



## 付録

---

- [Video Mesh ノード デモ用ソフトウェア](#) (1 ページ)
- [コンソールからの Video Mesh ノードの管理](#) (2 ページ)
- [既存のハードウェアプラットフォームからの Video Mesh ノードへの移行](#) (10 ページ)
- [Collaboration Meeting Room Hybrid から Video Mesh への移行パスと機能比較](#) (12 ページ)
- [TelePresence 相互運用性プロトコルとセグメント切り替え](#) (14 ページ)

## Video Mesh ノード デモ用ソフトウェア

Video Mesh ノード デモソフトウェアは基本的なデモのためだけに使用してください。デモノードを既存の本稼働クラスタに追加しないでください。デモ用クラスタは、本稼働のクラスタよりも受け入れるコールが少なく、クラウドに登録してから 90 日で期限が切れます。



- (注)
- Video Mesh ノード デモ用ソフトウェアは、Cisco TAC ではサポートされていません。
  - Video Mesh ノード デモソフトウェアを完全な実稼働ソフトウェアバージョンにアップグレードすることはできません。

[このリンク](#)からデモソフトウェアイメージをダウンロードしてください。

### 仕様

Video Mesh ノード ソフトウェアのスペックベースの構成については、「[Video Mesh ノード ソフトウェアのシステム要件とプラットフォーム要件](#)」を参照してください。

デモソフトウェアは、単一のネットワークインターフェイスまたはデュアルネットワークインターフェイスのいずれかをサポートします。

## 容量

キャパシティに対するデモイメージは、テストしません。これは、ミーティングの基本的なシナリオをテストするためだけに使用してください。ガイダンスとして、次のユースケースを参照してください。

### Video Mesh ノード デモソフトウェアのユースケース

#### メディアがオンプレミスに固定されている

- デモ用ソフトウェアを使用して、ノードを展開し、構成する。
- 次の参加者を含むミーティングを実行する。Webex アプリ の参加者、Webex エンドポイントの参加者、および Cisco Webex Board。
- ミーティングが終了したら、<https://admin.webex.com> のカスタマービューで [分析 (Analytics) ] に移動して Video Mesh レポートにアクセスします。このレポートで、メディアがオンプレミスのままだったことがわかります。

#### クラウドとオンプレミスの参加者によるミーティング

- オンプレミスで Webex の参加者が数人とクラウドから 1 人参加している別のミーティングを実行します。
- すべての参加者がミーティングにシームレスに接続して参加できることを確認します。

# コンソールからの Video Mesh ノードの管理

クラウドに登録されている Video Mesh ノードのネットワークを変更する前に、Control Hub を使用してノードをメンテナンスモードにする必要があります。詳細および従うべき手順については、「[ノードのメンテナンスモードへの移行](#)」を参照してください。



---

**注意** メンテナンスモードは、特定のネットワーク設定の変更 (DNS、IP、FQDN) を行ったり、RAM やハードドライブの置き換えなどのハードウェア メンテナンスの準備を行ったりできるよう、ノードのシャットダウンまたは再起動を準備することのみを意図しています。

ノードがメンテナンスモードになっている場合、アップグレードは行われません。

---

ノードをメンテナンスモードにすると、コールサービスのグレースフルシャットダウンを実行します (新しいコールの受け入れを停止し、既存のコールが完了するまで最大 2 時間待機します)。コールサービスのグレースフルシャットダウンの目的は、コールのドロップを引き起こすことなく、ノードの再起動またはシャットダウンを可能にすることです。

## コンソールでの Video Mesh ノードネットワーク設定の変更

ネットワークトポロジが変更された場合は、各 Video Mesh ノードのためにコンソールインターフェイスを開いて、そこでネットワーク設定を変更する必要があります。ネットワーク構成の変更については注意が表示されますが、Video Mesh ノードの設定を変更した後にネットワークに変更を加える場合は、変更を保存することができます。

### 手順

- ステップ 1** VMware vSphere クライアントを通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。

