



# Cisco TelePresence MCU 45X0、53X0 および MCU MSE 8510 Cisco TelePresence 展開ガイド

---

2012 年 5 月

D14962

**【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/](http://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。

# 目次

<b>概要</b> .....	<b>5</b>
対象読者 .....	5
範囲.....	5
<b>背景説明</b> .....	<b>7</b>
MCU の概要.....	7
会議の開始.....	7
スケジュール済み会議 .....	7
スケジュールされていない会議.....	7
ネットワーク トポロジ.....	8
ベースライン設定.....	8
MCU のセキュリティ保護.....	9
SSL 証明書.....	9
カスケード.....	10
<b>展開方式の選択</b> .....	<b>11</b>
Cisco TelePresence VCS を使用した MCU の展開.....	11
拡張性および復元性 .....	12
既知の制限事項 .....	12
Cisco TelePresence Conductor を使用した MCU の展開 .....	12
拡張性および復元性 .....	13
既知の制限事項 .....	13
Unified CM を使用した MCU の展開.....	14
拡張性および復元性.....	15
既知の制限事項 .....	15
ソリューションの組み合わせ.....	15
展開タイプの概要.....	16
<b>Cisco TelePresence VCS に登録された MCU の展開</b> .....	<b>17</b>
展開の概要.....	17
前提条件 .....	17
マニュアル リスト.....	17
手順の概要.....	18
設定手順 .....	18
手順 1 : ダイヤル プラン .....	18
手順 2 : Cisco VCS の設定 .....	19
手順 3 : MCU のインストールと設定 .....	23
手順 4 : Cisco TMS の設定 .....	29
実装の検証.....	31
<b>Cisco TelePresence Conductor を使用した MCU の展開</b> .....	<b>32</b>
展開の概要.....	32

マニュアル リスト .....	32
<b>Unified CM メディア リソースとしての MCU の展開 .....</b>	<b>33</b>
展開の概要 .....	33
マニュアル リスト .....	33
設定手順 .....	33
手順 1 : MCU を設定する .....	33
手順 2 : Unified CM で会議機能を設定する .....	33
手順 3 : Unified CM で MCU を追加する .....	34
手順 4 : Unified CM でメディア リソース グループ リストを設定する .....	34
手順 5 : Unified CM で、デバイスにメディア リソース グループ リストを割り当てる .....	34
オプション : Unified CM で「Meet Me」サービスを設定する .....	34

## 表

表 1 : ソフトウェア リビジョン .....	5
表 2 : 推奨されるベースライン MCU 設定 .....	8
表 3 : VCS を使用した MCU の展開の機能の概要 .....	11
表 4 : Conductor による MCU の展開の機能の概要 .....	13
表 5 : Unified CM による MCS の展開の機能の概要 .....	14
表 6 : 展開の選択の概要 .....	16
表 7 : 対象機能の概要 .....	17
表 8 : 5 桁を使用したアドレス計画の概要 .....	18
表 9 : SIP ドメインの設定 .....	19
表 10 : Cisco VCS で SIP ゾーンを作成する場合の設定 .....	20
表 11 : Cisco VCS で検索ルールを作成する場合の設定 .....	21
表 12 : Cisco VCS で検索ルールを作成する場合の設定 .....	22
表 13 : Multiway を有効にするための設定 .....	22
表 14 : Cisco VCS で Multiway 検索ルールを作成する場合の設定 .....	23
表 15 : 必須 MCU キー .....	24
表 16 : MCU の IP 設定 .....	24
表 17 : MCU の DNS 設定 .....	24
表 18 : MCU のサービス設定 .....	25
表 19 : MCU の SNMP 設定 .....	25
表 20 : MCU の暗号化の設定 .....	25
表 21 : MCU の会議の設定 .....	26
表 22 : MCU の H.323 の設定 .....	26
表 23 : MCU の SIP 設定 .....	27
表 24 : 事前設定された会議の設定 .....	27
表 25 : 自動応答の設定 .....	28
表 26 : カスタム ローカル SSL 証明書の設定 .....	29
表 27 : 信頼ストアの SSL 証明書の設定 .....	29
表 28 : TMS でスケジュール済み MCU の予約を許可する .....	30

---

表 29 : TMS のスケジュール済み MCU の拡張設定 .....	30
表 30 : TMS でスケジュール済み MCU の予約を却下する .....	30
表 31 : 優先的に使用される MCU タイプの使用の設定 .....	31
表 32 : 実装の検証のテスト .....	31
表 33 : Unified CM に登録したときの MCU の設定.....	33



図 1 : VCS 展開 : メディア、シグナリング、およびスケジューリングの概要 .....	11
図 2 : Conductor による VCS 展開 : メディア、シグナリング、およびスケジューリングの概要 .....	13
図 3 : Unified CM 展開 : メディア、シグナリング、およびスケジューリングの概要.....	14
図 4 : 組み合わせソリューションにおける MCU プール .....	15

## 概要

Cisco TelePresence MCU（このマニュアルでは「MCU」と呼びます）を展開し、ビデオ コールができるよう設定するにはさまざまな方法があります。このマニュアルでは、将来に向け非常に幅広い機能セットおよび最適な拡張性を実現する多数の設定オプションについて説明します。

## 対象読者

このマニュアルは、該当の製品すべてとそれらがどのように連携するかについて十分に理解しているパートナーまたはテクニカル セールス担当者を対象にしています。Cisco Unified CM、Cisco VCS、Cisco TMS、および Cisco TelePresence MCU の個別製品としての設置、設定方法を最低限理解している必要があります。ソリューションのすべてのコンポーネントが設置され、ネットワーク上で設定を行う準備が整っていることが前提となっています。したがって、このマニュアルはエンドカスタマー向けの完全な設置マニュアルではありません。

## 範囲

このマニュアルは、4500 シリーズ MCU デバイス、5300 シリーズ MCU デバイス、およびシャーシベースの MSE 8510 の展開を、Cisco インフラストラクチャを使用して可能な以下の展開方式で実施する場合の手順について、順を追って説明します。

- Cisco TelePresence Video Conferencing Server（Cisco VCS）に登録された MCU
- Cisco TelePresence Conductor（Conductor）を使用する展開において VCS に登録された MCU
- Cisco Unified Collaboration Manager（Unified CM）のメディア リソースとしての MCU

（スタンドアロン MCU 展開は、推奨される展開タイプではないため考慮されていません）。

各展開方式については、個別の項で説明します。たとえば、「VCS に登録されている場合」のシナリオでは、次の点について説明します。

- MCU の登録および電話会議ルーティングに必要な Cisco VCS 設定。
- MCU のセットアップと設定。
- 会議の予約と管理を行うための Cisco TelePresence Management Suite（Cisco TMS）の設定（Cisco TMS を使用する場合）。
- 確認とトラブルシューティングの手順。
- 既知の制限事項。

すべての展開について、MCU 展開の範囲外のセットアップについてはアドミニストレーション ガイドを参照し、『Conductor Deployment Guide』などの既存の展開ガイドも適宜参照します。

このマニュアルは、次のソフトウェア リビジョンに対してテスト済みです。

表 1: ソフトウェア リビジョン

デバイス	ソフトウェア リビジョン
Unified CM	8.6.1
VCS	X7.0.1

---

デバイス	ソフトウェア リビジョン
MCU	4.3
Conductor	XC1.1

# 背景説明

## MCU の概要

MCU は、SIP または H.323 ベースの 1 画面エンドポイントを仮想の会議室に接続する場合に主に使用されます。

MCU のポート数により、同時参加者の総数は制限されます。ポート数は、Cisco MSE 8000 の MCU のモデル/ブレード数、それらに適用されているライセンス、およびそれらの動作モードにより決まります。

MCU モデルの詳細については、シスコの Web サイトをご覧ください。

## 会議の開始

以下に詳しく説明するさまざまな方法で MCU において会議を開始できますが、すべての方法があらゆる展開方式で使用できるわけではありません。

**注：**また、スケジュール済み会議に使用するリソースは、スケジュール済みコールで確実にポートが使用できるようにするため、アドホック会議に使用してはなりません。したがって、スケジュール済み会議に使用する MCU はアドホック コールには使用せず、アドホック会議には別途 MCU を用意することを推奨します。

## スケジュール済み会議

スケジュール済み会議とは、あらかじめ予約された会議です。開始時間と終了時間が決まっており、参加者が事前に定義されています。MCU のスケジュール済み会議は、TMS 経由で予約を行います。TMS を直接使用して行うか、Microsoft Exchange などの統合ポイントを通じて行います。

