コラボレーション エンドポイント ソフトウェア バージョン 97
2019 年4月

# 管理者ガイド

Cisco Webex Room Kit Mini 用

Cisco 製品をお選びいただきありがとうございます。

お使いの Cisco 製品は、長年にわたり安全かつ信頼できる操作を行えるよう設計されています。

製品ドキュメンテーションのこの部分は、ビデオ システムのセットアップと設定を担当する管理者を対象としています。

このアドミニストレータ ガイドの主な目的は、ユーザの目標とニーズに対応することです。本書についてのご意見やご感想があれば、ぜひお伝えください。

定期的に Cisco の ウェブ サイトにアクセスし、このガイドの最新版を入手することを推奨します。

各種ユーザ マニュアルは次の URL から入手できます。
► https://www.cisco.com/go/room-docs

## 本ガイドの使用方法

本書上部のメニュー バーと目次の各項目には、すべてハイパーリンクが設定されています。クリックすると、そのトピックに移動します。

# 目次

第 1 章

# はじめに

# ユーザ ドキュメンテーションとソフトウェア

## このガイドの対象となる製品

- Cisco Webex Room Kit Mini

## ユーザ ドキュメンテーョン

このガイドでは、ビデオ システムの管理に必要な情報を提供します。

主にオンプレミス登録のビデオ システム (CUCM、VCS) の機能と設定について説明していますが、クラウド サービス (Cisco Webex) 登録のデバイスにも、その機能と設定の一部が適用されます。

この製品に関する詳しいガイドは、付録 ▶「Cisco ウェブ サイト内のユーザ マニュアル」を参照してください。

### Cisco ウェブ サイト内のドキュメンテーション

次のCisco ウェブ サイトに定期的にアクセスして、ガイドの最新バージョンを確認してください。

▶ https://www.cisco.com/go/room-docs

### クラウドに登録されたデバイスのドキュメンテーション

Cisco Webex cloud サービスに登録されているデバイスについての詳細は、以下を参照してください:

▶ https://help.webex.com

### Cisco Project Workplace

オフィスやミーティング ルームをビデオ会議用に整備する際にインスピレーションを得たり、ガイドラインを確認したりするには、次の Cisco Project Workplace をご覧ください。

▶ https://www.cisco.com/go/projectworkplace

## ソフトウェア

次の Cisco ウェブ サイトからエンドポイント用のソフトウェアをダウンロードします。

▶ https://software.cisco.com/download/home

ソフトウェア リリース ノート (CE9) を参照することをお勧めします。

▶ https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-room-kit-series/tsd-products-support-series-home.html

# CE9 の最新情報

この章では、 CE9.6 と比較した、Cisco Collaboration Endpoint ソフトウェア バージョン 9.x (CE9.x) の新規および変更されたシステム設定の概要と、新機能および改善点を説明しています。

CE9 では以下の製品が新しくなっています:

- CE9.0 - Room Kit
- CE9.1 - Codec Plus、および Room 55
- CE9.2 - Room 70
- CE9.4 - Codec Pro、Room 70 G2、および Room 55 Dual
- CE9.6 - Room Kit Mini

詳細については、次のソフトウェア リリース ノートを読むことをお勧めします。

► https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-room-kit-series/tsd-products-support-series-home.html

## CE9.7 の新機能および改善点

### xAPI に WebSocket 経由で接続します

*(すべての製品)*

xAPI に WebSocket 経由で接続しています。WebSocket 経由の 通信チャネルは明示的に閉じるまで両方の方法で開いています。これはつまり、サーバは新しいデータが利用可能にあんり次第データをクライアントに送信可能で、すべてのリクエストで再認証の必要がないことを意味します。これは、HTTP と比較してかなりスピードを改善します。

各メッセージには完全な JSON ドキュメント以外何も含まれていません。WebSocket と JSON-RPC では多くのプログラミング言語の優れたライブラリサポートがあります。

WebSocket はデフォルトでは有効ではありません。Websocket を使用する前に、WebSocket が HTTP に関連付けられていること、および HTTP または HTTPS が有効になっていることに注意してください。

詳細は、►WebSocket 経由の xAPI ガイドを参照してください。

### 音声コンソールで使用可能なグラフィックサウンドミキサー

*(Codec Pro、MX700、MX800、Room 70 G2、Room 70D G2、SX80)*

オーディオコンソールではグラフィックサウンドミキサーが利用できるようになりました。これには 8 つのユーザー定義可能なパラメータ化された均等化設定があります。設定は、1 つのフィルタタイプ、ゲイン、中央、クロスオーバー周波数、および Q 値を持つ最大 6 つのセクションで構成されています。各セクションは独自の色で表示され、パラメータのいずれかを変更した結果がすぐにグラフに表示されるようになります。

詳しくは、次のリンク先にある *カスタマイズ ガイド*CE9.7 向け を参照してください ► https://www.cisco.com/go/in-room-control-docs

### 周囲ノイズレポート

*(Codec Plus、Codec Pro、Room 55、Room 55 Dual、Room 70、Room 70 G2、Room Kit、Room Kit Mini)*

ルームシリーズデバイスは、室内の固定周囲ノイズを報告するように設定可能です。レポートされた値はA荷重デシベル値(dBA)で、人間の耳の応答に反響します。レポートされたノイズを元に、施設管理または建物マネージャーは介入して問題をトラブルシュートできます。

この機能に関連するすべてのシグナリング処理はローカルで、転送されるデータは算出されたノイズレベルだけです。

### マルチ SRG-120DH/PTZ-12 カメラのサポート *(Codec Plus)*

HDMI およびイーサネット スイッチを使って最大 3 代の SRG-120DH/PTZ-12 を Codec Plus に接続できるようになりました。

### その他のアップデート

- 1080p は USB カメラとして使用されている場合に Room Kit Mini をサポートします。*(Room Kit Mini)*
- 通話中にビデオをオフまたはオンにできます。*(すべての製品)*
- システム管理者は HTTP の使用を防ぎ、HTTPS ポストおよび HTTPS プットリクエストだけを許可できます。*(すべての製品)*

# CE9.7 でのシステム設定の変更点

## 新しい設定

HttpClient AllowHTTP *(すべての製品)*

ロギングデバック WiFi *(Codec Plus、Codec Pro、DX70、DX80、Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2)*

ロギング内部モード *(すべての製品)*

NetworkServices SNMP モード *(すべての製品)*

Phonebook サーバ [1] Pagination *(すべての製品)*

*RoomAnalytics AmbientNoiseEstimation モード (Codec Plus, Codec Pro, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2)*

ユーザーインターフェースには通話ビデオミュートが備わっています *(Codec Plus、Codec Pro、MX200 G2、MX300 G2、MX700、MX800、Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2、SX10、SX20、SX80)*

UserInterface Features Whiteboard Start *(DX70, DX80)*

ユーザーインターフェースセキュリティモード *(すべての製品)*

ユーザーインターフェース設定メニューモード *(すべての製品)*

ユーザーインターフェース UsbPromotion *(Room Kit Mini)*

## 変更された設定

音声入力ライン [1..4] VideoAssociation VideoInputSource
- 旧: 1/2/3/4/5
- 新: 1/2/3/4

音声入力マイク [1..8] VideoAssociation VideoInputSource
- 旧: 1/2/3/4/5
- 新: 1/2/3/4/5/6

音声入力マイク [1..8] VideoAssociation VideoInputSource
- 旧: 1/2/3/4/5
- 新: 1/2/3/4

通話履歴モード *(すべての製品)*
- 旧: パブリック: 偽
- 新: パブリック: 真

会議マルチポイントモード *(Codec Plus、Codec Pro、MX200 G2、MX300 G2、MX700、MX800、Room Kit、Room Kit Mini、Room 55、Room 55D、Room 70、Room 70 G2、SX20、SX80)*
- 旧: パブリック: 偽
- 新: パブリック: 真

ロギング内部モード *(すべての製品)*
- 旧: パブリック: 偽
- 新: パブリック: 真

ロギング外部プロトコル *(すべての製品)*
- 旧: パブリック: 偽
- 新: パブリック: 真

ロギング 外部サーバのアドレス *(すべての製品)*
- 旧: パブリック: 偽
- 新: パブリック: 真

ロギング外部サーバポート *(すべての製品)*
- 旧: パブリック: 偽
- 新: パブリック: 真

SIP ANAT *(すべての製品)*

旧: パブリック: 偽

新: パブリック: 真

ビデオ入力コネクタ [n] CameraControl モード *(Codec Pro、Room 70 G2)*

旧 : デフォルトは On です。

新 : デフォルトは Off です。

旧: オン

新: オン/オフ

ビデオ プレゼンテーションの優先順位 *(全製品)*

旧: パブリック: 偽

新: パブリック: 真

旧: 等しい/高

新: 等しい/高/低

## 削除された設定

RoomAnalytics PeopleCountOutOfCall *(MX700、MX800)*

# Room Kit の概要

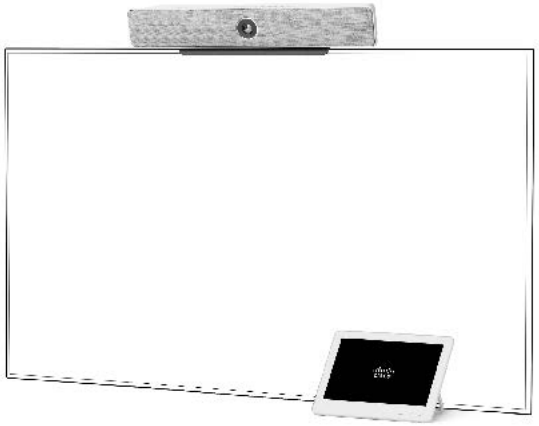
Cisco Webex Room Kit Mini では、カメラ、コーデック、スピーカー、およびマイクが 4K 画面に統合されています。簡単に設置でき、HDMI CEC によってフラット パネル ディスプレイとの優れた統合が実現されます。

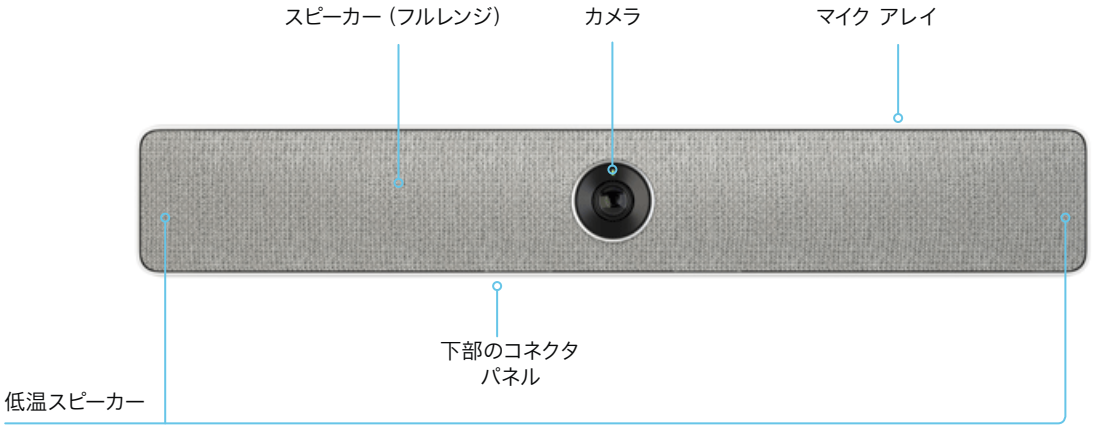
Room Kit Mini は、120 度の視野によって 3 ~ 5 人がいるスペース向けに設計されています。以前はハイエンドのビデオ会議室の領域であった洗練された機能が、あらゆる部屋とあらゆるチームに提供されます。

この Room Kit mini は、クラウド (Cisco Webex) とオンプレミス (CUCM および VCS) の両方で展開できるように構築されています。

