging アカウントの [社内電子メールアドレス（Corporate Email Address）] を使用してシングル インボックスを有効にします。

Unity Connection と Active Directory の統合により、ユーザ情報のインポートが可能になります。Unity Connection と Active Directory の統合にはさまざまなメリットがあります。

- ユーザの作成：Active Directory からデータをインポートして Unity Connection ユーザを作成できます。
- データの同期：Unity Connection は、Unity Connection データベースのユーザ データと Active Directory のデータを自動的に同期するように設定されています。
- 1 つのクレデンシャル セット：Unity Connection Web アプリケーションのユーザ名とパスワードを Active Directory に対して認証するように Unity Connection を設定します。これにより、ユーザが複数のアプリケーション パスワードを管理する必要がなくなります。

Active Directory の設定については、コール制御の章を参照してください。

ユニティコネクションのパーティションと CSS

この導入環境のすべてのユーザは、デフォルトのコーリング サーチ スペース（US-CUC1 サーチ スペース）で設定されています。このサーチ スペースにはデフォルトのパーティション（US-CUC1 パーティション）が含まれています。

規制テーブル

Unity Connection は、ボイスメール システムが未承認の電話番号を呼び出すことがないようにするため、規制テーブルを使用します。通常、これらのルールは許可されている番号またはブロックされている番号のいずれかに完全一致するように設定されています。この展開では、Unity Connection システムがボイスメール システムでのコール ブロッキングの規制ルールを使用せず、代わりに SIP トランク着信コーリング サーチ スペース（CSS）を使用して、Unity Connection からの不正なコールを阻止します。Unity Connection がネット上の宛先のみをダイヤルできるように、SIP トランク CSS を設定します。C：表 5-15 に、デフォルトの転送規制テーブルの設定を示します。

C：表 5-15　Unity Connection の規制テーブル

順序	ブロック	パターン
0	このチェックボックスをオフにします。	+*
1	このチェックボックスをオフにします。	9+*
2	このチェックボックスをオフにします。	91???????*
3	このチェックボックスをオフにします。	9011???????*

C：表 5-15　Unity Connection の規制テーブル（続き）

順序	ブロック	パターン
4	このチェックボックスをオフにします。	9???????????*
5	このチェックボックスをオフにします。	900
6	このチェックボックスをオフにします。	*

Unity Connection には、この他に、デフォルトのファクス、デフォルトの発信ダイヤル、デフォルトのシステム転送、およびユーザ定義および自動追加の代行内線番号用の 4 つの規制テーブルがあります。これらの規制テーブルも、C：表 5-15 で説明する設定を使用して無効にすることができます。

サービス クラス

サービス クラス（CoS）は、Unity Connection ボイスメールのユーザに対する制限と機能を定義します。サービス クラスは一般にユーザ テンプレートで定義され、このテンプレートがユーザ アカウントの作成時にアカウントに適用されます。この導入環境では、デフォルトのボイスメール ユーザ の COS がすべてのユーザに関連付けられています。

ユーザー プロビジョニング

ユーザを Unity Connection にインポートするには、Active Directory サーバのユーザ テンプレートを使用します。このユーザ テンプレートには、特定のユーザのグループに共通する設定が含まれています。ユーザ アカウントの作成時に、ユーザ テンプレートの共通設定がユーザに継承されます。ローカル タイム ゾーンの各サイトに個別のユーザ テンプレートを作成する必要があります。C：表 5-16 に、ユーザ テンプレートの設定を示します。

C：表 5-16　ボイスメール ユーザ テンプレート

セクション	フィールド	値
[基本設定（Basics）]	[エイリアス（Alias）]	SJC_User_Template
	[表示名（Display Name）]	SJC_User_Template
	[表示名の生成（Display Name Generation）]	[名、姓の順（First name, then last name）]
	[電話システム（Phone System）]	電話システム
	[サービスクラス（Class of Service）]	[ボイスメールユーザの COS（Voice Mail User COS）]
	[次回ログイン時に自己登録を設定する（Set for Self-enrollment at Next Login）]	オン
	[ディレクトリに登録（List in Directory）]	オン
	[タイムゾーン（Time Zone）]	[(GMT-08:00) アメリカ / ロサンゼルス ((GMT-8:00) America/Los_Angeles）]
	[言語（Language）]	[英語 (アメリカ合衆国) （English(United States)）]
	[社内電子メールアドレスから SMTP プロキシアドレスを生成（Generate SMTP Proxy Address from the Corporate Email Address）]	オン
[パスワード設定 - VM（Password Settings - VM）]	[次回サインイン時に、ユーザによる変更が必要（User Must Change at Next Sign-In）]	オン
	[期限切れなし（Does Not Expire）]	オン
	[認証規則（Authentication Rule）]	[ボイスメール認証規則 (推奨)（Recommended Voice Mail Authentication Rule）]
[パスワードの変更 - ボイスメール（Change Password-Voicemail）]	[PIN]	*<PIN>*

