



Cisco Unified Communications Manager と Cisco VCS との併用 導入ガイド

Cisco VCS X7.2
CUCM 8.x、9.x
SIP トランク

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

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報
につきましては、日本語版掲載時点で、英語版にアップデートがあ
り、リンク先のページが移動/変更されている場合がありますことを
ご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サ
イトのドキュメントを参照ください。

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

D14602.12

2012 年 9 月

目次

はじめに	5
目的および対象読者	5
導入シナリオ	5
設定プロセスの要約	6
システム設定の前提条件	6
Cisco VCS Control に登録されたエンドポイント間のコールの有効化	7
Cisco VCS Control の設定	7
Cisco VCS Control の SIP ドメインの設定	7
トラバーサル サブゾーン設定の確認	8
トランスフォーメーションの作成	8
CUCM の設定	10
Cisco VCS Control へのエンドポイントの登録	11
エンドポイントの設定	11
登録の確認	11
テスト コール	11
CUCM に登録されたエンドポイント間のコールの有効化	12
Cisco VCS Control の設定	12
CUCM の設定	12
SIP プロファイルの設定	12
電話デバイスの追加	15
デバイスの電話番号の設定	15
CUCM からの設定を取得する電話エンドポイントの設定	16
登録の確認	16
テスト コール	16
CUCM に登録されたエンドポイントにコールするための VCS Control に登録されたエンドポイントの有効化	17
CUCM の設定	17
SIP トランク セキュリティ プロファイルの設定	17
SIP トランク デバイスの設定	18
Cisco VCS Control の設定	22
CUCM のネイバー ゾーンの作成	22
CUCM ネイバー ゾーンにコールをルーティングする検索ルールの作成	24
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	26
テスト コール	26
VCS Control に登録されたエンドポイントにコールするための CUCM に登録されたエンドポイントの有効化	27
Cisco VCS Control の設定	27

Cisco VCS のローカルおよびネイバーゾーンをコールするための CUCM のトランスフォームの設定	27
VCS が CUCM とのコールのシグナリングパスに留まることの確認	28
CUCM の設定	30
シスコの電話機から Cisco VCS への番号によるダイヤルの許可	30
シスコの電話機から Cisco VCS ドメインへのダイヤルの許可	31
テストコール	33
詳細設定	34
CUCM SIP 最大着信メッセージサイズ	34
付録 1 : トラブルシューティング	35
Cisco VCS Control のローカルコールへの接続の問題	35
[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	35
[検索履歴 (Search history)] でのコール進捗の確認	36
エラーの確認	36
コールのトレース	36
H.323 から SIP CUCM へのコールが動作しない	36
422 セッションタイマーが小さすぎます (422 Session Timer too small)	36
Cisco TelePresence Server とのコールの失敗	37
In-Call の問題	37
コールは最大 15 分間まで維持されます。	37
CUCM のビデオ電話機から VCS にコールが転送がされるときに、コールが消去される	38
Multiway を使用した CUCM エンドポイントの会議への参加が失敗する	38
RTMT を使用する CUCM でのトレースの取得	38
トレースを有効にするための CUCM の設定	38
RTMT (Real Time Monitoring Tool) のインストール	38
RTMT の実行	39
RTMT を使用するトレースの取得	39
付録 2 : 既知のインターワーキング機能および制限	40
機能	40
基本コールを発信する SIP および H.323 エンドポイント	40
Cisco TelePresence Conductor	40
制限事項	40
E20 暗号化	40
L6.0 コードを実行する T150	40
H.323 MXP および 9971	40
付録 3 : CUCM の Cisco VCS ピアのクラスタへの接続	41
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	41
Cisco 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	42
付録 4 : Cisco VCS の CUCM ノードのクラスタへの接続	44
オプション 1 : 単一のネイバーゾーンの使用	44
CUCM の設定	44

Cisco VCS Control の設定.....	44
オプション 2 : DNS ゾーンの使用.....	45
CUCM の設定.....	45
DNS サーバの設定.....	45
Cisco VCS Control の設定.....	46
オプション 3 : 複数のネイバー ゾーンの使用.....	49
Cisco VCS Control の設定.....	49
付録 5 : Cisco TelePresence Multiway および CUCM.....	50
VCS の設定.....	50
CUCM の設定.....	50
付録 6 : エンドポイント固有の設定.....	52
L6.x を実行する T150.....	52
その他の製品.....	52
付録 7 : Cisco Unified Communications Manager の [詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] で設定されたパラメータ.....	53
付録 8 : TCP でなく TLS を使用した Cisco VCS の CUCM への接続.....	55
CUCM が Cisco VCS サーバ証明書を信頼していることの確認.....	55
CUCM での SIP トランク セキュリティ プロファイルの構成.....	56
Cisco VCS への CUCM トランクを TLS を使用するように更新.....	56
CUCM への VCS ネイバー ゾーンを TLS を使用するように更新.....	57
TLS 接続が動作していることを確認します。.....	57
VCS のネットワーク.....	58
CUCM に登録されたエンドポイントへの暗号化されたコール.....	58
付録 9 : SIP URI で許可される文字.....	59
付録 10 : デュアル ビデオまたはプレゼンテーション共有での BFCP の有効化.....	60
VCS の設定.....	60
CUCM の設定.....	60
マニュアルの変更履歴.....	61

はじめに

目的および対象読者

この導入ガイドでは、Cisco TelePresence Video Communication Server (Cisco VCS) バージョン X7.2 および Cisco Unified Communications Manager (CUCM) バージョン 8.x および 9.x を SIP トランク経由でインターワークするための設定方法に関するガイドラインを示します。

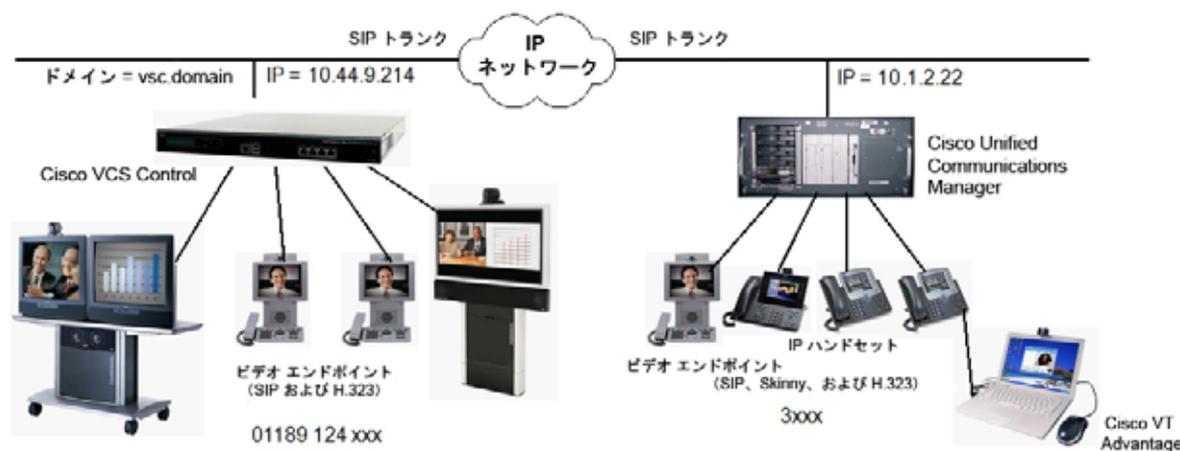
Cisco VCS および CUCM がインターワークできるように接続するには、次の方法があります。

- H.323 トランクを使用する
- CUCM をゲートウェイとして Cisco VCS に登録するように設定する (通常 CUCM バージョン 4.1 以前のバージョンと一緒に使用)

導入シナリオ

自社の電話システムですでに CUCM を稼働している企業があります。この企業は、CUCM を、既存または新しいビデオ会議システムと接続された Cisco 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、CUCM 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、Cisco VCS Control に接続されているエンドポイントは **01189 124 xxx** の電話番号で識別されます。つまり、4 桁の内線番号か、11 桁のフル番号 (Cisco VCS Control に登録されたエンドポイントの場合) で電話をかけることができます。

CUCM および Cisco 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。Cisco VCS Control ドメインは **vcs.domain** です。CUCM に送信されるコールのドメイン部分は <ip address of cucm> である必要があります。CUCM から Cisco VCS へのコールは、<ip address of vcs>:5060 として設定されるドメイン部分と一緒に到着します。

Cisco VCS Control はバージョン X6 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。

- H323-SIP インターワーキング
- 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、CUCM および Cisco 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。

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

システム設定の前提条件

このマニュアルを使用する前に、Cisco VCS Control および CUCM がインターワークするように設定し、次が設定されて動作していることを確認してください。

- CUCM 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 (Region)]
 - [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)]
- Cisco VCS Control に IP アドレス、DNS および NTP 情報が設定されており、Web ブラウザ インターフェイスを介した管理を行うためにアクセスできること。『*VCS Basic Configuration (Single VCS Control) Deployment Guide*』を参照してください。

Cisco VCS Control に登録されたエンドポイント間のコールの有効化

Cisco VCS Control の設定

Cisco 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する設定は、次の手順に従います。

1. Cisco 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。
2. トラバーサル サブゾーンの設定を確認します。トラバーサル サブゾーンは、H.323 エンドポイントと SIP エンドポイントとのインターワーキングを処理します。
3. 次のようにトランスフォーメーションを作成します。
 - ダイヤル番号にドメイン情報がない場合は、ドメイン情報を追加します。これにより、SIP エンドポイントおよび H.323 エンドポイントからのダイヤル番号情報が共通フォーマットの `number@domain` になります。
 - 4 桁の Cisco VCS 内線番号 (4xxx) を 11 桁のフル電話番号に拡張します。SIP エンドポイントと H.323 エンドポイントの両方が、`11_digit_number@domain` (11 桁のフル電話番号にドメイン情報が付加されたもの) のフォーマットの URI (H323 ID) を使用して Cisco VCS Control に登録されます。このトランスフォーメーションによって、4 桁 (4xxx) または 11 桁の番号は、ドメイン情報を持っているかどうかにかかわらず、ルーティングのための正しい 11 桁の URI フォーマットにトランスフォーメーションされるように変換されます。
3xxx へのコールは、`3xxx@domain` にフォーマットされます。

Cisco VCS Control の SIP ドメインの設定

SIP エンドポイントは、`11_digit_number@vcs.domain` のフォーマットで AOR (Address Of Record) を使用して Cisco VCS Control に登録されます。Cisco VCS Control 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. [VCS 設定 (VCS configuration)] > [プロトコル (Protocols)] > [SIP] > [ドメイン (Domains)] 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。

