

# Unified CM への Cisco VCS SIP トランク

## 導入ガイド

初版発行：2010年1月

最終更新：2015年11月

Cisco VCS X8.7

Unified CM 8.6.x、9.x、10.x、11.x

## はじめに

この導入ガイドでは、Cisco TelePresence Video Communication Server (VCS) バージョン X8.7 および Cisco Unified Communications Manager (Unified CM) バージョン 8.6.x および 9.x が SIP トランク経由でインターワークするように設定する方法のガイドラインを示します。

## 導入シナリオ

ある企業では、自社の Unified CM ですでに電話およびビデオ システムを実行しています。この企業は、Unified CM を、既存または新しいビデオ会議システムと接続された VCS Control に統合し、音声端末やビデオ端末が 1 つの統合ネットワーク全体で相互に通信できるような環境を求めています。

既存の電話システムは、電話（デジタル専用）番号を使用してコール先を指定しています。この機能がビデオ システムに拡張されれば、すべてのエンドポイントは電話番号でアクセスできるようになります。



このシナリオでは、Unified CM に接続されているエンドポイントは 3xxx の内線番号で識別され、VCS Control に接続されているエンドポイントは 4xxx の内線番号で識別されます（英数字を含む、より複雑なダイヤル プランもサポートできることに注意してください。その場合は、追加のトランスフォーム/ルーティングの設定が必要です）。

Unified CM および VCS Control は、SIP トランクを介して IP ネットワーク全体で相互に接続されます。VCS Control ドメインは vcs.domain です。Unified CM に送信されたコールは、ドメイン部分が VCS ドメインに設定されます。Unified CM から VCS へのコールは、TCP の場合は <FQDN of VCS>:5060、TLS の場合は、<FQDN of VCS>:5061 のように設定されたドメイン部分とともに着信します。

VCS Control はバージョン X7 以降のコードを実行しており、次のオプション キーがインストールされていることを前提としています。

- トラバーサル コール
- 非トラバーサル コール

## 設定プロセスの要約

このマニュアルでは、Unified CM および VCS Control の両方を設定し、次のコールを発信する方法を示します。

- VCS に接続されたビデオ エンドポイントから、同じ VCS に接続された他のビデオ エンドポイントへのコール
- Unified CM に接続された IP ハンドセットまたは他のデバイスから、同じ Unified CM に接続された他の IP ハンドセットまたはデバイスへのコール
- VCS に接続されたビデオ エンドポイントから、Unified CM に接続された IP ハンドセットまたは他のデバイスへのコール
- Unified CM に接続された IP ハンドセットまたは他のデバイスから、VCS に接続されたビデオ エンドポイントへのコール

この設定プロセスでは、これらの各段階について個別に説明します。そのため、段階ごとに実装でき、次に移行する前にテストできます。

最初に、トラブルシューティングが簡単になるため、この設定では非セキュア TCP 接続を使用します。次に、TLS でのセキュアなビデオ ネットワークを確立する方法について説明します。

## システム設定の前提条件

このマニュアルを使用して VCS Control と Unified CM がインターワークするように設定する前に、次のことを確認してください。

- Unified CM に基本設定が含まれており、少なくとも次がすでに設定されていること。
  - [システム (System) ] > [サーバ (Server) ]
  - [システム (System) ] > [Cisco Unified CM]
  - [システム (System) ] > [Cisco Unified CM グループ (Cisco Unified CM Group) ]
  - [システム (System) ] > [日時グループ (Date/Time Group) ]
  - [システム (System) ] > [プレゼンス グループ (Presence Group) ]
  - [システム (System) ] > [リージョン情報 (Region Information) ]
  - [システム (System) ] > [デバイス プール (Device Pool) ]
  - [システム (System) ] > [DHCP]
  - [システム (System) ] > [ロケーション (Location) ]
  - [システム (System) ] > [物理ロケーション (Physical location) ]
  - [システム (System) ] > [エンタープライズ パラメータ (Enterprise parameters) ]
  - [システム (System) ] > [ライセンス (Licensing) ]

- VCS Control は IP アドレス、DNS、および NTP 情報を使用して設定されている必要があり、それにより Web インターフェイス経由で管理するためのアクセスが可能となります（『[VCS Basic Configuration \(Single VCS Control\) Deployment Guide](#)』を参照してください）。

## VCS Control に登録されたエンドポイント間のコールの有効化

### VCS Control の設定

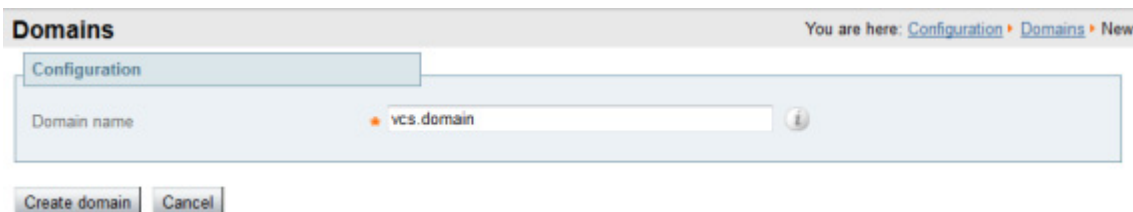
VCS Control に登録されたデバイス間で、コールを発信できるように設定するには、次の手順に従います。

- VCS Control の SIP ドメインを設定します。この設定は、SIP の登録に必要です。
- ドメインを含まない着信番号に確実にドメイン情報が追加されるようにトランスフォームを作成します。これにより、SIP および H.323 エンドポイントからの着信番号情報を強制的に共通の形式である `number@domain` にします。

### VCS Control の SIP ドメインの設定

SIP エンドポイントは、`4_digit_number@vcs.domain` の形式で AOR (Address Of Record) を使用して VCS に登録されます。VCS は、これらの登録を受け入れるように、SIP ドメイン情報を使用して設定される必要があります。

1. [設定 (Configuration)] > [ドメイン (Domains)] に移動します。
2. [新規 (New)] をクリックします。
3. `vcs.domain` など、[ドメイン名 (Domain name)] にドメイン名を入力します。
4. [ドメインの作成 (Create domain)] をクリックします。



### トランスフォームの作成

この導入シナリオでは、ユーザは内線番号 `4xxx` を使用して VCS に登録された他のエンドポイントにダイヤルできるようにする必要があります。Unified CM エンドポイントは `3xxx` の番号を使用してダイヤルできます。このダイヤル モデルは H.323 によってサポートできますが（エンドポイントが 4 桁の番号 E.164 エイリアスを登録する場合）、SIP では番号のみでのダイヤルはサポートされません。番号（ドメインが付加されていないもの）が SIP エンドポイントからダイヤルされる場合、そのエンドポイントのドメインが自動的に付加されます。

SIP および H.323 のダイヤルの整合性を保つため、この導入シナリオでは、コールのルーティングに常に URI フォームを使用します（`dialed_digits@domain` のフォーム）。VCS がコール要求を受信するとき、着信番号は次のようになります。

- ルーティングするための特定のエンドポイントを指定する 4 桁の番内線番号を含み、
- ドメインが含まれる場合と含まれない場合があります（SIP エンドポイントがコールを発信するときのみ含まれます）。

そのため、確実に着信番号を一貫した形式に変換するために、トランスフォームが必要です。この場合、必要であれば、ドメイン (vcs.domain) を追加します。これを実現するには、次のような正規表現を使用します。([<sup>^</sup>@]<sup>\*</sup>) を \<sup>1</sup>@vcs.domain に変換します（ドメインを含まないダイヤル情報は「@」を含まないので、@vcs.domain を追加します）。

詳細については、『[VCS Administrator Guide](#)』の付録の「Regular Expression Reference」の項を参照するか、または「Regular Expression（正規表現）」という用語をインターネットで検索してください。

トランスフォームを作成する手順は、次のとおりです。

1. [設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [トランスフォーム (Transforms)] に移動します。
2. [新規 (New)] をクリックします。
3. フィールドを次のように設定します。

プライオリティ (Priority)	2
説明 (Description)	たとえば「ドメインが設定されていない場所にドメインを追加」
パターンタイプ (Pattern type)	Regex
パターン文字列 (Pattern string)	([ <sup>^</sup> @] <sup>*</sup> )
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	\ <sup>1</sup> @vcs.domain
状態 (State)	有効 (Enabled)

4. [トランスフォームの作成 (Create transform)] をクリックします。

The screenshot shows the 'Create transform' configuration page. The breadcrumb trail at the top reads: 'You are here: Configuration > Dial plan > Transforms > Create transform'. The configuration fields are as follows:

- Priority: 2
- Description: Add domain where none exists
- Pattern type: Regex
- Pattern string: ([<sup>^</sup>@]<sup>\*</sup>)
- Pattern behavior: Replace
- Replace string: \<sup>1</sup>@vcs.domain
- State: Enabled

At the bottom of the form, there are 'Create transform' and 'Cancel' buttons.

## Unified CMの設定

VCS にローカルで登録されたエンドポイント間でコールをルーティングするために、VCS 対応の Unified CM で設定を行う必要はありません。

## VCS Control へのエンドポイントの登録

### エンドポイントの設定

H.323 の場合、エンドポイントを次のように設定します。

- H.323 ID (たとえば、4000@vcs.domain、4001@vcs.domain など)
- H.323 コール セットアップ = ゲートキーパー
- ゲートキーパー IP アドレス = VCS の IP アドレス

SIP の場合、エンドポイントを次のように設定します。

- SIP アドレス (URI) (たとえば 4000@vcs.domain、4001@vcs.domain など)
- サーバアドレス (プロキシ アドレス) = VCS の IP アドレス

### 登録の確認

登録ステータスは、Cisco VCS Control で [ステータス (Status)] > [登録 (Registrations)] に移動して確認できます。

デフォルトでは、VCS は指定した SIP ドメイン内のすべての H.323 登録とすべての SIP 登録を受け入れます。個別の登録を明示的に許可または拒否することで、登録を制限できます。詳細については、『*VCS Administrator Guide*』の「VCS Configuration」を参照してください。

### テスト コール

いくつかのテスト コールを発信します。

通話履歴は VCS で [ステータス (Status)] > [コール (Calls)] > [履歴 (History)] に移動して確認できます。

## Unified CM に登録されたエンドポイント間のコールの有効化

### VCS Control の設定

Unified CM にローカルで登録されたエンドポイント間でコールをルーティングするために、Unified CM 対応の VCS で設定を行う必要はありません。

## Unified CMの設定

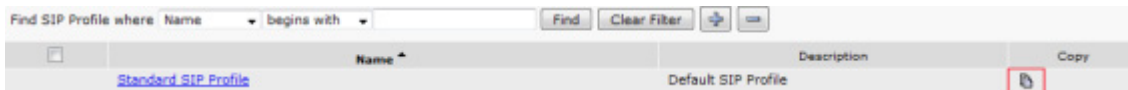
電話間でのコールの発信を有効にするための Unified CM およびシスコの電話の設定には、SIP プロファイルの設定、Unified CM での電話の指定、電話への電話番号の設定、および電話での設定のロードがあります。これは次の手順で実行します。