テンプレートに基づいて新規ユーザ設定を行うことで、個々のユーザ アカウントで変更する必要がある設定の数を最小限に抑えるとともにユーザ追加作業にかかる時間も短縮され、エラーが発生しにくくなります。

これ以降（テンプレートを使用してユーザ アカウントを作成した後）に行うすべてのユーザ テンプレート変更は、既存のユーザ アカウントには適用されません。つまり、共通設定はユーザ アカウント作成時点でのみテンプレートから取得されます。テンプレートを使用して Unity Connection アカウントを作成した後で、テンプレートまたは他のユーザに影響を及ぼさずに個々のユーザの設定を変更できます。

ここでは Web アプリケーション パスワードを変更しないでください。これは、Unity Connection は LDAP と統合されており、Active Directory からユーザが認証されるためです。これらの PIN とパスワードをユーザに指定する必要があります。これにより、ユーザは Unity Connection システム電話ユーザ インターフェイス（TUI）と Cisco Personal Communications Assistant（PCA）にサインインできます。

[ボイスメールユーザ COS サービスクラス（Voice Mail User COS class of Service）] 下の [Messaging Assistant の使用をユーザに許可する（Allow Users to Use the Messaging Assistant）] オプションと [Web Inbox と RSS フィードの使用をユーザに許可する（Allow Users to Use the Web Inbox and RSS Feeds）] オプションを選択して、ユーザが Cisco PCA を使用して Web Inbox にアクセスできるようにします。

前述の説明で作成したテンプレートを使用して LDAP からユーザをインポートします。

ユニティコネクションユーザー自己登録

エンドユーザを Unity Connection ユーザとして登録する必要があります。Unity Connection 管理者は各ユーザの ID（通常はユーザのデスク電話の内線番号）と一時 PIN（ユーザー プロビジョニングで設定）を指定する必要があります。初回登録ガイダンスは、あらかじめ録音された一連のプロンプトであり、ユーザはこのガイダンスに従って次のタスクを実行します。

- ユーザ名を録音します。
- ユーザが電話に応答しないときに外部発信者に対して再生されるグリーティングを録音します。
- ユーザ PIN を変更します。（ユーザの新しい PIN が PIN 同期を使用して Unified CM に伝播されます）。
- 電話帳に登録するかどうかを選択します（ユーザが電話帳に登録されていると、発信者はユーザの内線番号を知らない場合でも、ユーザの名前のスペルを言うか、ユーザ名を言うことでユーザに電話をかけられます。）

Unity Connection ユーザは組織内の IP エンドポイントまたは外部ネットワークから、自己登録プロセスのためにボイスメール パイロット番号をダイヤルできます。ユーザは、組織内または外部の不明な内線番号から Unity Connection に発信している場合、Unity Connection が自己登録プロセスを続行するよう応答したら、*（スターキー）を押す必要があります。登録が完了する前にユーザが通話を切断すると、次回ユーザが Unity Connection にサインインしたときに、初回登録ガイダンスが再び再生されます。

4. シングル インボックスの有効化

シングル インボックスは、Unity Connection のユニファイド メッセージング機能の 1 つであり、Unity Connection のボイス メッセージと Microsoft Exchange メールボックスを同期します。ユーザがシングル インボックスを使用可能な場合、ユーザに送信されるすべての Unity Connection ボイス メッセージ（Unity Connection ViewMail for Microsoft Outlook から送信されたメッセージを含む）は、最初に Unity Connection に保存され、直ちにユーザの Exchange メールボックスにレプリケートされます。このセクションでは、Unity Connection を Microsoft Exchange と統合してシングル インボックスを有効にするために必要な設定タスクについて説明します。

ユニティコネクションでのシングルインボックス有効化の前提条件

- シングル インボックス機能を有効にする前に、Microsoft Exchange が設定されており、ユーザが電子メールを送受信できることを確認してください。
- Unified Messaging サービス アカウント認証には Microsoft Active Directory が必要です。
- Unity Connection ユーザがインポートされ、基本ボイス メッセージング用に設定されます。ユーザー プロビジョニングを参照してください。

ユニティコネクション証明書管理

Cisco Unity Connection をインストールすると、Cisco PCA と Unity Connection 間の通信、および IMAP 電子メール クライアントと Unity Connection 間の通信を保護するため、ローカル自己署名証明書が自動的に作成およびインストールされます。つまり、Cisco PCA と Unity Connection 間でのすべてのネットワーク トラフィック（ユーザ名、パスワード、その他のテキスト データ、ボイス メッセージを含む）は自動的に暗号化され、IMAP クライアントで暗号化を有効化している場合には IMAP 電子メール クライアントと Unity Connection 間のネットワーク トラフィックは自動的に暗号化されます。

認証局（CA）から発行された証明書を使用することをお勧めします。この場合は、Unity Connection 自己署名 Tomcat 証明書が、エンタープライズ CA によって発行および署名されたマルチサーバ証明書に置き換えられます。このプロセスの詳細については、セキュリティーの章を参照してください。