## 機能とメリット

- インテリジェントな表示機能を備えた目立たない内蔵カメラ : 会議出席者を検知し、ベスト オーバービューを表示します。
- 室内の人数のカウント : 優れたリソース プランニングのための分析を可能にします。
- 内蔵されたマイクとスピーカーによって優れたオーディオ エクスペリエンスが提供されます。
- ノイズ自動抑制機能により、会議室で発生するノイズを低減
- 誰かが会議室に入る時に、モバイル デバイスを介して入室者を認識し、システムがスリープ状態から自動で起動
- Cisco Touch 10 または Cisco Webex Teams アプリケーションで簡単に制御可能
- Cisco Touch 10 による照明やブラインドなどの周辺機器の制御 (室内制御)
- 4K コンテンツ共有 (ローカル会議では 30 fps、遠端では 5 fps)
- 有線またはワイヤレスでのコンテンツ シェアリング
- イーサネットと Wi-Fi
- USB カメラモード (ビデオシステムのカメラ、マイク、およびスピーカーを含む)
- Cisco Webex Room Kit mini の詳細については、► https://www.cisco.com/go/roomkit を参照してください。





# 電源のオンとオフ

## ユーザインターフェイスを使用した再起動とスタンバイ

### システムを再起動します。

1. ユーザ インターフェイスの左上隅にある連絡先情報を選択します。
2. *[設定 (Settings) ]*、*[再起動 (Restart) ]* の順に選択します。
3. *[再起動 (Restart) ]* を再度選択して、選択内容を確認します。

### スタンバイ モードの開始/終了

1. ユーザ インターフェイスの左上隅にある連絡先情報を選択します。
2. *[スタンバイ (Standby) ]* を選択します。

## リモートからシステムの電源をオフにするか再起動する

ウェブ インターフェイスにサインインして、*[メンテナンス (Maintenance) ] > [再起動 (Restart) ]* に移動します。

### システムを再起動します。

*[デバイスの再起動... (Restart device...) ]* をクリックします。

システムが使用可能になるまでに、数分かかります。

### システムの電源をオフにする

*[デバイスのシャットダウン... (Shutdown device...) ]* をクリックします。

システムの電源をリモートで再度オンにすることはできません。

システムの電源を入れるには、電源プラグを抜いてから再度接続する必要があります。

# LED インジケータ

## システム LED

*アイドル モード時 (スクリーンはアウェイク) :*

点灯状態になります。

*スタンバイ モード時 (スクリーンはオフ) :*

点灯状態になります。

*スリープ モード時 (低電力モード) :*

LED がゆっくり点滅します。

*要注意時 (ネットワーク接続がないなど) :*

LED が 2 回ずつ、繰り返し点滅します。

*スタートアップ (起動) 時:*

LED が点滅します。システムが使用可能なると点灯状態になります。

## カメラの LED

*コールの着信時:*

LED が点滅します。

*コール中:*

点灯状態になります。

*セルフビュー オン時:*

点灯状態になります。

# ビデオ システムの管理方法 (1/4 ページ)

一般的には、このアドミニストレータ ガイドに記載されているように、ウェブ インターフェイスを使用してビデオ システムを管理/保守することをお勧めします。

次のような方法でもビデオ システムの API にアクセスできます。

- HTTP または HTTPS (ウェブ インターフェイスでも使用される)
- SSH
- シリアル インターフェイス (RS-232)

別のアクセス方法、および API の使用方法の詳細については、ビデオ システムの*API ガイド*を参照してください。

| アクセス方式 | 注 | 方式の有効化/無効化方法 |
|---|---|---|
| HTTP/HTTPS | • ビデオ システムの ウェブ インターフェイスで使用<br>• 非セキュア (HTTP) 通信またはセキュア (HTTPS) 通信<br>• HTTPS : デフォルトで*有効*<br>• HTTP : 以前のソフトウェア バージョンから CE9.4 (以降) にアップグレードされ、アップグレード後に工場出荷時の設定にリセットされていない状態で提供されるビデオシステムのみ、デフォルトで*有効*となります。 | *[ネットワークサービス (NetworkServices) ] > [HTTP] > [モード (Mode) ]*<br>変更を有効にするには、ビデオ システムを再起動します。 |
| SSH | • セキュアな TCP/IP 接続<br>• *デフォルトでイネーブルになっている。* | *[ネットワークサービス (NetworkServices) ] > [SSH] > [モード (Mode) ]*<br>ビデオ システムを再起動する必要はありません。変更が有効になるまでに少し時間がかかる場合があります。 |
| シリアル インターフェイス (RS-232) | • ケーブルを使用してビデオ システムに接続IP アドレス、DNS、ネットワークは不要。<br>• *デフォルトでイネーブルになっている。*<br>• セキュリティ上の理由から、デフォルトではサインインするよう求められます (*[シリアル ポート (SerialPort) ] > [ログインが必須 (LoginRequired) ]*) | *[シリアルポート (SerialPort) ] > [モード (Mode) ]*<br>変更を有効にするには、ビデオ システムを再起動します。 |

すべてのアクセス方式を無効にする ([オフ (Off) ] )に設定する) と、ビデオ システムを設定できなくなります。再度有効にする ([オン (On) ] に設定する) ことはできないため、復元するにはビデオ システムを工場出荷時設定にリセットする必要があります。

**Tip**

設定またはステータスが API で使用可能な場合、ウェブ インターフェイスの設定またはステータスは次のような API の設定またはステータスに変換されます。

*X > Y > Z* への **Value** の設定 (Web)
次と同等です。
`xConfiguration X Y Z: 値` (API)

(Web で) *X > Y > Z* ステータスにチェックマークを付けることは
以下と同じです。
`xStatus X Y Z` (API)

次に例を示します。

*[システムユニット (SystemUnit) ] > [名前 (Name) ]* を [**MySystem**] と設定すると、
次と同等です。
`xConfiguration SystemUnit Name: MySystem`

*[システムユニット (SystemUnit) ] > [ソフトウェア (Software) ] > [バージョン (Version) ]* ステータスにチェックマークを付けることは
以下と同じです。
`xStatus SystemUnit Software Version`

ウェブ インターフェイスでは、API の場合よりも多くの設定とステータスを使用できます。

ビデオ システムの管理方法 (2/4 ページ)

# ビデオ システムの ウェブ インターフェイス

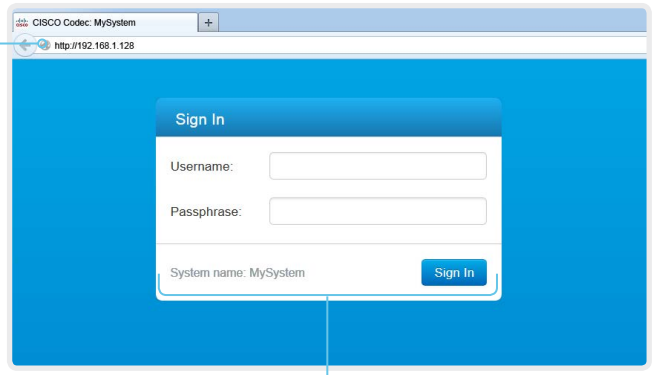
ウェブ インターフェイスは、ビデオ システムの管理ポータルです。コンピュータから接続して、システムをリモートで管理できます。フル設定アクセスが提供され、メンテナンス用のツールやメカニズムを利用できます。

注 : ウェブ インターフェイスを使用するには HTTP または HTTPS が有効になっている必要があります *([ネットワークサービス (NetworkServices) ] > [HTTP] > [モード (Mode) ]* 設定を参照) 。

ウェブ ブラウザは最新版を使用することを推奨します。

## ビデオ システムへの接続

ウェブ ブラウザを開き、ビデオ システムの IP アドレスをアドレス バーに入力します。




**IP アドレスの確認方法**

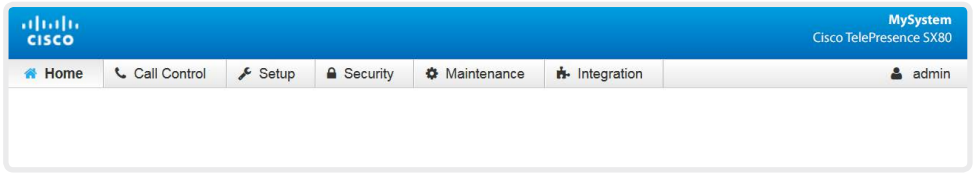
1. ユーザ インターフェイスの左上隅にある連絡先情報を選択します。
2. *[このデバイスについて (About this device) ]* に続き、*[設定 (Settings) ]* を選択します。

## サインイン

エンドポイントのユーザ名とパスフレーズを入力して、*[サインイン (Sign In) ]* をクリックします。

システムには、パスフレーズなしの *admin* というデフォルトのユーザが提供されています。初めてサインインするときは、*[パスフレーズ (Passphrase) ]* フィールドを空白のままにします。

*admin* ユーザのパスワードを設定する必要があります。




## サインアウト

ユーザ名の上にカーソルを移動し、ドロップダウン リストから *[サインアウト (Signout) ]* を選択します。

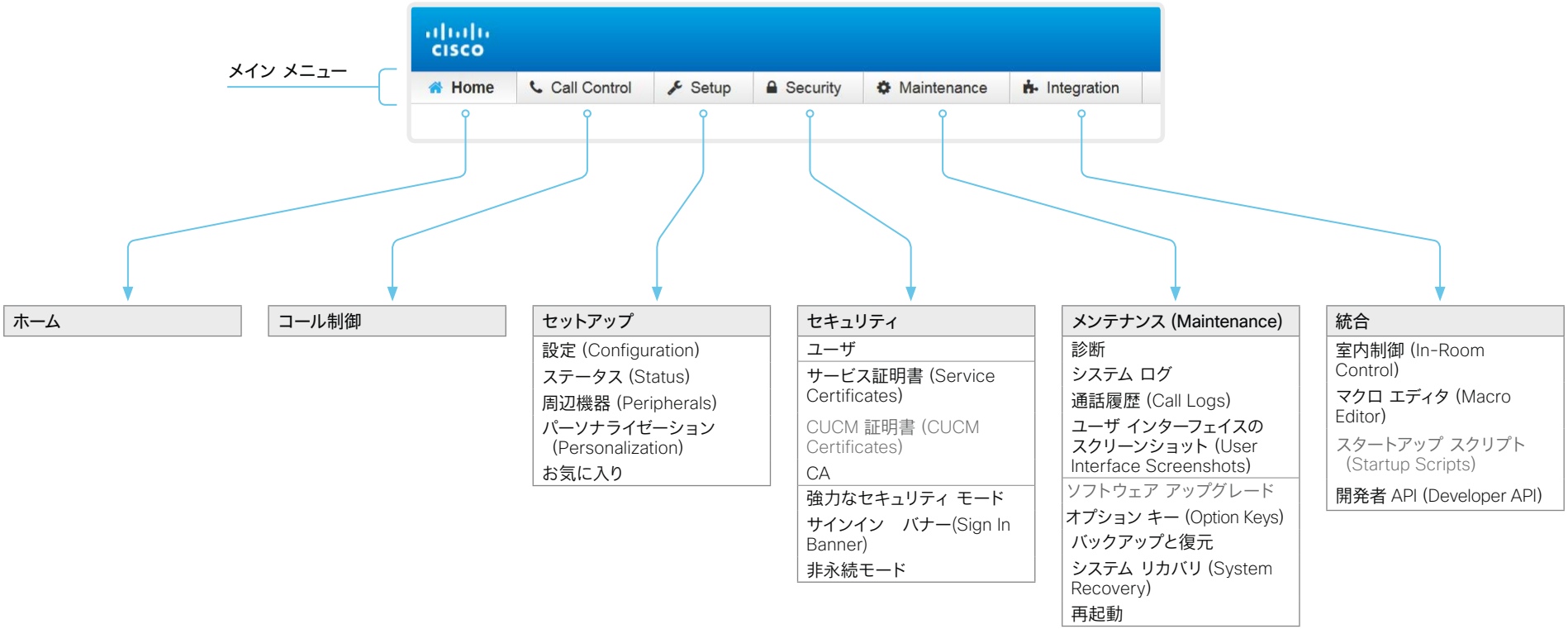
ビデオ システムの管理方法 (3/4 ページ)

# ウェブ インターフェイスの構成

ウェブ インターフェイスは、各サブページから構成されています。ビデオ システムがオンプレミス サービス (CUCM、VCS) に登録されているときは下に示すすべてのサブページを使用できます。ビデオ システムが Cisco のクラウド サービス (Cisco Webex) に登録されているときは灰色で示されているページを使用できません。