初めてネットワーク設定をセットアップした後、Video Meshが到達可能である場合は、セキュアシェル (SSH) を通じてノードインターフェイスにアクセスできます。
- ステップ 2** Video Mesh ノードコンソールのメインメニューで、**[2 構成の編集 (2 Edit Configuration)]** のオプションを選択し、**[選択 (Select)]** をクリックします。
- ステップ 3** Video Mesh ノードでのコールの終了を求めるプロンプトを読み、**[はい (Yes)]** をクリックします。
- ステップ 4** **[静的 (Static)]** をクリックして、内部インターフェイスの**[IP アドレス (IP address)]**、ネットワークの**[マスク (Mask)]**、**[ゲートウェイ (Gateway)]**、**[DNS]** の各値を入力します。
  - Video Mesh ノードは、内部 IP アドレスと解決可能な DNS 名を持っている必要があります。ノード IP アドレスは、Video Mesh ノード内部使用のために予約されている IP アドレスの範囲に属してはなりません。デフォルトの予約済み IP アドレスの範囲は 172.17.42.0 ~ 172.17.42.63 で、**[診断 (Diagnostic)]** メニューで設定できます。この IP アドレスの範囲は、Video Mesh ノード内、およびノードのさまざまなコンポーネント (SIP インターフェイスやメディアトランスコーディングなど) を保持するソフトウェアコンテナ間における通信のためのものです。
  - すべてのノードを同じサブネットまたは VLAN に展開します。これにより、クラスタ内のすべてのノードは、ネットワーク内のクライアントのどこからでも到達可能になります。
  - デュアル NIC DMZ を導入する場合は、内部ネットワーク構成を保存してノードをリブートした後、次の手順で外部 IP アドレスを設定することができます。
- ステップ 5** 組織の NTP サーバーまたは組織で使用可能な別の外部 NTP サーバーを入力します。

NTP サーバーを設定し、ネットワーク設定を保存した後は、「[コンソールからの Video Mesh ノードの正常性チェック \(7 ページ\)](#)」の手順に従って、指定された NTP サーバーを介して時刻が正しく同期されていることを確認できます。

(注) 複数の NTP サーバーを設定する場合、フェールオーバーのポーリング間隔は 40 秒です。
- ステップ 6** (オプション) 必要に応じて、ホスト名またはドメインを変更します。

- (注)
- クラウドに問題なく登録できるように、Video Mesh ノードに設定するホスト名は小文字のみを使用します。現時点では、大文字と小文字はサポートされていません。
  - FQDN またはホスト名を使用または設定する場合は、有効で解決可能なドメインを入力する必要があります。FQDN の長さは、64 文字以下にする必要があります。

**ステップ 7** [保存 (Save)] をクリックし、[変更を保存して再起動 (Save Changes & Reboot)] の順に選択します。

ドメインを指定した場合は、保存中に DNS の検証が行われます。指定された DNS サーバーアドレスを使用して FQDN (ホスト名とドメイン) を解決できない場合、警告が表示されます。警告を無視して保存を選択できますが、ノードに設定されている DNS で FQDN を解決できるまで、コールは機能しません。Video Mesh ノードリブート後、ネットワーク構成の変更が有効になります。

## Video Mesh ノード管理者のパスフレーズの変更

ノードのコンソールで Video Mesh ノード用の管理者のパスフレーズ (パスワード) を変更するには、次の手順を使用します。

### 手順

- ステップ 1** VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。
- ステップ 2** Video Mesh ノードの VM の VMware ESXi コンソールを開いてログインします。
- ステップ 3** メインメニューで、[3 管理者パスフレーズの管理 (3 Manage Administrator Passphrase)] オプションを選択し、次に [1 管理者パスフレーズの変更 (1 Change Administrator Passphrase)] を選択して **Enter** キーを押します。
- ステップ 4** [パスワードの有効期限が切れています] ページの情報を読み、**Enter** キーを押し、パスワードの有効期限のメッセージの後にもう一度押します。
- ステップ 5** Enter を押します。
- ステップ 6** コンソールからサインアウトすると [サインイン (Sign In)] 画面に戻るため、管理者のログイン名と期限切れのパスフレーズ (パスワード) を使用してサインインします。パスワードの変更を求めるプロンプトが表示されます。
- ステップ 7** [現在のパスワード (Old password)] に、現在のパスフレーズを入力してから **Enter** キーを押します。
- ステップ 8** [新しいパスワード (New password)] に新しいパスフレーズを入力し、**Enter** キーを押します。
- ステップ 9** [新しいパスワードの再入力 (Re-enter new password)] に新しいパスフレーズを再入力し、**Enter** キーを押します。