ユニティコネクションの交換認証および SSL 設定の確認

Exchange サーバが適切な Web ベース認証モード（NT LAN Manager つまり NTLM を推奨）および Web ベースのプロトコル（HTTPS を推奨）で設定されていることを確認します。認証モードは、互いに通信する Exchange と Unity Connection の両方で一致する必要があります。

Exchange サーバと Active Directory ドメイン コントローラ用に外部 CA によって署名された証明書を検証するためのオプションを選択します。エンタープライズ CA ルート証明書を入手して、Exchange サーバとドメイン コントローラ サーバの両方にインストールします。

ユニティコネクションでの SMTP プロキシアドレスの設定

シングル ボックスを設定すると、Unity Connection は SMTP プロキシ アドレスを使用して、Unity Connection ViewMail for Microsoft Outlook から送信されたメッセージの送信者を適切な Unity Connection ユーザにマップし、受信者を Unity Connection ユーザにマップします。

たとえば、電子メール クライアントが電子メール アドレス aross@ent-pa.com を使用して Unity Connection にアクセスするように設定されているとします。このユーザが Outlook 向けの ViewMail でボイス メッセージを録音し、そのメッセージをユーザ ahall@ent-pa.com に送信します。Unity Connection は SMTP プロキシ アドレスのリストで aross@ent-pa.com と ahall@ent-pa.com を検索します。これらのアドレスがそれぞれ Unity Connection ユーザである ahall および aross の SMTP プロキシ アドレスとして定義されている場合、Unity Connection はメッセージを Unity Connection ユーザ aross からのボイス メッセージとして Unity Connection ユーザ ahall に送信します。

ユーザ テンプレートを使用してユーザをインポートする場合、ユーザの SMTP プロキシ アドレスが自動的に作成されます。ユーザ テンプレートでは、SMTP プロキシ アドレスを作成するために [社内電子メールアドレスから SMTP プロキシアドレスを生成（Generate SMTP Proxy Address from the Corporate Email Address）] オプションを選択します。詳細については、ユーザー プロビジョニングを参照してください。

アクティブ　ディレクトリー での統一されたメッセージングサービスアカウントの作成およびユニティコネクションの権限の付与

シングル インボックスを使用するには、Active Directory のアカウント（ユニファイド メッセージング サービス アカウント）が必要です。このアカウントには、Unity Connection がユーザの代わりに操作を実行するために必要な権限が付与されている必要があります。Unity Connection は ユニファイド メッセージング サービス アカウントを使用して Exchange メールボックスにアクセスします。ユニファイド メッセージング サービス アカウントを作成する際には、次のガイドラインに従ってください。

- アカウントには Exchange メールボックスを作成しません。
- 管理者グループにはアカウントを追加しません。
- アカウントを無効にしないでください。無効にすると、Unity Connection がアカウントを使用して Exchange メールボックスにアクセスできなくなります。

Exchange Management Shell がインストールされているサーバにサインインし、次のコマンドを使用して、[アプリケーション偽装管理（ApplicationImpersonation Management）] の役割を Unity Connection のユニファイド メッセージング サービス アカウントに割り当てます。

new-ManagementRoleAssignment -Name: *RoleName* **-Role:ApplicationImpersonation -User:'** *Account* **'**

ここで、

- *RoleName* は、割り当てるロールの名前です（Unity ConnectionUMServicesAcct など）。**get-ManagementRoleAssignment** コマンドを実行すると、RoleName に入力する名前が表示されます。
- *Account* は、domain\alias 形式のユニファイド メッセージング サービス アカウントの名前です。

SMTP スマート ホスト

Unity Connection は、SMTP スマート ホストを使用してメッセージをユーザの電子メール アドレスにリ レーします。Unity Connection ユーザが新しいメッセージを受け取ると、Unity Connection がテキスト形式の到着通知を電子メール アドレスに送信できますこのタイプの通知では、Cisco PCA へのリンクを電子メール メッセージの本文に組み込むように Unity Connection を設定できます。ユーザ設定で、ユーザの [通知デバイスの編集（Edit Notification Device）] ページに移動し、[メッセージテキストに Cisco Unity Connection Web Inbox へのリンクを含める（Include a Link to the Cisco Unity Connection Web Inbox in Message Text）] オプションを選択します。C：表 5-17 に、SMTP スマート ホストの設定を示します。

C：表 5-17　SMTP スマート ホストの詳細（[システム設定（System Settings）] > [SMTP の設定（SMTP Configuration）] > [スマートホスト（Smart Host）]）

パラメータ	値
SmartHost	US-EXCH1.ent-pa.com

ユニファイド メッセージング サービス

Cisco Unity Connection Administration で、[ユニファイドメッセージング（Unified Messaging）] を展開し、[ユニファイドメッセージングサービス（Unified Messaging Services）] を選択します。