どちらの場合も、サインインしているユーザには、アクセス権のあるページだけが表示されます。

ユーザ管理、ユーザ ロール、およびアクセス権の詳細については、
► 「ユーザ管理」の章をお読みください。



ビデオ システムの管理方法 (4/4 ページ)

# ユーザ インターフェイスの設定とシステム情報

ビデオ システムのユーザ インターフェイスでシステム情報と一部の基本設定およびシステム テストにアクセスできます。

システムの重要な設定と機能 (ネットワーク設定、サービスの有効化、向上出荷時設定へのリセットなど) は、パスフレーズで保護できます。► 「[設定 (Settings) ] メニューへのアクセスの制限」の章を参照してください。

一部の設定とテストは、ビデオ システムの電源を初めて入れたときに起動される*セットアップ アシスタント*の一部にもなっています。セットアップ アシスタントについては、CE ソフトウェアを実行しているシステムの『スタートアップ ガイド』を参照してください。

## アクセス設定

1. ユーザ インターフェイスの左上隅にある連絡先情報を選択します。
2. *[設定 (Settings) ]* を選択します。

   南京錠の記号 は、設定が保護されている (ロックされている) ことを示しています。
3. 変更する設定または実行するテストを選択します。

   設定がロックされている場合は認証ウィンドウが表示され、続行するには ADMIN クレデンシャルでサインインする必要があります。

第 2 章

# 設定

# ユーザ管理

ウェブとコマンドライン インターフェイスにアクセスするには、サインインする必要があります。ユーザには、アクセス権を持つ対象を決める、異なるロールを割り当てることができます。

## デフォルトのユーザ アカウント

ビデオ システムには、フル アクセス権が与えられたデフォルトの管理者ユーザ アカウントが付属しています。ユーザ名は *admin* で、パスフレーズは初期状態では設定されていません。

必ず *admin* ユーザのパスフレーズを設定する必要があります。

パスフレーズの設定方法については、► 「システム パスフレーズの変更」の章を参照してください。

## 新しいユーザ アカウントの作成

1. ウェブ インターフェイスにサインインして、*[セキュリティ (Security) ] > [ユーザ (Users) ]* に移動します。
2. *[新規ユーザを追加 (Add New User) ]* を選択します。.
3. *[ユーザ名 (Username) ]*、*[パスフレーズ (Passphrase) ]*、*[パスフレーズの確認 (Repeat passphrase) ]* の各入力フィールドに入力します。

   デフォルトでは、ユーザが初めてサインインしたときにパスフレーズを変更する必要があります。

   認証にクライアント証明書を使用する場合にのみ、[クライアント証明書 DN（識別名）(*Client Certificate DN*) ] フィールドに値を入力してください。
4. 適切な *[ロール (Roles) ]* チェックボックスをオンにします。

   ADMIN ロールをユーザに割り当てた場合は、*[自分のパスフレーズ (Your passphrase) ]* 入力フィールドに自分自身のパスフレーズを確認のために入力します。
5. ユーザをアクティブにするには、*[ステータス (Status) ]* を [アクティブ (**Active**) ] に設定します。
6. [*Create User*] をクリックします。

   変更を加えないで終了するには、[戻る (Back) ] ボタンを使用します。

## 既存のユーザ アカウントの編集

ADMIN ロールが割り当てられているユーザを変更する場合は 常に、[パスフレーズ (Your passphrase) ] 入力フィールドに確認のため各自のパスフレーズを入力する必要があります。

### ユーザ特権を変更する

1. ウェブ インターフェイスにサインインして、*[セキュリティ (Security) ] > [ユーザ (Users) ]* に移動します。
2. リスト内の該当ユーザをクリックします。
3. ユーザ ロールを選択し、ステータスを [アクティブ（**Acitve**) ] または [非アクティブ (**Inactive**) ] に設定してから、そのユーザが次回ログインしたときにパスフレーズを変更する必要があるかどうかを決定します。

   HTTPS で証明書ログインを使用する場合にのみ、[クライアント証明書 DN（識別名）(Client Certificate DN) ] フィールドに値を入力してください。
4. *[ユーザの編集 (Edit User) ]* をクリックして変更内容を保存します。

   変更を加えないで終了するには、*[戻る (Back) ]* ボタンを使用します。

### パスフレーズを変更する

1. ウェブ インターフェイスにサインインして、*[セキュリティ (Security) ] > [ユーザ (Users) ]* に移動します。
2. リスト内の該当ユーザをクリックします。
3. 該当する入力フィールドに新しいパスフレーズを入力します。
4. *[パスフレーズの変更 (Change Passphrase) ]* をクリックして、変更を保存します。

   変更を加えないで終了するには、[戻る (Back) ] ボタンを使用します。

### ユーザ アカウントを削除する

1. ウェブ インターフェイスにサインインして、*[セキュリティ (Security) ] > [ユーザ (Users) ]* に移動します。
2. リスト内の該当ユーザをクリックします。
3. *[ユーザの削除... (Delete user...) ]* をクリックし、プロンプトが表示されたら確定します。

## ユーザ ロール

1 つのユーザ アカウントは、1 つのユーザ *ロール*または複数の組み合わせを保持できます。デフォルトの *admin* ユーザなどの、フル アクセス権を持つユーザ アカウントは、admin、user、audit の各役割も持つ必要があります。

これらは*ユーザ ロール*です。

**ADMIN**：このロールを持つユーザは、新規ユーザの作成、ほとんどの設定の変更、通話、および連絡先リストの検索ができます。このユーザは監査証明書のアップロードもセキュリティ監査設定の変更も行えません。

**USER**：このロールを持つユーザはコールの発信と連絡先リストの検索が可能です。このユーザは呼び出し音量の調整や時刻と日付の表示形式の変更など、いくつかの設定を変更できます。

**AUDIT**：このロールを持つユーザは、セキュリティ監査の設定の変更および監査証明書のアップロードが可能です。

**RoomControl**：このロールを持つユーザは、室内制御を作成できます。ユーザは室内制御エディタおよび対応する開発ツールにアクセスできます。

**INTEGRATOR**： このロールを持つユーザは、高度な AV シナリオを設定し、ビデオ システムをサードパーティの機器と統合するために必要な設定、コマンド、およびステータスにアクセスできます。このユーザは、室内制御を作成することもできます。

# システム パスフレーズを変更する

次の操作を行うには、システム パスフレーズを知っている必要があります。

- ウェブ インターフェイスへのログイン
- コマンドライン インターフェイスへのログインと、その使用

## デフォルトのユーザ アカウント

ビデオ システムは、デフォルトのユーザ アカウントにフル アクセス権が付与された状態で提供されます。ユーザ名は*admin*で、初期状態ではパスフレーズは設定されていません。

システム設定へのアクセスを制限するために、必ず、デフォルトの *admin* ユーザ用のパスフレーズを設定する必要があります。さらに、管理者権限を持つ他のすべてのユーザにもパスフレーズを設定する必要があります。

*admin* ユーザのパスフレーズが設定されるまでは、システム パスフレーズが設定されていないことを示す警告が画面上に表示されます。

## 他のユーザ アカウント

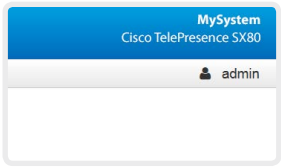
ビデオ システムのユーザ アカウントを複数作成することができます。

ユーザ アカウントを作成および管理する方法の詳細については、▶「ユーザ管理」の章を参照してください。

## パスフレーズを変更する

1. ウェブ インターフェイスにログインし、ユーザ名の上にマウスを移動し、ドロップダウン リストから *[パスフレーズの変更 (Change Passphrase) ]* を選択します。
2. 入力フィールドに現在のパスフレーズと新しいパスフレーズを入力して、*[パスフレーズの変更]* をクリックします。

   パスフレーズの形式は、0 ～ 64 文字の文字列です。




現在パスフレーズが設定されていない場合は、*[現在のパスフレーズ (Current passphrase) ]* フィールドを空白のままにします。

## 別のユーザのパスフレーズの変更

管理者アクセス権がある場合は、すべてのユーザのパスフレーズを変更できます。

1. ウェブ インターフェイスにサインインして、*[セキュリティ (Security) ] > [ユーザ (Users) ]* に移動します。
2. リスト内の該当ユーザをクリックします。
3. 新しいパスフレーズを、*[パスフレーズ (Passphrase) ]* および [パスフレーズの確認 (*Repeat passphrase) ]* 入力フィールドに入力します。

   該当ユーザが admin ロールを持っている場合は、*[自分のパスフレーズ (Your passphrase) ]* 入力フィールドに自分自身のパスフレーズを確認のために入力する必要があります。
4. *[パスフレーズの変更 (Change Passphrase) ]* をクリックして、変更を保存します。

   変更を加えないで終了するには、[戻る (Back) ] ボタンを使用します。

# [設定 (Settings) ] メニューへのアクセスの制限

デフォルトでは、任意のユーザが、ユーザ インターフェイスの [設定 (Settings) ] メニューにアクセスできます。

権限のないユーザがビデオ システムの設定を変更できないようにするために、このアクセスを制限することをお勧めします。

## [設定 (Settings) ] メニューをロックする

1. ウェブ インターフェイスにサインインして、*[セットアップ (Setup) ] > [設定 (Configuration) ]* に移動します。
2. *[ユーザインターフェイス (UserInterface) ] > [設定メニュー (SettingsMenu) ] > [モード (Mode) ]* に移動して、*[ロック (Locked) ]* を選択します。
3. *[保存 (Save) ]* をクリックして変更を有効にします。

   これにより、ユーザは、ADMIN クレデンシャルでサインインしないとユーザ インターフェイス (タッチ コントローラ) でシステムの重要な設定にアクセスできなくなります。

## [設定 (Settings) ] メニューのロック解除

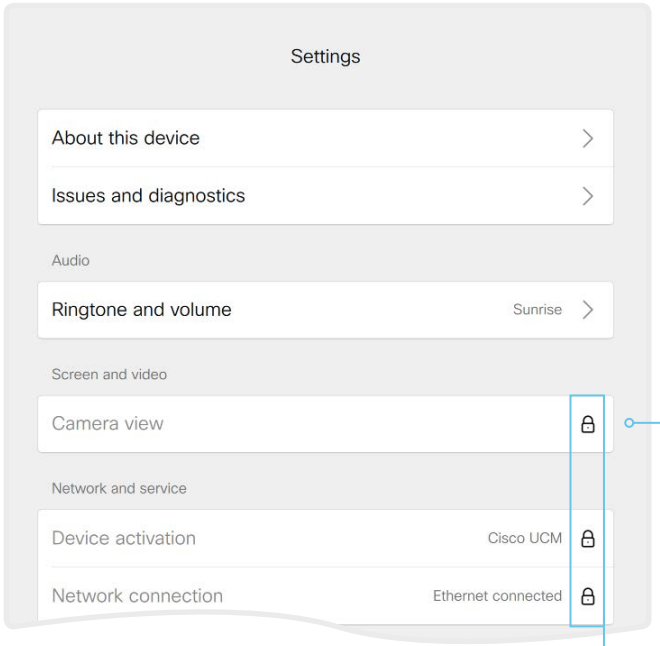
1. ウェブ インターフェイスにサインインして、*[セットアップ (Setup) ] > [設定 (Configuration) ]* に移動します。
2. *[ユーザインターフェイス (UserInterface) ] > [設定メニュー (SettingsMenu) ] > [モード (Mode) ]* に移動して、*[ロックなし (Unlocked) ]* を選択します。
3. *[保存 (Save) ]* をクリックして変更を有効にします。

   これにより、任意のユーザが、ユーザインターフェイス (タッチ コントローラ) ですべての [設定 (Settings) ] メニューにアクセスできるようになります。

## ユーザ インターフェイスの [設定 (Settings) ] メニュー

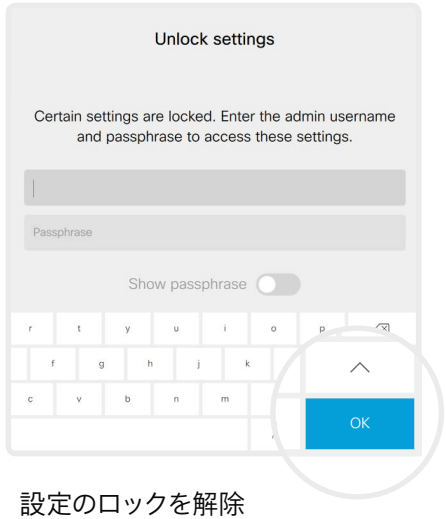
このメニューがロックされている場合は、サインインしないと、システムの重要な設定にアクセスできません。