名前 (Name)	必要なドメイン (たとえば vcs.domain)
-----------	---------------------------

4. [ドメインの作成 (Create domain)] をクリックします。

トラバーサル サブゾーン設定の確認

- [VCS 設定 (VCS configuration)] > [ローカル ゾーン (Local Zone)] > [トラバーサル サブゾーン (Traversal Subzone)] に移動します。
 - ポート範囲はデフォルトの値 (50000 ~ 54999) のままにするか、必要に応じて設定できません (詳細については、『Cisco VCS Administrator Guide』の「Zones and Neighbors」を参照)。
 - 帯域幅の値はデフォルトの値 ([無制限 (Unlimited)]) のままにするか、必要に応じて設定できません (詳細については、『Cisco VCS Administrator Guide』の「Bandwidth Control」を参照)。
- [保存 (Save)] をクリックします。

Traversal Subzone status	
Number of registrations	0
Number of calls	0
Bandwidth used on this VCS	0 kbps
Total bandwidth used across this cluster	0 kbps

トランスフォーメーションの作成

この導入シナリオでは、ユーザは、11 桁の E.164 番号 (01189 124 xxx) または 4 桁の内線番号 (4xxx) を使用して、Cisco VCS Control 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なります。CUCM エンドポイントには 4 桁の番号 (3xxx) を使用してダイヤルします。このダイヤリング モデルは、H.323 でサポートされます (エンドポイントが 4 桁の番号および 11 桁の E.164 エリアスの両方で登録される場合)。ただし、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)。

Cisco VCS Control が受信するコール要求の場合、ダイヤル番号は次のようになります。

- 11 桁（Cisco VCS 登録エンドポイント）の番号の最初の 7 桁が含まれる場合と含まれない場合がある
（4 桁の内線番号がダイヤルされたときは含まれない）
- ルーティング先の特定のエンドポイントを識別するダイヤル番号の最後の 4 桁の番号（内線部分）は必ず含まれる
- ドメインが含まれる場合と含まれない場合がある
（SIP エンドポイントがコールを発信するときのみ含まれる）

トランスフォーメーションは、受信するフォーマットがどれであっても、ダイヤル番号が一貫したフォームに変換されるために必要です。この場合は次のようになります。

- ドメインが追加される（つまり **dialed_digits@domain**）。
（この例では、追加される **domain** は Cisco VCS Control のドメイン **vcs.domain**）
- 4xxx へのコールにはプレフィックス 0118912 が追加され、11 桁のフル電話番号に変換される

このため、次の 2 つの正規表現が使用されます。

- $(4\d{3})(@vcs.domain)?$ は $0118912\1@vcs.domain$ に変換される
- $([^@]*)$ は $\1@vcs.domain$ に変換される

（最初の表現では、4xxx 番号は「@vcs.domain」がある場合でもない場合でも、 $01189124xxx@vcs.domain$ に変換されます。2 番目の表現では、ドメインを示す「@」を含まないダイヤル情報には、すべて「@vcs.domain」が追加されます）

詳細については、『Cisco VCS Administrator Guide』の付録「Regular Expression Reference」を参照するか、WWW で「正規表現」という用語を使用して検索してください。

最初のトランスフォームを作成するには、次の手順を実行します。

1. [VCS 設定 (VCS configuration)] > [ダイヤル プラン (Dial plan)] > [トランスフォーメーション (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)	1
説明 (Description)	たとえば「4 から 11 桁のダイヤル」
パターン タイプ (Pattern type)	Regex
パターン文字列 (Pattern string)	$(4\d{3})(@vcs.domain)?$
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	0118912\1@vcs.domain
状態 (State)	有効 (Enabled)

4. [トランスフォーメーションの作成 (Create transform)] をクリックします。

2 番目のトランスフォームを作成するには、次の手順を実行します。

1. [VCS 設定 (VCS configuration)] > [ダイヤル プラン (Dial plan)] > [トランスフォーメーション (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「ドメインがない場合に追加」
パターンタイプ (Pattern type)	Regex
パターン文字列 (Pattern string)	([^@]*)
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	\1@vcs.domain
状態 (State)	有効 (Enabled)

4. [トランスフォーメーションの作成 (Create transform)] をクリックします。

CUCM の設定

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

Cisco 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 01189124000@vcs.domain、01189124001@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 = Cisco VCS Control 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 01189124000@vcs.domain、01189124001@vcs.domain など)
- サーバアドレス (プロキシアドレス) = Cisco VCS Control 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、Cisco VCS Control 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、『*Cisco VCS Administrator Guide*』の「Cisco VCS Configuration」を参照してください。

テスト コール

4 桁のダイヤルと 11 桁のダイヤルの両方を使用して、テスト コールを何度か発信します。

コール履歴は Cisco VCS Control 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。

CUCM に登録されたエンドポイント間のコールの有効化

Cisco VCS Control の設定

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

CUCM の設定

電話機間でのコールの発信を有効にするための CUCM およびシスコの電話機の設定には、SIP プロファイルの設定、CUCM での電話機の指定、電話機への電話番号の設定、および電話機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。

- SIP プロファイルを設定します。
- 電話デバイスの追加：CUCM でサポートされてい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の設定：この電話エンドポイントの呼び出し音が鳴る電話番号を指定します。
- CUCM 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。設定プロセスをアクティブにするには、電話機を再起動する必要があります。

SIP プロファイルの設定

1. CUCM 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. テーブルの [コピー (Copy)] (二重に重なった紙アイコン) 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)	標準の SIP プロファイル : VCS 用
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
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 (CUCM 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 トミー サービス URI (Meet Me Service URI)	x-cisco-serviceuri-meetme
ユーザ情報 (User Info)	なし (None)
DTMF DB レベル (DTMF DB Level)	基準 (Nominal)
コール保留時の呼び出し音 (Call Hold Ring Back)	オフ (Off)
非通知着信拒否 (Anonymous Call Block)	オフ (Off)
発信者 ID ブロック (Caller ID Blocking)	オフ (Off)
サイレントコントロール (Do Not Disturb Control)	ユーザ (User)
7940 と 7960 の Telnet レベル (Telnet Level for 7940 and 7960)	ディセーブル (Disabled)
キープアライブのタイムアウト値 (Timer Keep Alive Expires)	120
サブスクライブのタイムアウト値 (Timer Subscribe Expires)	120
サブスクライブ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)

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | admin | Search Documentation | About | Logout

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

SIP Profile Configuration Related Links: Back To Find/List

Save Delete Copy Reset Apply Config Add New

Status

- Status: Ready
- All SIP devices using this profile must be restarted before any changes will take affect.

SIP Profile Information

Name *	Standard SIP Profile - for VCS
Description	Default SIP Profile
Default MTP Telephony Event Payload Type *	101
Resource Priority Namespace List	< None >
Early Offer for G.Clear Calls *	Disabled
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites *	TIAS and AS
User-Agent and Server header information *	Send Unified CM Version Information as User-Agen

Redirect by Application
 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
 Allow Presentation Sharing using BFCP

Parameters used in Phone

Timer Invite Expires (seconds) *	180
Timer Register Delta (seconds) *	5
Timer Register Expires (seconds) *	3600
Timer T1 (msec) *	500
Timer T2 (msec) *	4000
Retry INVITE *	6
Retry Non-INVITE *	10
Start Media Port *	16384
Stop Media Port *	32768
Call Pickup URI *	x-cisco-serviceuri-pickup
Call Pickup Group Other URI *	x-cisco-serviceuri-opickup
Call Pickup Group URI *	x-cisco-serviceuri-gpickup

Meet Me Service URI*	x-cisco-serviceuri-meetme
User Info*	None
DTMF DB Level*	Nominal
Call Hold Ring Back*	OFF
Anonymous Call Block*	OFF
Caller ID Blocking*	OFF
Do Not Disturb Control*	User
Telnet Level for 7940 and 7960*	Disabled
Timer Keep Alive Expires (seconds)*	120
Timer Subscribe Expires (seconds)*	120
Timer Subscribe Delta (seconds)*	5
Maximum Redirections*	70
Off Hook To First Digit Timer (milliseconds)*	15000
Call Forward URI*	x-cisco-serviceuri-cfwdall
Speed Dial (Abbreviated Dial) URI*	x-cisco-serviceuri-abbrevial
<input checked="" type="checkbox"/> Conference Join Enabled <input type="checkbox"/> RFC 2543 Hold <input checked="" type="checkbox"/> Semi Attended Transfer <input type="checkbox"/> Enable VAD <input type="checkbox"/> Stutter Message Waiting	

Trunk Specific Configuration	
Reroute Incoming Request to new Trunk based on*	Never
RSVP Over SIP*	Local RSVP
<input checked="" type="checkbox"/> Fall back to local RSVP	
SIP Rel1XX Options*	Disabled
<input type="checkbox"/> Deliver Conference Bridge Identifier <input type="checkbox"/> Early Offer support for voice and video calls (insert MTP if needed) <input type="checkbox"/> Send send-receive SDP in mid-call INVITE	
SIP OPTIONS Ping	
<input type="checkbox"/> Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"	
Ping Interval for In-service and Partially In-service Trunks (seconds)*	60
Ping Interval for Out-of-service Trunks (seconds)*	120
Ping Retry Timer (milliseconds)*	500
Ping Retry Count*	5

- Save Delete Copy Reset Apply Config Add New

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. 必要に応じて設定します。
BFCP が使用される場合、[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)] チェックボックスが選択されている SIP プロファイルが使用されることを確認します。
4. [保存 (Save)] 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)。

CUCM からの設定を取得する電話エンドポイントの設定

シスコの電話機で次の手順を実行します。

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 CUCM 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。
 - a. 設定 ボタンを 2 回押し、設定メニューに戻ります。
 - b. [ロック解除 (Unlock)] を選択し、適切なパスワードを入力します。
 - c. [ネットワークの設定 (Network Configuration)] セクションを選択します。
 - d. [代替 TFTP (Alternate TFTP)] = [はい (YES)] に設定します。
 - e. [TFTP サーバ (TFTP Server)] = <IP address of CUCM> に設定します。
 - f. [許可 (Accept)] を選択します。
 - g. [保存 (Save)] を選択します。
3. 電話機を再起動します (電話機のプラグを外し、電源を再接続します)。

電話機は、回線 1 が CUCM で指定した電話番号であることを示しているはずですが (たとえば 3001)。

これで、CUCM 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

CUCM に接続された電話機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。

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

CUCM の設定

CUCM に登録されたデバイス間で、コールを発信できるようにする設定は、次の 2 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します。
- SIP トランク デバイスを設定します。