「パスワードが変更されました (password changed)」というメッセージが表示され、[サインイン (Sign In)] 画面に戻ります。

**ステップ 10** 新しい管理者ログイン名とパスワード (パスワード) を使用してサインインします。

## Video Mesh ノードコンソールからの Ping の実行

Video Mesh ノードのコンソールインターフェイスから ping を実行できます。この手順では、入力した宛先をテストし、Video Mesh ノードが到達可能かどうかを確認します。

### 手順

- ステップ 1** VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。
- ステップ 2** Video Mesh ノードコンソールから、[4 診断 (4Diagnostics)] に移動し、[Ping] を選択します。
- ステップ 3** [Ping] フィールドに、IP アドレスやホスト名など、テストする宛先アドレスを入力し、[OK] をクリックします。

テストを実行すると、Ping の成功または失敗のメッセージが表示されます。失敗メッセージが表示される場合は、入力した宛先の値とネットワーク設定を確認します。

## コンソールを通じたデバッグユーザーアカウントの有効化

サポートが Video Mesh ノードへのアクセスを要求した場合、コンソールインターフェイスを使用してデバッグユーザーアカウントを一時的に有効にし、サポートがノードで詳細なトラブルシューティングを実行できるようすることができます。

### 手順

- ステップ 1** VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。
- ステップ 2** Video Mesh ノードコンソールから、[4 診断 (4Diagnostics)] に移動し、[2 デバッグユーザーアカウントの有効化 (2 Enable Debug User Account)] を選択して、プロンプトが表示されたら、[はい (Yes)] をクリックします。
- ステップ 3** デバッグユーザーアカウントが正常に作成されたことを示すメッセージが表示されたら、[OK] をクリックして、暗号化されたパスワードを表示します。

暗号化されたパスワードをサポートに送信します。トラブルシューティングのために、この一時的なアカウントを使用し、パスワードを解読して Video Mesh ノードに安全にアクセスします。このアカウントは、3 日後に有効期限が切れるか、サポートが終了した時点で無効にできます。

- ステップ 4** 暗号化されたデータの開始と終了を選択してコピーし、サポートに送信するサポートチケットまたは電子メールに貼り付けます。
- ステップ 5** この情報をサポートに送信した後、Video Mesh ノードコンソールに戻り、任意のキーを押してメインメニューに戻ります。

---

#### 次のタスク

アカウントの有効期間は3日間ですが、ノードのトラブルシューティングが終了した旨の通知がサポートからあった場合は、Video Mesh ノードコンソールに戻り、[4 診断 (4 Diagnostics)] に移動し、[3 デバッグユーザーアカウントを無効にする (3 Disable Debug User Account)] を選択して、失効前にアカウントを無効化できます。

## Video Mesh ノードコンソールからのログの送信

Cisco または Secure Copy (SCP) に、ログを直接送信するよう指示される場合があります。クラウドに登録した Video Mesh ノードからログを直接送信するには、次の手順を実行します。

#### 手順

- ステップ 1** VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。
- ステップ 2** メインメニューで、[4 診断 (4 Diagnostics)] オプションをクリックし、**Enter** キーを押します。
- ステップ 3** [4 ログファイルのエクスポート (4 Export Log Files)] をクリックし、必要に応じてフィードバックを提供し、[次へ (Next)] をクリックします。
- ステップ 4** 次のオプションを選択します。
- SCP を使用してログを送信し、ログのエクスポートを確認して、SCP の詳細 (ホスト、ユーザー名、Dest\_Folder) を入力し、[OK] をクリックします。
  - [Cisco にログを送信 (Send Logs to Cisco)] を選択し、ログをエクスポートすることを確認します。
- ステップ 5** Video Mesh ノードのメインメニューに戻るには、[OK] を選択します。
- ステップ 6** (任意) ログを Cisco に送信した場合は、[Cisco に送信したログファイルのステータスを確認 (Check Status of Log Files Sent to Cisco)] を選択します。

---

#### 次のタスク



- ヒント** ログを送信した後、Webex アプリ からフィードバックを直接送信することを推奨します。これにより、サポート連絡先にすべての情報を提供することができます。
-

## 関連トピック

[サポートに問い合わせる](#)

# コンソールからの Video Mesh ノードの正常性チェック

ノードの正常性は、Video Mesh ノードから直接表示できます。結果は情報提供に過ぎませんが、トラブルシューティング手順で役立つ場合があります。たとえば、NTP の同期が動作していないければ、ネットワーク構成の NTP サーバーの値を確認できます。