- ユニファイド メッセージング サービスは、Unity Connection が Microsoft Exchange と通信するために使用する認証方式と Microsoft Exchange のタイプを定義します。
- FQDN を使用して特定の Exchange サーバと通信するようにユニファイド メッセージング サービスを設定します。
- Unity Connection ユニファイド メッセージング サービスを、Microsoft Exchange で設定されているものと同じ Web ベース認証モード（NTLM を推奨）および Web ベース プロトコル（HTTPS を推奨）で設定します。
- アクティブ　ディレクトリー での統一されたメッセージングサービスアカウントの作成およびユニティコネクションの権限の付与の項で作成した Active Directory アカウントのクレデンシャルを入力します。
- [Exchange の予定表および連絡先にアクセス（Access Exchange Calendar and Contacts）] オプションと [Connection と Exchange のメールボックスを同期する (シングル インボックス) （Synchronize Connection and Exchange Mailboxes (Single Inbox)）] オプションを選択し、ユニファイド メッセージング機能を有効にします。
- Exchange サーバ証明書がエンタープライズ CA によって署名されている場合は、Unity Connection が自動的に Exchange からの SSL 証明書を検証します。これは、エンタープライズ CA ルート証明書が信頼ストアにインストールされるためです。

ユニファイド メッセージング アカウント

Unity Connection Administration で、[ユーザ（Users）] を展開し、次に [ユーザ（Users）] を選択します。[ユーザの基本設定の編集（Edit User Basics）] ページの [編集（Edit）] メニューで、[ユニファイドメッセージングアカウント（Unified Messaging Accounts）] を選択します。

- ユーザ アカウントを作成する際、Unity Connection はそのユーザのユニファイド メッセージング アカウントを自動的には作成しません。ユニファイド メッセージング アカウントは、1 人のユーザまたは複数のユーザに対して作成できます。多数のユーザを対象にユニファイド メッセージング アカウントを作成するには、一括管理ツール（BAT）を使用します。
- ユニファイド メッセージングでは、各 Unity Connection ユーザの Exchange メール アドレスを入力する必要があります。[ユニファイドメッセージングアカウント（Unified Messaging Account）] ページで、[社内電子メールアドレスを使用 : 指定なし（Use Corporate Email Address: None Specified）] を選択します。これにより、Unity Connection は [ユーザの基本設定の編集（Edit User Basics）] ページで指定した社内電子メール アドレスを Exchange 電子メール アドレスとして使用します。
- Active Directory 統合では、Unified CM の [メール ID（Mail ID）] フィールドが、Active Directory のメール フィールドと同期されます。これにより、LDAP メール フィールドが Unity Connection の [社内電子メールアドレス（Corporate Email Address）] フィールドに表示されます。

一括管理ツールを使用して複数ユーザのユニファイド メッセージング アカウントを作成する方法については、次の場所にある『*System Administration Guide for Unity Connection*』の最新版を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

ボイスメールユーザーの COS

ユーザがシングル インボックスを使用できるようにするため、ボイスメール ユーザのサービス クラスを編集します（[サービスクラス（Class of Service）] –> [ボイスメールユーザの COS（Voice Mail User COS）] ）。[ライセンス済み機能（Licensed Features）] で [IMAP クライアントやシングルインボックスを使用したボイスメールへのアクセスをユーザに許可する（Allow Users to Access Voicemail Using an IMAP Client and/or Single Inbox）] オプションを選択します。また、[メッセージ本文へのアクセスを IMAP ユーザに許可する（Allow IMAP Users to Access Message Bodies）] オプションも選択します。

ユーザ ワークステーションへの Outlook 向けの ViewMail のインストール

Cisco ViewMail for Microsoft Outlook のビジュアル インターフェイスにより、ユーザは Outlook 内で各自の Unity Connection ボイス メッセージを送信、再生、管理できます。シスコの Web サイトから Unity Connection ViewMail for Microsoft Outlook をダウンロードして、各ユーザ ワークステーションにインストールします。ViewMail のインストールが完了したら、ViewMail の設定または [オプション（Options）] タブを開き、Unity Connection サーバに電子メール アカウントを関連付けます。ユーザ情報と Unity Connection サーバの詳細情報を入力します。

他の電子メール クライアントを使用して Exchange の Unity Connection ボイス メッセージにアクセスする場合、または Outlook 向けの ViewMail がインストールされていない場合は、次の点に注意してください。

- メール クライアントは、Unity Connection ボイス メッセージを .wav ファイルが添付された電子メールとして処理します。
- ユーザが Unity Connection ボイス メッセージに返信またはボイス メッセージを転送すると、ユーザが .wav ファイルを添付した場合でも、返答または転送は電子メールとして処理されます。メッセージ ルーティングは、Unity Connection ではなく Exchange によって処理されます。したがって、メッセージは受信者の Unity Connection メールボックスに送信されません。

5. ビジュアル ボイスメールの有効化

ビジュアル ボイスメールにより、Jabber クライアントのボイスメール タブから Unity Connection に直接アクセスできます。ユーザは Jabber からボイス メッセージのリストを確認し、メッセージを再生できます。ユーザは、ボイス メッセージを削除することもできます。