## スケジュールされていない会議

アドホック MCU 会議の作成または会議への参加には、さまざまな方法があります。これらの方式は TMS がスケジュール済みコールに使用する MCU ではサポートされていませんが、一部の方式は、以下に詳しく説明するように MCU が特定の方式で展開されている場合に限りサポートされます。

## MCU 自動受付

MCU 自動受付は、ユーザが MCU の自動受付番号をダイヤルすると表示されるインタラクティブメニューです。新しい会議を作成したり、既存の会議に参加する場合に使用できます。一意のダイヤルイン番号をそれぞれ使用することで、複数の自動受付を設定できます。

**注：**MCU が Unified CM に展開されている場合、または Conductor を使用している場合、自動受付はサポートされていません。

## ダイナミック エスカレーション会議

2 種類のメカニズムで、ポイントツーポイント コールから MCU でホストされたマルチポイント コールにエスカレートする機能がサポートされています。Multiway は、Multiway をサポートしているエンドポイントでのみ開始できる VCS ベースのメカニズムです。Unified CM も、コールをエスカレートするため、エンドポイントで会議ボタンがサポートされている必要があるメカニズムをサポートしています。

Multiway エスカレーションは、VCS に登録されたアドホック MCU を使用している場合のみサポートされます。Conductor は、すべての Multiway 機能を完全にはサポートしていません。同様に、Unified CM 方式を使用したエスカレーションは、Unified CM でメディア リソースとして設定された MCU に対して行う必要があります。

## ランデブー会議

MCU 上のランデブー会議は、参加者がいつでも参加できる会議です。これらの会議は、個人向けの用途、または共同の先着順の会議向けに設定できます。

ランデブー会議は、デバイスで会議室を定義することで MCU 上に静的に設定できます。事前設定が不要になるよう、会議室を動的に作成することもできます。静的に設定された会議では、会議ごとに独自の設定が可能ですが、動的な会議は単一のテンプレートに従う必要があります。

Conductor ではなく VCS で MCU を使用する場合、静的な会議は個々の MCU で定義するため、シングル ポイント障害に対して脆弱です。

Conductor を使用する場合、ランデブー会議は Conductor で設定されるため、会議は 1 つの MCU で静的に定義されることはありません。これにより会議の復元性が高まると同時に、独自の会議設定を行う機能も維持されます。

MCU が Unified CM に登録されている場合、ランデブー会議を行うこともできます。管理者はランデブー会議に使用できる番号の範囲を定義します。ユーザが会議を要求する場合、[Meet Me] ボタンを押して会議番号を選択し、会議を開始します。

## ネットワーク トロロジ

MCU が原因となり、その場所においてビデオ トラフィックの集中が発生します。これは、各ポートでビデオ コールを最大 4Mbit/s（さらに 20% のオーバーヘッド）でポートに接続できるためです。したがって MCU は、これらのコールを十分ホストできる帯域幅を持つネットワーク ロケーションに配置する必要があります。

外部からのアクセスをファイアウォールで保護した社内ネットワークに MCU を配置することを推奨します。外部への発信については、ビデオ コールがファイアウォールを通過できるようにするため、Cisco TelePresence VCS Expressway を VCS Control と併せて使用する必要があります。

2 つ目のイーサネット ポートがアクティブ化されている場合（MCU 4500 および 5300 シリーズでは、これには Video Firewall Option キーが必要です）、このポートも社内ネットワーク上で使用し、MCU 管理トラフィックを MCU ビデオ トラフィックから分離するなどの目的で使用することを推奨します。

集中型アーキテクチャおよび分散型アーキテクチャの詳細については、『Cisco TelePresence Multipoint Conferencing Design Guidance』マニュアルを参照してください。

## ベースライン設定

一部の MCU の設定は、MCU の展開と無関係ですが、体感品質に影響を与えることがあります。以下の表に、それらの中で特に重要なものと、このマニュアルでの展開の前提となるその設定値を示します。

表 2: 推奨されるベースライン MCU 設定

MCU 設定	推奨
Maximum video size	Receive Max, transmit Max
Motion / sharpness tradeoff	Balanced (60fps が不要ない場合。必要な場合は Motion)



MCU 設定	推奨
Transmitted video resolutions	Allow all resolutions
Default bandwidth from MCU	4.00 Mbit/s
Default bandwidth to MCU	<same as transmit>
Use full screen view for two participants	イネーブル
Media port reservation	ディセーブル (Unified CM を使用して展開しない場合。必要な場合はイネーブルが必須)
ClearVision	イネーブル
Video format	NTSC – 30 fps
Video receive bit rate optimization	イネーブル
Flow control on video errors	イネーブル
Don't see yourself in small panes	イネーブル
Don't duplicate in small panes	イネーブル
Loudest speaker pane placement behavior	Never duplicate placed participants
Use local certificate for outgoing connections and registrations ([Settings] > [SIP] の SIP 設定の下)	イネーブル

## MCU のセキュリティ保護

MCU では、デフォルトの管理者パスワードが空欄となっていますが、パスワードを変更することを推奨します。

暗号キーをインストールした場合にのみ、MCU へのアクセスに https を使用できます。このキーは無償ですが、暗号化通信が可能な区域でのみ使用できます。

また、暗号キーによりビデオ コールを暗号化できます。これにより、H.323 メディアの AES 暗号化、SIP メディアの SRTP 暗号化、および SIP シグナリングの TLS 暗号化ができます。

[Settings] > [Security] で [Advanced account security mode] をイネーブルにすることを推奨します。この設定により、アカウントのセキュリティが強化されます (この設定を有効にする前に MCU のオンライン ヘルプ ページを確認して、設定の効果について理解してください)。設定を有効にすることにより生じる制限のため、この設定を有効にしたくない場合は、すべての MCU パスワードをハッシュするために設定をいったん有効にし、その後無効化することを推奨します (これにより、現在のアカウントすべてのパスワードの有効期限が切れる点に注意してください)。

**注：** 現在 MCU では、コールが暗号化されている場合、BFCP を SIP エンドポイントに送信できません。この場合、MCU は参加者が内容を確認できるよう、メイン ビデオ チャネルにコンポジット信号として内容を出力します。BFCP を送信するためには、SIP コールは暗号化されていない状態でなければなりません。

## SSL 証明書

MCU では、ローカル証明書と秘密キーが事前にインストールされており、これらは HTTPS で装置にアクセスする場合、または TLS 暗号化の場合にデフォルトで使用されます。ただし、新しい証明書と秘密キーをアップロードして ([Network] > [SSL Certificates]) セキュリティを確保することを推

奨めます。これは、工場から出荷されたすべての MCU のデフォルト証明書および秘密キーが同一であるためです。

## カスケード

非常に大規模な会議が必要な場合、1つの MCU で使用できる MCU ポート数では少なすぎる場合があります。こうした場合、大規模な会議を作成するためにある MCU を別の MCU に接続できます。この方法はカスケードと呼ばれ、ある MCU 会議から別の MCU 会議へのダイヤルを行います。各 MCU は、ローカル MCU 会議では追加の参加者と見なされます。この方法では、参加者が、1つまたは別の MCU 上の大体の参加者しか認識できないため、参加者のユーザ エクスペリエンスが制限されます。

最適なユーザ エクスペリエンスは常に、1つの MCU を使用して、すべての参加者がその MCU に接続されている状態により得られます。しかしこの場合、カスケードにより会議の最大サイズを拡大することはできません。