SIP トランク セキュリティ プロファイルの設定

1. CUCM で、[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)] 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。

名前 (Name)	非セキュア SIP トランク セキュリティ プロファイル
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

4. [保存 (Save)] をクリックします。

The screenshot shows the Cisco Unified CM Administration interface for configuring a SIP Trunk Security Profile. The page title is "SIP Trunk Security Profile Configuration" and the status is "Ready". The configuration form includes the following fields and options:

- Name:** Non Secure SIP Trunk Profile
- Description:** Non Secure SIP Trunk Profile authenticated by null Strin
- Device Security Mode:** Non Secure
- Incoming Transport Type:** TCP+UDP
- Outgoing Transport Type:** TCP
- Enable Digest Authentication
- Nonce Validity Time (mins):** 600
- X.509 Subject Name:**
- Incoming Port:** 5060
- Enable Application Level Authorization
- Accept Presence Subscription
- Accept Out-of-Dialog REFER**
- Accept Unsolicited Notification
- Accept Replaces Header
- Transmit Security Status
- SIP V.150 Outbound SDP Offer Filtering:** Use Default Filter

SIP トランク デバイスの設定

1. CUCM 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. [Next (次へ)] 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)	VCS_location、たとえば VCS_Ruscombe
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
ロケーション (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 (None)
メディア ターミネーション ポイントが必須 (Media Termination Point Required)	オーディオ デバイスが CUCM 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。 CUCM に登録されている任意のビデオ電話機が、Cisco VCS に登録されているエンドポイントとの間でビデオ通話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。

SRTP を許可 (SRTP Allowed)	チェックボックスをオンにする
--------------------------------	----------------

注：メディア ターミネーション ポイントの使用は、次の状況で役立ちます。

- ▶ CUCM 電話機から、Cisco VCS に登録された SIP ビデオ デバイスへのコールが、CUCM が SIP SDP を要求されたとおりに提供しないために失敗した場合（CUCM 6.1 で発生）。
- ▶ CUCM 電話機から、Cisco VCS に登録された H.323 ビデオ デバイスへのコールが、SDP がない INVITE が Cisco VCS で適切にインターワークされないために失敗した場合（この問題は Cisco VCS X5.1.1 以降で解決済み）。

しかし、メディア ターミネーション ポイントが原因で、CUCM および Cisco VCS 間のビデオ通話の発信時に問題が発生することがあります（CUPC で見られる）。

6. [コール ルーティング情報 (Call Routing Information)] > [インバウンド 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)] > [アウトバウンド 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 (Destination address)	<IP address of Cisco VCS> または <Domain of Cisco VCS / Cisco 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は、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にのみオンにします。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 Cisco VCS のクラスタに向けます。 IP アドレス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ないでください。
接続先ポート (Destination port)	5060
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)
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 セキュリティ プロファイル
SIP プロファイル (SIP Profile)	標準の SIP プロファイル : VCS 用
DTMF シグナリング方式 (DTMF Signaling Method)	RFC 2833
正規化スクリプト (Normalization Script) (CUCM 8.6 以降のみに該当)	vcs-interop (使用可能な場合)

9. [保存 (Save)] をクリックします。
10. [リセット (Reset)] をクリックします。
11. [リセット (Reset)] をクリックします。

The screenshot shows the 'Trunk Configuration' page in Cisco VCS. The 'Status' is 'Ready'. The 'Device Information' section is expanded, showing the following configuration:

- Product: SIP Trunk
- Device Protocol: SIP
- Trunk Service Type: None(Default)
- Device Name*: VCS_Ruscombe
- Description: VCS at Ruscombe
- Device Pool*: Default
- Common Device Configuration: LABCMS
- Call Classification*: OnNet
- Media Resource Group List: < None >
- Location*: Reston LABCMSAG1
- AAR Group: < None >
- Tunneled Protocol*: None
- QSIG Variant*: No Changes
- ASN.1 ROSE OID Encoding*: No Changes
- Packet Capture Mode*: None
- Packet Capture Duration: 0
- Media Termination Point Required:
- Retry Video Call as Audio:
- Path Replacement Support:
- Transmit UTF-8 for Calling Party Name:
- Transmit UTF-8 Names in QSIG APDU:
- Unattended Port:
- SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information:
- Consider Traffic on This Trunk Secure*: When using both sRTP and TLS
- Route Class Signaling Enabled*: Default
- Use Trusted Relay Point*: Default
- PSTN Access:
- Run On All Active Unified CM Nodes:

Intercompany Media Engine (IME)
E.164 Transformation Profile < None >

Multilevel Precedence and Preemption (MLPP) Information
MLPP Domain < None >

Call Routing Information
 Remote-Party-Id
 Asserted-Identity
 Asserted-Type* Default
 SIP Privacy* Default

Inbound Calls
 Significant Digits* All
 Connected Line ID Presentation* Default
 Connected Name Presentation* Default
 Calling Search Space LABCMS
 AAR Calling Search Space < None >
 Prefix DN
 Redirecting Diversion Header Delivery - Inbound

Incoming Calling Party Settings
 If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	Default		< None >	<input checked="" type="checkbox"/>

Connected Party Settings
 Connected Party Transformation CSS < None >
 Use Device Pool Connected Party Transformation CSS

Outbound Calls
 Called Party Transformation CSS < None >
 Use Device Pool Called Party Transformation CSS
 Calling Party Transformation CSS < None >
 Use Device Pool Calling Party Transformation CSS
 Calling Party Selection* Originator
 Calling Line ID Presentation* Default
 Calling Name Presentation* Default
 Caller ID DN
 Caller Name
 Redirecting Diversion Header Delivery - Outbound
 Redirecting Party Transformation CSS < None >
 Use Device Pool Redirecting Party Transformation CSS

SIP Information

Destination
 Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.50.152.7		5060

MTP Preferred Originating Codec* Follow
 Presence Group* Standard Presence group
 SIP Trunk Security Profile* Non Secure SIP Trunk Profile
 Rerouting Calling Search Space < None >
 Out-Of-Dialog Refer Calling Search Space < None >
 SUBSCRIBE Calling Search Space < None >
 SIP Profile* Standard SIP Profile - for VCS
 DTMF Signaling Method* RFC 2833

Normalization Script
 Normalization Script vcs-interop
 Enable Trace

Parameter Name	Parameter Value
1	

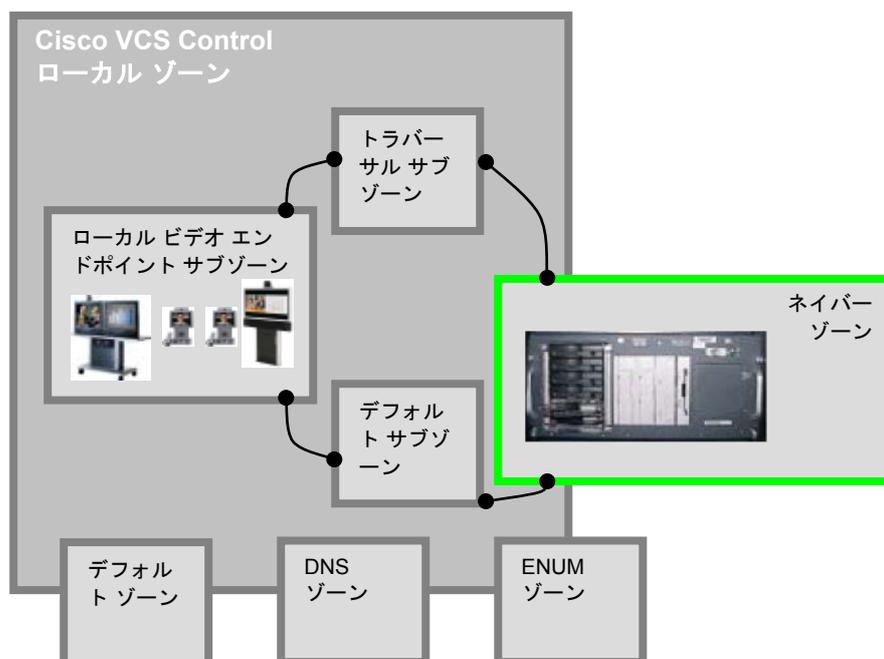
Geolocation Configuration
 Geolocation < None >
 Geolocation Filter < None >
 Send Geolocation Information

これで、Cisco VCS Control に登録されたハンドセットと、CUCM に登録されたハンドセットとの間でコールを発信することができます。

Cisco VCS Control の設定

Cisco VCS Control の設定は次の 3 段階の手順に従います。

- CUCM を含むネイバーゾーンを設定します。
- そのゾーンにコールをルーティングする検索ルールを設定します。
- 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します。



CUCM のネイバーゾーンの作成

1. [VCS 設定 (VCS configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] 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。

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 アクセスは CUCM との通信には不要)
SIP モード (SIP mode)	オン (On)
SIP ポート (SIP port)	5060 (CUCM の SIP アクセスポートが 5060 でない場合、SIP ポートの値を CUCM で使用すると同じ値に変更)
トランスポート (Transport)	TCP
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)	自動 (Auto)
認証ポリシー (Authentication policy)	認証ポリシーに従って認証設定を指定します。
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)	CUCM の IP アドレス、または CUCM のドメイン
ゾーン プロファイル (Zone profile) ([詳細設定 (Advanced)] セクション)	[Cisco Unified Communications Manager] または [カスタム モード (Custom mode)] を選択します。 カスタム モードは BFCP 動作を有効にするため、または TLS を使用するときに必要な場合があります。 Cisco Unified Communications Manager 設定での設定内容と、必要な場合のカスタム モードでの設定値の詳細については、「付録 7 : Cisco Unified Communications Manager の [詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] で設定されたパラメータ」を参照してください。

注 : これにより、Cisco VCS Control で CUCM との通信に TCP を介した SIP が使用されるように設定されます。TLS を使用する場合、TCP に対してここに示すとおりの実行し、「付録 8 : TCP でなく TLS を使用した Cisco VCS の CUCM への接続」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。

Status System **VCS configuration** Applications Maintenance

You are here: [VCS configuration](#) > [Zones](#) > [Zones](#) > [Create zone](#)