## 手順

- ステップ 1 VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。
- ステップ 2 Video Mesh ノードコンソールから [4 診断 (4 Diagnostics)] に移動し、[6 ノードの正常性を確認 (6 Check Node Health)] を選択してノードに関する次の情報を表示します。
  - 管理サービスコンテナ
  - ETCD (クラスタ全体でデータを確実に保存するキーバリュ型ストア)
  - 同期済み NTP
  - ディスク容量 (空き/使用済み %)
  - メモリ (空き/使用済み %)

# Video Mesh ノード上のコンテナネットワークの設定

Video Mesh ノードは、ノード内での内部使用のためのサブネット範囲を予約します。デフォルトの範囲は、172.17.42.0 ~ 172.17.42.63 です。ノードは、この範囲から発信される外部から Video Mesh ノードへのトラフィックには応答しません。ネットワーク内の他のデバイスと競合しないように、コンテナのブリッジ IP アドレスを変更するためにノードコンソールを使用することもできます。

## 手順

- ステップ 1 VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。
- ステップ 2 Video Mesh ノードコンソールのメインメニューから、[4 診断 (4 Diagnostics)] に移動し、[7 コンテナネットワークの構成 (7 Configure Container Network)] を選択します。このノードでアクティブなコールが終了することを示す注意が表示されたら、[はい (Yes)] をクリックします。
- ステップ 3 必要に応じて [コンテナブリッジ IP (Container Bridge IP)] と [ネットワークマスク (Network Mask)] の値を変更し、[保存 (Save)] をクリックします。

Video Mesh ノード上の内部操作作用として予約されている IP アドレスの範囲を含む、コンテナネットワーク情報を表示する画面が表示されます。

ステップ 4 [OK] をクリックします。

---

## コンソールでのリフレクタツールを使用したポートの問題の特定

必要な TCP/UDP ポートが Video Mesh ノードから開かれているかどうかを確認するため、リフレクタツール（Video Mesh ノードとクライアント上の Python スクリプトを使用したサーバーの組み合わせ）が使用されます。

始める前に

- [リフレクタツールクライアント（Python スクリプト）](#) のコピーをダウンロードし、簡単に見つけられる場所にそのファイルを解凍します。Zip ファイルには、スクリプトと Readme ファイルが含まれています。
- スクリプトを正常に動作させるには、使用している環境で Python 2.7.10 またはそれ以降を実行していることを確認してください。
- 現在、このツールでは、Video Mesh ノードおよびクラスタ内検証に SIP エンドポイントをサポートしています。

手順

- 
- ステップ 1 <https://admin.webex.com> のカスタマービューで、値リストコレクション作成者のメンテナンスノードを有効にするには、[次の手順に従います](#)。
  - ステップ 2 ノードが Control Hub で [メンテナンス可能 (Ready for maintenance)] ステータスを表示するまで待機します。
  - ステップ 3 VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。
  - ステップ 4 値リストコレクション作成者インターフェイスから、**[診断 (Diagnostics)]** > **[リフレクタサーバー (Reflector Server)]** > **[TCP または (UDP) 向けのリフレクタサーバ (Reflector Server for TCP or (UDP))]** の順に選択します。TCP または UDP のいずれかのサーバーを起動します。
  - ステップ 5 **[リフレクタツール (Reflector Tool)]** までスクロールし、使用するプロトコルに応じて **[TCP リフレクタサーバー (TCP Reflector Server)]** または **[UDP リフレクタサーバー (UDP Reflector Server)]** のいずれかを起動します。
  - ステップ 6 **[リフレクタサーバーの起動 (Start Reflector Server)]** をクリックし、サーバーが正常に起動するまで待機します。  
サーバーの起動時に通知が表示されます。

**ステップ7** Video Mesh ノードの到達先とするネットワーク上のシステム (PC など) から、次のコマンドでスクリプトを実行します。

```
$ python <local_path_to_client_script>/reflectorClient.py --ip <ip address of the server>
--protocol <tcp or udp>
```

実行の終了時に、必要なすべてのポートが開かれている場合、クライアントは成功メッセージを表示します。

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp
Please wait while verifying tcp for ports: ['5004', '5060-5061'] ...
[----->] 100.00% Success/Failed/Total: 3/0/3