ユニティコネクションの設定

- Unity Connection ユーザがインポートされ、基本ボイス メッセージング向けに設定されていることを確認します。ユーザー プロビジョニングの項を参照してください。
- Unity Connection の **Connection Jetty** サービスと **Connection REST Service** が稼働していることを確認します。これらのサービスはいずれもサービスのアクティベーションで [オプションサービス（Optional Services）] の下でアクティブ化されます。
- IMAP クライアントからボイスメールにアクセスできるように、[サービスクラス（Class of Service）] が有効になっていることを確認してください。ボイスメールユーザーの COS の項を参照してください。
- Unity Connection ボイスメール サービス クラス（CoS）を編集し、ユーザが Web インボックスを使用できるようにします。[機能（Features）] タブで [Unified Personal Communicator を使用したボイスメールへのアクセスをユーザに許可する（Allow Users to Use Unified Client to Access Voicemail）] オプションを選択します。

- [API 設定（API settings）]（[システム設定（System Settings）] > [詳細設定（Advanced）]）で、次のオプションを選択します。
  - [Cisco Unity Connection Messaging Interface（CUMI）経由でセキュアなメッセージ録音へのアクセスを許可する（Allow Access to Secure Message Recordings through Cisco Unity Connection Messaging Interface (CUMI)）]
  - CUMI を介してセキュア メッセージのメッセージ ヘッダー情報を表示する（Display Message Header Information of Secure Messages through CUMI）
  - [CUMI 経由のメッセージ添付ファイルを許可する（Allow Message Attachments through CUMI）]

統一された CM の設定

各 Unity Connection サーバ ノードに**ボイスメール** UC サービスを追加します。C：表 5-18 に、ボイスメール UC サービスの設定を示します。

C：表 5-18　ボイスメール サービスの設定（[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [UC サービス（UC Service）]）

パラメータ	値	注
[製品のタイプ（Product Type）]	Unity Connection	ボイスメール システムの製品名を入力します。
[名前（Name）]	us-cuc1	ボイスメール サービスの名前を入力します。パブリッシャ ボイスメール サービスとサブスクライバ ボイスメール サービスを区別できる表示名を選択します。
[説明（Description）]	us-cuc1	パブリッシャ ボイスメール サービスとサブスクライバ ボイスメール サービスを区別できる表示名を入力します。
[ホスト名 /IP アドレス（Host Name/IP address）]	us-cuc1.ent.pa.com	ボイスメール サービスの FQDN を入力します。
ポート	443	ボイスメール サービスに接続するポートを入力します。
[プロトコル（Protocol）]	HTTPS	ボイス メッセージを安全にルーティングするためのプロトコルを選択します。

以前に作成した**ボイスメール** UC サービスを**標準**サービス プロファイル（[ユーザ管理（User Management）] –> [ユーザ設定（User Settings）] –> [サービスプロファイル（Service Profile）]）に適用します。Unity Connection パブリッシャ（us-cuc1.ent.pa.com）に対して作成したボイスメール UC サービスがプライマリ プロファイルに設定されており、Unity Connection サブスクライバ（us-cuc2.ent.pa.com）に対して作成したボイスメール UC サービスがセカンダリ プロファイルに設定されていることを確認してください。ボイスメール サービスのクレデンシャルを同期する場合は、[ボイスメールサービスのクレデンシャルソース（Credentials source for voicemail service）] ドロップダウン リストから [Unified CM - IM/Presence（Unified CM - IM and Presence）] を選択します。

6. SRST モードでのボイスメール

集中型メッセージング導入モデルでは、WAN の停止中にブランチ サイトの Survivable Remote Site Telephony（SRST）が無応答コールおよび話中コールを中央の Unity Connection にルーティングします。ビジー信号を受けた着信コール、無応答コール、およびメッセージ ボタンを押して開始されたコールは、Unity Connection に転送されます。この設定では、電話のメッセージ ボタンをアクティブなままにできます。この機能を有効にするには、PRI を介した Unity Connection への POTS ダイヤル ピア アクセスを設定します。

コールが PSTN 経由で Unity Connection にルーティングされる場合は、Redirected Dialed Number Information Service（RDNIS）が非常に重要です。RDNIS 情報が誤っている場合、PSTN 経由で再ルーティングされるボイスメールへのコールに影響が及ぶ可能性があります。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、代わりに自動受付のプロンプトを受信します。その場合、発信者は、到達先の内線番号を再入力するように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。

統一された CM の設定

C：表 5-19 で説明する設定が、中央サイトの PSTN ゲートウェイへの SIP トランクの Unified CM 設定で有効になっていることを確認します。

C：表 5-19　SRST モードでのボイスメール向け PSTN ゲートウェイへの SIP トランクの設定

パラメータ	値	注
[コールルーティング情報 - インバウンドコール（Call Routing Information - Inbound Calls）]		
[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）]	オン	リダイレクト情報要素、最初のリダイレクト番号、およびコール転送理由が着信メッセージの一部として送信され、受け入れられることを指定します。Unity Connection は最初のリダイレクト番号を使用してコールに応答します。
[コールルーティング情報 - アウトバウンドコール（Call Routing Information - Outbound Calls）]		
[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）]	オン	リダイレクト情報要素、最初のリダイレクト番号、およびコール転送理由が発信メッセージの一部として送信され、受け入れられることを指定します。Unity Connection は最初のリダイレクト番号を使用してコールに応答します。