Create zone

Configuration

Name * CUCM Neighbor ⓘ

Type * Neighbor ⓘ

Hop count * 15 ⓘ

H.323

Mode Off ⓘ

Port * 1719 ⓘ

SIP

Mode On ⓘ

Port * 5060 ⓘ

Transport TCP ⓘ

Accept proxied registrations Deny ⓘ

Media encryption mode Auto ⓘ

Authentication

Authentication policy Do not check credentials ⓘ

SIP authentication trust mode Off ⓘ

Location

Peer 1 address 10.1.2.22 ⓘ

Peer 2 address ⓘ

Peer 3 address ⓘ

Peer 4 address ⓘ

Peer 5 address ⓘ

Peer 6 address ⓘ

Advanced

Zone profile Cisco Unified Communications Manager ⓘ

Create zone Cancel

CUCM ネイバーゾーンにコールをルーティングする検索ルールの作成

検索ルールによって、このネイバー CUCM が処理する電話番号および 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。

この実装では、上記の「トランスフォーメーションの作成」セクションでのトランスフォームの設定は、ダイヤル文字列が URI フォーマットの **number@vcs.domain** であることを確認済みです。CUCM ではダイヤル番号が 3xxx@<IP address of CUCM> のフォームである必要があるため、3xxx@vcs.domain のアドレスの CUCM へのコールを、そのフォーマットに変換するトランスフォームが必要です。

1. [VCS 設定 (VCS 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. 着信 ID を **3xxx@vcs.domain** のフォーマットから **3xxx@<IP address of CUCM>** に変換し、コールを CUCM にルーティングするため、フィールドを次のように設定します。

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)	いずれか (Any)
ソース (Source)	いずれか (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)	(3\d{3})@vcs.domain(.*)
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	\1@<ip address of CUCM>\2、たとえば \1@10.1.2.22
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。

The screenshot shows the 'Create search rule' configuration page in the Cisco VCS web interface. The form fields are as follows:

- Rule name: Route to CUCM
- Description: Send 3xxx@vcs.domain calls to CUCM
- Priority: 100
- Protocol: Any
- Source: Any
- Request must be authenticated: No
- Mode: Alias pattern match
- Pattern type: Regex
- Pattern string: (3\d{3})@vcs.domain(.*)
- Pattern behavior: Replace
- Replace string: \1@10.1.2.22
- On successful match: Stop
- Target: CUCM Neighbor
- State: Enabled

Buttons at the bottom: Create search rule, Cancel

詳細については、『Cisco VCS Administrator Guide』の「Zones and Neighbors」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

CUCM から Cisco VCS へのコールが発信されると、コールバック アドレスが number@<ip address of cucm> として示されます。Cisco VCS がこれを CUCM にルーティングするため、ドメイン部分の IP アドレスは削除され、ビデオ ドメインが追加される必要があります。これにより、既存の検索ルールでコールを CUCM にルーティングできます。

1. [VCS 設定 (VCS configuration)] > [ダイヤル プラン (Dial plan)] > [トランスフォーメーション (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 CUCM>(: ;).*?
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. [トランスフォーメーションの作成 (Create transform)] をクリックします。

The screenshot shows the 'Create transform' configuration page in the Cisco VCS web interface. The breadcrumb trail is 'VCS configuration > Dial plan > Transforms > Create transform'. The form contains the following fields and values:

- 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

Buttons for 'Create transform' and 'Cancel' are visible at the bottom of the form.

テスト コール

必要な CUCM 内線番号 (3xxx) を Cisco VCS エンドポイントでダイヤルすることで、Cisco VCS Control に登録されたエンドポイントから、CUCM 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。

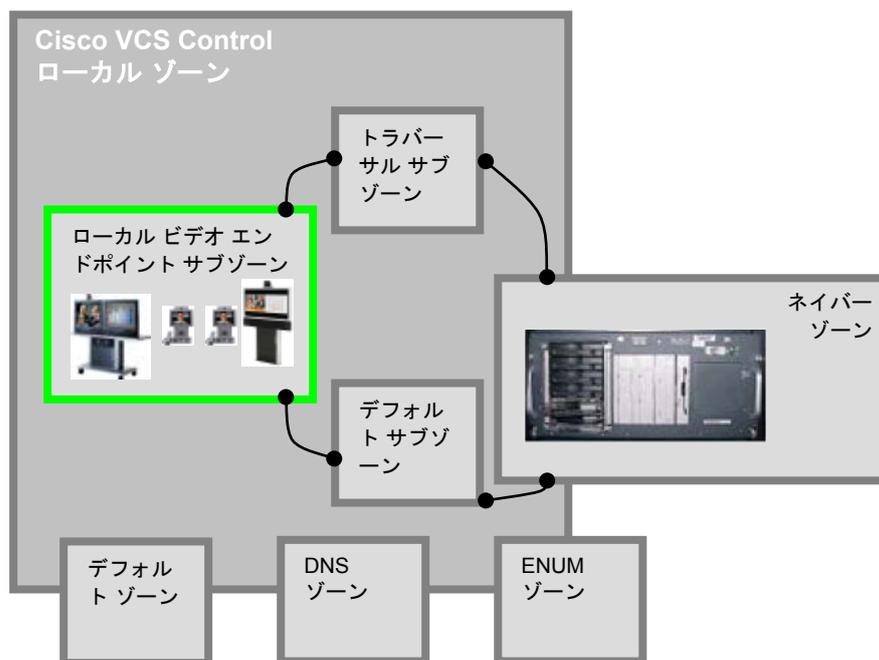
Cisco VCS に登録されたエンドポイントは、CUCM に登録されたエンドポイントの 3000 などの内線番号をダイヤルします。

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

Cisco VCS Control の設定

Cisco VCS Control の設定は次の 2 段階の手順に従います。

- CUCM によって付加される着信ドメイン情報を取得する検索ルール (VCS:IP ポートの IP アドレス) を使用して Cisco VCS Control を設定し、登録されたエンドポイントが使用する SIP ドメインに変換し、コールをローカルゾーンにルーティングします。エンドポイントは 11 桁のフル電話番号で登録されるため、トランスフォームは受信した短い 4 桁の番号を 11 桁のフル電話番号に拡張する必要があります。
- (X7.0 以降) VCS が CUCM とのコールのシグナリングパスに留まることを確認します。これにより、CUCM はそのシグナリングメッセージが SIP トランクを介してビデオネットワークに転送される必要があることを識別できます。



Cisco VCS のローカルおよびネイバゾーンをコールするための CUCM のトランスフォームの設定

このトランスフォームは CUCM から受信した URI を VCS のローカルゾーンで使用するフォーマットに変換し、ネイバゾーン内で想定されるフォーマットに合わせられます。

注: このルールは、CUCM から受信する URI と一致しており、(0118912)?(4xxx@<ip address of vcs>:<port>) から 01189124xxx@vcs.domain にトランスフォームされる必要があります。

1. [VCS 設定 (VCS configuration)] > [ダイヤル プラン (Dial plan)] > [トランスフォーメーション (Transforms)] に移動します。
2. [新規 (New)] をクリックします。

注: この検索ルールでは、URI へのすべてのコールが **(0118912)?(4\d{3})@<IP address of VCS>:<port>** のフォーマットで処理され、0118912\2@vcs.domain にトランスフォームされます。たとえば、このシナリオでは、01189124000@10.44.9.214:5060 は 01189124000@vcs.domain に変換され、4000@10.44.9.214:5060 は 01189124000@vcs.domain に変換されます。

3. フィールドを次のように設定します。

説明 (Description)	CUCM から登録デバイス
プライオリティ (Priority)	5 (たとえば、このトランスフォームのプライオリティは、ローカルゾーンおよびネイバーゾーンを検索するための適用するトランスフォームよりも上である必要がある)
パターンタイプ (Pattern type)	Regex
パターン文字列 (Pattern string)	たとえば、(0118912)?(4\d{3})@%ip%(:.*)?
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	0118912\2@vcs.domain
状態 (State)	有効 (Enabled)

4. [トランスフォーメーションの作成 (Create transform)] をクリックします。

The screenshot shows the 'Create transform' configuration page in the Cisco VCS web interface. The breadcrumb trail indicates the path: VCS configuration > Dial plan > Transforms > Create transform. The configuration fields are as follows:

- Priority: 5
- Description: CUCM to registered devices
- Pattern type: Regex
- Pattern string: (0118912)?(4\d{3})@%ip%(:.*)?
- Pattern behavior: Replace
- Replace string: 0118912\2@vcs.domain
- State: Enabled

Buttons for 'Create transform' and 'Cancel' are visible at the bottom of the form.

VCS が CUCM とのコールのシグナリングパスに留まることの確認

GRUU を使用してコールを処理するには、コンタクトアドレスが IP アドレスでなく、コンタクト IP が CUCM でルーティング可能でない場合 (Multiway が使用されており、MCU が VCS に登録されているときなど)、コールシグナリングが適切にルーティングされるようにするには、VCS はシグナリングパスに留まる必要があります。これは、ゾーンプロファイルを次のようにすることで設定できます。

- VCS がバージョン X7.0.n の場合、CUCM ネイバーゾーンに移動して次のように設定します。

- a. [詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] を [Cisco Unified Communications Manager] から [カスタム (Custom)] に変更します。
 - b. 「付録 7 : Cisco Unified Communications Manager の [詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] で設定されたパラメータ」の記述のとおりパラメータを設定します。
 - c. [コール シグナリング ルーティング モード (Call signaling routed mode)] を [常時 (Always)] に設定します。
- VCS がバージョン X7.1 以降の場合、これらの設定はデフォルトで *Cisco Unified Communications Manager* のゾーン プロファイルに適用されるため、これを変更する必要はありません。

CUCM の設定

シスコの電話機から Cisco VCS への番号によるダイヤルの許可

CUCM 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。

01189124xxx および 4xxx としてダイヤルされたコールを 4xxx として Cisco VCS にルーティングするように CUCM を設定するには、次の手順を実行します。

1. CUCM 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. [ルートパターン (Route Pattern)] を上記のように設定し、01189124xxx にダイヤルされたコールを、最初の 0118912 を除去して 4xxx を残した後に、Cisco VCS トランクにルーティングします。

パターン定義を次のように設定します。

ルートパターン (Route Pattern)	0118912.4XXX
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 01189 124 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)	Cisco 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
コール分類 (Call Classification)	OnNet
外部ダイヤル トーンの提供 (Provide Outside Dial Tone)	オフ

着信側トランスフォーメーションを次のように設定します。

番号の削除 (Discard Digits)	PreDot
------------------------	--------

4. 4xxx にダイヤルされたコールを、ダイヤル番号を変更せずに、Cisco VCS トランクにルーティングするように、2 番目の [ルートパターン (Route Pattern)] を設定します。

パターン定義を次のように設定します。

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)	Cisco 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
コール分類 (Call Classification)	OnNet

外部ダイヤル トーンの提供 (Provide Outside Dial Tone)	オフ
着信側トランスフォーメーションを次のように設定します。	
番号の削除 (Discard Digits)	< なし > (< None >)

The screenshot shows the Cisco Unified CM Administration interface for configuring a route pattern. The main configuration area is titled "Route Pattern Configuration" and includes the following sections:

- Status:** Status: Ready
- Pattern Definition:**
 - Route Pattern*: 0118912.4XXX
 - Route Partition: LABCM6
 - Description: Route 01189 124 xxx to VCS SIP trunk
 - Numbering Plan: -- Not Selected --
 - Route Filter: < None >
 - MLPP Precedence*: Default
 - Gateway/Route List*: VCS_Ruscombe (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: [Empty]
 - Prefix Digits (Outgoing Calls): [Empty]
 - 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: PreDot
 - Called Party Transform Mask: [Empty]
 - Prefix Digits (Outgoing Calls): [Empty]
- ISDN Network-Specific Facilities Information Element:**
 - Network Service Protocol: -- Not Selected --
 - Carrier Identification Code: [Empty]
 - Network Service: -- Not Selected --
 - Service Parameter Name: < Not Exist >
 - Service Parameter Value: [Empty]

At the bottom, there are buttons for Save, Delete, Copy, and Add New. A note indicates that an asterisk (*) denotes a required item.