- VCS 用の SIP プロファイルを設定します（バージョン 9.x を使用している場合は、すでに SIP プロファイルは存在します）。
- ビデオ コールに適切なセッション ビット レートを使用してリージョンを設定
- 電話デバイス用の SIP プロファイルを設定
- 電話デバイスを追加： Unified CM でサポートされるエンドポイントのリストに新しい電話デバイスを追加します。
- デバイスの電話番号を設定：この電話の呼び出し音が鳴る電話番号を指定します。
- Unified CM からの設定を取得する電話エンドポイントを設定します。

## VCS 用の SIP プロファイルの設定

**注：**新しいバージョンには「Cisco VCS 用の標準の SIP プロファイル」があるため、この手順は Unified CM バージョン 9.x 以降には適用されません。

1. Unified CM で、[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [SIP プロファイル (SIP Profile)] に移動します。
2. [標準 SIP プロファイル (Standard SIP Profile)] に対して [コピー (Copy)] をクリックします。



3. 次のようにフィールドを設定します（他のフィールドはデフォルト値のままにします）

名前 (Name)	Standard SIP Profile For Cisco VCS
デフォルト MTP テレフォニー イベント ペイロード タイプ (Default MTP Telephony Event Payload Type)	101
アプリケーションによるリダイレクト (Redirect by Application)	チェックボックスをオンにする
SIP 要求で完全修飾ドメインを使用 (Use Fully Qualified Domain in SIP Requests)	チェックボックスをオンにする
BFCP を使用するプレゼンテーション共有を許可 (Allow Presentation Sharing using BFCP)	チェックボックスをオンにする (Unified CM 8.6.1 以降)
インバイトのタイムアウト値 (Timer Invite Expires)	180
レジスタの再送間隔の調整値 (Timer Register Delta)	5
レジスタのタイムアウト値 (Timer Register Expires)	3600
タイマー T1 (Timer T1)	500

タイマー T2 (Timer T2)	デフォルトのままにする (通常 4000 または 5000)
インバイトの再試行値 (Retry INVITE)	6
非インバイトの再試行値 (Retry non-INVITE)	10
開始メディアポート (Start Media Port)	16384
終了メディアポート (Stop Media Port)	32766
コールピックアップ URI (Call Pickup URI)	x-cisco-serviceuri-pickup
コールピックアップグループ別 URI (Call Pickup Group Other URI)	x-cisco-serviceuri-opickup
コールピックアップグループ URI (Call Pickup Group URI)	x-cisco-serviceuri-gpickup
ミーティングサービス URI (Meet Me Service URI)	x-cisco-serviceuri-meetme
キープアライブのタイムアウト値 (Timer Keep Alive Expires)	120
サブスクリプションのタイムアウト値 (Timer Subscribe Expires)	120
サブスクリプションの再送間隔の調整値 (Timer Subscribe Delta)	5
最大リダイレクト (Maximum Redirections)	70
オフフックから最初の数字タイマー (Off Hook To First Digit Timer)	15000
コール転送 URI (Call Forward URI)	x-cisco-serviceuri-cfwdall
短縮ダイヤル URI (Abbreviated Dial URI)	x-cisco-serviceuri-abbrdial
着信要求を新規トランクへと再ルーティングする基準 (Reroute Incoming Request to new Trunk based on)	なし (Never)

4. [保存 (Save)] をクリックします。

## ビデオ コールに適切なセッション ビット レートを使用したリージョンの設定

リージョンにビデオ コールに適切なセッション ビット レートが設定されていることを次の手順で確認します。

1. [システム (System)] > [リージョン情報 (Region Information)] > [リージョン (Region)] に移動します。
2. リージョンを選択します (たとえば、[デフォルト (Default)] リージョン)。
3. システムに適した上限に、[ビデオコールの最大セッション ビット レート (Maximum Session Bit Rate for Video Calls)] を設定します (6000 kbps など)。
4. [保存 (Save)] をクリックして、[設定を適用 (Apply Config)] をクリックします。

## 電話デバイス用の SIP プロファイルの設定

ここでは、すべての電話デバイスに適用される SIP プロファイルを作成します。

1. Unified CM で、[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [SIP プロファイル (SIP Profile)] に移動します。
2. [標準 SIP プロファイル (Standard SIP Profile)] に対して [コピー (Copy)] をクリックします。



3. 次のフィールドを設定します。他のすべてのフィールドをデフォルト値のままにします。

名前 (Name)	電話デバイス用の標準 SIP プロファイル
SIP 要求で完全修飾ドメインを使用 (Use Fully Qualified Domain in SIP Requests)	チェックボックスをオンにする
BFCP を使用するプレゼンテーション共有を許可 (Allow Presentation Sharing using BFCP)	BFCP (デュアル ビデオ/プレゼンテーションの共有) が必要な場合は、チェックボックスをオンにします。

4. [保存 (Save)] をクリックします。

## 電話デバイスの追加

1. [デバイス (Device)] > [電話 (Phone)] の順に移動します。
2. [新規追加 (Add New)] をクリックします。
3. [電話デバイス用の標準 SIP プロファイル (Standard SIP Profile - for phone devices)] の [SIP プロファイル (SIP Profile)] を選択します。
4. 必要に応じて、他のフィールドを設定します。
5. [保存 (Save)] をクリックし、[OK] をクリックします。
6. [設定を適用 (Apply Config)] をクリックし、[OK] をクリックします。

または、別の電話機がすでに設定されている場合、[スーパーコピー (Super Copy)] を選択し、新しい電話機の MAC アドレスを入力し、説明を変更 (特に説明の MAC アドレス部分を修正) することで、電話機の設定をコピーします。

## デバイスの電話番号の設定

1. [デバイス (Device)] > [電話 (Phone)] の順に移動します。
2. 関連するデバイス名を選択します。
3. 左側から回線を選択します。
4. 必要な電話番号を設定します (この例では 3xxx 番号を使用)。

## Unified CM からの設定を取得する電話エンドポイントの設定

### Cisco Phones

1. 設定ボタンを押します。
2. [ネットワークの設定 (Network Configuration)] セクションを選択し、[TFTP サーバ (TFTP Server)] が Unified CM の IP アドレスであるかどうかを確認します。設定されていない場合は、次の操作を実行します。
  1. 設定ボタンを 2 回押し、設定メニューに戻ります。

- 2.[ロック解除 (Unlock) ]を選択し、適切なパスワードを入力します。
- 3.[ネットワークの設定 (Network Configuration) ]セクションを選択します。
- 4.[代替 TFTP (Alternate TFTP) ] = [はい (YES) ] に設定します。
- 5.[TFTP サーバ (TFTP Server) ] = <IP address of Unified CM> に設定します。
- 6.[許可 (Accept) ]を選択します。
- 7.[保存 (Save) ]を選択します。

電話は、回線 1 が Unified CM で指定した電話番号であることを示します (たとえば 3001) 。

### TE6 ソフトウェアを使用する EX60/EX90

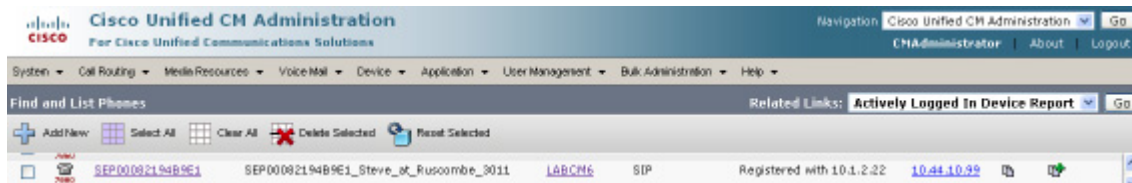
関連するプロビジョニングの詳細を入力します。

- Cisco UCM の [プロビジョニング モード (Provisioning Mode) ]を選択します。
- [プロビジョニング マネージャのアドレス (Address of the provisioning manager) ]を入力します。

これで、Unified CM に登録されたハンドセット間でコールを発信することができます。

## 登録の確認

Unified CM に接続された電話の登録ステータスは、[デバイス (Device) ] > [電話 (Phone) ] ページで表示できます。



## テスト コール

登録された電話の番号 (たとえば 3001) をダイヤルし、テスト コールを何度か発信します。

## Unified CM に登録されたエンドポイントにコールするための VCS に登録されたエンドポイントの有効化

### Unified CMの設定

Unified CM に登録されたデバイス間で、コールを発信できるように設定するには、次の 3 段階の手順に従います。

- SIP トランク セキュリティ プロファイルを設定
- SIP トランク デバイスを設定

- クラスタの完全修飾ドメイン名を設定

## SIP トランク セキュリティ プロファイルの設定

1. [システム (System)] > [セキュリティ (Security)] > [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。
2. (バージョン 9.x より前) [新規追加 (Add New)] をクリックし、新しいプロファイルに名前を付けます。
3. (9.x 以降) [非セキュアな SIP トランク プロファイル (Non Secure SIP Trunk Profile)] を選択します。
4. フィールドを次のように設定します。

名前 (Name)	非セキュア SIP トランクプロファイル (Non Secure SIP Trunk Profile)
デバイスセキュリティモード (Device Security Mode)	非セキュア (Non Secure)
着信転送タイプ (Incoming Transport Type)	TCP+UDP
発信転送タイプ (Outgoing Transport Type)	TCP
着信ポート (Incoming Port)	5060
Unsolicited NOTIFYの許可 (Accept unsolicited notification)	チェックボックスをオンにする
Replacesヘッダーの許可 (Accept replaces header)	チェックボックスをオンにする

5. [保存 (Save)] をクリックします。

## SIP トランク デバイスの設定

1. Unified CM で、[デバイス (Device)] > [トランク (Trunk)] に移動します。
2. [新規追加 (Add New)] をクリックします。
3. [トランク タイプ (Trunk Type)] に [SIP トランク (SIP Trunk)] を選択します。
  - [デバイス プロトコル (Device Protocol)] に [SIP] が表示されます。
  - [トランク サービス タイプ (Trunk Service Type)] の指定を求められた場合、[なし (デフォルト) (None (Default))] を選択します。
4. [次へ (Next)] をクリックします。
5. [デバイス情報 (Device Information)] フィールドを次のように設定します。