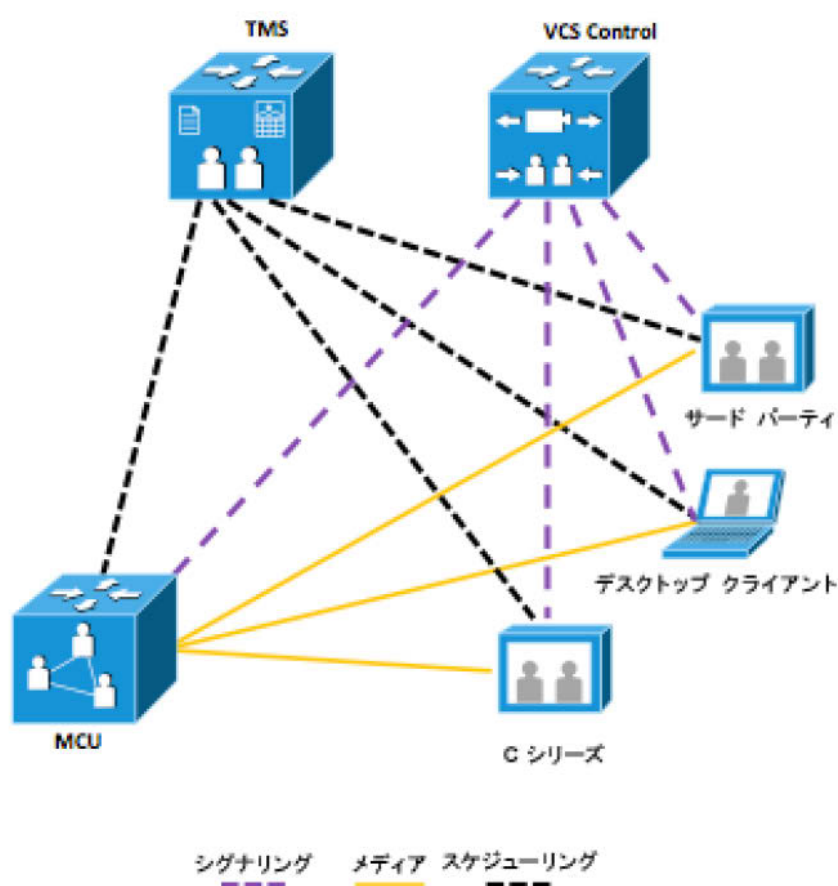
## 展開方式の選択

展開方式ごとに、以下で説明するような独自の利点があります。

### Cisco TelePresence VCS を使用した MCU の展開

この展開では、VCS を MCU のコール制御デバイスとして使用します（下図を参照）。（ただし、Unified CM が設置されている展開では、VCS にトランキングでき、いずれかのコール制御プラットフォームに登録されたデバイスで MCU へコールできます。詳細については、以下の MCU の組み合わせに関する項を参照してください）。

図 1：VCS 展開：メディア、シグナリング、およびスケジューリングの概要



この展開では、次の表で説明しているスケジュール済み会議およびアドホック方式で開始された会議が可能です。

表 3：VCS を使用した MCU の展開の機能の概要

会議の種類	オプション
スケジュール済み	<ul style="list-style-type: none"> <li>TMS を直接使用、または Microsoft Exchange などとの統合から使用</li> </ul>
アドホック	<ul style="list-style-type: none"> <li>自動受付</li> <li>ランデブー：MCU で静的に設定、または会議番号をダイヤルするときに MCU により動的に作成</li> </ul>

会議の種類	オプション
	<ul style="list-style-type: none"> <li>ダイナミック エスカレーション : Multiway を使用</li> </ul>

## 拡張性および復元性

VCS がサポートできる MCU の数の上限は、VCS の総登録数およびコール ライセンスにより許可された数になります。MCU は個々の会議を登録するよう設定できますが、H.323 サービス プレフィックスおよび SIP トランクを使用することでより拡張性を高めて、会議を個々に登録せずにすべてのコールを MCU にルーティングできます。これにより、VCS で直接使用する MCU を非常に大規模に展開できるようになります。VCS では、H.323 のみを介して登録された MCU 間のロード バランシングおよび復元性を実現できます。詳細については、『[Cisco VCS MCU Connection Using H323 Deployment Guide](#)』を参照してください。

スケジュール済みコールについては、スケジュール済み会議前または会議中に MCU が使用できなくなった場合、TMS は会議を別の MCU に再スケジュールできます。

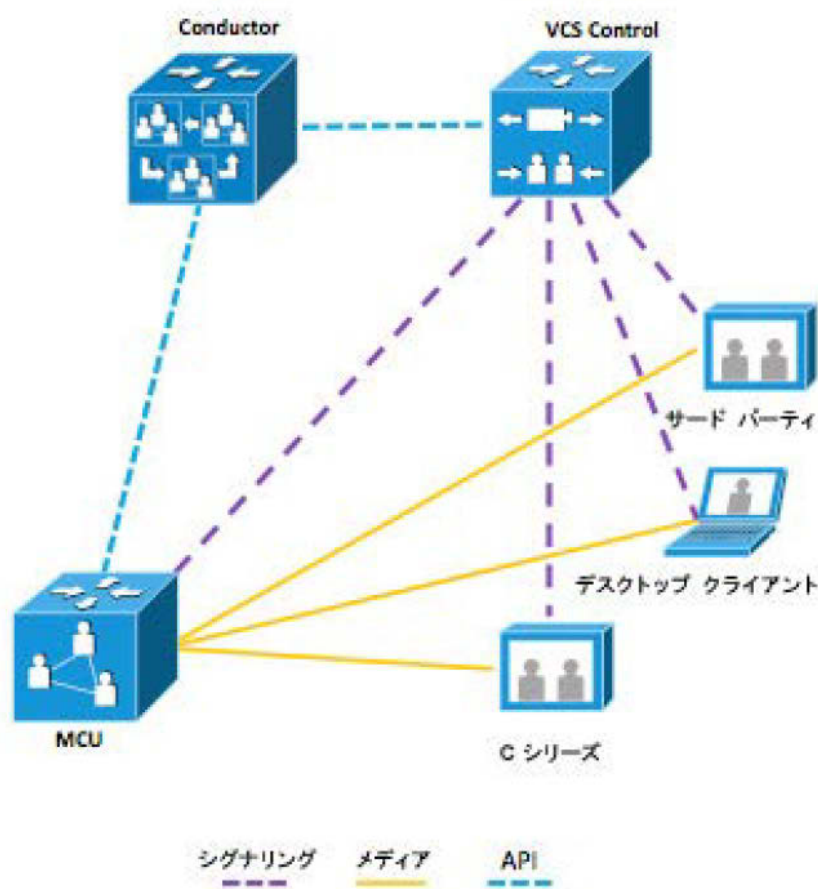
## 既知の制限事項

- MCU の（VCS を通じた）ロード バランシングおよび復元性は、H.323 の会議のみに制限され、本来は基本的な機能です。
- MCU カスケードは、事前設定が必要な手動のプロセスです。MCU をカスケードする必要があるのは、1 つの MCU の最大数を超える参加者による会議が必要な場合のみです。

## Cisco TelePresence Conductor を使用した MCU の展開

この展開では、MCU は VCS に登録されていますが、会議は Conductor で制御され、アドホックのみです。詳細については、以下の図と表を参照してください。

図 2 : Conductor による VCS 展開 : メディア、シグナリング、およびスケジューリングの概要



サポートされるアドホック方式を、以下の表で説明します。

表 4 : Conductor による MCU の展開の機能の概要

会議の種類	オプション
アドホック	<ul style="list-style-type: none"> <li>ランデブー : Conductor で設定し、会議の開始時に MCU に動的に配置される。</li> <li>ダイナミック エスカレーション : Multiway を使用 (部分的なサポート)</li> </ul>

## 拡張性および復元性

単独の Conductor または Conductor クラスタでは 30 台の MCU をサポートし、必要に応じて複数の Conductor クラスタを同一の VCS に展開できます。また Conductor により、MCU を動的にカスケードして複数のデバイスにわたる会議を形成することで、1 つの MCU のポート数の制限を超えてシームレスに会議を拡大させることができます。

Conductor では、個々の MCU で会議を直接設定する必要性をなくすことで、優れた復元性を実現しています。また、Conductors をクラスタ化して Conductor レベルでも復元性を提供できます。

## 既知の制限事項

- Multiway の限定サポート : カスケード コール中に Multiway を使用するなどのまれなケースは、サポート対象外です。

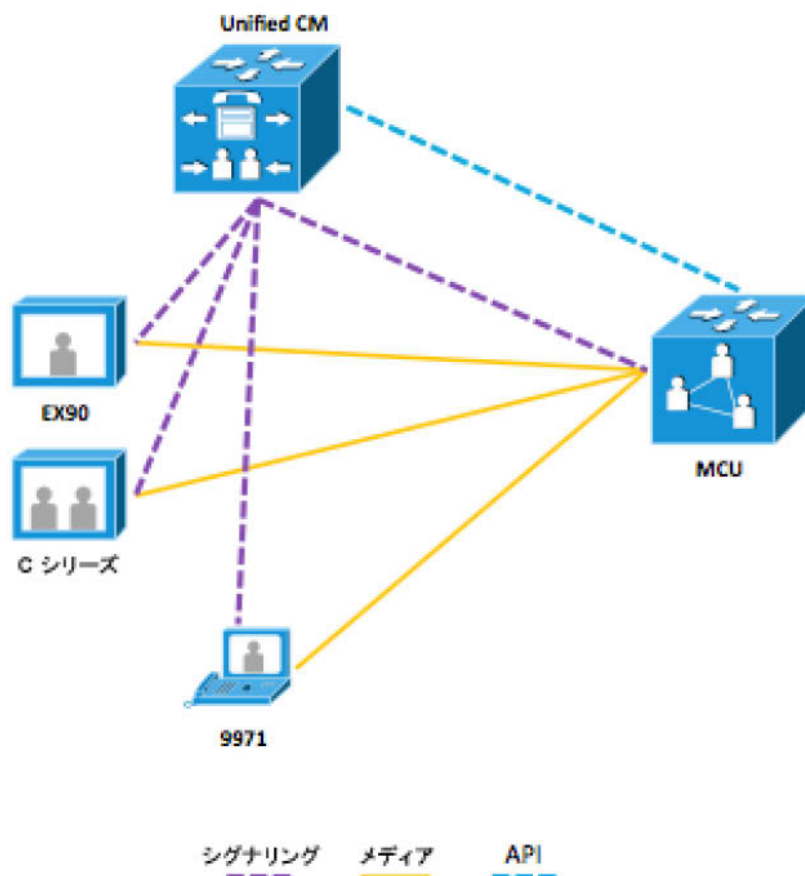
- Conductor が制御する MCU は、スケジュール済み会議には使用できません。
- 会議中に MCU が使用できなくなった場合、参加者は新しい MCU に参加するためにリダイヤルを行う必要があります。