#####
No ports are blocked for tcp in ['5004', '5060-5061']
#####
Exiting Reflector Client tool...
$
```

必要なポートが開いていない場合、クライアントは、失敗した旨を通知するメッセージを示します。

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp --start-port 5060 --end-port 5062
Please wait while verifying tcp for port range: 5060 - 5062 ...
[----->] 100.00% Success/Failed/Total: 2/1/3

Failed ports in the first try: ['5062']
Retrying(4 times) the above failed ports:
Retry number 1:
  Verifying port -> 5062
Retry number 2:
  Verifying port -> 5062
Retry number 3:
  Verifying port -> 5062
Retry number 4:
  Verifying port -> 5062
#####
Ports which are not open for tcp are: ['5062']
#####
Exiting Reflector Client tool...
```

**ステップ8** ファイアウォール上のポートの問題を解決してから、上記の手順を再実行します。

**ステップ9** 詳細については、**--help** を使用してクライアントを実行してください。

```
$ python reflectorClient.py --help
Usage:
  --ip and --protocol are mandatory.
  If start-port is specified, end-port is considered mandatory. If no starting port is specified, default ports are verified for connectivity.
  By default, tool checks for QoS ports unless --non-qos option is specified.
  Default QoS ports include: TCP - 5004, 5060, 5061 and UDP - 5004, 52500-59499 and 63000-64667.
  Default non QoS ports include: TCP - 5004, 5060, 5061 and UDP - 5004, 34000-34999.
  To verify single port, both start and end port should be the required port to verify.
Examples:
Below run is to verify non-qos ports using an input port range:
  python reflectorClient.py --ip <hmn-ip-address> --protocol <udp/tcp> --start-port 52000 --end-port 52501 --non-qos
Below run in to verify default qos ports:
  python reflectorClient.py --ip <> --protocol <udp/tcp>
$
```

## コンソールからの Video Mesh ノードの工場出荷時状態へのリセット

登録解除のクリーンアップの一部として、Video Mesh ノードを初期設定へのリセットすることができます。この手順では、ノードがアクティブだったときに設定した内容が削除されますが、仮想マシンのエントリは削除されません。後で、最初から構築した別のクラスタの一部として、このノードを再登録できます。

### 始める前に

Control Hub を使用して、Control Hub に登録されているクラスタから Video Mesh ノードを登録解除する必要があります。

### 手順

- 
- ステップ 1** VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。
  - ステップ 2** Video Mesh ノードコンソールで、[4 診断 (4 Diagnostics)] に移動して、[8 初期設定へのリセット (8 Factory Reset)] を選択します。
  - ステップ 3** 注意事項に表示される情報を理解したら、[リセット (Reset)] をクリックします。  
初期設定へのリセット後、ノードは自動的に再起動します。
- 

## 既存のハードウェアプラットフォームからの Video Mesh ノードへの移行

サポートされている既存のプラットフォーム (Cisco Meeting Server を実行する CMS1000 など) を Video Mesh に移行できます。次の手順を使用して、移行プロセスを実行します。



- 
- (注) この手順は、ハードウェアプラットフォーム上の ESXi のバンドルバージョンに応じて異なります。
- 

### 始める前に

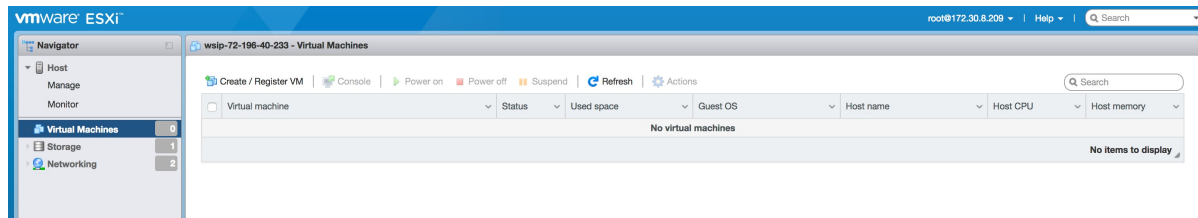
最新の [Video Mesh ノードソフトウェア](#) のイメージ (OVA) の新しいコピーをダウンロードします。前にダウンロードした OVA を使用して新しい Video Mesh ノードを展開しないでください。