シスコの電話機から Cisco VCS ドメインへのダイヤルの許可

ドメイン `vcs.domain` など、Cisco VCS SIP トランクに送信するために必要な情報を CUCM 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. CUCM 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)
パターン (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)	Cisco 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。

CUCM に登録されたエンドポイントによって NNNN@vcs.domain がダイヤルされた場合、CUCM はそのコールを NNNN@<IP address of VCS>:5060 (TCP) または NNNN@<IP address of VCS>:5061 (TLS) として VCS にルーティングします。

これで、CUCM から、01189124xxx@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

4 桁の内線番号 4xxx および 11 桁のフル電話番号 01189124xxx をダイヤルすることで、CUCM 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にテスト コールを発信します。

CUCM に登録されたエンドポイントで、そのエンドポイントの 4 桁の内線番号と 11 桁のフル番号、たとえば 4000 と 01189124000 をダイヤルします。

詳細設定

CUCM SIP 最大着信メッセージ サイズ

ビデオの SIP メッセージは、音声コールの SIP メッセージよりもかなりサイズが大きくなります。特に、Cisco TelePresence Server がビデオ ネットワークに使用されている場合、SIP メッセージは、CUCM 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 バイトよりも大きいことがあります。

CUCM の [SIP 最大着信メッセージ サイズ (SIP Max Incoming Message Size)] を増やすには、次の手順を実行します。

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)] を選択します。
5. [デバイス (Device)] > [SIP] の [クラスタワイド パラメータ (Clusterwide Parameters)] で、フィールド次のように設定します。

SIP 最大着信メッセージ サイズ (SIP Max Incoming Message Size)	12000
--	-------

SIP Station UDP Port Throttle Threshold *	50	50
SIP Trunk UDP Port Throttle Threshold *	200	200
SIP V.150 Outbound SDP Offer Filtering *	No Filtering	No Filtering
SIP Max Incoming Message Size *	12000	5000
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

6. [保存 (Save)] をクリックします。

付録 1：トラブルシューティング

Cisco VCS Control のローカル コールへの接続の問題

[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。
要約に、コールの発信元と宛先のエイリアスと、宛先のエイリアスが見つかっ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
 - コールを受け入れられるゾーンが見つかるまで、または優先順位が付けられた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)

これは、Cisco VCS Control のゾーン リンクが適切に設定されていないことが原因の可能性がありま
す。コマンドラインから、次のように実行します。

```
xcommand DefaultLinksAdd
```

Cisco VCS Control のデフォルト ゾーンのために必要なリンクを設定します。また、作成されている
他のゾーンのリンクも確認します。

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 検索では、リンクまたはリンク帯域幅は考慮されず、リンクが存在しない、またはリンク帯域
幅が十分でない場合、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。

[検索履歴 (Search history)] でのコール進捗の確認

1. [ステータス (Status)] > [検索履歴 (Search history)] に移動します。
要約に、コールの発信元と宛先のエイリアスと、コール所要時間およびコールが SIP、H.323、または SIP< -->H.323 インターワーキング コールのいずれであるかが示されます。
2. 関連するコールの試行を選択します。
エントリには発着信コール レッグの詳細、コールのステータス、Cisco VCS Control がコールのルーティングに使用するゾーンが示されます。

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

SIP / H.323 レベルでのコールのトレース

X7 以降の場合、次の手順を実行します。

1. admin として Cisco VCS Control Web インターフェイスにログインします。
2. [メンテナンス (Maintenance)] > [診断 (Diagnostics)] > [診断ログ (Diagnostics logging)] に移動します。
3. ログレベルはすべて [デバッグ (DEBUG)] に送信されることを確認し、[新しいログの開始 (Start new log)] をクリックします。
4. コールの設定など、問題が発生した操作を再試行します。
5. [ログの停止 (Stop logging)] をクリックし、[ログのダウンロード (Download log)] をクリックします。

ログ ファイルに、ステップ 4 で実行した操作でトリガーされたイベントに関する情報が格納されます。

H.323 から SIP CUCM へのコールが動作しない

422 セッション タイマーが小さすぎます (422 Session Timer too small)

H.323 から SIP へのコールをインターワークするときに、X4 以前のバージョンの Cisco VCS が SIP を処理せず、CUCM から「422 セッション タイマーが小さすぎます (422 Session Timer too small)」という応答が返されます。H.323 コールが SIP コールから CUCM へインターワークされる場合、CUCM は「422 セッション タイマーが小さすぎます (422 Session Timer too small)」というメッセージを送信し、Cisco VCS はコールを消去します。

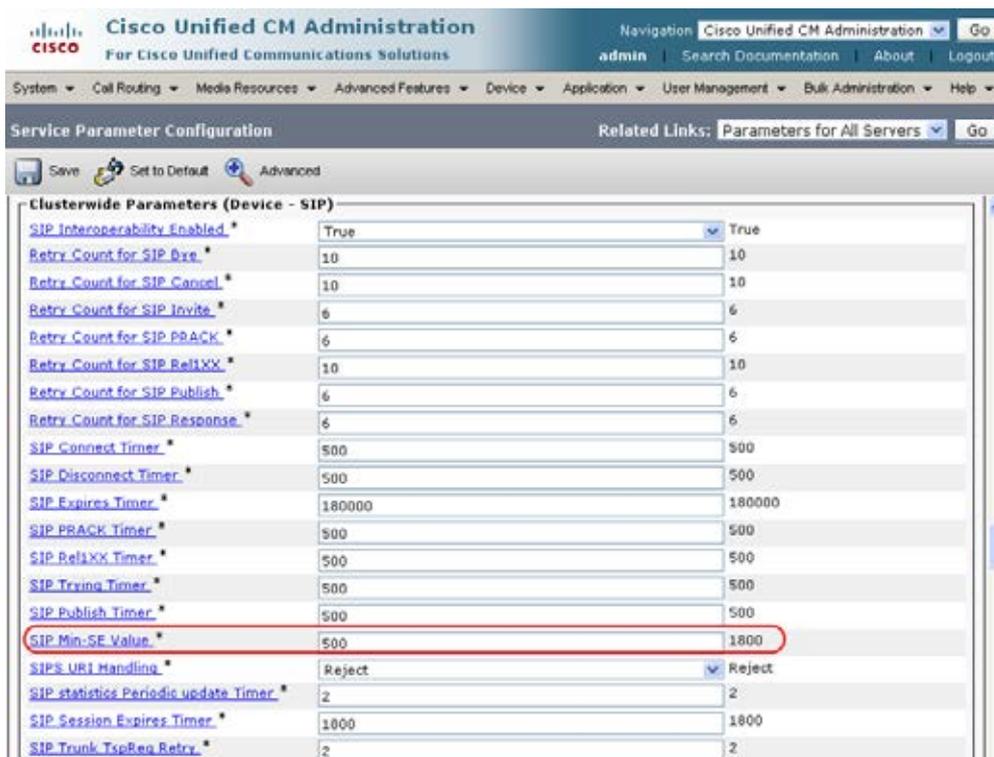
X5.0 以降、ネイバー ゾーンを Cisco Unified Communications Manager に設定することで、Cisco VCS は CUCM と交換されるセッション タイマーを処理できるようになり、以下に示す CUCM での設定の変更は必要なくなります。

Cisco VCS コードの X4.x 以前のバージョンでは、この問題の回避方法は、エンドポイントに要求される値と一致するセッションの最小タイムアウト値をサポートするように CUCM を設定することです。

ビデオ エンドポイントは、通常セッションのタイムアウト値 500 を要求し、CUCM のデフォルトの Min-SE（セッションの最小タイムアウト値）は 1800 です。

CUCM に 500 以下のセッションの最小タイムアウト値を設定するには、次の手順を実行します。

1. [システム (System)] > [サービス パラメータ (Service Parameters)] に移動します。
2. [サーバ (Server)] として、たとえば <IP> (アクティブ) (<IP> (Active))] などの現在のサーバを選択します。
3. [サービス (サービス)] として [Cisco CallManager (アクティブ) (Cisco CallManager (Active))] を選択します。
4. [SIP Min-SE 値 (SIP Min-SE Value)] を探し、500 に設定します。
5. [保存 (Save)] をクリックします。



Cisco TelePresence Server とのコールの失敗

Cisco TelePresence Server からの SIP メッセージは、CUCM 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 バイトよりも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)] を増やすには、「CUCM SIP 最大着信メッセージ サイズ」を参照してください。

In-Call の問題

コールは最大 15 分間まで維持される

CUCM バージョン 8.0 以前から、CallerID が FindMe ID に設定された Cisco VCS FindMe に対してコールが発信される場合、CUCM は Cisco VCS から送信されたセッション リフレッシュ メッセージ

を処理せず（メッセージには更新された From: ヘッダーが含まれる）、そのためにセッションのリフレッシュに失敗し、コールはセッション リフレッシュ タイマーによって消去されます。

CUCM のバージョンが 8.0 より後の場合、この問題は発生しません。

CUCM のビデオ電話機から VCS にコールが転送がされるときに、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、CUCM および Cisco 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 CUCM 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、CUCM は 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、CUCM の CUCM から Cisco VCS への SIP トランクで、DTMF シグナリング方式が [RFC 2833] に設定されていることを確認します。