デバイス名 (Device Name)	必要に応じて、VCS_system など
デバイスプール (Device Pool)	([システム (System) ] > [デバイス プール (Device Pool) ] で設定したとおり)
コールの分類 (Call Classification)	OnNet
参照先 (Location)	([システム (System) ] > [ロケーション (Location) ] で設定したとおり)
パケット キャプチャ モード (Packet Capture Mode)	なし
メディア ターミネーション ポイントが必須 (Media Termination Point Required)	Unified CM に登録された任意のビデオ電話が、VCS に登録されたエンドポイントとの間でのビデオ コールを発信または着信する場合、このチェックボックスをオフにします。 音声デバイスのみが Unified CM に登録されている場合、このチェックボックスをオンにします。
SRTP を許可 (SRTP Allowed)	このチェックボックスをオンにします。背景については、『 <a href="#">Secure RTP between CUCM and VCS or Expressway Configuration Example</a> 』をご覧ください。
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)	チェックボックスをオンにする


6. [コール ルーティング情報 (Call Routing Information) ] > [着信コール (Inbound Calls) ] フィールドを次のように設定します。

有意な数字 (Significant digits)	すべて (All)
接続側回線 ID の表示 (Connected Line ID Presentation)	デフォルト (Default)
接続先名の表示 (Connected Name Presentation)	デフォルト (Default)
コーリングサーチスペース (Calling Search Space)	([コール ルーティング (Call Routing) ] > [コントロールのクラス (Class of Control) ] > [コーリング サーチ スペース (Calling Search Space) ] で設定したとおり)
プレフィックス DN (Prefix DN)	<空白>
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)	チェックボックスをオンにする

7. [コール ルーティング情報 (Call Routing Information) ] > [発信コール (Outbound Calls) ] フィールドを次のように設定します。

発呼者の選択 (Calling Party Selection)	発信元 (Originator)
発呼者回線 ID の表示 (Calling Line ID Presentation)	デフォルト (Default)
発呼者名の表示 (Calling Name Presentation)	デフォルト (Default)
発信者 ID DN (Caller ID DN)	<空白>
発信者名 (Caller Name)	<空白>

8. [SIP 情報 (SIP Information)] フィールドを次のように設定します。

接続先アドレスは SRV (Destination address is an SRV)	接続先アドレスに対してドメインが指定されている場合、このチェックボックスをオンにします。そうすることで、DNS サーバは DNS SRV レコードを使用して、ドメインを VCS のクラスタに転送します。  IP アドレスが [宛先アドレス (Destination address)] として指定されている場合は、このチェックボックスをオンにしないでください。
接続先アドレス (Destination address)	<FQDN of VCS / VCS cluster>。または、<IP address of VCS> を入力できます。SRV レコードを使用しておらず、複数のピアを指定する必要がある場合は、さらに [宛先アドレス (Destination address)] 行を追加するために  をクリックします。  「 <a href="#">Unified CM が提供するドメイン情報を VCS SIP ドメインに変換するためのトランスフォームの作成 [p.19]</a> 」で設定される VCS トランスフォームの内容は、ここで入力したアドレスの形式によって異なります。
接続先ポート (Destination port)	5060 (SRV レコードを使用する場合は、ゼロが表示されます)
プレゼンス グループ (Presence Group)	標準プレゼンス グループ (または [システム (System)] > [プレゼンス グループ (Presence Group)] で設定されたプレゼンス グループのいずれか)
SIP トランクセキュリティプロファイル (SIP Trunk Security Profile)	非セキュア SIP トランクプロファイル (Non Secure SIP Trunk Profile)
SIP プロファイル (SIP Profile)	Cisco VCS 用の標準 SIP プロファイル
DTMF シグナリング方式 (DTMF Signaling Method)	RFC 2833
正規化スクリプト (Normalization Script)	vcs-interop (使用可能な場合)

9. [保存 (Save)] をクリックします。

10. [Reset] をクリックします。

11. [Reset] をクリックします。

## クラスタの完全修飾ドメイン名を設定

<address>@domain 形式のアドレスへのコールを受信できるように、Unified CM を、[クラスタの完全修飾ドメイン名 (Cluster Fully Qualified Domain Name)] で設定する必要があります (これは、Unified CM がクラスタ化されるときも必要とされ、それにより、VCS が任意の Unified CM ノードにコールを送信できるようになります)。

1. [システム (System)] > [エンタープライズ パラメータ (Enterprise parameters)] に移動し、[クラスタ全体のドメイン設定 (Clusterwide Domain Configuration)] セクションを見つけます。
2. [クラスタの完全修飾ドメイン名 (Cluster Fully Qualified Domain Name)] を、vcs.domain などのビデオ ネットワークと同じドメインに設定します。

このパラメータに、このクラスタの 1 つまたは複数の完全修飾ドメイン名 (FQDN) を定義します。複数の FQDN はスペースで区切る必要があります。ホスト部分がこのパラメータの FQDN と一致する URL を含む要求 (たとえば、SIP コール) は、このクラスタまたはこのクラスタに接続されたデバイスあるいはその両方に対する要求として認識されます。

3. [保存 (Save)] をクリックします。

Clusterwide Domain Configuration	
Organization Top Level Domain	
Cluster Fully Qualified Domain Name	vcs.domain

## VCS Control の設定

VCS Control の設定は、次の 3 段階の手順に従います。

- Unified CM を含むネイバー ゾーンを設定
- 該当ゾーンにコールをルーティングするように検索ルールを設定
- number@<IP address of cucm> を number@vcs.domain に変換するトランスフォームを設定

## Unified CM 用のネイバー ゾーンを作成

1. [設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] へ移動します。
2. [新規 (New)] をクリックします。
3. 次のようにフィールドを設定します (他のすべてのフィールドはデフォルト値のままにします)。

名前 (Name)	CUCM ネイバー
タイプ (Type)	ネイバー (Neighbor)
ホップ数 (Hop count)	15
H.323 モード (H.323 Mode)	オフ (Off) (H.323 は VCS と Unified CM 間ではサポートされません)

SIP モード (SIP mode)	オン
SIP ポート (SIP port)	TCP の場合は 5060、または TLS の場合は 5061 (SIP トランクで設定されたポートと一致している必要があります)
トランスポート (Transport)	TCP または TLS トランスポートと暗号化メディアを保護する場合は、[TLS] を選択します
プロキシ経由の登録を許可 (Accept proxied registrations)	拒否 (Deny)
メディア暗号化モード (Media encryption mode)	Auto
SIP 認証信頼モード (SIP authentication trust mode)	オフ (Off)
ピア 1 アドレス (Peer 1 address)	Unified CM の IP アドレス、または Unified CM の FQDN。 最終的に TLS 接続を使用する場合、Unified CM によって提示される証明書を認証するために使用される名前であるため、通常は、Unified CM の FQDN をここで指定する必要があります。
ゾーン プロファイル (Zone profile) ([詳細設定 (Advanced)] セクション)	<p>これは、次のように Unified CM のバージョンにより異なります。</p> <ul style="list-style-type: none"> <li>8.6.1 より前のバージョンでは、[Cisco Unified Communications Manager] を選択します。</li> <li>8.6.1 または 8.6.2 では、[Cisco Unified Communications Manager (8.6.1 以降) (Cisco Unified Communications Manager (8.6.1 or later))] を選択します。</li> <li>9.x 以降では [カスタム (Custom)] を選択し、次の手順を実行します。                     <ul style="list-style-type: none"> <li>[コール シグナリングルーテッド モード (Call signaling routed mode)] を [常時 (Always)] に設定します。</li> <li>すべての他のフィールドをデフォルト値のままにします。</li> </ul> </li> </ul> <p>Unified CM 8.6.1 以降が BFCP (デュアル ビデオ/プレゼンテーションの共有) に必要であることに注意してください。</p>

ここでは、Unified CM との通信に TCP 経由で SIP を使用するように VCS を設定します。TLS を使用するには、ここで説明するように TCP 用の設定を完了してから、「[TLS を使用した Unified CM への VCS の接続 \[p.23\]](#)」を参照してください。

4. [ゾーンの作成 (Create zone)] をクリックします。

### Edit zone

Type Neighbor

Hop count  ⓘ

---

**H.323**

Mode  ⓘ

---

**SIP**

Mode  ⓘ

Port  ⓘ

Transport  ⓘ

Accept proxied registrations  ⓘ

Media encryption mode  ⓘ

ICE support  ⓘ

---

**Authentication**

Authentication policy  ⓘ

SIP authentication trust mode  ⓘ

---

**Location**

Peer 1 address  ⓘ

Peer 2 address  ⓘ

Peer 3 address  ⓘ

Peer 4 address  ⓘ

Peer 5 address  ⓘ

Peer 6 address  ⓘ

---

**Advanced**

Zone profile  ⓘ

Monitor peer status  ⓘ

Call signaling routed mode  ⓘ

## Unified CM ネイバーゾーンへコールをルーティングするための検索ルールの作成

検索ルールで、このネイバー Unified CM によって処理されるように電話番号および URI の範囲が指定されます。ネイバーへの送信前に、URI をトランスフォームするために使用することもできます。



この導入例では、「[VCS Control に登録されたエンドポイント間のコールの有効化 \[p.4\]](#)」で設定されたトランスフォームによって、ダイヤル文字列は必ず URI 形式の `number@vcs.domain` になります。

1. [設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [検索ルール (Search rules)] に移動します。
2. [新規 (New)] をクリックします。
3. コールを Unified CM にルーティングするように、次のようにフィールドを設定します。

ルール名 (Rule name)	CUCM へのルート
説明 (Description)	たとえば、「3xxx@vcs.doman コールを CUCM に送信」
プライオリティ (Priority)	100
プロトコル (Protocol)	任意 (Any)
ソース (Source)	任意 (Any)
リクエストは認証される必要がある (Request must be authenticated)	認証ポリシーに従ってこの設定を指定する
モード (Mode)	エイリアスのパターン マッチ (Alias pattern match)
パターンタイプ (Pattern type)	Regex
パターン文字列 (Pattern string)	<code>(3\d{3})@vcs.domain(.*)</code>
パターン動作 (Pattern behavior)	変更なし (Leave)  ([クラスタの完全修飾ドメイン名 (Cluster Fully Qualified Domain Name)] エンタープライズ パラメータによって、形式化された @domain アドレスは Unified CM で動作します)
正常に一致する場合 (On successful match)	停止 (Stop)
転送先ゾーン (Target zone)	CUCM ネイバー
状態 (State)	有効 (Enabled)

4. [検索ルールの作成 (Create search rule)] をクリックします。

詳細については、『[VCS Administrator Guide](#)』の「Zones and Neighbors」の項を参照してください。

## number@<IP address of cucm> を number@vcs.domain に変換するトランスフォームの作成

Unified CM から VCS へコールが発信される時、コールバック アドレスが `number@<IP address of cucm>` として示されます。VCS に登録済みのエンドポイントがコールを返す場合は、VCS が Unified CM に、そのコールをルーティングして返すことができなければなりません。そのためには、アドレスのドメイン部分の IP アドレスを削除し、ビデオ ドメインを追加する必要があります (それにより、既存の検索ルールが Unified CM にコールをルーティングできます)。トランスフォーメーションが必要な場合：

1. [設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [トランスフォーム (Transforms)] に移動します。
2. [新規 (New)] をクリックします。
3. フィールドを次のように設定します。

プライオリティ (Priority)	3
説明 (Description)	たとえば「ドメインへの CUCM IP」
パターンタイプ (Pattern type)	Regex
パターン文字列 (Pattern string)	(.*)@<ip address of Unified CM>(: ;).*? Unified CM クラスタの使用中に、regex (正規表現) は、使用するすべてのノードの IP アドレスに対応する必要があります (たとえば、(.*) @ (10\.1\.2\.22 10\.1\.2\.23) (: ;) .*? など)。
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	\1@vcs.domain\2
状態 (State)	有効 (Enabled)

4. [トランスフォームの作成 (Create transform)] をクリックします。

The screenshot shows the 'Create transform' configuration page. The breadcrumb trail at the top reads: 'You are here: Configuration > Dial plan > Transforms > Create transform'. The configuration fields are as follows:

- Priority: 3
- Description: CUCM IP to domain
- Pattern type: Regex
- Pattern string: (.\*)@<ip address of CUCM>(:|;).\*?
- Pattern behavior: Replace
- Replace string: \1@vcs.domain\2
- State: Enabled

At the bottom of the form, there are 'Create transform' and 'Cancel' buttons.