ブランチ SRST ルータの設定

ブランチ サイトの SRST ルータで、PRI を介したボイスメール アクセスを有効にするため次のコマンドを設定します。

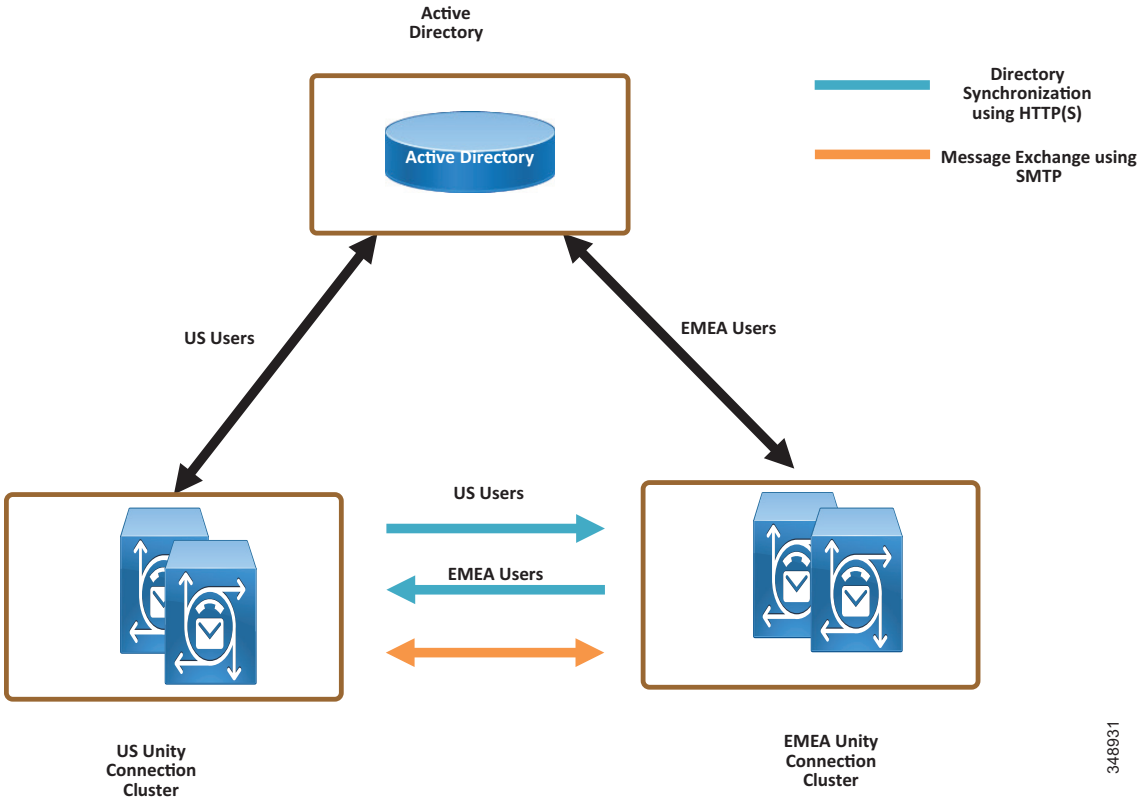
```
!
!
dial-peer voice 10 pots
destination-pattern +14085554999
direct-inward-dial
port 1/0:15
!
!
voice register pool 1
call-forward b2bua busy +14085554999
call-forward b2bua noan +14085554999 timeout 12
!
!
```

7. 2 つのユニティコネクションクラスタの HTTPS インターネットワーキング

C：図 5-4 に、2 つの Unity Connection クラスタの HTTPS インターネットワーキングを示します。HTTPS ネットワーキングにより複数の Unity Connection クラスタが接続されます。これにより、接続されたこれらのクラスタ間でディレクトリ情報を共有し、ボイス メッセージを交換できます。複数の Unity Connection サーバまたはクラスタを接続して、Unity Connection サイトと呼ばれる適切に接続されたネットワークを形成できます。サイトに接続するサーバは、*ロケーション*と呼ばれます。サイト内の各ロケーション間のディレクトリ情報の交換には HTTPS プロトコルが使用され、ボイス メッセージの交換には SMTP プロトコルが使用されます。

サイト内の Unity Connection ロケーションはディレクトリ情報を自動的に交換するため、受信側 / 送信先ユーザが発信側 / 送信元ユーザの検索範囲内で到達できる場合は、あるロケーションの受信側 / 送信先ユーザが別のシステムの発信側 / 送信元ユーザに対し、名前または内線番号を使用して発信するか、またはメッセージを送信できます。ネットワーク接続されたシステムは、1 つのディレクトリを共有しているかのように機能します。