[設定 (Settings) ] メニューを開くには、ユーザ インターフェイスの左上隅にある連絡先情報を選択し、*[設定 (Settings) ]* を選択します。




### ロックされた設定

ロックされた設定には南京錠のマークが付いています。




### 設定のロックを解除

南京錠をクリックすると、ADMIN ユーザでサインインするように求められます。

サインインすると、[設定 (Settings) ] メニューを閉じるまで、すべての設定にアクセスできます。

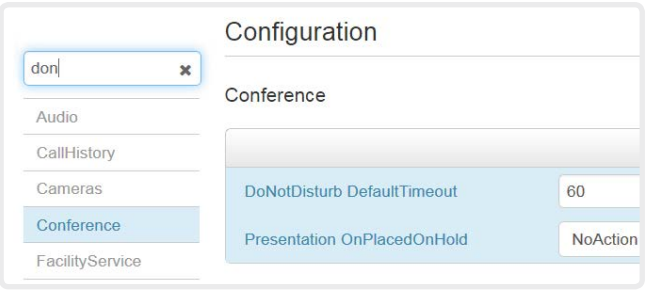
# システム設定

ウェブ インターフェイスにサインインして、*[セットアップ (Setup) ] > [設定 (Configuration) ]*を移動します。

## システム設定を検索する

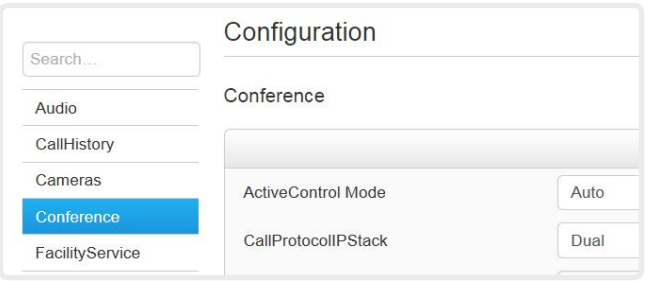
### 設定を検索する

検索フィールドに必要な数の文字を入力します。これらの文字が含まれているすべての設定が右側のペインに表示されます。値スペースにこれらの文字が含まれている設定も表示されます。




### カテゴリを選択して設定に移動する

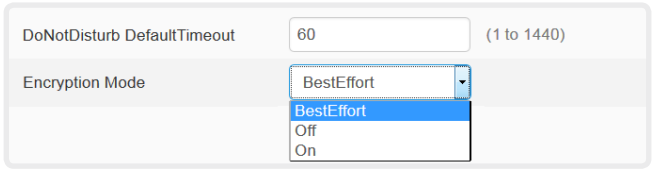
システム設定は各カテゴリにグループ化されています。左側のペインのカテゴリを 1 つ選択して、関連付けられている設定を表示します。




## システム設定を変更する

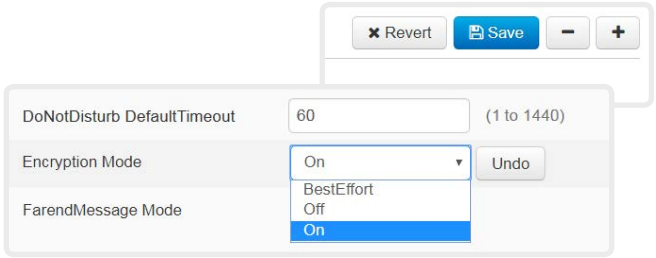
### 値スペースを確認する

設定の値スペースは、入力フィールドに続くテキストか、矢印をクリックすると開くドロップダウン リストで指定します。




### 値の変更

1. ドロップダウン リストから望ましい値を選択するか、入力フィールドに新しいテキストを入力します。
2. *[保存 (Save) ]* をクリックして変更を有効にします。
   変更しない場合は、*[元に戻す (Undo) ]* ボタンまたは *[復元 (Revert) ]* ボタンを使用します。




変更が保存されていないカテゴリには、編集記号 ( ) のマークが付きます。

## システム設定について

ウェブ インターフェイスからすべてのシステム設定を変更できます。

個別のシステム設定については
▶ 「システム設定」の章を参照してください。

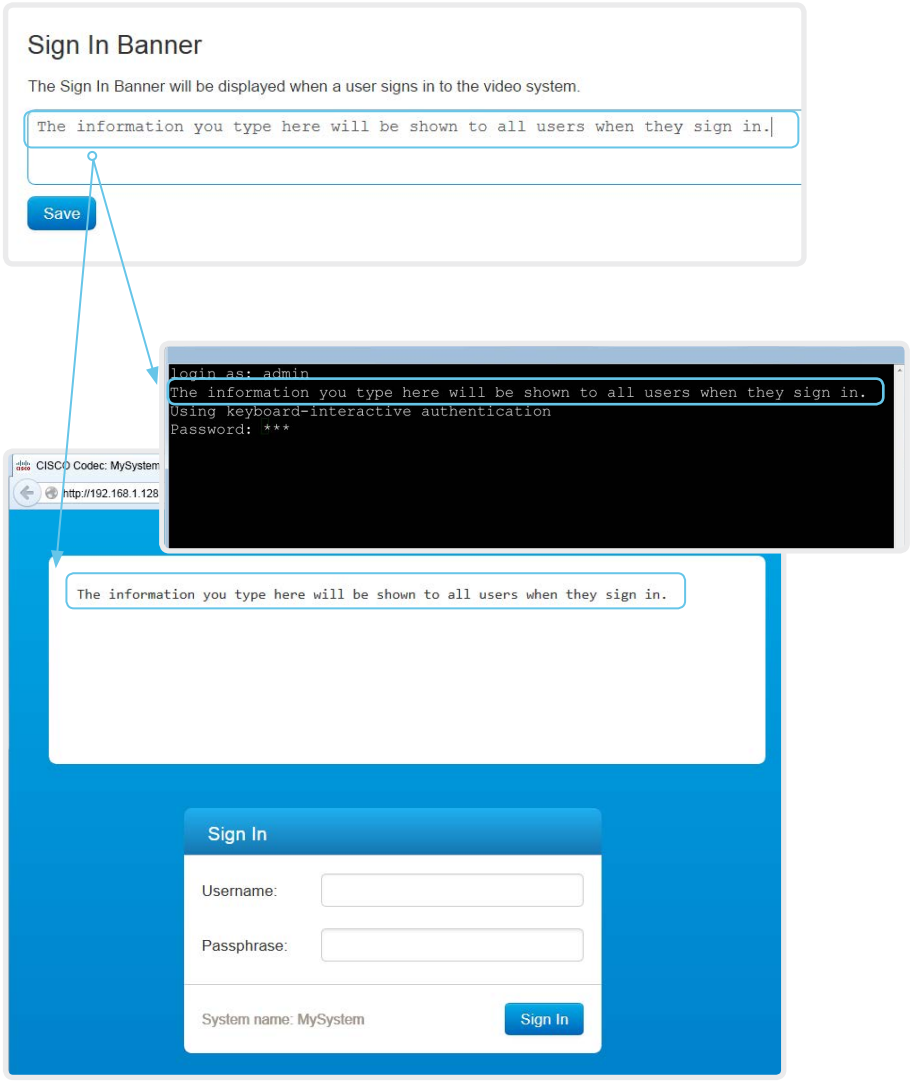
異なる設定には、異なるユーザ クレデンシャルが必要である場合があります。管理者はすべてのシステム設定を変更できるように、すべてのユーザ ロールを所有している必要があります。

ユーザ管理およびユーザ ロールに関する詳細情報は、▶ 「ユーザ管理」の章で確認できます。

# サインイン バナーの追加

ウェブ インターフェイスにサインインして、*[設定 (Configuration) ] > [サインイン バナー (Sign In Banner) ]* に移動します。

1. サインインしたユーザに表示するメッセージを入力します。
2. *[保存 (Save) ]* をクリックしてバナーをアクティブにします。




## サインイン バナーについて

システム管理者がすべてのユーザに初期情報を提供したい場合、サインイン バナーを作成できます。メッセージは、ユーザが ウェブ インターフェイスまたはコマンドライン インターフェイスにサインインすると表示されます。

最大サイズは 4 kByte です。

### ウェルカムバナーとサインインバナーの比較

サインインバナー

- バナーは、ユーザーが ウェブ インターフェイスまたはコマンドラインインターフェイスにサインインする*前*に表示されます。

ウェルカムバナー

- バナーは、ユーザーが ウェブ インターフェイスまたはコマンドラインインターフェイスにサインインした*後*に表示されます。

# ウェルカムバナーの追加

ウェルカムバナーの追加は API コマンドを使用してのみ利用可能です。専用のユーザーインターフェイスは提供されません。

## API コマンド

```
xCommand SystemUnit WelcomeBanner Set
```

これはマルチライン コマンドです。このコマンド実行後に入力した文字が、コマンドに対する入力となります （改行を含む）。ピリオドを含み改行で終わる別の行を用いて、入力を終了します。

他にもいくつかウェルカムバナーのコマンドが存在します。API ガイドにて詳細をご確認ください。

```
xCommand SystemUnit WelcomeBanner Clear
xCommand SystemUnit WelcomeBanner Get
```

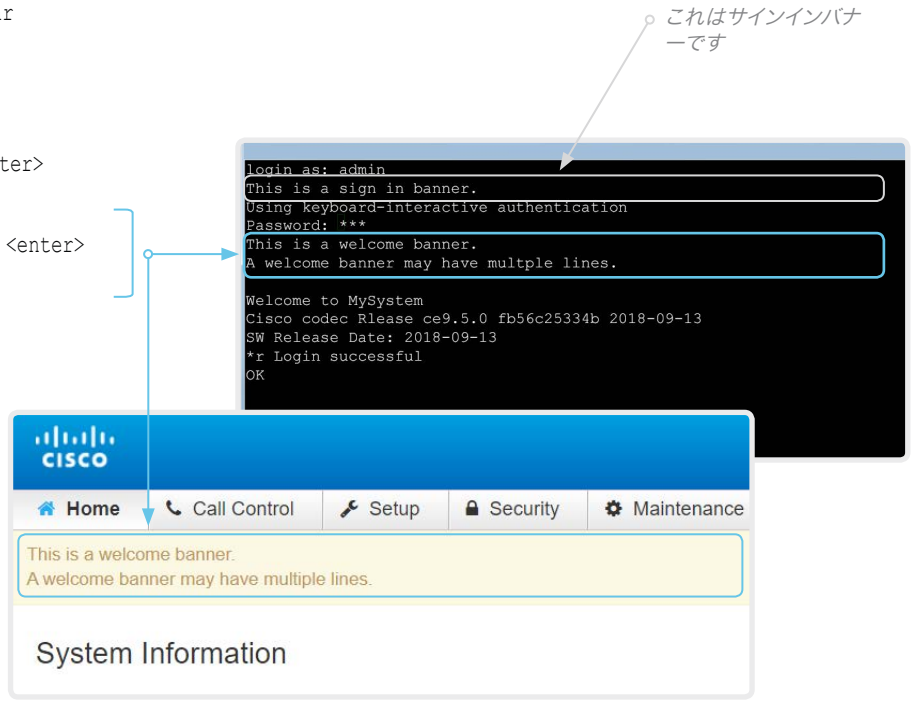
## 例

```
xCommand SystemUnit WelcomeBanner Set <enter>
```

**これはウェルカムバナーです。**<enter>

**ウェルカムバナーには複数の行を表示することができます。**<enter>

. <enter>




## ウェルカムバナーについて

ビデオシステムのウェブインターフェイスまたはコマンドラインインターフェイスに、ユーザーがログイン後で表示されるウェルカムバナーを設定できます。バナーには、複数の行を表示することができます。