## テスト コール

必要な Unified CM 内線番号 (3xxx) を VCS エンドポイントでダイヤルすることで、VCS Control に登録されたエンドポイントから、Unified CM に登録されたエンドポイントにテスト コールを発信します。

## Unified CM に登録されたエンドポイントにコールするための VCS に登録されたエンドポイントの有効化

### VCS Control の設定

#### Unified CM が提供するドメイン情報を VCS SIP ドメインに変換するためのトランスフォームの作成

このトランスフォームは Unified CM から受信した URI を VCS のローカルゾーンで使用する形式に変換し、ネイバーゾーン内で想定される形式に一致させます。

Unified CM から受信した URI のドメイン部分は、それ自体の SIP トランク設定により異なります（「[SIP トランク デバイスの設定 \[p.11\]](#)」を参照してください。そのため、これは VCS の IP address:port、または VCS か VCS クラスタの FQDN になります。

この例では、`4xxx@vcs-name.vcs.domain:<port>` の形式で Unified CM から受信した URI にマッチングし、それを `4xxx@vcs.domain` に変換します。

1. [設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [トランスフォーム (Transforms)] に移動します。
2. [新規 (New)] をクリックします。
3. フィールドを次のように設定します。

説明 (Description)	Unified CM が提供するドメイン情報を VCS SIP ドメインに変換
プライオリティ (Priority)	5 などの高いプライオリティを指定します（このトランスフォームのプライオリティは、ローカルおよびネイバーゾーンの検索に適用されるすべてのトランスフォームの前である必要があります）。
パターンタイプ (Pattern type)	Regex
パターン文字列 (Pattern string)	例: <code>(4\d{3})@vcs-name.vcs.domain(:.*)?</code>
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	例: <code>\1@vcs.domain</code>
状態 (State)	有効 (Enabled)

4. [トランスフォームの作成 (Create transform)] をクリックします。

**Create transform** You are here: [Configuration](#) > [Dial plan](#) > [Transforms](#) > Create transform

**Configuration**

Priority: 5

Description: Convert Unified CM supplied domain information to the VCS SIP domain

Pattern type: Regex

Pattern string: \*(4d(3))@vcs-name.vcs.domain.\*?

Pattern behavior: Replace

Replace string: 1@vcs.domain

State: Enabled

Buttons: Create transform, Cancel

## Unified CMの設定

### Cisco 電話から VCS の番号へのダイヤルの許可

Unified CM はプレフィックスを取得し、特定のプレフィックスに基づいてコールを SIP トランクにルーティングするように設定できます。VCS へ 4xxx としてダイヤルされたコールをルーティングするように Unified CM を次の手順で設定します。

1. Unified CM で、[コールルーティング (Call Routing)] > [ルート/ハント (Route/Hunt)] > [ルートパターン (Route Pattern)] に移動します。
2. [新規追加 (Add New)] をクリックします。
3. 4xxx にダイヤルされたコールを (着信番号を変更せずに) VCS トランクにルーティングするようにルートパターンを設定します。

#### パターン定義 (Pattern Definitions)

ルートパターン (Route Pattern)	4XXX
ルートパターン (Route Pattern)	([システム (System)] > [デバイス プール (Device Pool)] で設定したとおり)
説明 (Description)	必要に応じる (たとえば 4 xxx から VCS SIP トランクへのルーティング)
ゲートウェイ/ルートリスト (Gateway/Route List)	VCS Control へのコールのルーティングのために必要なトランク
コールの分類 (Call Classification)	OnNet
外部ダイヤルトーンの提供 (Provide Outside Dial Tone)	オフ
<b>着信側トランスフォーメーション (Called Party Transformations)</b>	
番号の削除 (Discard Digits)	< なし > (< None >)

**Pattern Definition**

Route Pattern\* 4XXX

Route Partition LABCM6

Description Route 4xxx to VCS SIPtrunk

Numbering Plan -- Not Selected --

Route Filter < None >

MLPP Precedence\* Default

Gateway/Route List\* VCS\_system (Edit)

Route Option

Route this pattern

Block this pattern No Error

Call Classification\* OnNet

Allow Device Override  Provide Outside Dial Tone  Allow Overlap Sending  Urgent Priority

Require Forced Authorization Code

Authorization Level\* 0

Require Client Matter Code

---

**Calling Party Transformations**

Use Calling Party's External Phone Number Mask

Calling Party Transform Mask

Prefix Digits (Outgoing Calls)

Calling Line ID Presentation\* Default

Calling Name Presentation\* Default

---

**Connected Party Transformations**

Connected Line ID Presentation\* Default

Connected Name Presentation\* Default

---

**Called Party Transformations**

Discard Digits < None >

## Cisco 電話から VCS ドメインへのダイヤルの許可

ドメイン exp.domain など、VCS SIP トランクに送信するために必要な情報を Unified CM に提供するように SIP ルートパターンを設定します。この設定は、ドメインがある SIP URI をサポートするエンドポイントからのダイヤルを許可し、特定のシグナリングに対する VCS へのリバースパスを有効にするために必要です。

1. Unified CM で [コール ルーティング (Call Routing)] > [SIP ルート パターン (SIP Route Pattern)] に移動します。
2. [新規追加 (Add New)] をクリックします。
3. フィールドを次のように設定します。

パターンの使い方 (Pattern Usage)	ドメインルーティング (Domain Routing)
IPv4 パターン (IPv4 Pattern)	コールのドメイン (たとえば vcs.domain)
ルートパターン (Route Pattern)	デフォルトは [< なし > (< None >)] (ダイヤル プラン制限に応じて設定)
SIP トランク (SIP TRUNK)	VCS Control へのコールのルーティングのために必要なトランク

4. [保存 (Save)] をクリックします。

Pattern Definition	
Pattern Usage	Domain Routing
IPv4 Pattern*	vcs.domain
IPv6 Pattern	
Description	VCS system domain
Route Partition	LABCM6
SIP Trunk/Route List*	VCS_system <a href="#">(Edit)</a>
<input type="checkbox"/> Block Pattern	

Calling Party Transformations	
<input type="checkbox"/> Use Calling Party's External Phone Mask	
Calling Party Transformation Mask	
Prefix Digits (Outgoing Calls)	
Calling Line ID Presentation*	Default
Calling Line Name Presentation*	Default

Connected Party Transformations	
Connected Line ID Presentation*	Default
Connected Line Name Presentation*	Default

Unified CM に登録されたエンドポイントが nnnn@vcs.domain にダイヤルするときは、Unified CM が、nnnn@<FQDN of VCS>:5060 (TCP) または nnnn@<FQDN of VCS>:5061 (TLS) のように、VCS へコールをルーティングします (ドメインは、SIP トランクの [宛先ドレス (Destination Address)] として何が設定されるかによって、代替的に VCS の IP アドレスになる場合があります)。

これで、Unified CM から、4xxx@vcs.domain として登録された VCS のエンドポイントに対してコールを発信することができます。

## テスト コール

Unified CM に登録されたエンドポイントから VCS Control に登録されたエンドポイントへテスト コールを発信します。

## TLS を使用した Unified CM への VCS の接続

この手順では、VCS と Unified CM との間で TCP 相互接続を使用して、すでに設定され動作しているシステムを把握し、TCP の代わりに TLS を使用するようにその接続を変換する方法を説明します。このプロセスには、次の作業が必要です。

- Unified CM と VCS 間の信頼証明書を確認
- Unified CM のクラスタ セキュリティ モードを 1 に設定（混合モード）
- Unified CM で SIP トランク セキュリティ プロファイルを設定
- TLS を使用するように Unified CM トランクを VCS へ更新
- TLS を使用するように VCS のネイバー ゾーンを Unified CM へ更新

### Unified CM と VCS 間の信頼証明書を確認

Unified CM と VCS で TLS 相互接続を確立するために、次を考慮します。

- +VCS と Unified CM の両方で、ロードされた有効なサーバ証明書が必要です（VCS のデフォルトのサーバ証明書を有効なサーバ証明書に置き換える必要があります）。
- VCS は Unified CM のサーバ証明書を信頼する必要があります（Unified CM サーバ証明書のルート CA を VCS にロードする必要があります）。
- Unified CM は、VCS のサーバ証明書を信頼する必要があります（VCS サーバ証明書のルート CA を Unified CM にロードする必要があります）。

証明書のロード、および認証局（CA）から証明書を取得するために VCS で CSR を生成する手順の詳細については、『[Expressway Certificate Creation and Use Deployment Guide](#)』を参照してください。

**注：**クラスタ化された環境では、個別のピア/ノードそれぞれに CA 証明書とサーバ証明書をインストールする必要があります。

実稼働環境で自己署名証明書を使用しないことを強く推奨します。

### VCS にサーバ証明書と信頼証明書をロード

#### VCS サーバ証明書

VCS では、サーバ証明書は 1 つだけです。デフォルトでは、このサーバ証明書は一時的な認証局によって署名された証明書です。この証明書を信頼できる認証局が生成した証明書に置き換えることを推奨します。

サーバ証明書をアップロードするには、次の手順を実行します。

1. [メンテナンス (Maintenance)] > [セキュリティ証明書 (Security certificates)] > [サーバ証明書 (Server certificate)] へ移動します。