C：図 5-4　　2 つの Unity Connection クラスタの HTTPS インターネットワーキング



HTTPS ネットワーキングでは、ハブアンドスポーク トポロジを使用して Unity Connection クラスタが相互に接続します。このトポロジでは、スポーク間のすべてのディレクトリ情報が、スポークに接続するハブを介して共有されます。HTTPS ネットワークで接続できる Unity Connection ロケーションの数と、HTTPS ネットワーキングの最大ユーザ数は、導入されている OVA テンプレートに応じて異なります。サポートされているロケーション最大数とディレクトリ最大サイズの詳細については、『*System Requirements for Cisco Unity Connection*』の最新版でディレクトリ オブジェクト制限に関する情報を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-guides-list.html

HTTPS ネットワーキングでは、ネットワーク内の各ロケーションで稼働しているリーダー サービスとフィーダー サービスによって、ディレクトリ レプリケーションが行われます。リーダー サービスは、リモート ロケーションを定期的にポーリングして、前回のポーリング間隔以降に行われたディレクトリ変更情報を収集します。フィーダー サービスは、変更トラッキング データベースを調べてディレクトリ変更が行われたかどうかを確認し、必要な情報を使用してポーリング要求に応答します。

HTTPS ネットワーキングでは、クラスタ ロケーションのパブリッシャ サーバが稼働している場合、このサーバがディレクトリ情報の同期化を行います。ただしパブリッシャ サーバがダウンしている場合は、サブスクライバ サーバがディレクトリ情報を同期します。

ディレクトリ同期が実行されるクラスタのサーバ（パブリッシャまたはサブスクライバ）に応じて、ディレクトリ同期は次のいずれかのタイプになります。

- [標準（Standard）] : ディレクトリ同期が、パブリッシャ サーバにより接続ロケーションとの間で実行されることを示します。
- [アラート（Alert）] : パブリッシャ サーバに接続できず、サブスクライバ サーバが接続ロケーションにディレクトリ情報を提供することを示します。ただし、サブスクライバ サーバに格納されているディレクトリ情報は、パブリッシャ サーバの稼働時にパブリッシャ サーバとの間で最後に同期されたディレクトリ情報です。

パブリッシャで障害が発生すると、ディレクトリ同期はアラート モードで実行されます。アラート モードでは、HTTPS ネットワーク上の接続ノードに対し、サブスクライバとのディレクトリ同期へのアクセスが制限されます。制限付きアクセスとは、接続ノードが、パブリッシャの稼働時にパブリッシャとの間で最後に同期されたディレクトリ情報のみを取得できることを意味します。パブリッシャが復旧すると、パブリッシャに直接接続しているノードはパブリッシャを介して最新のディレクトリ情報を同期します。したがって、アラート モードの主要なメリットとしては、パブリッシャがダウンした場合でも接続ノードが引き続きサブスクライバ サーバと同期する点が挙げられます。

相互にネットワーク接続されたクラスタには、TCP/IP ポート 25（SMTP）を介して直接アクセスできます。加えて、両方のロケーションはポート 8444 上で HTTPS を介して相互にルーティングできる必要があります。

展開の解説という本書の目的に沿って、米国と EMEA の Unity Connection クラスタ間で HTTPS インターネットワーキングが設定されると想定します。C：表 5-20 に、HTTPS ネットワークにより接続されるこの 2 つのクラスタのサーバ ノード情報を示します。

C：表 5-20　HTTPS ネットワークでの Unity Connection クラスタの詳細

	US Unity Connection クラスタ		EMEA Unity Connection クラスタ	
サーバ	**ホスト名**	**IP アドレス**	**ホスト名**	**IP アドレス**
パブリッシャ	US-CUC1	*<IP_Address_US_CUC1>*	EMEA-CUC1	*<IP_Address_EMEA_CUC1>*
サブスクライバ	US-CUC2	*<IP_Address_US_CUC2>*	EMEA-CUC2	*<IP_Address_EMEA_CUC2>*

2 つの Unity Connection クラスタ間で HTTPS ネットワーキングをセットアップするには、次のタスクを実行します。

各ユニティコネクションサーバの表示名および SMTP ドメインの確認

- HTTPS ネットワークに接続する Unity Connection サーバには、一意の表示名と SMTP ドメインが設定されている必要があります。
- HTTPS ネットワークを有効にする前に、[ネットワーク（Networking）] –> [ロケーション（Locations）] の設定で、Unity Connection パブリッシャ サーバの表示名と SMTP ドメインを確認します。

ユニティコネクションクラスタ間の HTTPS ネットワークの作成

- Unity Connection サーバの HTTPS ネットワークを作成するには、最初に HTTPS リンクを作成して 2 つのクラスタをリンクし、その後各クラスタのサブスクライバが SMTP アクセスのために追加されていることを確認します。
- 各 Unity Connection パブリッシャで、新しい HTTPS リンクを追加します。C：表 5-21 に、HTTPS リンクの設定を示します。