バナーには作業開始に必要な情報や、システムのセットアップ時に注意しなければならないことなどが含まれています。

最大サイズは 4 kByte です。

### ウェルカムバナーとサインインバナーの比較

サインインバナー

- サインインバナーは、ユーザーが ウェブインターフェイスまたはコマンドラインインターフェイスにサインインする*前*に表示されます。

ウェルカムバナー

- ウェルカムバナーは、ユーザーが ウェブインターフェイスまたはコマンドラインインターフェイスにサインインした*後*に表示されます。

# ビデオ システムのサービス証明書を管理する

ウェブ インターフェイスにサインインして、*[セキュリティ (Security) ] > [サービス証明書 (Service Certificates) ]* に移動します。

次のファイルが必要です。

- 証明書 (ファイル形式 : .PEM)
- 個別のファイルとして、または証明書と同じファイルに含まれる秘密キー (ファイル形式 : .PEM 形式)
- パスフレーズ (秘密キーが暗号化されている場合にのみ必要)

証明書と秘密キーは、ビデオ システムの同じファイル内に保存されます。

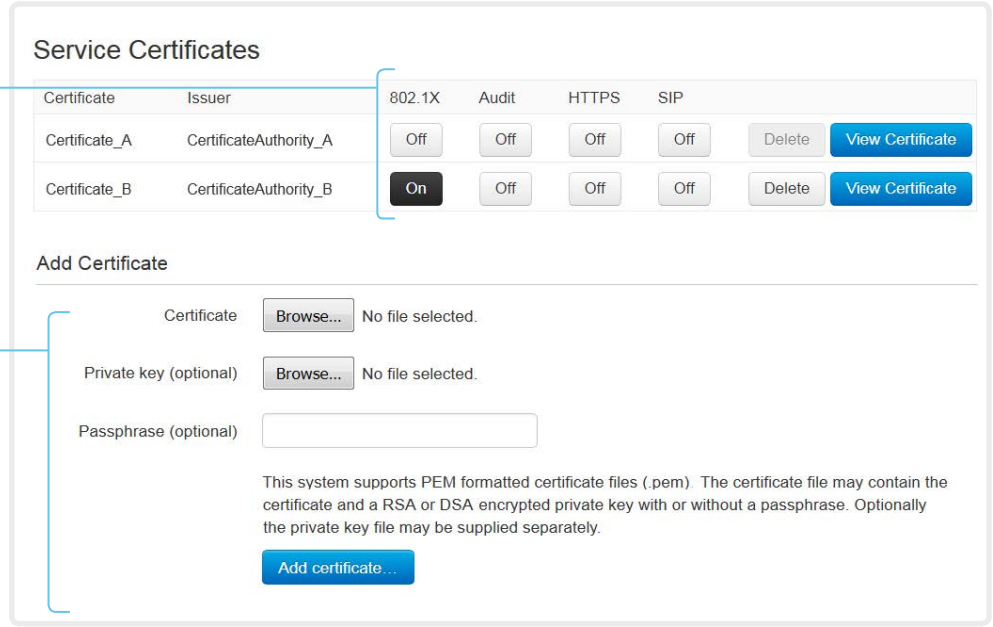
## 証明書を有効/無効にし、表示、または削除する

各サービスの証明書を有効または無効にするには、[オン (On) ] および [オフ (Off) ] ボタンを使用します。

証明書を表示または削除するには、それぞれ対応するボタンを使用します。

## 証明書の追加

1. [参照 (Browse) ] ボタンを押して、コンピュータ上の証明書ファイルと秘密キー ファイル (オプション) を見つけます。
2. 必要な場合には *[パスフレーズ (Passphrase) ]* に入力します。
3. *[証明書の追加... (Add certificate...) ]* をクリックして、証明書をビデオ システムに保存します。




図に示している証明書および証明書発行者は一例です。お使いのシステムには別の証明書があります。

## ビデオ システムのサービス証明書について

証明書の検証は、TLS (Transport Layer Security) を使用する場合に必要になることがあります。

通信をセットアップする前に、有効な証明書をビデオ システムが提供するよう、サーバまたはクライアントが要求することがあります。

ビデオ システムの証明書は、システムの信頼性を確認するテキスト ファイルです。これらの証明書は、認証局 (CA) によって発行されます。

これらの証明書は、HTTPS サーバ、SIP、IEEE 802.1X、および監査ロギングの各サービスで使用されます。

複数の証明書をビデオ システムで保存できますが、サービスごとに一度に有効化できる証明書は 1 つだけです。

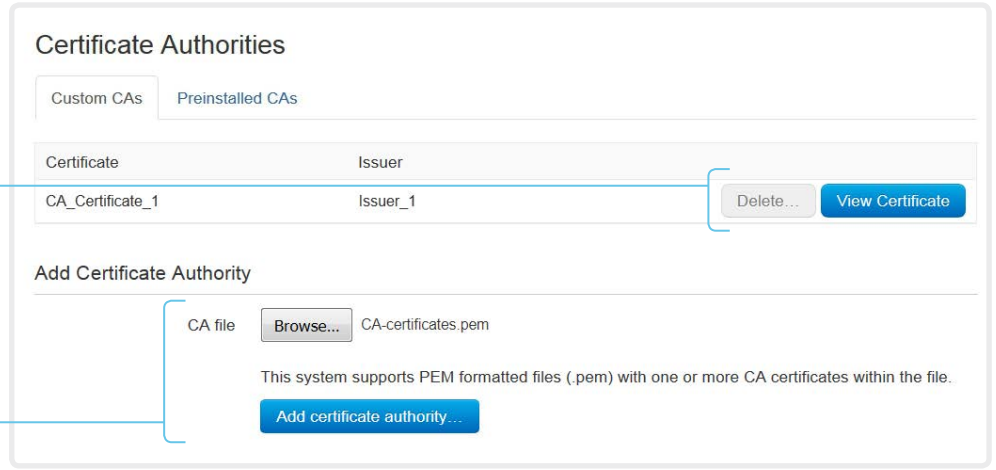
認証が失敗した場合、接続は確立されません。

# 信頼できる認証局 (CA) のリストを管理する

ウェブ インターフェイスにサインインし、*[セキュリティ (Security) ] > [証明機関 (Certificate Authorities) ]* に移動して、*[カスタム CA (Custom CAs) ]* タブを開きます。

次のファイルが必要です。

- CA 証明書のリスト (ファイル形式 : .PEM) 。




図に示している証明書および証明書発行者は一例です。お使いのシステムには別の証明書があります。

### 証明書を表示または削除する

証明書を表示または削除するには、それぞれ対応するボタンを使用します。

### 認証局のリストのアップロード

1. [参照 (Browse) ] ボタンを押して、CA 証明書のリストを含むファイル (ファイル形式 .PEM) をコンピュータ上で見つけます。
2. *[認証局の追加... (Add certificate authority...) ]* をクリックして、新しい CA 証明書をビデオ システムに保存します。

以前に保存した証明書は自動的には削除されません。

CA 証明書を含む新しいファイル内のエントリが既存のリストに付加されます。

## 信頼できる CA について

証明書の検証は、TLS (Transport Layer Security) を使用する場合に必要になることがあります。

通信をセットアップする前に、サーバまたはクライアントからシステムに証明書を提示することを要求するよう、ビデオ システムを設定できます。

証明書は、サーバまたはクライアントの信頼性を確認するテキスト ファイルです。証明書は、信頼できる CA により署名されている必要があります。

証明書の署名を検証するには、信頼できる CA のリストがビデオ システム上に存在する必要があります。

このリストには、監査ロギングとその他の接続の両方の証明書を検証するために必要なすべての CA が含まれている必要があります。

認証が失敗した場合、接続は確立されません。

# セキュア監査ロギングのセットアップ

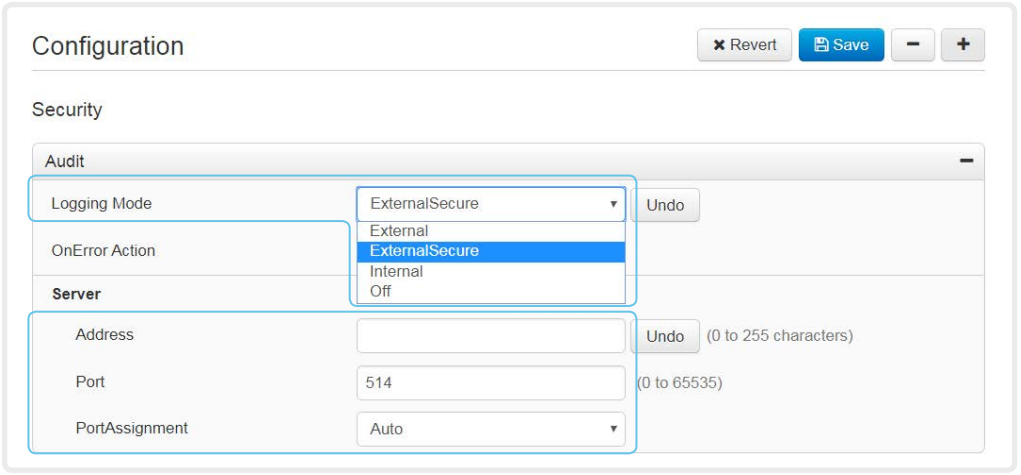
ウェブ インターフェイスにサインインして、*[セットアップ (Setup) ] > [設定 (Configuration) ]*に移動します。

監査サーバの証明書を検証する認証局 (CA) が、ビデオ システムの信頼できる認証局のリスト内に存在する必要があります。含まれていない場合は、外部サーバにログが送信されません。

リストの更新方法については、▶ 「信頼できる認証局 (CA) のリストの管理」の章を参照してください。

1. *[セキュリティ (Security) ]* カテゴリを開きます。
2. *[監査 (Audit) ] > [サーバ (Server) ]* 設定を探して、監査サーバの *[アドレス (Address) ]* を入力します。

   *[ポート割り当て (PortAssignment) ]* を **[手動 (Manual) ]** に設定した場合は、監査サーバの *[ポート (Port) ]* 番号も入力する必要があります。
3. *[監査 (Audit) ] > [ロギング モード (Logging Mode) ]* を **[外部セキュア (ExternalSecure) ]** に設定します。
4. *[保存 (Save) ]* をクリックして変更を有効にします。




## 安全な監査ロギングについて

監査ロギングを有効にすると、ビデオ システムでのすべてのサインイン アクティビティと設定変更が記録されます。

*[セキュリティ (Security) ] > [監査 (Audit) ] > [ロギング モード (Logging Mode) ]* 設定を使用して、監査ロギングを有効にします。監査ロギングは、デフォルトでは無効になっています。

ExternalSecure 監査ログ モードでは、ビデオ システムは暗号化された監査ログを外部監査サーバ (syslog サーバ) に送信します。そのサーバの ID は署名された証明書によって検証される必要があります。

監査サーバの署名は、他のサーバ/クライアントと同じ CA リストを使用して検証されます。

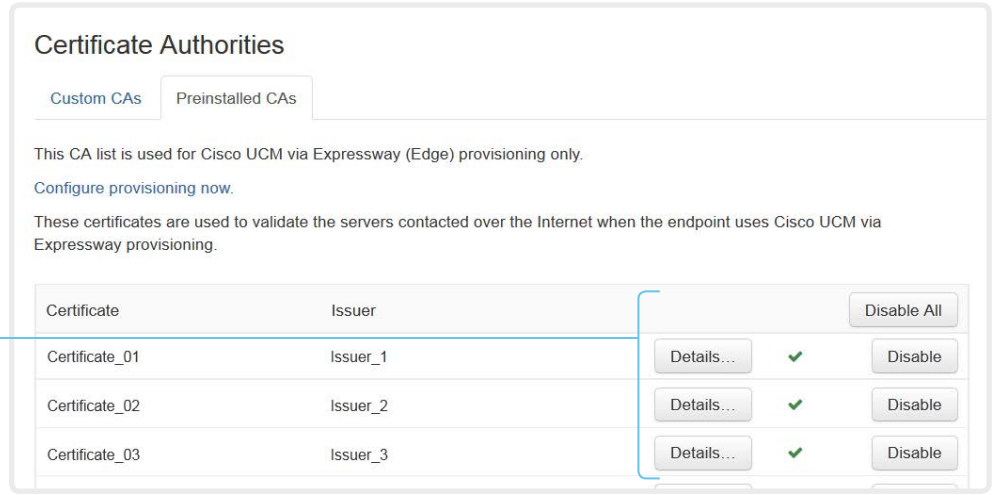
監査サーバ認証に失敗した場合は、監査ログが外部サーバに送信されません。

# Expressway プロビジョニング経由の CUCM 用のプレインストール済み証明書の管理

ウェブ インターフェイスにサインインし、*[設定 (Configuration) ] > [セキュリティ (Security) ]* に移動して、*[プレインストール済み CA (Preinstalled CAs) ]* タブを開きます。