## Unified CM を使用した MCU の展開

この展開では、MCU は Unified CM のメディア リソースとして使用され（下図を参照）、また、Unified CM により MCU の管理も行います。Unified CM は VCS にトランキングでき、いずれかのコール制御プラットフォームに登録されたデバイスから発信できるようになります。

このシナリオではスケジューリングがありませんが、会議ソフトキーをサポートする Unified CM に登録されたデバイスは、複数のコールを MCU 上でまとめて結合でき、ユーザが参加できるようランデブー会議を設定できます。

図 3 : Unified CM 展開 : メディア、シグナリング、およびスケジューリングの概要



サポートされるアドホック方式を、以下の表で説明します。

表 5 : Unified CM による MCS の展開の機能の概要

会議の種類	オプション
アドホック	<ul style="list-style-type: none"> <li>• ランデブー : [Meet Me] ボタンを使用</li> <li>• ダイナミック エスカレーション : 会議ボタンを使用</li> </ul>

## 拡張性および復元性

CUCM では、個々の MCU で会議を直接設定する必要性をなくすことで、優れた復元性を実現しています。使用できるポートの大規模なプールを提供するため、多数の MCU を CUCM に追加できます。

## 既知の制限事項

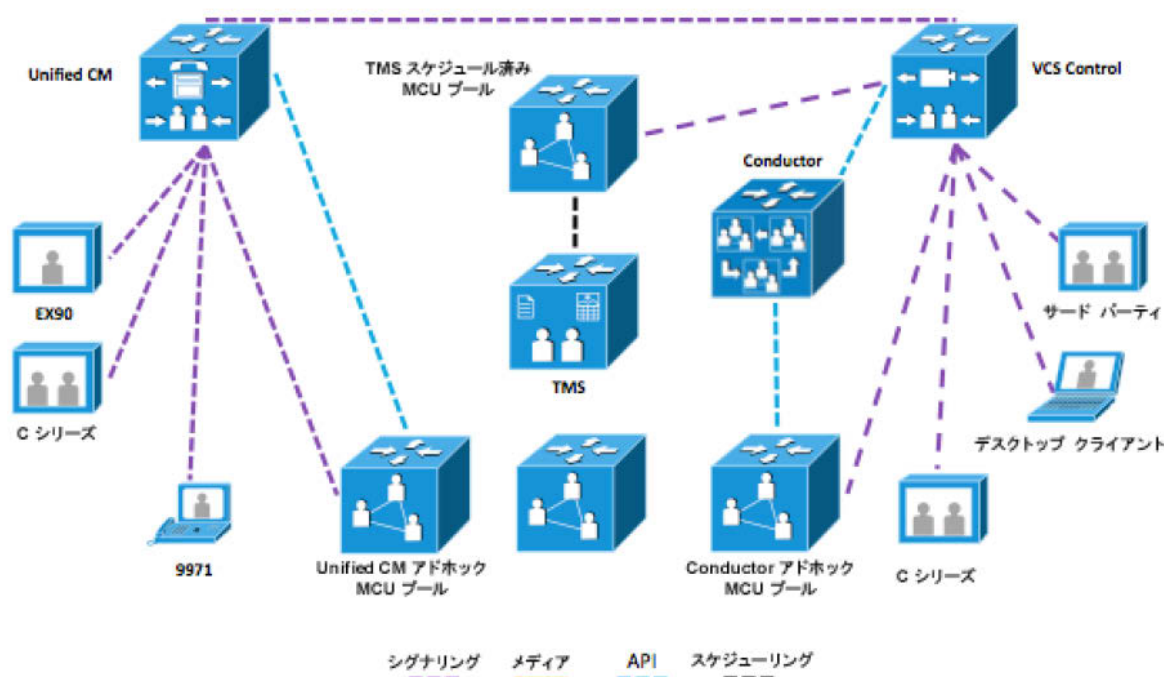
現在 Unified CM 8.6.1 を使用している場合、以下の制限があります。

- スケジュール済み会議はサポートされません。
- カスケードはサポートされません。
- TLS はサポートされません。
- BFCP はサポートされません。

## ソリューションの組み合わせ

MCU 展開の各タイプを個別に説明していますが、以下に示すように 3 種類の展開を同時に使用できます。

図 4：組み合わせソリューションにおける MCU プール



各タイプの MCU プールで使用する MCU リソースが個別にある限り、このソリューションは実行可能です。

Unified CM に登録されたエンドポイントは、コールの Multiway へのエスカレーションをサポートしていませんが、VCS でそのメカニズムをサポートするエンドポイントによりエスカレートできます。

同様に、VCS に登録されたエンドポイントは、ランデブー会議用の [Meet Me] ボタン、またはダイナミック エスカレーション用の会議ボタンをサポートしていませんが、Unified CM 会議リソースでコールに参加させることができます。これら VCS 登録エンドポイントは、ダイヤルイン番号をコー

ルするか、または Unified CM でそのメカニズムをサポートするエンドポイントでエスカレートできません。

## 展開タイプの概要

表 6：展開の選択の概要

	VCS に展開された MCU	Conductor により VCS に展開された MCU	Unified CM にメディアリソースとして展開された MCU
機器およびバージョンの最低要件	MCU 4.2 VCS X7	MCU 4.2 Conductor XC1.1 VCS X7	Unified CM 8.6.1 MCU 4.2
サポートされているアドホック コール方式	自動受付 ランデブー Multiway	ランデブー Multiway（部分的なサポート）	[Conference] ボタン Unified CM ランデブー
スケジュール済みコール	TMS によるサポート	未サポート	未サポート
拡張性	基本的な拡張性	高い拡張性	高い拡張性
復元性	基本的な復元性	高い復元性	高い復元性
制限事項	非常に大規模な会議を開催するためには、MCU の手動カスケードが必要です。	Multiway は部分的にサポートされています。たとえば、MCU をカスケードしている場合、Multiway エスカレーションは失敗する場合があります。 アドホック専用会議の作成。	TLS はサポートされません。 BFCP はサポートされません。 アドホック専用会議の作成。



# Cisco TelePresence VCS に登録された MCU の展開

## 展開の概要

この展開では、VCS が MCU の登録メカニズムとして使用され、会議は TMS を使用してスケジュールされます。スケジュールリングおよびアドホック会議には別途 MCU が使用されます。VCS に登録されたエンドポイント（つまり VCS にランキングされた Unified CM）は MCU コールに参加できます。すべての MCU には、コールを正しくルーティングし、スケジュール済み会議またはアドホック会議で同一の会議番号が発生しないよう、一意のプレフィックスが提供されています。この展開は、次の内容で構成されています。

表 7: 対象機能の概要

機能	説明
管理	MCU は TMS から管理できます。MCU への管理アクセスは管理者に制限されています。
アドホック会議	会議について、次の内容が可能です。 <ul style="list-style-type: none"> <li>サービス プレフィックスおよび会議の数値 ID をダイヤルすることによるオンザフライでの作成。</li> <li>MCU での静的な設定</li> <li>自動受付による作成と参加</li> <li>Multiway メカニズムを使用した作成と参加</li> </ul>
事前定義された無期限の会議	管理者は無期限の会議を作成できます。
セキュア会議	<ul style="list-style-type: none"> <li>AES、SRTP、および TLS 暗号化コールを使用した暗号化メディアおよびシグナリング。</li> <li>会議へのコールの限定的なアクセス。発信者は、会議に接続するのに PIN を入力する必要があります。</li> </ul>