Multiway を使用した CUCM エンドポイントの会議への参加が失敗する

VCS および CUCM が「付録 5 : Cisco TelePresence Multiway および CUCM」の説明のとおりを設定されていることを確認します。

RTMT を使用する CUCM でのトレースの取得

RTMT はシステムの状態の監視や、CUCM 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。CUCM 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 CUCM の設定

1. CUCM 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 CUCM 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. [検索（Find）] で [指定の名前で始まる（Name begins with）] の <空白> および [かつプラグインタイプが次に等しい（Plugin Type equals）] の [インストール（Installation）] 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。

- 完了したら、[完了 (Done)] をクリックして、インストールを完了します。

RTMT の実行

- RTMT を実行します。
たとえば、Windows の場合、[スタート (Start)] > [すべてのプログラム (All Programs)] > [Cisco] > [CallManager 有用性 (CallManager Serviceability)] > [Real-Time Monitoring Tool] にあります。
- ログイン 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。
- [OK] をクリックします。

RTMT を使用するトレースの取得

- [Trace & Log Central] を選択します。
- [リアルタイムトレース (Real Time Trace)] をダブルクリックします。
- [リアルタイムデータ (Real Time Data)] をダブルクリックします。
- トレースを取得する CUCM インスタンスが実行されているノードを選択します。
- [次へ (Next)] をクリックします。
- 次を選択します。
 - [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]
- [終了 (Finish)] をクリックします。

次の点に注意してください。

- 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。

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、CUCM に登録されたエンドポイントに対し、Cisco VCS Control 経由でコールを発信できます。
- CUCM に登録されたエンドポイントは、Cisco VCS Control 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。

Cisco TelePresence Conductor

Cisco VCS が Conductor と連動するように構成されている場合、CUCM から SIP トランク上に発信されるコールは、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。

制限事項

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、CUCM 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 CUCM 8.0 以前に対して発信された場合、CUCM 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 [オフ (Off)] に設定されている場合、BFCP が提供されない場合、CUCM 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

Cisco VCS に登録された MXP が、CUCM 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 : CUCM の Cisco VCS ピアのクラスタへの接続

CUCM バージョン 8.5 以降、CUCM を Cisco VCS ピアのクラスタに接続するには、CUCM に VCS クラスタ ピアのアドレスを提供する次の 2 種類の方法があります。

- 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

CUCM 8.5 より前のバージョンでは、VCS へのトランクに、Cisco VCS クラスタの DNS SRV アドレスを指定する 1 種類の方法のみでした。

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

CUCM が使用する DNS サーバに、Cisco 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、各ピアに同じ優先順位と同じ重み付け値が設定されている必要があります。

1. CUCM 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. [SIP 情報 (SIP Information)] セクションにスクロールします。
4. [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)	このチェックボックスをオンにします。
接続先アドレス (Destination address)	<DNS SRV name of VCS cluster>

5. [保存 (Save)] をクリックします。
6. [リセット (Reset)] をクリックします。
7. [リセット (Reset)] をクリックします。

The screenshot displays the 'SIP Trunk Configuration' page in Cisco Unified CM Administration. The configuration is for a SIP Trunk named 'VCS at Ruscombe'. Key settings include:

- Device Information:** Product: SIP Trunk; Device Protocol: SIP; Device Name: VCS_Ruscombe; Description: VCS at Ruscombe; Device Pool: LABCM5; Common Device Configuration: < None >; Call Classification: Inlet; Media Resource Group List: < None >; Location: Region LABCM5 AS1; AAR Group: < None >; Packet Capture Mode: None; Packet Capture Duration: 0.
- Multilevel Precedence and Preemption (MLPP) Information:** MLPP Domain: < None >.
- Call Routing Information:**
 - Inbound Calls:** Significant Digits: All; Connected Line ID Presentation: Default; Connected Name Presentation: Default; Calling Search Space: LABCM5; AAR Calling Search Space: < None >; Prefix DN: (empty).
 - Outbound Calls:** Calling Party Selection: Originator; Calling Line ID Presentation: Default; Calling Name Presentation: Default; Caller ID DN: (empty); Caller Name: (empty).
- SIP Information:** Destination Address: 10.44.9.214; Destination Port: 5040; RTP Preferred Originating Codec: G.711ulaw; Presence Group: Standard Presence group; SIP Trunk Security Profile: Non Secure SIP Trunk Profile; Resulting Calling Search Space: < None >; Out-Of-Dialog Refer Calling Search Space: < None >; SUBSCRIBE Calling Search Space: < None >; SIP Profile: Standard SIP Profile; DTMF Signaling Method: No Preference.

8. VCS で、[VCS 設定 (VCS configuration)] > [プロトコル (Protocols)] > [SIP] > [ドメイン (Domains)] のクラスタ名が、SIP ドメインとして設定されていることを確認します。

Cisco 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. CUCM 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. [SIP 情報 (SIP Information)] セクションにスクロールします。

4. [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)	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。
接続先アドレス 1 (Destination address 1)	VCS ピア 1 の IP アドレスまたは DNS 名
接続先ポート 1 (Destination port 1)	接続 (TCP または TLS) に応じて 5060 または 5061
接続先アドレス 2 (Destination address 2)	VCS ピア 2 の IP アドレスまたは DNS 名
接続先ポート 2 (Destination port 2)	接続 (TCP または TLS) に応じて 5060 または 5061
接続先アドレス 3 (Destination address 3)	VCS ピア 3 がある場合、その IP アドレスまたは DNS 名
接続先ポート 3 (Destination port 3)	接続 (TCP または TLS) に応じて 5060 または 5061
接続先アドレス 4 (Destination address 4)	VCS ピア 4 がある場合、その IP アドレスまたは DNS 名
接続先ポート 4 (Destination port 4)	接続 (TCP または TLS) に応じて 5060 または 5061
接続先アドレス 5 (Destination address 5)	VCS ピア 5 がある場合、その IP アドレスまたは DNS 名
接続先ポート 5 (Destination port 5)	接続 (TCP または TLS) に応じて 5060 または 5061
接続先アドレス 6 (Destination address 6)	VCS ピア 6 がある場合、その IP アドレスまたは DNS 名
接続先ポート 6 (Destination port 6)	接続 (TCP または TLS) に応じて 5060 または 5061

追加の接続先アドレス エントリを取得するには、[+] を選択します。

5. [保存 (Save)] をクリックします。
6. [リセット (Reset)] をクリックします。
7. [リセット (Reset)] をクリックします。

付録 4 : Cisco VCS の CUCM ノードのクラスタへの接続

Cisco VCS を CUCM ノードのクラスタに接続するときに、Cisco VCS は、それらの各 CUCM ノードに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 3 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 CUCM ノードがある VCS 内の単一のネイバーゾーンを使用します。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 Cisco VCS DNS ゾーンを使用します。
3. CUCM ノードごとに 1 つの複数のゾーンを設定し、コールを任意の順序で各ゾーンにルーティングする優先順位を付けた検索ルールを設定します（優先順位の値は検索ルールごとに異なる）。

オプション 1 と 2 は、Cisco VCS から CUCM へのコールの負荷が CUCM ノード間で確実に共有されるため、推奨されます。オプション 3 でのみ、冗長性が提供されます。負荷分散は提供されません。

オプション 1 : 単一のネイバーゾーンの使用

このオプションは、バージョン X7.0 以降を実行する Cisco VCS に対してのみ使用できます。

CUCM の設定

クラスタ内では、CUCM は `number@<ip address of CUCM>` 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、Cisco 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 CUCM に送信できます。

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。

Clusterwide Domain Configuration	
Organization Top Level Domain	<input type="text"/>
Cluster Fully Qualified Domain Name	<input type="text"/>

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。

Cisco VCS Control の設定

Cisco VCS の設定には次の 1 段階の手順が必要です。

- ネイバーゾーンの更新

ネイバーゾーンの更新

1. [VCS 設定 (VCS configuration)] > [ゾーン (Zones)] に移動します。

2. CUCM 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。

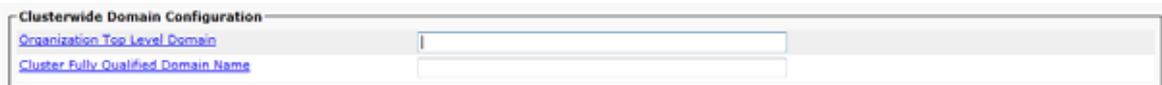
ピア 1 アドレス (Peer 1 address)	CUCM ノード 1 の IP アドレス、または CUCM ノード 1 のドメイン
ピア 2 アドレス (Peer 2 address)	CUCM ノード 2 の IP アドレスまたはドメイン
ピア 3 アドレス (Peer 3 address)	CUCM ノード 3 の IP アドレスまたはドメイン、または CUCM ノード 3 がない場合は空白
ピア 4 アドレス (Peer 4 address)	CUCM ノード 3 の IP アドレスまたはドメイン、または CUCM ノード 4 がない場合は空白
ピア 5 アドレス (Peer 5 address)	CUCM ノード 3 の IP アドレスまたはドメイン、または CUCM ノード 5 がない場合は空白
ピア 6 アドレス (Peer 6 address)	CUCM ノード 3 の IP アドレスまたはドメイン、または CUCM ノード 6 がない場合は空白

オプション 2 : DNS ゾーンの使用

CUCM の設定

クラスタ内では、CUCM は number@<ip address of CUCM> 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、Cisco 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 CUCM に送信できます。

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。

DNS サーバの設定

CUCM クラスタのための DNS SRV レコードを使用し、DNS サーバ (Cisco VCS が使用) を設定します。

- `_sips._tcp.fqdn_of_cucm_cluster` TLS 接続のレコード (各 CUCM ノードにつき 1 つのレコード)
または
- `_sip.tcp.fqdn_of_cucm_cluster` TCP 接続のレコード (各 CUCM ノードにつき 1 つのレコード)

Cisco VCS Control の設定

Cisco VCS の設定には次の 3 段階の手順が必要です。

- CUCM DNS ゾーン作成
- 検索ルールの調整
- 古い CUCM ネイバー ゾーン削除

CUCM DNS ゾーン作成

1. [VCS 設定 (VCS configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] 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。

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 CUCM との通信には不要)
SIP モード (SIP mode)	オン (On)
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)	自動 (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)	[Cisco Unified Communications Manager] を選択します。 この設定での設定内容詳細については、「付録 7 : Cisco Unified Communications Manager の [詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] で設定されたパラメータ」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。