C：表 5-21　HTTPS リンクの設定（[ネットワーク（Networking）] > [HTTP(S) リンク（HTTP(s) Links）]）

パラメータ	値	注
[Cisco Unity Connection のリモートロケーションへのリンク（Link to Cisco Unity Connection Remote Location）]		
[パブリッシャ（IP アドレス /FQDN/ ホスト名）（Publisher (IP address/FQDN/ Hostname)）]	emea-cuc1.ent-pa.com	リモート Unity Connection パブリッシャ ノードの FQDN を入力します。
[ユーザ名（Username）]	管理ユーザの名前	上記のパブリッシャ フィールドに指定したロケーションの管理者のユーザ名を入力します。管理者のユーザ アカウントには、システム管理者ロールを割り当てておく必要があります。
[パスワード（Password）]	管理ユーザのパスワード	[ユーザ名（Username）] フィールドに指定された管理者のパスワードを入力します。
[転送プロトコル（Transfer Protocol）]		
[Secure Sockets Layer(SSL) を使用する（Use Secure Sockets Layer (SSL)）]	オン	このオプションは、さまざまな HTTPS ロケーション間のディレクトリ同期トラフィックを SSL により暗号化できるようにします。

クラスター　サブスクライバーサーバーの ＳＭＴＰ アクセスの設定

Unity Connection クラスタ サーバ ペアを含む HTTPS ネットワークでは、ペアのパブリッシャ サーバだけをネットワークに接続できます。クラスタのサブスクライバがプライマリ サーバである場合に、ネットワーク上のすべてのロケーションがクラスタ サブスクライバ サーバ ノードと直接通信できるようにするには、すべてのネットワーク ロケーションで、サブスクライバ サーバからの SMTP 接続を許可するように設定する必要があります。

この例では、EMEA サブスクライバを US パブリッシャの SMTP 設定に追加し、US サブスクライバを EMEA パブリッシャの SMTP 設定に追加します。

- US パブリッシャの US クラスタで、EMEA サブスクライバを SMTP 設定（[システム設定（System Settings）]）に追加します。[編集（Edit）] メニューで [IP アドレスアクセスリストの検索（Search IP Address Access List）] を選択します。[IP アドレスの新規作成（New IP Address）] ページで、EMEA サブスクライバ サーバの IP アドレス（*<IP_Address_EMEA_CUC2>*）を入力します。[接続を許可する（Allow Connection）] オプションが選択されていることを確認します。
- EMEA クラスタのパブリッシャ（emea-cuc1.ent-pa.com）で上記の手順を繰り返し、US クラスタ サブスクライバの IP アドレスを追加します。

ロケーション間でのレプリケーション

HTTPS ネットワークの作成後に、ネットワークに追加された 2 つのロケーション間でデータベース全体がレプリケートされることを確認します。初回のレプリケーションが開始されると、データが全ロケーション間で完全にレプリケートされるまでには、ディレクトリのサイズによって数分間から数時間かかることがあります。

前述のステップで作成した **HTTP（S）リンク**を開き、次の値を確認します。

- [前回の同期時刻（Time of Last Synchronization）]

  ローカルのリーダー サービスが前回、リモート ロケーションのフィーダー サービスにポーリングしてリモート ロケーションのディレクトリ変更の確認を試みた時刻（応答の有無にかかわらず）のタイムスタンプを示します。

- [前回のエラー時刻（Time of Last Failure）]

  ローカルのリーダー サービスが前回リモート ロケーションのフィーダー サービスのポーリングを試行中にエラーが発生した時点のタイムスタンプを示します。このフィールドの値が 0 の場合、または [前回の同期時刻（Time of Last Synchronization）] の値が [前回のエラーの時刻（Time of Last Error）] の値よりも遅い場合、レプリケーションは問題なく進行している可能性が高くなります。

- [オブジェクト数（Object Count）]

  ローカル Unity Connection ロケーションが同期したリモート ロケーションのユーザの数を示します。

ローカルユニティコネクション CSS へのリモートロケーションパーティションの追加

ロケーション間のネットワークを初めてセットアップする場合、US クラスタでプロビジョニングされたユーザは、EMEA クラスタのユーザにボイス メッセージを送信できません。これは、各ロケーションのユーザは個別のパーティションに属しており、個々のユーザ検索スペースには他のロケーションのユーザのパーティションが含まれていないためです。

- US Unity Connection サーバの us-cuc1 コーリング サーチ スペース（CSS）を編集して、EMEA ロケーションの Unity Connection サーバ パーティション emea-cuc1 を追加します。
- EMEA Unity Connection サーバの emea-cuc1 コーリング サーチ スペース（CSS）を編集して、US ロケーションの Unity Connection サーバ パーティション us-cuc1 を追加します。

関連資料

ボイス メッセージングと Cisco Unity Connection に関する追加情報については、下記リンクから入手可能な次のドキュメントの最新版を参照してください。

- 『*Cisco Collaboration System SRND*』の「*Voice Messaging*」の章

  https://www.cisco.com/go/srnd

- 『*Design Guide for Cisco Unity Connection*』

  https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-implementation-design-guides-list.html

- 『*HTTPS Networking Guide for Cisco Unity Connection*』

  https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

- 『*Unified Messaging Guide for Cisco Unity Connection*』

  https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html