2. [新規証明書のアップロード (Upload new certificate)] セクションの [参照 (Browse)] ボタンを使用して、サーバ証明書の PEM ファイルを選択しアップロードします。
3. 証明書署名要求 (CSR) を生成するために外部システムを使用する場合、サーバ証明書を暗号化するために使用された **サーバ秘密キー** の PEM ファイルもアップロードする必要があります (VCS を使用して、このサーバ証明書用の CSR が作成された場合、秘密キー ファイルは、前もって自動的に生成および保存されます)。
  - **サーバ秘密キー** の PEM ファイルをパスワードで保護する必要はありません。
  - 証明書署名要求の進行中は、サーバ秘密キーをアップロードできません。
4. [サーバ証明書データをアップロード (Upload server certificate data)] をクリックします。

**注:** Unified CM バージョン 8.5(1) 以前を使用しており、VCS と Unified CM との間の TLS 接続の確立に問題がある場合は、次の x509 拡張キー属性を CSR に追加することをお勧めします。

- serverAuth (1.3.6.1.5.5.7.3.1) -- TLS Web サーバ認証
- clientAuth (1.3.6.1.5.5.7.3.2) -- TLS Web クライアント認証
- ipsecEndSystem (1.3.6.1.5.5.7.3.5) -- IP セキュリティ エンド システム

### VCS の信頼できる CA 証明書

[信頼できる CA 証明書 (Trusted CA certificate)] ページ ([メンテナンス (Maintenance)] > [セキュリティ証明書 (Security certificates)] > [信頼できる CA 証明書 (Trusted CA certificate)]) で、この VCS が信頼する認証局 (CA) の証明書のリストを管理できます。VCS への TLS 接続で証明書検証が必須の場合、VCS に示される証明書は、このリスト内の信頼できる CA によって署名され、ルート CA への完全な信頼チェーン (中間 CA) が存在する必要があります。

Unified CM サーバ証明書のルート CA を VCS の信頼できる CA 証明書のリストにロードする必要があります。

1 つまたは複数の CA 証明書を含む新しいファイルをアップロードするには、必須の PEM ファイルを参照するために [参照 (Browse)] をクリックし、[追加できる CA 証明書 (Append CA certificate)] をクリックします。この手順によって、CA 証明書の既存のリストに新しい証明書を追加します。特定の発行者およびサブジェクトの既存の証明書を交換する場合は、手動で以前の証明書を削除する必要があります。

この Unified CM と通信するすべての VCS で、このプロセスを繰り返します。

## Unified CM にサーバ証明書と信頼証明書をロード

Unified CM のための証明書管理を、[Cisco Unified OS 管理 (Cisco Unified OS Administration)] アプリケーションで実行します。

すべての既存の証明書は、[セキュリティ (Security)] > [証明書管理 (Certificate Management)] で一覧表示されます。サーバ証明書のタイプは *certs* であり、信頼できる CA 証明書のタイプは *trust-certs* です。



## Unified CM サーバ証明書

デフォルトでは、Unified CM に自己署名サーバ証明書 **CallManager.pem** がインストールされます。この証明書を信頼できる認証局から生成された証明書に置き換えることを推奨します。

## Unified CM の信頼できる CA 証明書

(まだロードされていない場合) VCS の証明書を発行した機関のルート CA 証明書をロードするには、次の手順を実行します。

1. [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate chain)] をクリックします。
2. [CallManager-trust] の [証明書名 (Certificate Name)] を選択します。
3. [参照 (Browse)] をクリックし、VCS 証明書を発行した機関のルート CA 証明書を含むファイルを選択します。
4. [ファイルのアップロード (Upload File)] をクリックします。

VCS と通信するすべての Unified CM サーバで、このプロセスを繰り返します。これは、通常、CallManager サービスを実行しているすべてのノードです。

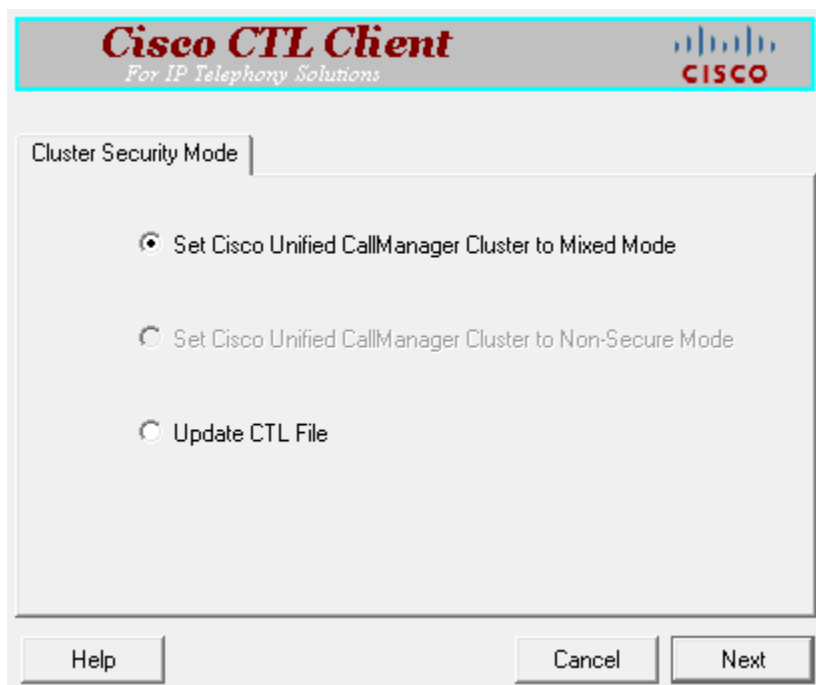
## クラスタ セキュリティ モードを混合モードに設定

セキュア デバイスと非セキュア デバイスを両方登録できるようにするには、Cisco Unified Communications Manager のクラスタを混合モードにする必要があります。これにより、VCS と Cisco Unified Communications Manager 間のベスト エフォートの暗号化が可能になります。VCS と Unified CM の間のベスト エフォートの暗号化の背景については、『[Secure RTP between CUCM and VCS or Expressway Configuration Example](#)』をご覧ください。

バージョン 10.0 では、CLI を使用してクラスタのセキュリティ モードを変更できます。それより前のバージョンでは、クラスタ セキュリティ モードを変更するには、Cisco CTL クライアント プラグインを使用する必要があります。セキュリティ モードを変更すると CTL ファイルが更新されるため、変更後に Cisco CallManager と Cisco TFTP サービスを再起動する必要があります。

プロセスを以下に要約しますが、お使いのバージョンの『[Cisco Unified Communications Manager Security Guide](#)』（「[Cisco Unified Communications Manager \(CallManager\) Maintain and Operate Guides](#)」ページ）を参照してください。

1. ハードウェアのセキュリティ トークンなど、Unified CM パブリッシャ ノードへのアクセス権を取得します (CTL クライアント プラグインを使用している場合)。
2. (10.0 より前) Unified CM から Cisco CTL クライアント プラグインをダウンロードしてインストールします。
3. 混合モードをイネーブルにするには、CTL クライアント プラグインを実行します。10.0 以降では、CLI で `utils ctl set-cluster mixed-mode` を使用できます。



4. CTL ファイルを更新します（プラグインまたは `utils ctl update CTLFile` を使用）。
5. Cisco CallManager と Cisco TFTP サービスを再起動します（Cisco Unified Serviceability を使用して）。

## Unified CM での SIP トランク セキュリティ プロファイルの設定

Unified CM で、次の手順を実行します。

1. [Cisco Unified CM の管理 (Cisco Unified CM Administration)] を選択し、[移動 (Go)] をクリックしてログインします。
2. [システム (System)] > [セキュリティ (Security)] > [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。
3. [新規追加 (Add New)] をクリックします。
4. フィールドを次のように設定します。

名前 (Name)	これが暗号化されたプロファイルであることを示す名前。
説明 (Description)	必要に応じて説明テキストを入力します。
デバイスセキュリティモード (Device Security Mode)	暗号化 (Encrypted)。
着信転送タイプ (Incoming Transport Type)	TLS

発信転送タイプ (Outgoing Transport Type)	TLS
ダイジェスト認証を有効化 (Enable Digest Authentication)	オフのままにします。
X.509 のサブジェクト名 (X.509 Subject Name)	VCS の証明書内で VCS が提供するサブジェクト名またはサブジェクトの代替名を指定します。VCS クラスターでは、すべてのピアの証明書に含まれるすべての名前が、このリストに含まれることを確認します。複数の X.509 名を指定するには、スペース、カンマ、セミコロン、またはコロンでそれぞれの名前を区切ります。
着信ポート (Incoming Port)	5061
Unsolicited NOTIFYの許可 (Accept unsolicited notification)	チェックボックスをオンにする
Replacesヘッダーの許可 (Accept replaces header)	チェックボックスをオンにする
その他のパラメータ	その他すべてのパラメータをオフのままにします。

5. [保存 (Save)] をクリックします。

## TLS を使用するように Unified CM トランクを VCS へ更新

Unified CM で、次の手順を実行します。

1. [デバイス (Device)] > [トランク (Trunk)] に移動します。
2. [検索 (Find)] を使用し、前の手順で VCS へのトランクに設定したデバイス名を選択します。
3. 次のフィールドを設定します。

[SIP 情報 (SIP Information)] セクション

接続先ポート (Destination Port)	5061 (DNS SRV を使用しない場合、つまり SRV レコードが正しく設定されていることが確認できる場合)。  Unified CM のバージョンによっては TLS SRV ルックアップを実施できないことに注意してください。詳細については、「 <a href="#">Unified CM が SRV トランクの宛先を使用する際の TLS コールのエラー [p.35]</a> 」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 (SIP Trunk Security Profile)	上記で設定したトランク プロファイルを選択します。

その他のパラメータは、前の手順で設定したままにします。

4. [保存 (Save)] をクリックします。
5. [Reset] をクリックします。

## TLS を使用するように VCS のネイバーゾーンを Unified CM へ更新

TCP を使用して Unified CM と通信中でも、Unified CM ゾーンがアクティブであることを VCS がレポートすることに注意してください。次の変更は、TLS 経由の通信を有効にするために必要です。

VCS で次の手順を実行します。

1. [設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] へ移動し、Unified CM へのゾーンを選択します。
2. 次のフィールドを設定します。

[SIP] セクション	
ポート (Port)	5061
トランスポート (Transport)	TLS
TLS 検証モード (TLS verify mode)	オン
SIP 認証信頼モード (Authentication trust mode)	オフ (Off)

その他のパラメータは、前の手順で設定したままにします。

3. [保存 (Save)] をクリックします。

## TLS 接続が動作可能であることの確認

TLS の適切な動作を確認するには、VCS ゾーンレポートのステータスがアクティブであることを確認し、テストコールを何回か発信します。

1. 次のように、VCS ゾーンがアクティブであることを確認します。
  - 1.[設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] に移動します。
  - 2.ゾーンの [SIP ステータス (SIP status)] を確認します。