## 前提条件

Cisco VCS、Cisco MCU、および Cisco TMS の設定を行う前に、次の前提条件が満たされていることを確認します。

- X7.0 ソフトウェアを実行している 1 つ以上の Cisco TelePresence VCS。
- スケジュール済み会議用の 4.2 ソフトウェアを使用している 1 つ以上の MCU。
- アドホック会議用の追加 MCU。
- 13.1.2 ソフトウェアを実行している Cisco TMS。
- Cisco VCS および TMS が設置され、該当する展開ガイド（以下に記載）を使用して基本操作のために設定されている。
- 使用している MCU が前記の表 2 に記載の基本設定で起動している。
- Cisco TMS に、該当する数の MCU を追加するのに十分なシステム ライセンスがある。

## マニュアル リスト

[『VCS Deployment Guide』](#)

[『Deploying VCS with Unified CM』](#)[『Deploying MCUs with Resilience and Resiliency using H.323』](#)[『Configuring Multiway』](#)

## 手順の概要

プロセスは以下の構成となっています。

1. ダイアルプランの設計
2. MCU の Cisco VCS でのゾーンおよびドメインの設定。
3. MCU の設置および設定
4. MCU の管理およびスケジューリングに向けた Cisco TMS の設定。

## 設定手順

### 手順 1 : ダイアルプラン

ビデオ展開のダイアルプランは、スケーラブルで使いやすいソリューションを展開するため、早期に検討する必要があります。このダイアルプランは、任意の 1 カ所ではなくさまざまなシステムで定義される概念上のプランです。したがって、展開全体を通して同じガイドラインに従うことが大切です。これら核となる要件を満たす推奨事項が提供されています。ただし、一部の展開では異なる実装が必要な特定の要件が存在する場合があります。

会議ごとに数値 ID があります。Cisco TMS を使用して会議を予約する場合、Cisco TMS は事前に設定された番号の範囲を使用して会議を作成します。これにより Cisco VCS に数値 ID が登録され、参加者は会議にダイヤルできます。スケジュール済み会議については、Cisco TMS は MCU を設定し、(Cisco VCS を通して) 参加者にコールを開始できます。これは、MCU からエンドポイントへのダイアルアウトコールとして最も一般的に使用されます。

特定の MCU で実行しているすべての会議は、プレフィックスをアドレス計画から割り当てた数字を使用してアドレス指定できます。たとえば 81xxx の場合、8 はデータセンター リソースの予約プレフィックスで、1 は特定の MCU のプレフィックスです。また、ユニフォーム リソース識別子 (URI) を使用して同じ会議に到達できます。たとえば、(インターワークされた) SIP および H.323 両方のシグナリング プロトコルで xxx@mcu1.cisco.com となります。(アドホック MCU 会議にロードバランシングを実現するため、同じプレフィックスを使用して複数の MCU を登録することもできます)。

プレフィックスを使用するとダイアルプランが単純化され、ユーザは SIP または H.323 のいずれを使用していても、<prefix><conference number>@domain をダイヤルするだけです。

以下の表は、会議サービスのアドレス計画の例を示します。アドホック会議および無期限の会議に割り当てられた範囲は、必要に応じて分割できます。両方の場合で、会議アドレスを複数のセッションで使用できます。たとえば、81555 は特定のチームの共有会議に使用できます。会議を事前に登録することで、セッション間で整合性を保ちながらレイアウトまたは設定を変更できるようになります。

表 8 : 5 桁を使用したアドレス計画の概要

プレフィックス/サフィクス	範囲	目的	ダイヤルの例
8 – 中央リソース 1 – Cisco MCU/MCU プール番号	000 ~ 010	自動受付コール	H.323 : 81001 SIP : 001@mcu1.cisco.com または 81001@cisco.com

プレフィックス/サフィクス	範囲	目的	ダイヤルの例
			H.323 から SIP へのインターワーク : 81001@mcu1.cisco.com
	011 ~ 909	アドホック会議または事前設定会議	H.323 : 81123 SIP : <a href="mailto:123@mcu1.cisco.com">123@mcu1.cisco.com</a> または <a href="mailto:81123@cisco.com">81123@cisco.com</a> H.323 から SIP へのインターワーク : 123@mcu1.cisco.com
	910 ~ 999	Multiway に予約	直接ダイヤルされない
8 – 中央リソース 2 – Cisco MCU 番号	100 ~ 999	スケジュール済み会議	ダイヤルインのみ (TMS はデフォルトで MCU ダイヤルアウトをします) : H.323 : 82812 SIP <a href="mailto:812@mcu2.cisco.com">812@mcu2.cisco.com</a> または <a href="mailto:82812@cisco.com">82812@cisco.com</a>

## 手順 2 : Cisco VCS の設定

Cisco VCS Control は『*Cisco VCS Base configuration*』または『*Unified CM with VCS deployment guide*』の推奨事項にしたがって展開する必要があります (両方とも [http://www.cisco.com/en/US/partner/products/ps11337/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/partner/products/ps11337/products_installation_and_configuration_guides_list.html) をご覧ください)。MCU の設置に備えて Cisco VCS を設定するには、次の手順が必要です。

1. MCU SIP サブドメインの設定。
2. MCU SIP ゾーンの作成。
3. 検索規則の設定。
4. 任意指定 : Multiway の設定。

**注 :** この項では、MCU に到達するために SIP コールを設定します。H.323 発信は (MCU 内の以降の項で設定された) H.323 プレフィックスから処理されます。これらの手順の設定は、以下の表で説明しています。

### MCU SIP ドメインの設定

MCU は、mcu1.cisco.com などのサブドメインを使用して Cisco に登録されます。したがって、Cisco VCS は MCU サブドメインと一致する SIP ドメイン名で設定する必要があります。そうしない場合、Cisco VCS は MCU からの SIP 登録要求を拒否します。

次のように SIP ドメインを設定します。

1. [VCS configuration] > [Protocols] > [SIP] > [Domains] をクリックします。
2. [New] をクリックします。
3. ドメイン名を [Name] フィールドに入力します。

表 9 : SIP ドメインの設定

VCS 設定	値	コメント
Name	MCU 完全修飾ドメイン名 (FQDN)	例 : mcu1.cisco.com または mcu1.cisco.net

4. [Create domain] をクリックします。

## MCU SIP ゾーンの設定

H.323 と同じコール動作を SIP にも提供するには、MCU にポイントする SIP ネイバー ゾーンで Cisco VCS を設定します (H.323 を使用する場合、MCU はサービス プレフィックスを登録しますが、SIP にはありません)。H.323 サービス プレフィックスに対応するパターン マッチでネイバー ゾーンを設定します。URI (たとえば、<会議 ID>@mcu1.cisco.com など) を使用して MCU へのアドホック コールを許可するには、サフィックスのパターン文字列が @mcu1.cisco.com に一致する SIP ゾーンを設定します。

本書では、ダイヤル可能なすべてのビデオ インフラ デバイスが、アドレス計画に基づいて 8 プレフィックスを使用することを前提とします。ビデオ ネットワーク内の 1 つ目の MCU には、サービス プレフィックス 1 を割り当てます。したがって、MCU プレフィックスは 81 になります。

次のように、VCS で SIP ゾーンを作成します。

1. [VCS configuration] > [Zones] に移動します。
2. [New] をクリックします。
3. 次のように、VCS のフィールドを設定します。

表 10 : Cisco VCS で SIP ゾーンを作成する場合の設定

VCS 設定	値	コメント
Name	ゾーン名	例 : ToMCU1
Type	ネイバー	
Hop count	15	
H.323 Mode	オフ	
SIP Mode	オン	
SIP Port	5061	暗号化を使用しない場合は、5060 に設定します。
SIP Transport	TLS	暗号化を使用しない場合は、TCP に設定します。
SIP TLS verify mode	セキュリティ ポリシーに従って TLS 検証の設定を指定します。	
Authentication policy	認証ポリシーに従って認証設定を指定します。	詳細については、VCS オンラインヘルプの認証ポリシー設定オプションを参照してください。
Peer 1 address	MCU の IP アドレスまたは FQDN	例 : mcu1.cisco.com
Zone profile	インフラストラクチャ デバイス	

4. [Create zone] をクリックします。

## 検索ルールの設定

検索ルールは、MCU SIP ゾーンにルーティングされるコールを決定します。

次のように、VCS で検索ルールを作成します。

1. [VCS configuration] > [Dial plan] > [Search rules] に移動します。
2. [New] をクリックします。
3. 次のように、VCS のフィールドを設定します。