## 手順

**ステップ1** 仮想マシンインターフェイスにサインインし、プラットフォーム上で実行されているソフトウェアをシャットダウンします。

**ステップ2** プラットフォーム上で実行されていたソフトウェアアプリケーションを削除します。

プラットフォーム上にソフトウェアイメージが残っていないようにする必要があります。また、同じプラットフォーム上の他のソフトウェアと一緒に **Video Mesh** ノードソフトウェアを実行することはできません。



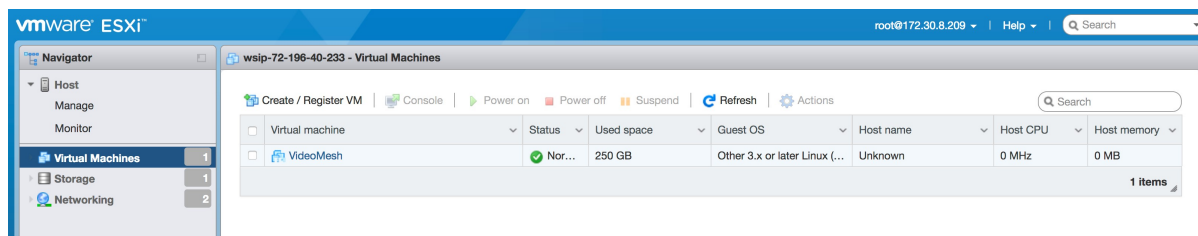
**ステップ3** 新しい OVF または OVA ファイルから新しい仮想マシンを展開します。

**ステップ4** 仮想マシンの名前を入力し、**Video Mesh** ノードの OVA ファイルを選択します。

**ステップ5** ディスクプロビジョニングを [Thick (シック)] に変更します。

**ステップ6** ダウンロードした **mfusion.ova** ソフトウェアイメージをアップロードします。

Task	Target	Initiator	Queued	Started	Result	Completed
Upload disk - mfusion_2018.10.04.1692m...	VideoMesh	root	10/08/2018 11:15:31	10/08/2018 11:15:31	Running... 85 %	
Destroy	Cisco Meeting Server	root	10/08/2018 03:42:54	10/08/2018 03:42:54	Completed successfully	10/08/2018 03:43:00
Power Off VM	Cisco Meeting Server	root	10/08/2018 03:41:45	10/08/2018 03:41:45	Completed successfully	10/08/2018 03:41:49



**ステップ7** 仮想マシンが実行されている場合は、「**Video Mesh** ノード コンソールへのログイン」に戻って、**Video Mesh** ノードの初期設定を続行します。

# Collaboration Meeting Room Hybrid から Video Mesh への移行パスと機能比較

## 機能の比較

CMR ハイブリッドから Video Mesh に移行する際の利点を把握するために役立つよう、この表では、各オファターの主要機能を並べて比較しています。Video Mesh に関して下記に詳述されている新機能同様、Video Mesh と組み合わせた際は、既存の Webex 機能もこれまで通り作動します。ミーティングの機能拡張に加えて、Video Mesh は、クラウドベースの管理へのアジリティを利用し、既存の投資を継続的に保護することができます。

機能	Video Mesh および Cisco Webex Meeting Center ビデオ	CMRハイブリッド
会議の種類	スケジュール済み ワンクリック (インスタント) パーソナルミーティング (PMR) オンプレミスとクラウドベースのミーティングで一貫性のあるエクスペリエンス	スケジュール済みのみ
スケジューリング	Webex 生産性向上ツール (Windows および Mac) @webex を使用したハイブリッドカレンダーのスケジュール設定 Webex ポータル	Webex 対応 TelePresence の Windows および Mac 生産性向上ツール TMS のスケジュール設定
ミーティング参加オプション	ダイヤルインとダイヤルアウト PIN による保護 (ホスト) ワンボタン機能 (OBTP)	ダイヤルインのみ OBTP
ミーティング中のエクスペリエンス	統一名簿 (Webex クライアント) 統一されたコントロール (Webex クライアント) ミーティングのロック/ロック解除 TelePresence 参加者のミュート/ミュート解除	統一名簿なし (Webex クライアントと Telepresence Server) ばらばらのコントロール (Webex クライアントと Telepresence Server)

機能	Video Mesh および Cisco Webex Meeting Center ビデオ	CMRハイブリッド
キャパシティと展開モデル	無制限のキャパシティ オンプレミスと自動オーバーフロー スイッチングとトランスコーディング	トランスコーディングキャパシティは TelePresence Server に限定