ゾーンがアクティブでない場合、再度、Unified CM でトランクをリセットまたは再起動してください。
2. VCS に登録されたエンドポイントから Unified CM 電話に対してテストコールを発信します。
3. Unified CM 電話から VCS に登録されたエンドポイントに対してテストコールを発信します。

## VCS のネットワーク

この Unified CM に対する VCS ネイバーの背後に VCS のネットワークがある場合、次のいずれかを行います。

- Unified CM はネットワーク（「最適な」ルーティング モード）上のすべての VCS の証明書を信頼する必要があります。または、
- Unified CM への VCS のネイバー ゾーンはシグナリングを「常に」ルーティングする必要があります。実際には、この手順では Unified CM へのゲートウェイとして、この VCS を設定します。そして、これは推奨されるオプションです。*Cisco Unified Communications Manager* と *Cisco Unified Communications Manager (8.6.1 以降)* のゾーンのプロファイルがシグナリングを「常に」ルーティングするように事前設定されるため、使用されるゾーン プロファイルの 1 つを提供する追加の設定は必要ありません。

## Unified CM に登録されたエンドポイントへの暗号化されたコール

Unified CM に登録されたエンドポイントは、「SIP セキュア プロファイル」を使用して、暗号化されたメディアおよびコール ネゴシエーションを提供するように設定される必要があります。このようなプロファイルがデフォルトでは使用できない場合、[システム (System)] > [セキュリティ (Security)] > [電話セキュリティ (Phone Security)] から作成する必要があります。

Cisco CTL クライアントの使用とセキュアな通信のための Unified CM の設定の詳細については、『[Securing Cisco TelePresence Products](#)』を参照してください。

## Unified CM メッセージ サイズ制限の確認

ビデオ用の SIP メッセージは、音声コール用の SIP メッセージより非常に大きく、特に、Cisco TelePresence サーバがビデオ ネットワークで使用されるときに非常に大きくなります。

Unified CM での [SIP 最大着信メッセージのサイズ (SIP Max Incoming Message Size)] が 11000 に設定されていることを、次の手順で確認します。

1. [システム (System)] > [サービス パラメータ (Service Parameters)] に移動します。
2. 該当するサーバを選択します。
3. サービスとして [Cisco CallManager (アクティブ) (Cisco CallManager (Active))] を選択します。
4. [詳細設定 (Advanced)] をクリックします。
5. [クラスタワイド パラメータ (デバイス - SIP) (Clusterwide Parameters (Device - SIP))] で、次のようにフィールドを設定します。

**SIP 最大着信メッセージ サイズ (SIP Max Incoming Message Size)**

| 11000

6. [保存 (Save)] をクリックします。

The screenshot shows the Cisco Unified CM Administration interface. The page title is "Service Parameter Configuration". The navigation menu includes "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", and "Bulk Administration". The "SIP Max. Incoming Message Size" parameter is highlighted with a red box. The table below shows the configuration for various SIP parameters.

Parameter Name	Current Value	Default Value
SIP Station UDP Port Throttle Threshold	50	50
SIP Trunk UDP Port Throttle Threshold	200	200
SIP V.150 Outbound SDP Offer Filter	No Filtering	No Filtering
<b>SIP Max. Incoming Message Size</b>	<b>11000</b>	<b>11000</b>
SIP Max. Incoming Message Headers	100	100
Send SIP Multicast TTL in SDP	False	False
Default Publish Expiration Timer	3600	3600
Minimum PUBLISH Expiration Timer	60	60

## 付録 1：トラブルシューティング

### VCS Control のローカル コールの接続問題

#### [検索履歴 (Search history) ] での適用されているトランスフォームの確認

H323 の SETUP/ARQ /LRQ から、または SIP の INVITE/OPTIONS から開始された任意の検索に、検索履歴エントリが報告されます。

1. [ステータス (Status) ] > [検索履歴 (Search history) ] に移動します。  
サマリーに、発信元および宛先コールのエイリアスと、宛先エイリアスが検出されたかどうかが表示されます。
2. 関連する検索の試行を選択します。

検索の試行の検索履歴に、次の内容が表示されます。

- 着信コールの詳細
- 管理者ポリシーかユーザ ポリシー、または CPL によって適用されるトランスフォーム
- 次にに関して報告される、トランスフォームされた必要な宛先と一致する優先順位でのゾーン
  - ゾーンが適用される可能性があるトランスフォーム
  - 見つかったか見つからないかのステータス
  - 見つからなかった場合、ゾーンの検索応答に表示されるものと同様のエラー コード
  - コールを受け入れ可能なゾーンが見つかるまで、またはゾーンの照合がすべて試行されるまで繰り返される（検索は帯域幅の不足、ゾーンからの検索が H.323 の拒否理由になった、または SIP 要求に対する応答が 2xx でないために、「見つからない」ステータスになることがある）

検索に次のように示される場合

- 検出：False (Found: False)
- 理由：480 一時的に使用できません (Reason: 480 Temporarily Not Available)

VCS のゾーン リンクが正しくセットアップされていない可能性があります。コマンドラインから、VCS のデフォルト ゾーンに必要なリンクを設定するために `xcommand DefaultLinksAdd` を実行し、また、作成された他のゾーンのリンクを確認します。

各 H.323 コールにつき、検索履歴に 2 つのエントリがあることに注意してください。

- 最初は ARQ のエントリであり、エンドポイントが見つかったかどうかを示します。
- 2 番目は、実際にコールをルーティングするセットアップのエントリです。

ARQ 検索はリンクまたはリンク帯域幅に依存せず、リンクが存在しない、またはリンク帯域幅が十分ではない場合、後続のセットアップ検索が失敗しても通過することがあります。

各 SIP コールには、通常 SIP INVITE の 1 つの検索履歴のみがあります。

## [通話履歴 (Call History)] を確認し、コールの進行状態を調べる

1. [ステータス (Status)] > [コール (Calls)] > [履歴 (History)] に移動します。

サマリーでは、送信元コールのエイリアスと宛先コールのエイリアス、通話時間、およびプロトコルを示します (すべての相互運用を含みます)。

2. 次に関連するコール試行および関連するコールのコンポーネントを選択します。

これは着信コールと発信コール レッグの詳細およびゾーン ルーティングとサブゾーン ルーティングを示します。

## エラーの確認

Web ブラウザから [ステータス (Status)] > [ログ (Logs)] > [イベント ログ (Event Log)] に移動してアクセスできるイベント ログを確認します。

## コールのトレース

### VCS の SIP/H.323 レベルでのコールのトレース

1. [メンテナンス (Maintenance)] > [診断 (Diagnostics)] > [診断ログ (Diagnostics logging)] に移動します。
2. オプションで、[ロギング中に tcpdump を採取 (Take tcpdump while logging)] を選択します。
3. [新規ログを開始 (Start new log)] をクリックします。
4. (任意) マーカー テキストを入力して、[マーカーを追加 (Add marker)] をクリックします。
  - 特定のアクティビティが実行される前に、マーカー機能を使用して、ログ ファイルにコメント テキストを追加できます。これは、ダウンロードされた診断ログ ファイルで関連するセクションを後で識別するのに役立ちます。
  - 診断ログの進行中に、必要なだけマーカーを追加できます。
  - マーカー テキストは「`DEBUG_MARKER`」タグと一緒にログに追加されます。
5. 診断ログでトレースするシステムの問題を再現します。
6. [ログの停止 (Stop Logging)] をクリックします。
7. [ログのダウンロード (Download log)] をクリックして、ローカル ファイル システムに診断ログ アーカイブを保存します。アーカイブを保存するように要求されます (実際の表現は、ブラウザによって異なります)。

## Cisco TelePresence Server とのコールの失敗

Cisco TelePresence Server からの SIP メッセージは、(Unified CM で設定される [SIP 最大着信メッセージ サイズ (SIP Max Incoming Message Size)] のデフォルトである) 5,000 バイトより大きいことがあります。



[SIP 最大着信メッセージ サイズ (SIP Max Incoming Message Size) ]を増やします。「[Unified CM メッセージ サイズ制限の確認 \[p.29\]](#)」を参照してください。

## In-Call の問題

### Unified CM のビデオ電話から VCS にコールが転送されるときに、コールが消去される

メディア ターミネーション ポイント (MTP) の使用が、Unified CM と VCS 間の SIP トランクで要求されない場合でも、DTMF シグナリング方式が Unified CM の SIP トランクで [初期設定なし (No preference) ]として設定されている場合、Unified CM はメディア転送ポイント (Media Transfer Point) の使用を試行し、コールは失敗します。

これを解決するために、Unified CM から VCS への SIP トランクで、DTMF シグナリング方式が Unified CM の RFC 2833 として設定されていることを確認します。

### Multiway を使用した Unified CM エンドポイントの会議への参加の失敗

「[付録 5 : Multiway および Unified CM \[p.43\]](#)」に従ってネットワークがセットアップされていることを確認します。

### Unified CM からの粗悪なビデオ品質

「[ビデオ コール用の適切なセッション ビット レートを使用してリージョンを設定 \[p.8\]](#)」に従って、Unified CM リージョンで、ビデオ コールに適切なセッション ビット レートが設定されていることを確認します。

## RTMT を使用した Unified CM でのトレースの取得

RTMT はシステムの状態の監視や、Unified CM からのグラフの表示とログの収集を行うために使用できるツールです。

Windows と Linux の両方のバージョンが用意されています。Unified CM はトレース対象を指定するように構成される必要があります。

### トレースを有効にするための Unified CM の設定

1. Cisco Unified CM にログインします。
2. [ナビゲーション (Navigation) ] ドロップダウンで、[Cisco Unified Serviceability] を選択し、[移動 (Go) ] をクリックします。
3. [トレース (Trace) ] > [トレースの設定のトラブルシューティング (Troubleshooting Trace Settings) ] の [トレースの設定のトラブルシューティング (Troubleshooting Trace Settings) ] ページに移動します。
4. [すべてのサービスの確認 (Check All Services) ] チェックボックスをオンにします。
5. [保存 (Save) ] をクリックします。

## RTMT (Real Time Monitoring Tool) のインストール

1. Linux または Windows PC を使用して Unified CM にログインします。
2. [アプリケーション (Application)] > [プラグイン (Plugins)] に移動します。
3. 「空白で始まる名前 (Name begins with <blank>)」 と 「インストールと同じプラグイン タイプ (Plugin Type equals Installation)」 を入力し、[検索 (Find)] を選択します。
4. 必要に応じて [Cisco Unified CM Real-Time Monitoring Tool - Linux] または [Cisco Unified CM Real-Time Monitoring Tool - Windows] のエントリにスクロールします。
5. [ダウンロード (Download)] リンクをクリックします。
6. ダウンロードされたら、ダウンロードされたインストール ファイルを実行します。
7. インストール ウィザードの指示に従います。
8. 完了したら、[完了 (Done)] をクリックして、インストーラを終了します。