Status System **VCS configuration** Applications Maintenance

You are here: [VCS configuration](#) > [Zones](#) > [Zones](#) > Create zone

Create zone

Configuration

Name * CUCM Cluster Neighbor DNS Zone ⓘ

Type * DNS ⓘ

Hop count * 15 ⓘ

H.323

Mode Off ⓘ

SIP

Mode On ⓘ

TLS verify mode Off ⓘ

Media encryption mode Auto ⓘ

Advanced

Include address record Off ⓘ

Zone profile Cisco Unified Communications Manager ⓘ

Create zone Cancel

検索ルールの調整

この CUCM 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。また、IP アドレスを使用する代わりに、ドメインを DNSSRV レコードで使用するよう設定します。

検索ルールは、このネイバー CUCM が処理する電話番号および URI の範囲を指定するために使用されます。また、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。

この実装では、「トランスフォーメーションの作成」セクションで設定したトランスフォームは、ダイヤル文字列が URI フォーマットの [number@vcs.domain](#) であることを確認済みです。以前の手順のとおり、CUCM ではダイヤル番号 3xxx@<IP address of CUCM> のフォームである必要があります。トランスフォームによって、CUCM へのコールは 3xxx@vcs.domain からそのフォームに変換されます。このトランスフォームは不要です。

1. [VCS 設定 (VCS 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「CUCM へのルート」検索ルールを選択します。
3. フィールドを次のとおりに変更して、着信 ID は **3xxx@vcs.domain** のフォーマットのまま、CUCM へのコールをルーティングします。グレー表示のフィールドは既存の値のままです。

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
ソース (Source)	いずれか (Any)
リクエストは認証される必要がある (Request must be authenticated)	いいえ (No)

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)	(3\d{3})@vcs.domain(.*)
パターン動作 (Pattern behavior)	変更なし (Leave)
正常に一致する場合 (On successful match)	停止 (Stop)
転送先ゾーン (Target zone)	CUCM クラスタ ネイバー DNS ゾーン
状態 (State)	有効 (Enabled)

4. [保存 (Save)] をクリックします。

The screenshot shows the 'Edit search rule' configuration page in the Cisco VCS administration console. The configuration is as follows:

- Rule name: * Route to CUCM
- Description: Send 3xxx@vcs.domain calls to CUCM
- Priority: * 100
- Protocol: Any
- Source: Any
- Request must be authenticated: No
- Mode: Alias pattern match
- Pattern type: Regex
- Pattern string: *(3\d{3})@vcs.domain(.*)
- Pattern behavior: Leave
- On successful match: Stop
- Target: * CUCM Cluster Neighbor DNS Zone
- State: Enabled

Buttons at the bottom: Save, Delete, Cancel

詳細については、『Cisco VCS Administrator Guide』の「Zones and Neighbors」を参照してください。

古い CUCM ネイバー ゾーンの削除

使用しないネイバー ゾーン「CUCM ネイバー」を削除します。

1. [VCS 設定 (VCS configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] に移動します。
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。

オプション 3 : 複数のネイバー ゾーンの使用

このオプションでのみ、冗長性が提供されます。負荷分散は提供されません。

Cisco VCS Control の設定

- ネイバー ゾーンの複製
- 検索ルールの複製

ネイバー ゾーンの複製

各 CUCM ノードの [名前 (Name)] および [ピア 1 アドレス (Peer 1 address)] を調整しながら、単一の CUCM ピア用に各ノードにつき 1 つ作成したネイバー ゾーンを複製します。

検索ルールの複製

[プライオリティ (Priority)] および [ターゲット (Target)] を調整しながら、単一の CUCM ピア用に各ノードにつき 1 つ作成した検索ルールを複製します。こうすることで、各検索ルールの対象がそれぞれの CUCM ネイバー ゾーンになります。

付録 5 : Cisco TelePresence Multiway および CUCM

CUCM 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、次の手順を実行します。

1. [コール シグナリング ルーティング モード (Call signaling routed mode)] が [常時 (Always)] に設定されているゾーン プロファイルが、VCS で CUCM へのゾーンに使用されていることを確認します。
2. ルート パターンを使用して、Multiway エイリアスで指定されたドメインがある VCS に対し、CUCM がコールをルーティングすることを確認します。
3. VCS への SIP トランクが使用する SIP プロファイルの [アプリケーションによるリダイレクト (Redirect by Application)] がオンになった状態で、CUCM が設定されていることを確認します。

VCS の設定

Cisco VCS X7.0.n が使用されている場合、またはカスタム ゾーン プロファイルが使用されている場合、Cisco VCS で CUCM ネイバー ゾーンに移動し、次の手順を実行します。

1. [詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] を [Cisco Unified Communications Manager] から [カスタム (Custom)] に変更します。
2. 「付録 7 : Cisco Unified Communications Manager の [詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] で設定されたパラメータ」の記述のとおりパラメータを設定します。
3. [コール シグナリング ルーティング モード (Call signaling routed mode)] が [常時 (Always)] に設定されていることを確認します。

CUCM の設定

ビデオ ドメインがある VCS に対し、CUCM がコールをルーティングすることを確認します。

1. 「エラー! 参照元が見つかりません。」の指示に従って操作します。

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. [保存 (Save)] をクリックします。
4. [設定の適用 (Apply Config)] をクリックします。
5. [OK] をクリックします。

SIP Profile Information	
Name*	Standard SIP Profile
Description	Default SIP Profile
Default MTP Telephony Event Payload Type*	101
Resource Priority Namespace List	< None >
Early Offer for G.Clear Calls*	Disabled
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	TIAS and AS
User-Agent and Server header information*	Send Unified CM Version Information as User-Agen
<input checked="" type="checkbox"/> Redirect by Application	
<input type="checkbox"/> Disable Early Media on 180	
<input type="checkbox"/> Outgoing T.38 INVITE include audio mline	
<input type="checkbox"/> Enable ANAT	
<input type="checkbox"/> Require SDP Inactive Exchange for Mid-Call Media Change	
<input type="checkbox"/> Use Fully Qualified Domain Name in SIP Requests	
<input checked="" type="checkbox"/> Allow Presentation Sharing using BFCP	

これで、Multiway をテストできます。

付録 6 : エンドポイント固有の設定

L6.x を実行する T150

T150 でデュアル ビデオが有効化されていることが原因で、7960 が T150 からのコールに応答するときにコールがドロップします。

T150 のデュアル ビデオを無効にするには、次のように設定します。

- [xConfiguration Conference H239] : [オフ (Off)]

その他の製品

Cisco VCS に登録されているデバイスに関し、エンドポイント設定に固有のその他の既知の要件はありません。

付録 7 : Cisco Unified Communications Manager の [詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] で設定されたパラメータ

Cisco Unified Communications Manager の [ゾーン プロファイル (Zone profile)] を選択し、次のように [詳細設定 (Advanced)] ゾーンパラメータを設定します。

パラメータ	値
ピア ステータスのモニタ (Monitor peer status)	Yes
コール シグナリングルーティング モード (Call signaling routed mode)	Always (X7.1 よりも前のバージョンの VCS では [自動 (Auto)])
H.323 検索に自動的に応答 (Automatically respond to H.323 searches)	Off
SIP 検索に自動的に応答 (Automatically respond to SIP searches)	Off
空の INVITE が許可されています (Empty INVITE allowed)	On
SIP Poison モード (SIP poison mode)	Off
SIP 暗号化モード (SIP encryption mode)	Auto
SIP SDP 属性回線制限モード (SIP SDP attribute line limit mode)	Off
SIP SDP 属性回線制限の長さ (SIP SDP attribute line limit length)	130
SIP マルチパート MIME 削除モード (SIP multipart MIME strip mode)	Off
SIP UPDATE 削除モード (SIP UPDATE strip mode)	Off (X7.2 よりも前のバージョンの VCS では、互換性の問題のため [オン (On)])
相互接続 SIP 検索戦略 (Interworking SIP Search Strategy)	Options
SIP UDP/BFCP フィルタ モード (SIP UDP/BFCP filter mode)	On
SIP デュオ ビデオ フィルタ モード (SIP Duo Video filter mode)	Off
SIP レコード ルート アドレス タイプ (SIP record route address type)	IP
SIP プロキシ - ヘッダー削除リストが必要 (SIP Proxy-Require header strip list)	<空白>

BFCP の使用

CUCM 8.6.1 以降に登録されたエンドポイントで BFCP を使用するには、[詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] の [カスタム (Custom)] を選択し、[SIP UDP/BFCP フィルタ モード (SIP UDP/BFCP filter mode)] を [オフ (Off)] に変更します。

CUCM で必要になるその他の設定については、「付録 10 : デュアル ビデオまたはプレゼンテーション共有での BFCP の有効化」を参照してください。

VCS X7.0.n 以前の場合の [コール シグナリング ルーティング モード (Call signaling routed mode)] が [常時 (Always)] の使用

Cisco VCS から CUCM に TLS 接続が使用されており、VCS にオプションのルーティングが設定されている場合、ネットワーク上のすべての VCS に対する証明書を信頼するように CUCM を設定するか、[詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] の [カスタム (Custom)] を選択して上記のようにエントリを設定し、[コール シグナリング ルーティング モード (Call signaling routed mode)] を [常時 (Always)] に変更するか、いずれかを行う必要があります。これにより、CUCM との間のコールで、CUCM に対する VCS ネイバーがコールのシグナリングパスに留まるようにでき、CUCM はこの VCS クラスターの証明書のみを信頼すればよくなります。

[コール シグナリング ルーティング モード (Call signaling routed mode)] を [常時 (Always)] に設定することは、VCS X7.0 以降の場合にエンドポイントが GRUU コンタクトアドレスを使用しているか、ビデオ デバイスの IP アドレスが CUCM に直接ルーティング可能でないときに重要です。また、Multiway のために CUCM と MCU との間でインターフェイスする場合にも、設定する必要があります。VCS がシグナリングパスに留まることで、メッセージングが適切にルーティングされることを保証できます。

暗号化された SRTCP の使用

サードパーティ製エンドポイントとの互換性を最大限にするため、VCS H.323 または SIP のインターワーキング機能は、暗号化されていない SRTCP のみを提供するようにデフォルトで設定されます。この設定は、CUCM に登録された特定のエンドポイント（特に CTS）では許可されませんが、その代わりに、CUCM ゾーン プロファイルで、暗号化された SRTCP を設定できます。