表 11 : Cisco VCS で検索ルールを作成する場合の設定

VCS 設定	値	コメント
Rule name	検索ルールの記述名	例 : MCU1 ゾーン ドメインなし
Description	ルールの詳細な説明	例 : SIP 会議の MCU1 ゾーン の検索
Priority	50	一致の優先度は、ローカル ゾーン の完全な URI と同じであること
Source	任意	
Request must be authenticated	認証ポリシーに従って認証設定を指定します。	詳細については、VCS オンラインヘルプの認証ポリシー設定オプションを参照してください。
Mode	エイリアスのパターン マッチ	
Pattern type	Regex	
Pattern string	<mcu サービス プレフィックス >(\d+)*	企業間のコールでは、ダイヤルにおいて完全な E.164 が使用されることを想定します (+1753810001@companyb.com など)
Pattern behavior	置換	
Replace string	\1@<mcu-fqdn>	例 : \1@mcu1.cisco.com 注 : 必ず FQDN を使用してください
On successful match	Stop	
Target	<上記で設定されたゾーンの名前>	例 : mcu1
State	イネーブル	

## 4. [Save] をクリックします。

この検索ルールは、完全な番号を使用して発信された SIP コールをプレフィックスに照合し、URI が MCU で想定されるものになるよう操作します。

例 :

SIP call: 801111@cisco.com

この例では、プレフィックスが 80 の MCU1 の検索ルールを照合しますが、MCU は会議 1111@mcu1.cisco.com へのコールを着信することを予期しているため、検索ルールは MCU ゾーンにコールを渡す前に変更を加えます。

このルールでは、発信者は H.323 を使用する場合でも SIP を使用する場合でも同じ番号にダイヤルできるとともに、エンドポイント ドメインの自動付加を許可します（発信時に、ユーザがドメインを指定しなければ、エンドポイントがこの処理を行います）。

次のように、VCS で別の検索ルールを作成します。

1. [VCS configuration] > [Dial plan] > [Search rules] に移動します。
2. [New] をクリックします。
3. 次のように、VCS のフィールドを設定します。

表 12 : Cisco VCS で検索ルールを作成する場合の設定

VCS 設定	値	コメント
Rule name	検索ルールの記述名	例 : MCU1 ゾーン – SIP ドメイン
Description	ルールの詳細な説明	例 : SIP 会議の MCU1 ゾーンを検索
Priority	50	一致の優先度は、ローカル ゾーンの完全な URI と同じであること
Source	任意	
Request must be authenticated	認証ポリシーに従って認証設定を指定します。	詳細については、VCS オンラインヘルプの認証ポリシー設定オプションを参照してください。
Mode	エイリアスのパターン マッチ	
Pattern type	サフィックス	
Pattern string	@<mcu-fqdn>	例 : @mcu1.cisco.com
Pattern behavior	Leave	
On successful match	Continue	
Target zone	<上記で設定されたゾーンの名前>	例 : MCU1
State	イネーブル	

## 4. [Save] をクリックします。

この検索ルールは、MCU のドメインを使用した SIP コールを照合させます。これは、たとえば、スケジュール済み会議に対して TMS が使用するコール スtring です。

例 :

SIP call: 1111@mcu1.cisco.com

これは、ドメインが mcu1.cisco.com の MCU1 の検索ルールを照合しますが、MCU はこの形式の URI を受信することを予期しているため、コールが MCU ゾーンに発信される前には変更は行われません。

**オプション : Multiway の設定**

次のように、VCS で Multiway を有効にします。

1. [Applications] > [Conference Factory] に移動します。
2. 次のように、VCS のフィールドを設定します。

表 13 : Multiway を有効にするための設定

VCS 設定	値	コメント
Mode	オン	
Alias	この Conference Factory の URI (これは、Multiway 会議を開始する場合の発信先のエンドポイントに設定された Multiway ID です)	例 : multiway@cisco.com
Template	MCU のアドホック会議にコールをルーティングする URI のテンプレート	例 : 819%%@cisco.com 注 : これらのコールは、上記で設定された検索ルールに基づき、MCU にルーティングされます。
Number range start and end	ダイヤル プランに照合する範囲	例 : 10-99

3. [Save] をクリックします。

Multiway 要求が迅速に処理されるよう、次のように VCS で検索ルールを設定します。

1. [VCS configuration] > [Dial plan] > [Search rules] に移動します。
2. [New] をクリックします。
3. 次のように、VCS のフィールドを設定します。

表 14 : Cisco VCS で Multiway 検索ルールを作成する場合の設定

VCS 設定	値	コメント
Rule name	検索ルールの記述名	例 : Multiway ゾーン
Description	ルールの詳細な説明	例 : Multiway ゾーンの検索
Priority	1	コールが開始される前に、遅延を最低限に抑えるため
Source	任意	
Request must be authenticated	認証ポリシーに従って認証設定を指定します。	詳細については、VCS オンラインヘルプの認証ポリシー設定オプションを参照してください。
Mode	エイリアスのパターン マッチ	
Pattern type	Exact	
Pattern string	[Applications] > [Conference Factory] で設定された Conference Factory のエイリアス	例 : multiway@cisco.com
Pattern behavior	Leave	
On successful match	Stop	
Target zone	LocalZone	
State	イネーブル	

4. [Save] をクリックします。

詳細については、『[Multiway Deployment Guide](#)』を参照してください。

Multiway は、アドホック利用されるよう設定された MCU でのみ使用されます。Multiway を使用し、スケジュール済みのコールで使用される MCU に出席者を招集すると、リソース不足により、スケジュール済みのコールのいくつかに障害が発生することがあります。

エンドポイントは、Multiway および上記と同じ Conference Factory エイリアスを使用し、設定する必要があります。詳細については、エンドポイントの管理者ガイドを参照してください。

### 手順 3 : MCU のインストールと設定

MCU をインストールし、設定するには、次の手順を行います。

1. 機能キーのインストール
2. ネットワークの設定
3. 暗号化の設定
4. 会議の設定
5. ゲートキーパーの設定
6. SIP の設定
7. オプション : 会議の事前設定

8. オプション：自動応答の設定
9. オプション：カスタム SSL 証明書の設定

これらの手順の設定については、以下で説明します。

### 機能キーのインストール

次のように、MCU 機能キーをインストールします。

1. [Setting] > [Upgrade] に移動します。
2. 次のキーがあることを確認するか、インストールします。

表 15：必須 MCU キー

キー	Name	使用法
Activation	アクティベーション キー	MCU をアクティブ化するために必要です。
Encryption	暗号化オプション キー	展開において暗号化が使用される場合にのみ必要です。

3. [Update features] をクリックします。

注：8510 を動作させる前に、スーパーバイザを使用してポート ライセンスを適用する必要があります。

### ネットワークの設定

次のように、MCU の IP を設定します。

1. [Network] > [Port A] に移動します。
2. 次のように、MCU のフィールドを設定します。

表 16：MCU の IP 設定

MCU 設定	値	コメント
IP configuration	Manual	
Manual configuration	IPv4 または IPv6 アドレス、サブネットマスク、デフォルト ゲートウェイ	

3. [Update IP configuration] をクリックします。

次のように、MCU の DNS を設定します。

1. [Network] > [DNS] に移動します。
2. 次のように、MCU のフィールドを設定します。

表 17：MCU の DNS 設定

MCU 設定	値	コメント
DNS configuration	Manual	
Host name	MCU のホスト名	例：mcu1
Name server	DNS サーバの IP	
Domain name (DNS suffix)	Domain	例：cisco.com

3. [Update DNS configuration] をクリックします。

次のように、MCU のネットワーク サービスを設定します。



1. [Network] > [Services] に移動します。
2. 次のように、MCU のフィールドを設定します。

表 18 : MCU のサービス設定

MCU 設定	値	コメント
Secure web	ポート 443 をイネーブル	暗号キーが必要です
Encrypted SIP (TLS)	ポート 5061 をイネーブル	暗号キーが必要です
SNMP	ポート 161 をイネーブル	

3. [Apply Changes] をクリックします。

次のように、MCU の SNMP を設定します。

1. [Network] > [SNMP] に移動します。
2. 次のように、MCU のフィールドを設定します。

表 19 : MCU の SNMP 設定

MCU 設定	値	コメント
Name	MCU 名	例 : MCU1
Enable traps	イネーブル	
Trap receiver address 1	TMS の IP アドレス	
RO community	TMS のコミュニティ名	デフォルト : public
RW community	TMS のコミュニティ名	デフォルト : private
Trap community	TMS のコミュニティ名	デフォルト : public