## RTMT の実行

1. RTMT を実行します。(たとえば、Windows では、[スタート (Start)] > [すべてのプログラム (All Programs)] > [Cisco] > [CallManager Serviceability] > [Real-Time Monitoring Tool] にあります。)
2. [ログイン (Login)] ウィンドウで [ホスト IP アドレス (Host IP Address)]、[ユーザ名 (User Name)]、および [パスワード (Password)] を入力します。
3. [OK] をクリックします。

## RTMT を使用したトレースの取得

1. [トレース & ログ セントラル (Trace & Log Central)] を選択します。
2. [リアル タイム トレース (Real Time Trace)] をダブルクリックします。
3. [リアル タイム データを表示 (View Real Time Data)] をダブルクリックします。
4. トレースを取得する Unified CM インスタンスが実行されているノードを選択します。
5. [次へ (Next)] をクリックします。
6. 次のことを選択します。
  - [製品 (Products)] = [UCM]
  - [サービス (Services)] = [Cisco CallManager]
  - [トレース ファイル タイプ (Trace File Type)] = [sdi]
7. [完了 (Finish)] をクリックします。

(注)

- ログのダウンロードには時間がかかる場合があります。
- sdi (System Diagnostic Interface) トレースにはアラーム、エラー情報、SIP スタック トレース情報が含まれます。

## コールの失敗

### Unified CM が SRV トランクの宛先を使用する際の TLS コールのエラー

Unified CM からのコールは TLS トランク セキュリティ プロファイルおよび SRV トランクの宛先を使用する場合に失敗することがあります (「\_sips.\_tcp」DNS での SRV レコード の検索が必要です)。

この問題が修正済みである Unified CM のバージョンに関する最新の情報については、「[Cisco の不具合検索ツール](#)」の「不具合：CSCue37440」を参照してください。

1 つまたは複数の VCS のピアに対処する必要がある場合は、SRV レコードを使用しないことで、この問題を回避できます。代わりに、SIP トランクでは、DNS A-レコードまたはスタティック IP アドレスを使用して各 VCS の [宛先アドレス (Destination Address)] を個別に指定します。ただし、これらのアドレスが、Unified CM から VCS が受信した URI のドメイン部分に影響することに注意してください。これを考慮して、VCS で適切なトランスフォームを設定する必要があります (「[Unified CM が提供するドメイン情報を VCS SIP ドメインに変換するためのトランスフォームの作成 \[p.19\]](#)」を参照してください)。

### 暗号化されたコールの失敗

Unified CM のエンドポイントでベスト エフォートの暗号化が必要で、他のエンドポイントが暗号化をサポートしない場合、Unified CM に登録されたエンドポイントと VCS に登録された (または VCS 経由でプロキシ化される) エンドポイント間のコールは失敗します。(Unified CM には、VCS は現在サポートしていない、非暗号化へのフォールバック (X-cisco-srtp-fallback) を示すための独自の方法があります)。

## 付録 2：既知のインターワーキング機能および制限

### 機能

#### 基本コールを発信する SIP および H.323 エンドポイント

- SIP および H.323 エンドポイントは、Unified CM に登録されたエンドポイントに対し、VCS 経由でコールを発信できます。
- Unified CM に登録されたエンドポイントは、VCS 上の SIP および H.323 エンドポイントに対してコールを発信できます。

### 制限事項

#### Cisco TelePresence Conductor

VCS が TelePresence Conductor と連動するように構成されている場合、Unified CM から SIP トランク上に発信されるコールは、TelePresence Conductor によって制御される会議の開始または参加が可能です。Unified CM に登録された Cisco TelePresence System (CTS) シリーズ エンドポイントが存在する場合、VCS は TelePresence Conductor のバックツーバック ユーザ エージェントに接続され、会議は TelePresence Server でホストされます。CTS からの暗号化されたコールは、SIP セッションが更新されたときにドロップされます。このシナリオの場合、SIP トランクを直接、Unified CM から TelePresence Conductor へ作成することを推奨します。この詳細については、『[Optimized Conferencing for Cisco Unified Communications Manager Solution Guide](#)』を参照してください。

#### E20 暗号化

E20 の [暗号化モード (Encryption Mode)] = [ベスト エフォート (Best Effort)] の場合、Unified CM からのコールは、E20 がコールに応答したときに消去されます。[暗号化モード (Encryption Mode)] = [オフ (Off)] に設定します。

#### L6.0 コードを実行する T150

SIP コールが L6.0 コードを実行する T150 から Unified CM 8.0 以前に対して発信された場合、Unified CM はコールの応答直後に T150 が送信する UPDATE メッセージを処理しません。そのコールに応答するコールは、即時に消去されます。

**xConfiguration Conference H239** が Off に設定されている場合、BFCP が提供されないと、Unified CM は T150 からの UPDATE を処理し、コールは目的に従って完了します。

#### H.323 MXP および 9971

VCS に登録された MXP が、Unified CM に登録された 9971 があるコール内にあり、その MXP コールが H.323 の場合、MXP のビデオは、VGA (フル サイズ画像) でなく CIF (小さい画像) になります。(MXP F9.0 および 9971 バージョン 9.0.2 で見られる)

MXP コールが SIP の場合、フル サイズ画像が見られます。

## 付録 3：VCS クラスタへの Unified CM の接続

Unified CM バージョン 8.5 以降、VCS ピアのクラスタと Unified CM を接続するために、VCS クラスタ ピアのアドレスが設定された Unified CM を提供する方法として次の 2 通りがあります。

- VCS へのトランクに VCS クラスタのための DNS SRV アドレスを指定する
- VCS へのトランクに VCS ピアのリストを指定する

Unified CM の 8.5 より前では、VCS へのトランクは、VCS クラスタの DNS SRV のアドレスを指定する必要がありました。

### VCS へのトランクに VCS クラスタの DNS SRV アドレスを指定するための設定

Unified CM が使用する DNS サーバに、VCS ピアのクラスタに対する DNS SRV レコードが存在することを確認します。DNS SRV レコードで、各ピアに同じプライオリティと同じウェイト値が設定されている必要があります。

1. Unified CM で、[デバイス (Device)] > [トランク (Trunk)] に移動します。
2. 以前設定したトランクを選択します。
3. 下へスクロールし、[SIP 情報 (SIP Information)] セクションのフィールドを次のように設定します。

接続先アドレス (Destination address)

<DNS SRV name of VCS cluster>

接続先アドレスは SRV (Destination address is an SRV)

このチェックボックスをオンにします。

4. [保存 (Save)] をクリックします。
5. [Reset] をクリックします。
6. [Reset] をクリックします。
7. VCS で、クラスタ名が SIP ドメインとして設定されていることを確認します ([設定 (Configuration)] > [ドメイン (Domains)])。

The screenshot shows the 'SIP Information' configuration page. The 'Destination' section is expanded, showing a table with columns for Destination Address, Destination Address IPv6, and Destination Port. The first row contains 'vcs-name vcs domain', an empty field, and '0'. Below this, several other fields are visible, including MTP Preferred Originating Codec (711ulaw), SIP Presence Group (Standard Presence group), SIP Trunk Security Profile (Non Secure SIP Trunk Profile), and others.

## VCS へのトランクに VCS ピアのリストを指定するための設定

1. Unified CM で、[デバイス (Device)] > [トランク (Trunk)] に移動します。
2. 以前設定したトランクを選択します。
3. 下へスクロールし、[SIP 情報 (SIP Information)] のフィールドを次のように設定します  
(追加の宛先アドレスのエントリを表示するには、[+] をクリックします)。

<b>接続先アドレスは SRV (Destination address is an SRV)</b>	このチェックボックスがオフになっていることを確認します。
宛先アドレス 1 (Destination address 1) 、および <b>接続先ポート 1 (Destination port 1)</b>	VCS ピア 1 の IP アドレスまたは DNS 名 接続 (TCP または TLS) に応じて 5060 または 5061
宛先アドレス 2 (Destination address 2) 、および <b>接続先ポート 2 (Destination port 2)</b>	VCS ピア 2 の IP アドレスまたは DNS 名 接続 (TCP または TLS) に応じて 5060 または 5061
宛先アドレス 3 (Destination address 3) 、および <b>接続先ポート 3 (Destination port 3)</b>	VCS ピア 3 がある場合、その IP アドレスまたは DNS 名 接続 (TCP または TLS) に応じて 5060 または 5061
...最大で宛先アドレス 6 (Destination address 6) まで、および <b>接続先ポート 6 (Destination port 6)</b>	... 存在する場合、VCS ピア 6 までの IP アドレスまたは DNS 名で繰り返します

4. [保存 (Save)] をクリックします。
5. [Reset] をクリックします。
6. [Reset] をクリックします。

The screenshot shows the 'SIP Information' configuration page. Under the 'Destination' section, there is a checkbox for 'Destination Address is an SRV' which is unchecked. Below this is a table with three columns: 'Destination Address', 'Destination Address IPv6', and 'Destination Port'. The first row is labeled '1\*' and has empty input fields for each column. To the right of the table are two buttons: a plus sign (+) and a minus sign (-).

## 付録 4：Unified CM ノードのクラスタへの VCS の接続

VCS を Unified CM ノードのクラスタに接続するとき、VCS は各 Unified CM ノードへのコールをルーティングできる必要があります。

これは、設定に応じて次の 2 種類の方法で実行できます。

1. ロケーションピアアドレスとしてリスト化された Unified CM ノードがある VCS の単一のネイバーゾーンでルーティングできます。このオプションは、VCS X7.0 以降でのみ使用できます。
2. DNS SRV レコードおよび VCS DNS ゾーンを使用します。

ロードされる Unified CM への VCS コールが Unified CM ノード全体で共有されることを両方のオプションが確認することに注意してください。

### オプション 1：単一のネイバーゾーンの使用

#### Unified CM の設定

クラスタ内では、Unified CM は (number@<ip address of Unified CM> ではなく) number@domain にルーティングされるコールを受け入れる必要があります。これにより、VCS は、ドメイン部分がコールの送信先のノードの IP アドレスと一致していることを確認する必要なく、コールを任意の Unified CM ノードに送信できます。

[クラスタの完全修飾ドメイン名 (Cluster Fully Qualified Domain Name)] ([クラスタ全体のドメイン設定 (Clusterwide Domain Configuration)] セクションの [システム (System)] > [エンタープライズパラメータ (Enterprise parameters)] に、ビデオネットワークと同じドメイン (vcs.domain など) が設定されていることを確認します。

#### VCS Control の設定

VCS の設定は、次の手順でのネイバーゾーンへの更新が必要です。

1. [設定 (Configuration)] > [ゾーン (Zones)] に移動します。
2. Unified CM のネイバーゾーンを選択します。
3. フィールドを次のように設定します。