## 証明書の表示または無効化

証明書を表示または無効にするには、*[詳細... (Details...) ]* ボタンまたは *[無効化 (Disable) ]* ボタンを使用します。




図に示している証明書および証明書発行者は一例です。お使いのシステムには別の証明書があります。

プレインストール済み証明書を使用する代わりに、必要な証明書を手動で証明書リストに付加することもできます。

信頼できる証明書のリストの更新方法については、▶ 「信頼できる認証局 (CA) のリストの管理」の章を参照してください。

## プレインストールされた証明書について

このページ内のプレインストールされた証明書は、ビデオ システムが Cisco Unified Communications Manager (CUCM) によって Expressway (エッジ) 経由でプロビジョニングされた場合にのみ使用されます。

Cisco Expressway インフラストラクチャ証明書のみがこのリストと照合されます。

Cisco Expressway インフラストラクチャ証明書の検証に失敗した場合は、ビデオ システムのプロビジョニングと登録が行われません。

ビデオ システムを初期設定にリセットしても、プレインストールされた証明書のリストは削除されません。

# CUCM 信頼リストを削除する

この章内の情報は、Cisco Unified Communications Manager（CUCM）に登録されているビデオ システムにのみ関連します。

ウェブ インターフェイスにサインインして、*[セキュリティ (Security) ] > [CUCM 証明書 (CUCM Certificates) ] に移動します。*

## CUCM 信頼リストを削除する

信頼リストを削除するには、*[CTL/ITL の削除 (Delete CTL/ITL) ]* をクリックします。

一般的に、以前の CTL（証明書信頼リスト）ファイルと ITL（初期信頼リスト）ファイルは削除しません。

次のようなケースでは、これらのファイルを削除する必要があります。

- CUCM の IP アドレスを変更する場合。
- CUCM クラスタ間でエンドポイントを移動する場合。
- CUCM 証明書を再生成または変更する必要がある場合。

## 信頼リスト フィンガープリントと証明書の概要

信頼リストのフィンガープリントとリストの証明書の概要は、ウェブ ページに表示されます。

この情報は、トラブルシューティングに役立ちます。

## 信頼リストの詳細

CUCM と信頼リストの詳細については、Cisco の ウェブ サイトから入手可能な『*Deployment guide for TelePresence endpoints on CUCM*』をお読みください。

# 永続モードを変更する

ウェブ インターフェイスにサインインして、*[セキュリティ (Security) ] > [非永続モード (Non-persistent Mode) ]* に移動します。

## 永続性ステータスの確認

アクティブなラジオ ボタンは、ビデオ システムの現在の永続性ステータスを示しています。

または、*[セットアップ (Setup) ] > [ステータス (Status) ]* に移動し、*[セキュリティ (Security) ]* カテゴリを開いて、*[永続性 (Persistency) ]* ステータスを確認することもできます。

## 永続設定を変更する

すべての永続設定がデフォルトで [永続 (Persistent) ] に設定されます。これらの設定は、[非永続 (Non-persistent) ] にする場合にのみ変更する必要があります。

1. 設定、通話履歴、内部ロギング、ローカル電話帳 (ローカル ディレクトリとお気に入り) 、および IP 接続 (DHCP) 情報の永続性を設定するには、ラジオ ボタンをクリックします。
2. *[保存して再起動... (Save and reboot...) ]* をクリックする。

   ビデオ システムが自動的に再起動します。再起動後、新しい永続設定に従って動作が変化します。

非永続モードに切り替える前に保存されたログ、設定および他のデータは、消去されたり削除されたりすることはありません。

## 永続モード

デフォルトでは、設定、通話履歴、内部ログ、ローカル電話帳 (ローカル ディレクトリとお気に入りリスト) 、および IP 接続情報が保存されます。すべての永続設定は **[永続 (Persistent) ]** に設定されているので、システムを再起動してもこの情報は削除されません。

通常は、永続設定は変更しないことをお勧めします。**[非永続 (Non-persistent) ]** モードへの変更は、前のセッションでログに記録された情報をユーザが参照したりトレースバックしたりしないようにする必要がある場合にのみ行ってください。

非永続モードでは、システムが再起動されるたびに次の情報が削除または消去されます。

- システム設定の変更
- 通話の発信および受信に関する情報 (通話履歴)
- 内部ログ ファイル
- ローカル連絡先またはお気に入りリストの変更
- 前回のセッション以降のすべての IP 関連情報 (DHCP)

[非永続 (Non-persistent) ] モードに変更する前に保存された情報は、自動的にクリアまたは削除されることはありません。そのような情報を削除するには、初期設定へのリセットを行う必要があります。

工場出荷時設定リセットの実行方法については、▶ 「ビデオ システムの工場出荷時設定リセット」の章を参照してください。

# 強力なセキュリティ モードの設定

ウェブ インターフェイスにサインインして、*[セキュリティ (Security)] > [強力なセキュリティモード (Strong Security Mode)]* に移動します。

## 強力なセキュリティ モードの設定

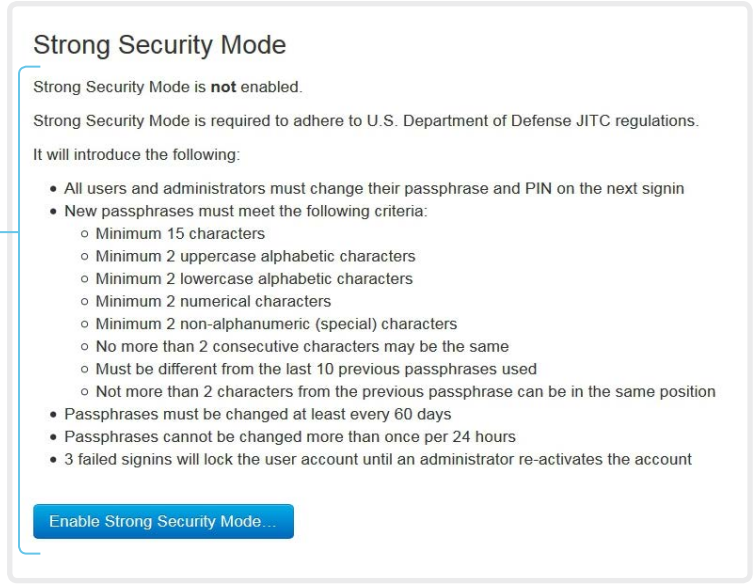
続行する前に、強力なセキュリティ モードの影響について注意してお読みください。

1. 強力なセキュリティモードを使用する場合は、*[強力なセキュリティモードの有効化... (Enable Strong Security Mode...)]* をクリックします。表示されるダイアログボックスで選択内容を確認します。

   ビデオ システムが自動的に再起動します。

2. プロンプトが表示されたら、パスフレーズを変更します。新しいパスフレーズは、説明に従って厳格な基準を満たす必要があります。

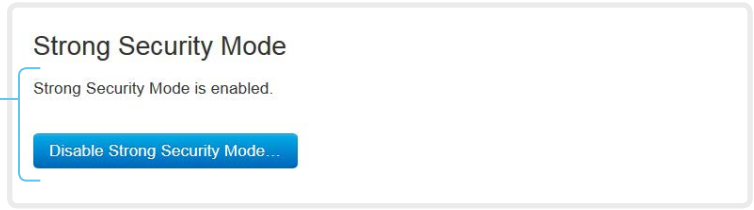
   システム パスフレーズの変更方法については、► 「システム パスフレーズの変更」の章を参照してください。




## 通常モードに戻る

ビデオ システムを通常モードに戻すには、*「強力なセキュリティ モードの無効化...」* をクリックします。表示されるダイアログボックスで選択内容を確認します。

ビデオ システムは自動的に再起動します。




## 強力なセキュリティ モードについて

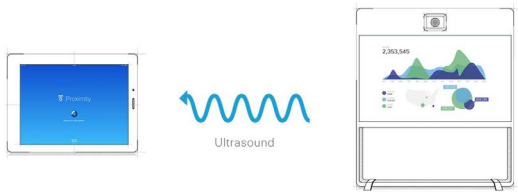
強力なセキュリティ モードは、DoD JITC 規制への準拠が必要な場合にのみ使用します。

強力なセキュリティ モードでは、非常に厳密なパスフレーズ要件が設定され、すべてのユーザが次回のサインイン時にパスフレーズを変更する必要があります。

# コンテンツ シェアリング用のインテリジェント プロキシミティのセットアップ (1/5 ページ)

Cisco Proximity を使用すると、ユーザは自分のモバイル デバイス (スマートフォン、タブレット、またはラップトップ) がビデオ システムの近くにある場合に、コンテンツをデバイスで直接表示、制御、キャプチャおよび共有することができます。

モバイル デバイスは、ビデオ システムから送信される超音波の範囲内に入ると、自動的にビデオ システムとペアリングできます。




Proximity の同時接続数は、ビデオ システムのタイプによって異なります。この最大接続数に達すると、新しいユーザはクライアントから警告されます。

| ビデオ システム | 最大接続数 |
|---|---|
| Room Kit, Room kit mini | 30/7 * |
| Room Kit、Room 55 Dual、Room 70、Room 70 G2 | 30/7 * |
| Codec Plus、Codec Pro | 30/7 * |
| SX80 | 10 |
| SX10, SX20 | 7 |
| MX700、MX800 | 10 |
| MX200 G2、MX300 G2 | 7 |
| DX70、DX80 | 3 |

* モバイル デバイスのプロクシミティ サービス上の*共有コンテンツの確認が無効化されているときは*、接続数は 30 になります。このサービスの有効時、接続数は 7 になります。

## プロキシミティ サービス

*コールの発信とビデオ システムの制御:*

- ダイヤル、ミュート、音量調節、切断
- ラップトップ (OS X と Windows) 、スマートフォンとタブレット (iOS と Android) で使用可能

*モバイル デバイス上での共有コンテンツの表示:*

- 共有コンテンツの表示、以前のスライドのレビュー、選択されたスライドの保存
- スマートフォンとタブレット (iOS と Android) で使用可能
- DX70 および DX80 の場合、このサービスは通話時にのみ利用できる。

*ラップトップからワイヤレスで共有:*

- プレゼンテーション ケーブルを接続しないコンテンツの共有
- ラップトップ (OS X と Windows) で使用可能


コールの発信とビデオ システムの制御


モバイル デバイスでの共有コンテンツの表示


モバイル デバイスからのワイヤレス共有

# コンテンツ シェアリング用のインテリジェント プロキシミティのセットアップ (2/5 ページ)

## Cisco Proximity クライアントをインストールする

### クライアントの入手場所

スマートフォンとタブレット (Android および iOS) 、およびラップトップ (Windows および OS X) 向けの Cisco Proximity クライアントは、► https://proximity.cisco.com から無償でダウンロードできます

また、Google Play (Android) や Apple App Store (iOS) でスマートフォン/タブレット用のクライアントを直接入手することもできます。

### エンド ユーザ ライセンス契約書

エンドユーザ ライセンス契約書をよく確認してください。
► https://www.cisco.com/c/en/us/td/docs/general/warranty/English/EU1KEN_.html

### サポートされるオペレーティング システム

- iOS 7 以降
- Android 4.0 以降
- Mac OS X 10.9 以降
- Windows 7 以降
  Windows 8 で導入されたタイル ベースのインターフェイスはサポートされていません。

# コンテンツ シェアリング用のインテリジェント プロキシミティのセットアップ (3/5 ページ)

## 超音波の放出

Cisco のビデオ システムは、プロキシミティ機能の一部として超音波を出力します。

*[プロキシミティ (Proximity) ] > [モード (Mode) ]* 設定を使用して、プロキシミティ機能 (および超音波の放出) の **[オン (On) ]/[オフ (Off) ]** を切り替えます。