3. [Update SNMP settings] をクリックします。

### 暗号化の設定

次のように、MCU の暗号化を設定します。

1. [Settings] > [Encryption] に移動します。
2. 次のように、MCU のフィールドを設定します。

表 20 : MCU の暗号化の設定

MCU 設定	値	コメント
Encryption status	イネーブル	
SRTP encryption	All transports	暗号キーが必要です。これにより、可能な場合に SIP メディアが暗号化されます。これを [Secure transports (TLS) only] に設定すると、シグナリングが TLS で暗号化されている場合にのみ SIP メディアが暗号化されます。

3. [Apply Changes] をクリックします。

### 会議の設定

次のように、MCU の会議を設定します。

1. [Settings] > [Conferences] に移動します。
2. 次のように、MCU のフィールドを設定します。

表 21 : MCU の会議の設定

MCU 設定	値	コメント
Incoming calls to unknown conferences or auto attendants	新しいアドホック会議を作成します	MCU がスケジュール済みのコールにのみ使用される場合は、これを [Disconnect caller] に設定できません。
Use conference name as the called ID	イネーブル	
Require H.323 gatekeeper callers to enter PIN	イネーブル	PIN が会議で設定される場合にのみ使用されます
Time to wait when setting up ad hoc conference PIN	Never configure PIN	

3. [Apply Changes] をクリックします。

### H.323 ゲートキーパーの設定

MCU で H.323 を設定します。

1. [Settings] > [H.323] に移動します。
2. 次のように、MCU のフィールドを設定します。

表 22 : MCU の H.323 の設定

MCU 設定	値	コメント
H.323 gatekeeper usage	Required	
H.323 gatekeeper address	VCS または VCS クラスターの FQDN	DNS A レコードは、VCS の IP アドレスに解決される必要があります
Gatekeeper registration type	MCU (標準)	同じプレフィックスが登録された MCU が 1 つ以上ある場合に、VCS が正しい MCU にアドホック コールをルーティングできるようにします
H.323 ID to register	URI	例 : <a href="mailto:mcu1@mcu1.cisco.com">mcu1@mcu1.cisco.com</a> 注 : ドメインは、SIP ドメインの VCS で設定された FQDN に照合する必要があります
Prefix for MCU registrations	プレフィックス	MCU 登録のプレフィックスと、MCU サービス プレフィックスは同一である必要があります (81 など)。
MCU service prefix	プレフィックス	MCU 登録のプレフィックスと、MCU サービス プレフィックスは同一である必要があります (81 など)。
Allow numeric ID registration for conferences	イネーブル	
Send resource availability indications	オプション : イネーブル ビデオ ポート : 数値	VCS の H.323 負荷分散機能を使用する場合は、デバイスにコールをルーティングしないことを VCS に通知するために、この機能が必要になります。

3. [Apply Changes] をクリックします。

### SIP レジストラの設定

MCU で SIP を設定します。

1. [Settings] > [SIP] に移動します。
2. 次のように、MCU のフィールドを設定します。

表 23 : MCU の SIP 設定

MCU 設定	値	コメント
SIP registrar usage	イネーブル	
SIP registrar domain	MCU の FQDN	例 : mcu1.cisco.com
SIP registrar type	Standard SIP	このオプションは 5300 シリーズでは使用できません。
Username	文字列	例 : mcu1 注 : H.323 URI の @ の前の文字列と同じであること
Password	なし	登録時に VCS で認証が必要な場合にのみ使用されます
Allow numeric ID registration for conferences	イネーブル	
SIP proxy address	VCS または VCS クラスターの FQDN	DNS A レコードは、VCS の IP アドレスに解決される必要があります
Outgoing transport	TLS	暗号キーが必要です。それ以外の場合は TCP を使用します。
Use local certificate for outgoing connections and registrations	イネーブル	TLS を使用する場合は、これを必ずイネーブルにする必要があります。

3. [Apply Changes] をクリックします。

#### オプション : 静的なランデブー会議の事前設定

この手順は、事前設定された会議ごとに行う必要があります。事前設定された会議は常に使用可能で（ただし、会議が設定された MCU が使用可能な状態で、リソースがある場合）、会議ユーザの一貫性のある設定を保持します（例：会議 PIN など）。

会議を事前設定するには、次の手順を実行します。

1. [Conferences] > [Conference list] に移動します。
2. [Add new conference] をクリックします。
3. 次のように、MCU のフィールドを設定します。

表 24 : 事前設定された会議の設定

MCU 設定	値	コメント
Name	会議の名前	会議を識別する名前。
Numeric ID	アドレス計画の、一意の 3 桁の数値識別子	会議にダイヤル インするときに使用されます。この ID には MCU 登録プレフィックスを含んではなりません。また、ID は、事前設定された会議に割り当てられたアドレス計画の範囲から取り出す必要があります。
Numeric ID registration – H.323 gatekeeper	オプション	MCU が上記のように設定されている場合、コールが会議に到達するために、会議を登録する必要はありません。
Numeric ID registration – SIP registrar	オプション	MCU が上記のように設定されている場合、コールが会議に到達するた

MCU 設定	値	コメント
		めに、会議を登録する必要はありません。
Permanent	イネーブル (オプション)	イネーブルではない場合、会議は設定された期間に使用可能になります。

4. [Add conference] をクリックします。

**注：**すべての会議を上記のように設定する必要はありません。また、MCU プレフィックスを使用し、MCU にアドホック会議を自動的に生成することもできます。たとえば、プレフィックス 81 を使用して MCU が上記のとおり設定された場合、ユーザが 81123 をダイヤルすると、会議はまだ存在しなければ、MCU が会議 123 を自動的に作成します。この方法を使用すると、会議ごとの設定は必要ありません。ただし、すべての会議はデフォルトのアドホック テンプレートを使用します。

### オプション：自動応答の設定

この手順は、展開における必要に応じ、最大 20 個の自動応答を作成するために実行します。自動応答は、常に使用可能です (ただし、自動応答が設定されている MCU が使用可能で、リソースがある場合)。自動応答の設定に応じ、ユーザは、自動応答ページから会議に出席したり、会議を作成したりできます。

自動応答を設定するには、次の手順を実行します。

1. [Conferences] > [Auto attendants] に移動します。
2. [Add new auto attendant] をクリックします。
3. 次のように、MCU のフィールドを設定します。

表 25：自動応答の設定

MCU 設定	値	コメント
Name	自動応答の名前	自動応答を識別する名前。
Numeric ID	アドレス計画の、一意の 3 桁の数値識別子	会議にダイヤルインするときに使用されます。この ID には MCU 登録プレフィックスを含んではなりません。また、ID は、自動応答に割り当てられたアドレス計画の範囲から取り出す必要があります。 例：001
Numeric ID registration – H.323 gatekeeper	オプション	MCU が上記のように設定されている場合、コールが会議に到達するために、会議を登録する必要はありません。
Numeric ID registration – SIP registrar	オプション	MCU が上記のように設定されている場合、コールが会議に到達するために、会議を登録する必要はありません。
Creation of new conferences	イネーブル (オプション)	イネーブルになっていなければ、ユーザは、自動応答を介してのみ既存のコールに参加することができます。
Access to ad hoc conferences	イネーブル (オプション)	イネーブルになっていなければ、ユーザには、MCU で事前設定された会議しか表示されません。

MCU 設定	値	コメント
All scheduled conferences	イネーブル (オプション)	選択されていない場合は、自動応答に表示される会議を指定できます。

4. [Add auto attendant] をクリックします。

### オプション : SSL 証明書の設定

MCU にカスタム ローカル証明書と秘密キーを追加することを推奨します。暗号化接続をネゴシエートするには、VCS に関連する証明書をインストールしておく必要があります。詳細については、『[VCS Certificate Creation and Use Deployment Guide](#)』を参照してください。

次のようにカスタム ローカル SSL 証明書を使用し、MCS を設定します。

1. [Network] > [SSL certificates] に移動します。
2. 次のように、MCU のフィールドを設定します。

表 26 : カスタム ローカル SSL 証明書の設定

MCU 設定	値	コメント
Certificate	ローカル サーバの証明書ファイル (PEM 形式) を選択します	
Private key	ローカル秘密キー ファイル (PEM 形式) を選択します	
Private key encryption password	秘密キー パスワードを追加します	暗号化された秘密キーを使用しなかった場合は、空白のままにしておきます。

3. [Upload certificate and key] をクリックします。

次のように信頼ストアの SSL 証明書を使用し、MCS を設定します。

1. [Network] > [SSL certificates] に移動します。
2. 次のように、MCU のフィールドを設定します。

表 27 : 信頼ストアの SSL 証明書の設定

MCU 設定	値	コメント
Trust store	信頼ストアまたは CA ファイル (PEM 形式) を選択します	複数の信頼認証局を追加する場合、証明書をコピーして貼り付けると、複数の証明書を .PEM ファイルに追加できます。
Certificate verification settings	セキュリティ ポリシーに従い、証明書の検証の設定を行います	