ピア 1 アドレス (Peer 1 address)	Unified CM ノード 1 の IP アドレス、または Unified CM ノード 1 のドメイン
ピア 2 アドレス (Peer 2 address)	Unified CM ノード 2 の IP アドレスまたはドメイン
ピア 3 アドレス (Peer 3 address)	Unified CM ノード 3 の IP アドレスまたはドメイン、または Unified CM ノード 3 が設定されていない場合は空白
... 最大でピア 6 アドレス (Peer 6 address) まで	...最大で Unified CM ノード 6 までの IP アドレスまたはドメインで繰り返すか、Unified CM ノードが設定されていない場合は、空白のままとする

## オプション 2 : DNS ゾーンの使用

### Unified CMの設定

[クラスタの完全修飾ドメイン名 (Cluster Fully Qualified Domain Name)] ([クラスタ全体のドメイン設定 (Clusterwide Domain Configuration)] セクションの [システム (System)] > [エンタープライズ パラメータ (Enterprise parameters)] ) に、ビデオ ネットワークと同じドメイン (vcs.domainなど) が設定されていることを確認します。

### DNS サーバ設定

Unified CM クラスタのために DNS SRV レコードを使用して DNS サーバ (VCS が使用) を設定します。

- TLS 接続 (各 Unified CM ノードに 1 つのレコード) の `_sips._tcp.fqdn_of_cucm_clusterrecords`、または
- TCP 接続 (各 Unified CM ノードに 1 つのレコード) の `_sip._tcp.fqdn_of_cucm_clusterrecords`。

### VCS Control の設定

VCS の設定では、次の 3 段階の手順が必要です。

- Unified CM DNS ゾーンを作成
- DNS ゾーンを使用するように検索ルールを調整
- 古い Unified CM のネイバー ゾーンを削除

### Unified CM DNS ゾーン の作成

1. [設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] へ移動します。
2. [新規 (New)] をクリックします。
3. フィールドを次のように設定します。

名前 (Name)	CUCM クラスタ ネイバー DNS ゾーン
タイプ (Type)	DNS
ホップ数 (Hop count)	15
H.323 モード (H.323 Mode)	オフ (Off) H.323 アクセスは Unified CM との通信には必要ありません
SIP モード (SIP mode)	オン
TLS 検証モード (TLS verify mode)	オフ (Off)



メディア暗号化モード (Media encryption mode)	Auto
アドレスレコードを含める (Include address record)	オフ (Off)
ゾーン プロファイル (Zone profile)	必要に応じて、[Cisco Unified Communications Manager] または [Cisco Unified Communications Manager (8.6.1 以降) (Cisco Unified Communications Manager (8.6.1 or later) ) ] を選択します。

4. [ゾーンの作成 (Create zone) ] をクリックします。

**Create zone** You are here: [Configuration](#) > [Zones](#) > [Zones](#) > [Create zone](#)

**Configuration**

Name  ⓘ

Type  ⓘ

Hop count  ⓘ

**H.323**

Mode  ⓘ

**SIP**

Mode  ⓘ

TLS verify mode  ⓘ

Media encryption mode  ⓘ

**Advanced**

Include address record  ⓘ

Zone profile  ⓘ

## 検索ルールの調整

この Unified CM DNS ゾーンをポイントするように、検索ルールを変更します。

1. [設定 (Configuration) ] > [ダイヤル プラン (Dial plan) ] > [検索ルール (Search rules) ] に移動します。
2. 既存の「Unified CM へのルーティング」検索ルールを選択します。
3. 上で作成した CUCM クラスタ ネイバー DNS ゾーンを使用するように [転送先ゾーン (Target zone) ] を更新します。
4. [保存 (Save) ] をクリックします。

## 古い Unified CM のネイバーゾーンを削除

現在未使用のネイバーゾーン「Unified CM ネイバー」を削除します。

1. [設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] へ移動します。
2. 「CUCM ネイバー」ゾーンの横にあるチェックボックスをオンにします。
3. [削除 (Delete)] をクリックします。

## 付録 5：Multiway および Unified CM

Unified CM に登録されたエンドポイントが Multiway 会議に参加できるようにするには、次のことを確認します。

1. Unified CM への VCS ゾーンが [コール シグナリング ルーテッド モード (Call Signaling Routed Mode) ] が [常時 (Always) ] に設定されたゾーン プロファイルを使用している。
2. Unified CM に、Multiway エイリアス ドメインのコールを VCS ヘルパーティングするルート パターンがある。
3. Unified CM では、VCS への SIP トランクが使用する SIP プロファイルで [アプリケーションによるリダイレクト (Redirect by Application) ] が選択されている。

### VCS の設定

Unified CM への VCS ゾーンは、[コール シグナリング ルーテッド モード (Call Signaling Routed Mode) ] が [常時 (Always) ] に設定されたゾーン プロファイルを使用している必要があります。これを実行するには、必要に応じて、ゾーン プロファイルが [Cisco Unified Communications Manager] または [Cisco Unified Communications Manager (8.6.1 以降) (Cisco Unified Communications Manager (8.6.1 or later)) ] に設定されていることを確認します。

### Unified CM の設定

1. Unified CM に ビデオ ドメインのコールを VCS ヘルパーティングするルート パターンがあることを確認します。「[Unified CM に登録されたエンドポイントにコールするための VCS に登録されたエンドポイントの有効化 \[p.19\]](#)」の手順に従ってください。
2. VCS への SIP トランクが使用する SIP プロファイルで、[アプリケーションによるリダイレクト (Redirect by Application) ] がオンになっていることを確認します。
  - 1.[デバイス (Device) ] > [デバイスの設定 (Device Settings) ] > [SIP プロファイル (SIP Profile) ] に移動します。
  - 2.[アプリケーションによるリダイレクト (Redirect by Application) ] チェックボックスをオンにします。
  - 3.[設定を適用 (Apply Config) ] をクリックし、[OK] をクリックします。

The screenshot shows the 'SIP Profile Information' configuration page. The 'Name' field is 'Standard SIP Profile' and the 'Description' is 'Default SIP Profile'. The 'Default MTP Telephony Event Payload Type' is '101'. The 'Resource Priority Namespace List' is '< None >'. The 'Early Offer for G.Clear Calls' is 'Disabled'. The 'SDP Session-level Bandwidth Modifier for Early Offer and Re-invites' is 'TIAS and AS'. The 'User-Agent and Server header information' section has 'Send Unified CM Version Information as User-Agen' selected. The 'Redirect by Application' checkbox is checked and highlighted with a red box. Other checkboxes include 'Disable Early Media on 180', 'Outgoing T.38 INVITE include audio mline', 'Enable ANAT', 'Require SDP Inactive Exchange for Mid-Call Media Change', 'Use Fully Qualified Domain Name in SIP Requests', and 'Allow Presentation Sharing using BFCP'.

これで、Multiway をテストできます。

## 付録 6：追加情報

### IP アドレスのダイヤル

Unified CM は、IP アドレスにダイヤルアウト接続できませんが、VCS では可能です。Unified CM に登録されたエンドポイントからの IP アドレスのダイヤルをサポートするには、ナレッジベース項目「[Dial IP Addresses from Endpoints Registered to CUCM with VCS/Expressway](#)」の手順に従うことをお勧めします。

### SIP URI で使用できる文字

次の文字セットが SIP URI で許可されます。詳細については、RFC 3261 で参照できます。

a-z、A-Z、0-9、-、\_、.、!、~、\*、'、(、)、&、=、+、\$、,、;、?、/

その他の文字が必要な場合は、必須の文字の ASCII 値を表す 2 桁の 16 進数の前に「%」を使用して「エスケープ」する必要があります。

たとえば、「alice smith@example.com」を「alice%20smithexample.com」としてエンコードする必要があります（この場合、「%20」は空白文字を表します）。

## マニュアルの変更履歴

次の表に、このマニュアルの変更履歴の要約を示します。

日付	説明
2015 年 11 月	新しいテンプレートを適用。バージョン番号を更新。X8.7 用に再発行。
2015 年 7 月	X8.6 に関する内容を更新。
2015 年 4 月	X8.5.2 に関する内容を更新。新しい IP アドレスのダイヤル項目へのリンク。
2014 年 12 月	X8.5 に関する内容を更新。IP アドレスのダイヤル情報を修正。
2014 年 6 月	X8.2 用に再発行。
2013 年 12 月	X8.1 に関する内容を更新。新しい <i>Cisco Unified Communications Manager (8.6.1 以降)</i> ゾーン プロファイルのサポートが組み込まれ、それにより、今後、カスタム プロファイルが不要なため、Unified CM ゾーン プロファイルパラメータと BFCP の有効化に関する付録を削除。
2013 年 3 月	ダイヤル プラン例をシンプル化。Unified CM クラスタ完全修飾ドメイン名を設定するための要件を、主な設定の一部とし移動。クラスタでは不要。TLS 接続手順をドキュメント本文へ移動。Unified CM DNS SRV ルックアップに関するトラブルシューティングの注を追加。
2012 年 9 月	暗号化された SRTCP の使用について、付録 7 および付録 8 を改定ドキュメントは現在 CUCM 8.x および 9.x のみを参照。
2012 年 8 月	VCS X7.2 に関する内容を更新。
2012 年 3 月	VCS X7.1 に関する内容を更新。
2011 年 10 月	コール シグナリングルーティング モードの Multiway のための設定に関するガイダンスの更新
2011 年 8 月	VCS X7.0 および BFCP に関する内容を更新。VCS の Unified CM ノードのクラスタに対する接続に関するガイダンスの更新。
2011 年 6 月	VCS X6 に関する内容を更新。
2011 年 3 月	付録 5 の VCS ピアのクラスタへの Unified CM の接続に関する Unified CM バージョン 8.5 の記述を更新。付録 12 で SIP URI で許可される文字列を追加
2010 年 10 月	Cisco Unified CM に関する内容を追加。Unified CM コールバック URI に戻されるコールの処理に関する内容を追加。コール転送の処理のための更新
2010 年 7 月	Cisco Unified Communications Manager を参照するようにマニュアル タイトルを更新このマニュアルの変更履歴表を追加Unified CM v8 で変更されたユーザ インターフェイスを反映するための全般的な更新を適用。
2010 年 6 月	付録 10 で TLS を使用した VCS の Unified CM への接続に関する内容を追加。
2010 年 4 月	VCS X5.1 に関する内容を更新。その他のトラブルシューティング情報を追加。
2010 年 1 月	初版。

## シスコの法的情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハード コピーおよびソフト コピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト ([www.cisco.com/go/offices](http://www.cisco.com/go/offices) [英語]) をご覧ください。

© 2015 Cisco Systems, Inc. All rights reserved.

## シスコの商標または登録商標

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. シスコの商標の一覧は [www.cisco.com/web/JP/trademark\\_statement.html](http://www.cisco.com/web/JP/trademark_statement.html) に掲載されています。Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)