業務用または商用アプリケーション、家電製品など、ほとんどの人は毎日さまざまな環境で、程度の差はあれ超音波にさらされています。

人によっては空中の超音波によって何らかの影響を自覚する場合もありますが、75 dB 未満のレベルで影響が生じることはほとんどありません。

*Room 70*、*Room 70 G2*、*Room 55*、*Room 55 Dual*、*Room Kit*、Room Kit Mini、*Room Kit Plus*、*SX10N および MX シリーズ:*

- スピーカーから 50 cm 以上の距離では、超音波の音圧レベルは 75 dB 未満になります。

*DX70 および DX80:*

- スピーカーから 20 cm 以上の距離では、超音波の音圧レベルは 75 dB 未満になります。

*Codec Plus*、*Codec Pro*、*SX10*、*SX20 および SX80 :*

- これらのビデオ システムでは、サードパーティのスピーカーで超音波が放出されるため、超音波の音圧レベルを予測できません。

  スピーカー自体の音量コントロール、および *[音声 (Audio) ] > [超音波 (Ultrasound) ] > [最大音量 (MaxVolume) ]* での設定は、超音波の音圧レベルに影響を与えます。リモートコントロールまたはタッチコントローラでの音量調節は効果ありません。

### ヘッドセット

*DX70*、*DX80*、*および SX10N :*

これらのシステムでは、次の理由からヘッドセットを常に使用できます。

- DX70 および DX80 には、超音波を出さない専用ヘッドセット出力があります。
- SX10N では、内蔵スピーカーで超音波が放出されます。超音波は、HDMI またはオーディオ出力では放出されません。

*Room 70*、*Room 70 G2*、*Room 55*、*Room 55 Dual*、*Room Kit*、*Room Kit Plus*、*Codec Plus*、*Codec Pro*、*SX10*、*SX20*、*SX80 および MX シリーズ:*

- これらのシステムは、ヘッドセットを使用するように設計されていません。
- これらのビデオ システムでヘッドセットを使用する場合は、超音波発生をオフにしておくことを強くお勧めします (*[プロキシミティ (Proximity) ] > [モード (Mode) ]* を **[オフ (Off) ]** に設定します)。この場合、[プロキシミティ (Proximity) ] 機能を使用することはできません。
- これらのシステムは専用のヘッドセット出力を備えていないため、接続されたヘッドセットから音圧レベルを制御することはできません。

*Room Kit Mini :*

- システムは、ヘッドセットを使用するように設計されていません。

# コンテンツ シェアリング用のインテリジェント プロキシミティのセットアップ (4/5 ページ)

## プロキシミティ サービスを有効にする

1. ウェブ インターフェイスにサインインして、*[セットアップ (Setup)] > [設定 (Configuration)]*を移動します。
2. [プロキシミティ (Proximity)] > [モード (Mode)] に移動します。プロキシミティが [オン (On)] (デフォルト) になっていることを確認します。この場合、ビデオ システムは超音波ペアリング メッセージを送信します。

   許可するサービスを有効にします。デフォルトでは、[デスクトップ クライアントからのワイヤレス共有 (Wireless share from a desktop client)] のみが有効になっています。

   プロキシミティ機能を最大限に活用するために、すべてのサービスを有効にすることをお勧めします。

   *コールの発信とビデオ システムの制御:*

   - *[プロキシミティ (Proximity)] > [サービス (Services)] > [通話制御 (CallControl)]* に移動して、**[有効 (Enabled)]** を選択します。

   *モバイル デバイス上での共有コンテンツの表示:*

   - *[プロキシミティ (Proximity)] > [サービス (Services)] > [コンテンツ共有 (ContentShare)] > [送信先クライアント (ToClients)]* に移動して、**[有効 (Enabled)]** を選択します。

   *デスクトップ クライアントからのワイヤレス共有:*

   - *[プロキシミティ (Proximity)] > [サービス (Services)] > [コンテンツ共有 (ContentShare)] > [クライアントから (FromClients)]* に移動して、**[有効 (Enabled)]** を選択します。

## プロキシミティ インジケータ

1 つ以上のプロキシミティ クライアントがシステムとペアになっていれば、スクリーンにプロキシミティ インジケータが表示されます。

最後のクライアントのペアリングが解除されても、インジケータはすぐには消えません。消えるまで数分かかることがあります。

## プロキシミティについて

プロキシミティ機能はデフォルトで**オン**に設定されています。

プロキシミティが**オン**になっていると、ビデオ システムは超音波のペアリング メッセージを発信します。

超音波のペアリング メッセージは、Proximity クライアントがインストールされた近くにあるデバイスによって受信され、デバイスの認証および許可をトリガーします。

セットアップでプロキシミティが適切であることを確認した場合は、ユーザ エクスペリエンスを最適化するために、プロキシミティを常に **[オン (On)]*** にしておくことをお勧めします。

プロキシミティに対する完全なアクセス権限を得るためには、プロキシミティ サービス ([プロキシミティ (Proximity)] > [サービス (Services)] > [...]) も **[有効 (Enabled)]** にする必要があります。

* プロキシミティ (超音波) を**オン**に切り替えた場合は、ヘッドセットを使用*しない*ことをお勧めします。

# コンテンツ シェアリング用のインテリジェント プロキシミティのセットアップ (5/5 ページ)

## 部屋の考慮事項

### 部屋の音響

- 壁/床/天井の表面が硬い部屋では、音の反響が大きいことが問題になる場合があります。最良の会議環境とインテリジェント プロキシミティのパフォーマンスを確保するために、会議室の音響処理を常に強く推奨します。
- 1 つの部屋の中でインテリジェント プロキシミティを有効にするビデオ システムは 1 つだけにすることを推奨します。複数あると、干渉が発生する可能性があり、デバイス検出とセッション メンテナンスの問題の原因となることがあります。

## プライバシーについて

Cisco Privacy ポリシーと Cisco Proximity 付録には、クライアントにおけるデータ収集とプライバシーの懸案事項が記載されており、この機能を組織に導入する際にはこれを考慮する必要があります。
次のページを参照してください。
► https://www.cisco.com/web/siteassets/legal/privacy.html

## 基本的なトラブルシューティング

### プロキシミティ クライアントを使用するデバイスを検出できない

- 一部の Windows ラップトップでは、超音波の周波数範囲 (20kHz-22kHz) の音を記録できません。これは、特定のデバイスのサウンドカード、サウンド ドライバ、または内蔵マイクに関する周波数の制限が原因である可能性があります。詳細については、サポート フォーラムを参照してください。
- ユーザーインターフェイスで *[設定 (Settings)] > [問題と診断 (Issues and diagnostics)]* を確認するか、ビデオシステムのウェブ インターフェイスで *[メンテナンス (Maintenance)] > [診断 (Diagnostics)]* を確認します。超音波に関する問題がリストに記載されていない場合 (超音波信号を確認できません {Unable to verify the ultrasound signal}) 、超音波のペアリングメッセージがビデオシステムから発信されます。クライアントで検出される問題のサポートには、プロキシミティの *サポート掲示板*を参照してください。

### オーディオ アーチファクト

- ハムノイズやクリッピングノイズなどが聞こえる場合は、最大超音波音量を下げてください *([オーディオ (Audio)] > [超音波 (Ultrasound)]* > [最大音量 (MaxVolume)]) 。

### ラップトップから内容を共有できない

- コンテンツ シェアリングを機能させるには、ビデオ システムとラップトップを同じネットワーク上に配置する必要があります。この理由から、プロキシミティ シェアリングは、ビデオ システムが Expressway 経由で企業ネットワークに接続されており、ラップトップが VPN 経由 (VPN クライアント依存) で接続されている場合には、失敗する可能性があります。

## 関連リソース

Cisco Proximity サイト:
► https://proximity.cisco.com

サポート フォーラム :
► https://www.cisco.com/go/proximity-support

# ビデオ品質対コール レート比の調整 (1/2 ページ)

## ビデオ入力品質の設定

ビデオをエンコードして送信する場合は、高解像度 (シャープさ) と高フレーム レート (動き) との間でトレード オフが生じます。

最適鮮明度設定を有効にするには、*Video Input Connector n Quality* 設定を **[モーション (Motion) ]** に設定する必要があります。ビデオ入力の品質を **[シャープネス (Sharpness) ]** に設定すると、エンドポイントはフレーム レートに関係なく、可能な限り高解像度で送信します。

## 最適鮮明度プロファイル

最適鮮明度プロファイルは、ビデオ会議室の光 (照明) の条件およびカメラ (ビデオ入力ソース) の品質を反映している必要があります。光の条件およびカメラの品質が良いほど、高いプロファイルを使用する必要があります。

通常、[中 (Medium) ] プロファイルが推奨されます。ただし照明条件が非常に良好な場合は、プロファイルを決定する前に、さまざまな最適鮮明度プロファイル設定でエンドポイントをテストすることをお勧めします。特定の帯域の解像度を上げるために、[高 (High) ] プロファイルを設定できます。

異なる最適鮮明度プロファイルに使用する一般的な解像度、コール レートおよび送信フレーム レートの一部を次のページの表に示します。解像度とフレーム レートは、発信側と着信側の両方のシステムでサポートされている必要があります。

## 60 fps のビデオの許可

デフォルトとして、カメラは 1 秒あたり 30 フレーム (30 fps) を出力します。これにより、通常の帯域と照明条件であってもクローズアップと広い視野両方の画像の品質が良くなります。条件がさらに良い場合、カメラからの出力が 60 fps となり、全般的に良い品質となる可能性があります。

カメラの出力フレーム レートを設定するには、*[カメラのカメラ フレーム レート (Cameras Camera Framerate) ]* 設定を使用します。

ウェブ インターフェイスにサインインして、*[セットアップ (Setup) ] > [設定 (Configuration) ]* に移動します。

1. *[ビデオ (Video) ] > [入力 (Input) ] > [コネクタ n (Connector n) ] > [品質 (Quality) ]* を選択して、ビデオ品質パラメータを **[モーション (Motion) ]** に設定します (Connector 1 (内蔵カメラ) ではこの手順をスキップします) 。
2. *[ビデオ (Video) ] > [入力 (Input) ] > [コネクタ n (Connector n) ] > [最適鮮明度 (OptimalDefinition) ] > [プロファイル (Profile) ]* に移動して、適切な最適鮮明度プロファイルを選択します。
3. *[カメラ (Cameras) ] > [カメラ (Camera) ] > [フレームレート (Framerate) ]* に進み、60fps のビデオを許可するかどうかを選択します。

# ビデオ品質対コール レート比の調整 (2/2 ページ)

| 解像度とフレーム レート [w×h@fps] は、異なる最適な定義プロファイルとコール レートから取得します。 | | | | | | |
|---|---|---|---|---|---|---|
| コール レート (kbps) | H.264、最大 30fps | | | H.264、最大 60fps | | |
| | *標準* | *中* | *高* | *標準* | *中* | *高* |
| *128* | 320×180@30 | 320×180@30 | 512×288@30 | 320×180@30 | 512×288@20 | 512×288@30 |
| *256* | 512×288@30 | 640×360@30 | 768×448@30 | 512×288@30 | 640×360@30 | 768×448@30 |
| *384* | 640×360@30 | 768×448@30 | 768×448@30 | 640×360@30 | 768×448@30 | 768×448@30 |
| *512* | 768x448@30 | 1024x576@30 | 1024x576@30 | 768x448@30 | 1024x576@30 | 1024x576@30 |
| *768* | 1024×576@30 | 1280×720@30 | 1280×720@30 | 1024×576@30 | 1280×720@30 | 1280×720@30 |
| *1152* | 1280×720@30 | 1280×720@30 | 1280×720@30 | 1280×720@30 | 1280×720@30 | 1280×720@60 |
| *1472* | 1280×720@30 | 1280×720@30 | 1920×1080@30 | 1280×720@30 | 1280×720@30 | 1280×720@60 |
| *1920* | 1280x720@30 | 1920x1080@30 | 1920x1080@30 | 1280x720@30 | 1280x720@60 | 1280x720@60 |
| *2560* | 1920x1080@30 | 1920x1080@30 | 1920x1080@30 | 1280x720@60 | 1280x720@60 | 1920x1080@60 |
| *3072* | 1920x1080@30 | 1920x1080@30 | 1920x1080@30 | 1280x720@60 | 1280x720@60 | 1920x1080@60 |
| *4000* | 1920x1080@30 | 1920x1080@30 | 1920x1080@30 | 1280x720@60 | 1920x1080@60 | 1920x1080@60 |
| *6000* | 1920×1080@30 | 1920×1080@30 | 1920×1080@30 | 1920×1080@60 | 1920×1080@60 | 1920×1080@60 |