3. [Upload trust store] をクリックします。
4. [Apply Changes] をクリックします。
5. これらの変更を有効にするには、MCU を再起動します。

## 手順 4 : Cisco TMS の設定

MCU をインストールし、設定した後、管理者は Cisco TMS で次の手順を実行する必要があります。

1. MCU を Cisco TMS に追加する。

2. MCU の拡張設定を編集する。
3. 外部 MCU の使用方法を設定する。

### MCU を Cisco TMS に追加する

通常の手順で MCU を Cisco TMS に追加します。[Advanced Settings] の [Discover Non-SNMP Systems] を必ず選択してください。

### MCU の拡張設定を編集する

グローバル管理者として Cisco TMS にログインしたまま、

1. 新たに追加された MCU をクリックし、
2. [Settings] タブを選択し、[Extended MCU Settings] タブを選択します。
3. 追加する MCU の種類に基づき、以下の関連するセクションを実行します。

#### スケジュール済みの MCU の場合

スケジュール済み MCU の予約を許可するには、次の手順を実行します。

1. [System] > [Navigator] > [MCU] > [Settings] に移動します。
2. 次のように、TMS のフィールドを設定します。

表 28 : TMS でスケジュール済み MCU の予約を許可する

TMS 設定	値	コメント
Allow bookings	イネーブル	

3. [Save] をクリックします。

TMS で、MCU のスケジュール済み会議の番号範囲を設定します。

1. [System] > [Navigator] > [MCU] > [Settings] に移動します。
2. 次のように、TMS のフィールドを設定します。

表 29 : TMS のスケジュール済み MCU の拡張設定

TMS 設定	値	コメント
First meeting id	100	ID の長さとダイヤル プランを照合させるために、TMS が受け入れることができる最小の数値は 100 です。
Meeting id Step	1	

3. [Save] をクリックします。

#### アドホック MCU の場合

スケジュール済みではない MCU の予約を許可しない場合は、次の手順を実行します。

1. [System] > [Navigator] > [MCU] > [Settings] > [Edit Settings] に移動します。
2. 次のように、TMS のフィールドを設定します。

表 30 : TMS でスケジュール済み MCU の予約を却下する

TMS 設定	値	コメント
Allow bookings	ディセーブル	

3. [Save] をクリックします。

## 優先的に使用される MCU タイプの使用の設定

TMS でスケジュールを設定するとき、エンドポイント マルチサイトではなく外部 MCU を優先的に使用するには、次の手順を実行します。

1. [Administrative Tools] > [Configuration] > [Conference Settings] に移動します。
2. 次のように、TMS のフィールドを設定します。

表 31 : 優先的に使用される MCU タイプの使用の設定

TMS 設定	値	コメント
Preferred MCU Type in Routing	TANDBERG Codian MCU	デフォルト

3. [Save] をクリックします。

## 実装の検証

次の表に、MCU の展開が正常に実装されたことを検証するために行う、最も重要なテストをまとめます。

表 32 : 実装の検証のテスト

テスト グループ	目的	テスト
管理	適切な管理コントロールを検証します	Cisco TMS に管理者としてログインし、以下を確認します。 1. MCU を Infrastructure フォルダから選択するとき、Cisco TMS が MCU と接続していること（注：拡張設定を指定できるかどうかを確認する）。 2. Conference Control Center に MCU へのアクセスが示されていること（Conference Control Center で MCU を表示するには、[Show MCU] を選択する）。
アドホック会議	アドホック会議を検証します	アドホックの範囲内の番号で MCU にダイヤル インし、以下を確認します。 1. H.323 および SIP でダイヤル インすると、同じ会議に到達できること。 2. 展開において暗号化が設定されている場合、MCU で着信、および MCU から発信するコールが暗号化されていること。
恒久的会議/集中的に予約を管理する会議	MCU で設定された会議を検証します	Web インターフェイスを使用し、固定的/一元的に予約された会議の範囲に、会議を設定します。特別なレイアウトを設定し、正しい会議レイアウトが表示されることを検証します。
スケジュール済み会議	スケジュール済み会議が動作していることを確認します	Cisco TMS に管理者としてログインし、少なくとも 2 人のダイヤルアウト出席者、1 人のダイヤルイン出席者、および 1 人の外部出席者のある会議をスケジュールします。以下を確認します。 1. すべての出席者が、暗号化されて自動的に接続されること。 2. 会議の確認メールが、予約を行ったユーザに正しく送信されること。 3. 電子メール（または予約時の確認メッセージ）に記載されている H.323 番号と SIP URI を使用し、会議にダイヤルできること。

# Cisco TelePresence Conductor を使用した MCU の展開

## 展開の概要

この展開では、VCS が必要です。MCU は VCS に登録されたままですが、VCS の設定と MCU の設定は異なります。Conductor では、会議が設定された MCU で直接会議を定義するのではなく、会議の仮想化などの独自の利点を追加します。Conductor は、MCU を VCS に直接登録するよりも高い柔軟性と拡張性を与えます。

この展開の詳細は、以下に示す『Cisco TelePresence Conductor Deployment Guide』に記載されているため、本書では詳しく説明しません。

## マニュアル リスト

『[Conductor Deployment Guide](#)』



# Unified CM メディア リソースとしての MCU の展開

## 展開の概要

本書では、アドホック コール機能を提供するために、Unified CM のメディア リソース管理機能を使用します。コールは、会議ボタンを使用して動的に昇格することも、[Meet Me] ボタンでランデブーベースで設定することもできます。

詳細の手順については、以下の『Unified CM Administrator and System』ガイドで説明します。展開プロセスの概要については、以下に示します。

## マニュアル リスト

概要：『Unified CM System Guide』の「[Conference bridges](#)」項

MCU の設定：『Unified CM Administrator Guide』の「[Conference Bridge Configuration](#)」項

メディア リソース グループ リストの設定：『Unified CM System Guide』の「[Media Resource Management](#)」項

「Meet Me」の設定方法：『Unified CM System Guide』の「[Conference Bridge Configuration Checklist](#)」項

## 設定手順

### 手順 1：MCU を設定する

1. [Settings] > [Conferences] に移動します。
2. 次のように、MCU のフィールドを設定します。

表 33：Unified CM に登録したときの MCU の設定

MCU 設定	値	コメント
Media port reservation	イネーブル	
Incoming calls to unknown conferences or auto attendants	Disconnect caller	

3. [Apply Changes] をクリックします。

### 手順 2：Unified CM で会議機能を設定する

最大出席者数などの会議機能を設定するには、次の手順を実行します。

1. [System] > [Service Parameters] に移動します。
2. 関連する Unified CM サーバを選択します。
3. サービスとして [Cisco CallManager (Active)] を選択します。
4. [Advanced] を選択し、詳細オプションを表示します。
5. 必要に応じ、[Clusterwide Parameters (Feature - Conference)] セクションを設定します。

### 手順 3 : Unified CM で MCU を追加する

次のように、MCU を管理可能デバイスとして Unified CM に追加します。

1. [Media Resources] > [Conference Bridge] に移動します。
2. [Add New] をクリックします。
3. Cisco TelePresence MCU として [Conference Bridge Type] を選択します。
4. 関連するフィールドを設定し、[Save] を保存します。

### 手順 4 : Unified CM でメディア リソース グループ リストを設定する

1. [Media Resources] > [Media Resource Group] に移動します。
2. [Add New] をクリックします。
3. 名前を選択し、MCU（複数可）を [Selected Media Resources] 領域に移動します。
4. [Save] をクリックします。
5. [Media Resources] > [Media Resource Group List] に移動します。
6. [Add New] をクリックします。
7. 名前を選択し、作成されたメディア リソース グループを [Selected Media Resource Groups] 領域に移動します。
8. [Save] をクリックします。

### 手順 5 : Unified CM で、デバイスにメディア リソース グループ リストを割り当てる

1. [Device] > [Phone] の順に移動します。
2. デバイスを選択します。
3. 先に作成したメディア リソース グループ リストを選択します。
4. [Save] をクリックします。

### オプション : Unified CM で「Meet Me」サービスを設定する

ランデブー サービスが必要な場合は、上記のドキュメント一覧に従って設定します。

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](http://www.cisco.com/go/trademarks). 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. (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。

Copyright © 2012 Cisco Inc.

Copyright © 2012, シスコシステムズ合同会社.