X7.0 以降でカスタム ゾーン プロファイルを設定する場合、管理者コマンドライン インターフェイスで次のように設定する必要があります。

1. admin として ssh を使用して VCS にログインします。
2. 次のコマンドを入力します。
`xconfiguration zones`
3. このコマンドからの出力を使用し、CUCM へのカスタム ゾーンの数値 ID を確認します。たとえば、次の出力では 4 がこの数値です。

```
*c xConfiguration ゾーン ゾーン 4 ネイバー ピア 1 アドレス: "10.1.2.3" (*c  
xConfiguration Zones Zone 4 Neighbor Peer 1 Address: "10.1.2.3")
```

4. 次のコマンドを使用して、前の手順で特定された CUCM ゾーンに割り当てられた数に 4 を変更することで、暗号化された SRTCP の設定を変更します。

```
xConfiguration Zones Zone 4 Neighbor Interworking SIP Encryption EncryptSRTCP:  
Yes
```

付録 8 : TCP でなく TLS を使用した Cisco VCS の CUCM への接続

この手順では、Cisco VCS と CUCM との間で TCP 相互接続がすでに構成されて動作しているシステムを、TCP の代わりに TLS を使用して接続するように変換する方法を説明します。

次の手順が含まれます。

- CUCM が Cisco VCS サーバ証明書を信頼していることの確認
- CUCM での SIP トランク セキュリティ プロファイルの構成
- Cisco VCS への CUCM トランクを TLS を使用するように更新
- CUCM への Cisco VCS ネイバー ゾーンを TLS を使用するように更新
- Cisco VCS 検索ルールをポート 5060 の代わりにポートを 5061 を使用するように更新

CUCM が Cisco VCS サーバ証明書を信頼していることの確認

CUCM が Cisco VCS への TLS 接続を確立するには、CUCM は VCS のサーバ証明書を信頼する必要があります。そのため、CUCM は、代わりに VCS の証明書を信頼するルート証明書を信頼する必要があります。

証明書を認証局 (CA) から取得するための CSR の生成方法の詳細については、『Certificate Creation and Use with Cisco VCS deployment guide』と、プライベート認証局の運用に関する情報を参照してください。

VCS と CUCM の両方が、同じ認証局の有効な証明書を使用してロードされ、ルート CA がすでに CUCM にロードされている場合、これ以上の設定は必要ありません。

CUCM のルート CA 証明書が受け入れる認証局からの証明書が VCS がない場合、次のように、CA を発行する証明書が CUCM にロードされる必要があります。

1. CUCM で、[Cisco Unified OS の管理 (Cisco Unified OS Administration)] を選択し、[移動 (Go)] をクリックしてログインします。
2. [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] に移動し、[証明書のアップロード (Upload Certificate)] に移動します。
3. フィールドを次のように設定します。

証明書の名前 (Certificate Name)	CallManager-trust。
説明 (Description)	必要に応じて説明テキストを入力します。
ファイルのアップロード (Upload File)	[参照 (Browse)] をクリックし、CA 証明書が格納されている .pem 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。
5. [閉じる (Close)] をクリックします。

CUCM での SIP トランク セキュリティ プロファイルの構成

CUCM 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)	このプロファイルが、特定の X.509 名のための暗号化されたプロファイルであることを示す名前を指定します。
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)] を選択します。
着信転送タイプ (Incoming Transport Type)	[TLS] を選択します。
発信転送タイプ (Outgoing Transport Type)	[TLS] を選択します。
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)	証明書内で Cisco VCS によって提供されるサブジェクト名または代替サブジェクト名を指定します (必要に応じて複数の X.509 を追加でき、それぞれの名前はスペース、カンマ、セミコロン、コロンで区切ります)。
着信ポート (Incoming Port)	5061
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。

Cisco VCS への CUCM トランクを TLS を使用するように更新

CUCM 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 Cisco 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。

[デバイス情報 (Device Information)] セクション	
デバイス名 (Device Name)	この名前は、セキュリティ プロファイルの X.509 サブジェクト名に使用されるのと同様に、Cisco VCS 証明書のサブジェクト名と一致している必要があります。
説明 (Description)	必要に応じて更新します。現在これが TLS 接続であることをここに記載できます。

[SIP 情報 (SIP Information)] セクション	
接続先ポート (Destination port)	5061
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. [設定の適用 (Apply Config)] をクリックします。
6. [OK] をクリックします。

CUCM への VCS ネイバーゾーンを TLS を使用するように更新

注: VCS では、CUCM と TCP を介して通信する場合でも、CUCM ゾーンがアクティブであると報告されます。以下の変更は、TLS を介して実行される通信を許可するために必要です。

VCS で次の手順を実行します。

1. [VCS 設定 (VCS configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] に移動し、CUCM へのゾーンを選択し、[ゾーンの編集 (Edit zone)] ページを表示します。
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)	オフ (Off)
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 接続が動作していることを確認します。

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。
 - a. [VCS 設定 (VCS configuration)] > [ゾーン (Zones)] に移動します。
 - b. ゾーンの状態を確認します。
ゾーンがアクティブでない場合、CUCM でトランクを再度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 CUCM 電話機に対してテストコールを発信します。
3. CUCM 電話機から 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。

注 : CUCM 8.0.2 以前のバージョンでは、受信した暗号タグが適切に処理されません。それらの暗号タグが受信されると、CUCM によってコールが消去されることがあります。これが発生する場合、エンドポイントの暗号化をオフに設定します。

VCS のネットワーク

この CUCM 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。

- CUCM はネットワーク上のすべての VCS の証明書を信頼する必要がある
- (X7.0 以降) シグナリングを常時ルーティングするように VCS ネイバー ゾーンを設定する

CUCM へのシグナリングを常時ルーティングする VCS の設定

VCS および CUCM の間の TLS の設定では、ルーティングを最適化するため、通常次のいずれかを行います。

- CUCM はネットワーク上のすべての VCS の証明書を信頼する必要がある
- VCS がバージョン X7.0.n の場合、またはカスタム ゾーンが使用されている場合、CUCM ネイバー ゾーンに移動し、次の手順を実行する
 - a. [詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] を [Cisco Unified Communications Manager] から [カスタム (Custom)] に変更します。
 - b. 「付録 7 : Cisco Unified Communications Manager の [詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] で設定されたパラメータ」の記述のとおりパラメータを設定します。
 - c. [コール シグナリング ルーティング モード (Call signaling routed mode)] を [常時 (Always)] に設定します。

CUCM に登録されたエンドポイントへの暗号化されたコール

CUCM 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、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。

VCS に登録された H.323 エンドポイントから、CUCM に登録された CTS エンドポイントに対し、暗号化されインターワークされたコールを発信するには、カスタム ゾーン プロファイルが BFCP サポートなどの目的で使用されている場合、暗号化された SRTCP モードを設定するための「付録 7 : Cisco Unified Communications Manager の [詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] で設定されたパラメータ」のステップを参照してください。

付録 9 : SIP URI で許可される文字

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 / "-" / "_" / "." / "!" / "~" / "*" / "'"/ "(" / ")" " & " /
"=" / "+" / "\$" / "," / ";" / "?" / "/"

これら以外の文字が必要な場合、"% HexDigit HexDigit" を使用してエスケープ処理する必要があります。

HexDigit HexDigit は、必要な文字の ASCII 値を示します。

たとえば、`firstname%20lastname@company.com` の `%20` はスペース文字です。

付録 10 : デュアル ビデオまたはプレゼンテーション共有での BFCP の有効化

これには、CUCM バージョン 8.6.1 以降が必要です。

VCS の設定

Cisco VCS で CUCM ネイバーゾーンに移動し、次の手順を実行します。

1. [詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] を [Cisco Unified Communications Manager] から [カスタム (Custom)] に変更します。
2. 「付録 7 : Cisco Unified Communications Manager の [詳細設定 (Advanced)] の [ゾーン プロファイル (Zone profile)] で設定されたパラメータ」の記述のとおりパラメータを設定します。
3. [SIP UDP/BFCP フィルタ モード (SIP UDP/BFCP filter mode)] が [オフ (Off)] に設定されていることを確認します。

CUCM の設定

VCS への SIP トランクが使用する SIP プロファイルで、[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)] がオンになっていることを確認します。

CUCM で次のように実行します。

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. [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)] の横のチェックボックスをオンにします。
3. [保存 (Save)] をクリックします。
4. [設定の適用 (Apply Config)] をクリックします。
5. [OK] をクリックします。

SIP Profile Information	
Name*	Standard SIP Profile
Description	Default SIP Profile
Default MTP Telephony Event Payload Type*	101
Resource Priority Namespace List	< None >
Early Offer for G.Clear Calls*	Disabled
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	TIAS and AS
User-Agent and Server header information*	Send Unified CM Version Information as User-Agen
<input checked="" type="checkbox"/> Redirect by Application	
<input type="checkbox"/> Disable Early Media on 180	
<input type="checkbox"/> Outgoing T.38 INVITE include audio mline	
<input type="checkbox"/> Enable ANAT	
<input type="checkbox"/> Require SDP Inactive Exchange for Mid-Call Media Change	
<input type="checkbox"/> Use Fully Qualified Domain Name in SIP Requests	
<input checked="" type="checkbox"/> Allow Presentation Sharing using BFCP	

これで、BFCP の動作をテストできます。

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。

リビジョン	日付	説明
1	2010 年 1 月	初版。
2	2010 年 4 月	Cisco VCS X5.1 用の更新 その他のトラブルシューティング情報
3	2010 年 6 月	付録 10 で TLS を使用した Cisco VCS の CUCM への接続を追加
4	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 CUCM 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
5	2010 年 10 月	クラスタ化された CUCM の追加 CUCM コールバック URI に戻されるコールの処理に関する追加 コール転送の処理のための更新
6	2011 年 3 月	付録 5 の Cisco VCS ピアのクラスタへの CUCM の接続に関する CUCM 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
7	2011 年 6 月	Cisco VCS X6 用の更新
8	2011 年 8 月	Cisco VCS X7.0 および BFCP 用の更新 Cisco VCS の CUCM 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
9	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
10	2012 年 3 月	Cisco VCS X7.1 用の更新
11	2012 年 8 月	Cisco VCS X7.2 用の更新
12	2012 年 9 月	暗号化された SRTP の使用について、付録 7 および付録 8 を改定 このマニュアルは現在 CUCM 8.x および 9.x のみを参照

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。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. その他の商標はそれぞれの権利者の財産です。The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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。

© 2012 Cisco Systems, Inc. All rights reserved.

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先: シスコ コンタクトセンター

0120-092-255(フリーコール、携帯・PHS含む)

電話受付時間: 平日 10:00~12:00、13:00~17:00

<http://www.cisco.com/jp/go/contactcenter/>