### 移行パスのチェックリスト

以下は、既存のサイトをビデオプラットフォームバージョン 2.0 に移行して、そのサイトを Video Mesh に統合するための準備方法に関するハイレベルの概要です。この手順は、既存の環境によって異なる場合があります。パートナーまたは [カスタマー サクセス マネージャ](#) と協力して、スムーズな移行を行います。

1. Meeting Center Video の会議機能が Webex サイトにプロビジョニングされていることを確認します。
2. サイト管理者が、管理ポータルアカウントを受け取ります。次に、管理者は Webex 組織の Video Mesh ノードを展開します。
3. サイト管理者は、CMR Hybrid ユーザーのすべてまたは一部が Cisco Webex Meeting Center ビデオを利用できるように CMR の権限を割り当てます。
4. (オプション) このサブセットに対する CMR Hybrid セッション タイプを無効にして、ユーザープロファイルの Cisco Webex Meeting Center ビデオを有効にします。
5. サイト管理者が設定 Video Mesh を行い、[**ud Collaboration Meeting Room オプション (Cloud Collaboration Meeting Room Options)**] でメディアリソースの種類として、[**ハイブリッド (Hybrid)**] を選択します。
6. サイト管理者が、オンプレミスの TelePresence Management Suite (TMS) とワンボタン機能 (OBTP) をセットアップし、Cisco Webex Meeting Center ビデオと連携させます。ガイダンスとして、『[Cisco Webex Meeting Center ビデオ会議エンタープライズ導入ガイド](#)』[英語] を参照してください。
7. ユーザーの CMR 権限を有効にすると、Webex 生産性向上ツールは、デフォルトの Cisco Webex Meeting Center ビデオバージョンに設定されます。ユーザーがスケジュールを設定した新しいミーティングは、すべて Cisco Webex Meeting Center ビデオミーティングです。
8. 招待に会議室が含まれている場合、OBTP 情報が TMS を介して会議室にプッシュされます (CMR ハイブリッドミーティングの場合のみ)。
9. CMR ハイブリッドユーザーが Cisco Webex Meeting Center ビデオに切り替わる前に設定した既存のミーティングは、オンプレミスの MCU と TMS の設定が維持される限り、引き続き機能するはずですが。

10. 既存の CMR ハイブリッド ミーティングを変更または更新して、Cisco Webex Meeting Center ビデオ ミーティング情報を反映させることはできません。ユーザーが新しい招待を使用する場合は、古いミーティングを削除し、新しいミーティングを作成する必要があります。
11. オンプレミスの MCU、TMS を廃止する場合、古い CMR ハイブリッド ミーティングは機能しなくなります。Cisco Webex Meeting Center ビデオ情報を使用して、新しいミーティングを作成する必要があります。

## TelePresence 相互運用性プロトコルとセグメント切り替え

Video Mesh 1 画面と 3 画面の両方の IX と TX エンドポイントに対して、TelePresence 相互運用性プロトコル (TIP) と多重化 (MUX) のネゴシエーションをサポートしています。

3 画面のエンドポイントでは、会議の参加者数が十分な場合、3 つのすべての画面にビデオを表示します。会議内に別の 3 画面システムが存在する場合は、部屋の切り替えではなく、セグメントの切り替えが行われます。つまり、別の 3 画面システムで誰かが話している場合に、3 つの画面すべてが拡大表示されるのではなく、アクティブなペインだけが拡大表示されます。他の 2 つのペインには、他のシステムからのビデオが表示されます。縮小表示されている場合、3 つのペインは 1 つの枠でまとめられ、名前ラベルとともに表示されます (1 画面または 3 画面のすべてのデバイス)。

クラウドのホスティングリソースに応じて、3 画面 ルームの 3 つの画面すべてがフィルム ストリップ状に表示されるエンドポイントと、1 つのペインしか表示されないエンドポイントがあります。メディアがオンプレミスの場合でも、Webex アプリ アプリには 1 つのペインだけが表示されます。

ミーティングの規模が大きく、1 つ目のノードからオーバーフローして 2 つ目のノードにカスケードする場合、別のノードにホストされるエンドポイントでも、3 画面システムをホストするエンドポイントと同じ画面が表示されます (レイアウトによって 1 つのペインのみを表示)。プレゼンテーションの共有には、コールパスを通じて BFCP のネゴシエーションが必要になります。

## 翻訳について

このドキュメントは、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。