| 解像度とフレーム レート [w×h@fps] は、異なる最適な定義プロファイルとコール レートから取得します。 | | | | | | |
|---|---|---|---|---|---|---|
| コール レート (kbps) | H.265、最大 30fps | | | H.265、最大 60fps | | |
| | *標準* | *中* | *高* | *標準* | *中* | *高* |
| *128* | 512×288@30 | 512×288@30 | 640×360@30 | 512×288@30 | 512×288@30 | 640×360@30 |
| *256* | 640×360@30 | 768×448@30 | 768×448@30 | 640×360@30 | 768×448@30 | 768×448@30 |
| *384* | 768×448@30 | 1024×576@30 | 1280×720@30 | 768×448@30 | 1024×576@30 | 1280×720@30 |
| *512* | 1024x576@30 | 1280x720@30 | 1280x720@30 | 1024x576@30 | 1280x720@30 | 1280x720@30 |
| *768* | 1280×720@30 | 1280×720@30 | 1920×1080@30 | 1280×720@30 | 1280×720@30 | 1280×720@60 |
| *1152* | 1280×720@30 | 1920×1080@30 | 1920×1080@30 | 1280×720@30 | 1280×720@60 | 1280×720@60 |
| *1472* | 1280×720@30 | 1920×1080@30 | 1920×1080@30 | 1280×720@60 | 1280×720@60 | 1280×720@60 |
| *1920* | 1920x1080@30 | 1920x1080@30 | 1920x1080@30 | 1280x720@60 | 1280x720@60 | 1920x1080@60 |
| *2560* | 1920x1080@30 | 1920x1080@30 | 1920x1080@30 | 1280x720@60 | 1920x1080@60 | 1920x1080@60 |
| *3072* | 1920x1080@30 | 1920x1080@30 | 1920x1080@30 | 1920x1080@60 | 1920x1080@60 | 1920x1080@60 |
| *4000* | 1920x1080@30 | 1920x1080@30 | 1920x1080@30 | 1920x1080@60 | 1920x1080@60 | 1920x1080@60 |
| *6000* | 1920×1080@30 | 1920×1080@30 | 1920×1080@30 | 1920×1080@60 | 1920×1080@60 | 1920×1080@60 |

# 画面および Touch 10 ユーザ インターフェイスに企業ブランディングを追加 (1/2 ページ)

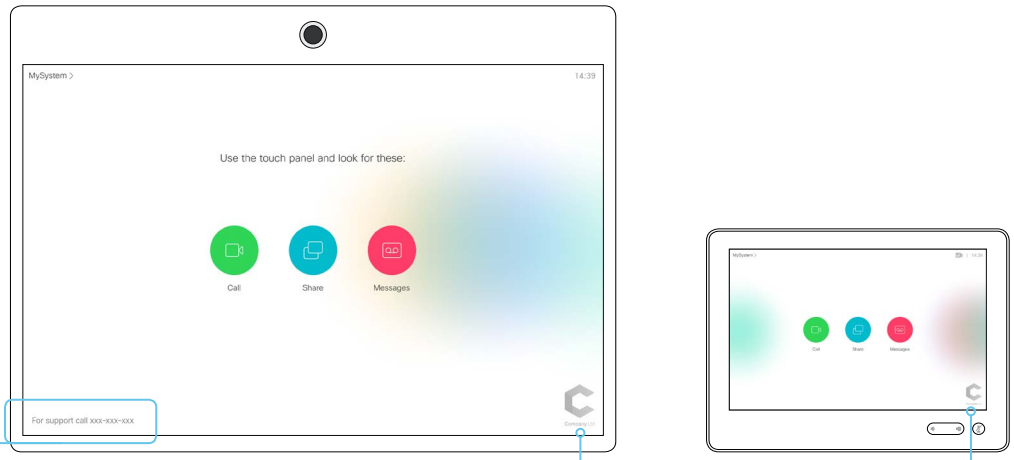
ウェブ インターフェイスにサインインして、*[セットアップ (Setup) ] > [ パーソナライゼーション (Personalization) ]* に移動し、*[ブランディング (Branding) ]* タブを開きます。

このページから、独自のブランディング要素 (背景ブランド イメージ、ロゴ、カスタム メッセージ) をビデオ システムに追加できます。

## アウェイク状態のブランディング

アウェイク状態では、次のことができます。

- 右下隅にロゴを追加します (画面および Touch 10) 。
- 左下隅に短いメッセージ (テキストのみ) を追加します (画面のみで、Touch 10 は不可) 。




カスタム テキスト

ロゴ

推奨事項:

- 黒色のロゴ (ビデオ システムでは不透明度が 40 % の白色のオーバーレイが追加されるため、ロゴおよびその他のユーザ インターフェイス要素が映えます)
- 背景が透明な PNG 形式
- 最小 272 × 272 ピクセル (自動的にスケーリングされます)

## ブランディングについて

この章で説明しているように、ブランディング機能により、Cisco の全体的なユーザ エクスペリエンスを損なうことなく、スクリーンとタッチ ユーザ インターフェイスの表示をカスタマイズできます。

従来のカスタム壁紙機能ではなく、この機能を使用することをお勧めします。カスタム壁紙機能を使用すると、ワンボタン機能などの機能を使用できなくなります。

**ブランド機能とカスタム壁紙は、同時に使用できません。**

ビデオ システムでカスタム壁紙がセットアップされている場合は、ブランディング要素を追加する前に *[カスタム壁紙を無効にする (Disable the custom wallpaper) ]* をクリックする必要があります。

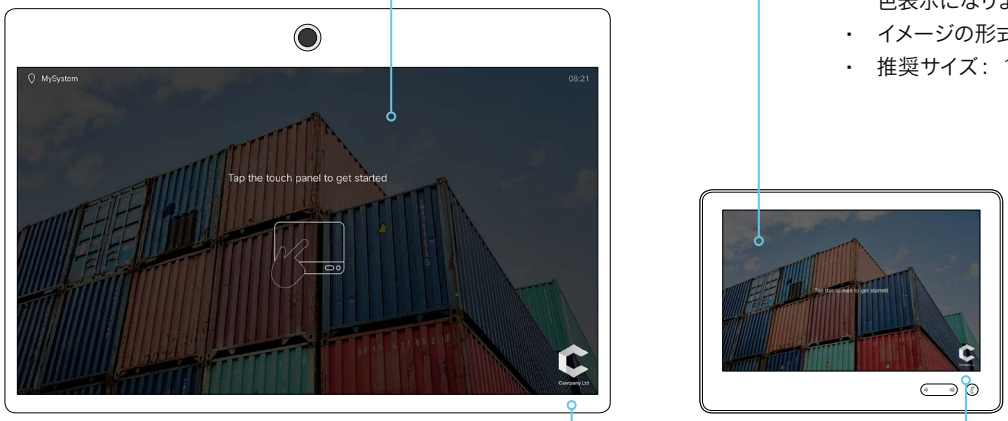
# 画面および Touch 10 ユーザ インターフェイスに企業ブランディングを追加 (2/2 ページ)

## ハーフウェイク状態のブランディング

ハーフウェイク状態では、次のことができます。

- 背景ブランド イメージを追加します (画面および Touch 10) 。
- 右下隅にロゴを追加します (画面および Touch 10) 。
- スクリーン中央のメッセージをカスタマイズまたは削除します (画面のみ。Touch 10 は不可) 。これは、ビデオ システムの使用開始方法をユーザに示すメッセージです。

  通常は標準メッセージのままにすることをお勧めします。サードパーティのユーザ インターフェイスがある場合など、別のシナリオに合わせる必要がある場合にのみ、メッセージを変更してください。




### 背景ブランド イメージ

- ビデオ システムがウェイクアップするとイメージがフルカラーで表示され、数秒後に自動的に淡色表示になります (透明な黒色のオーバーレイ)
- イメージの形式 : PNG または JPEG
- 推奨サイズ : 1920 × 1080 ピクセル

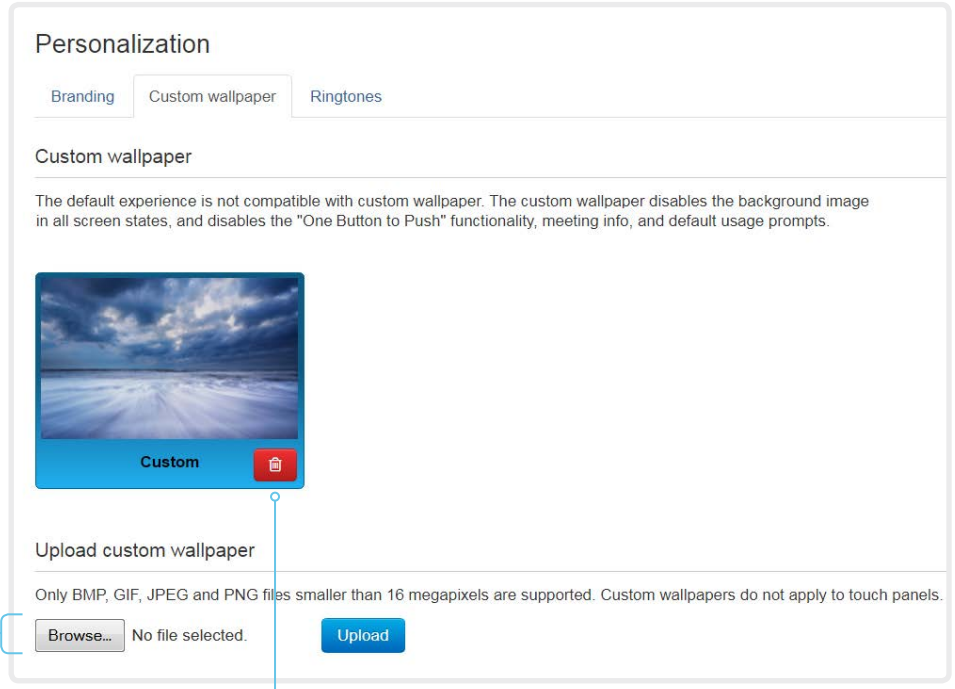
### ロゴ

推奨事項 :

- 白色のロゴ (暗い背景ブランド イメージに適合する)
- 背景が透明な PNG 形式
- 最小 272 × 272 ピクセル

# カスタム壁紙の追加

ウェブ インターフェイスにサインインして、*[セットアップ (Setup) ] > [パーソナライゼーション (Personalization) ]* に移動し、*[カスタム壁紙 (Custom wallpaper) ]* タブを開きます。




## カスタムの壁紙のアップロード

古いカスタム壁紙があれば上書きします。

1. [参照 (Browse) ] ボタンを押して、カスタム壁紙のイメージ ファイルを見つけます。
2. *[アップロード (Upload) ]* をクリックして、ファイルをビデオ システムに保存します。

   サポートされるファイル形式 : BMP、GIF、JPEG、PNG

   最大ファイル サイズ : 16 メガピクセル

カスタム壁紙をアップロードすると、自動的にアクティブになります。

## カスタムの壁紙の削除

*[削除 (Delete) ]* によって、カスタム壁紙がビデオ システムから完全に削除されます。

削除したカスタムの壁紙を再度使用する場合は、その壁紙を再度アップロードする必要があります。

## カスタム壁紙について

カスタム画像をスクリーンの背景にする場合は、*カスタム壁紙*をアップロードして使用することができます。カスタム壁紙はタッチ コントローラには表示されません。

ビデオ システムでは一度に 1 枚のカスタム壁紙しか保存できません。新しいカスタム壁紙は古いものを上書きします。

この従来のカスタム壁紙機能ではなく、新しいブランディング機能を使用することをお勧めします。それにより、Cisco の全体的なユーザ エクスペリエンスが向上し、ワンボタン機能や会議情報などの機能が使用できなくなることを回避できます。▶「 画面および Touch 10 ユーザ インターフェイスに企業ブランディングを追加」の章を参照してください。

**ブランド機能とカスタム壁紙は、同時に使用できません。**

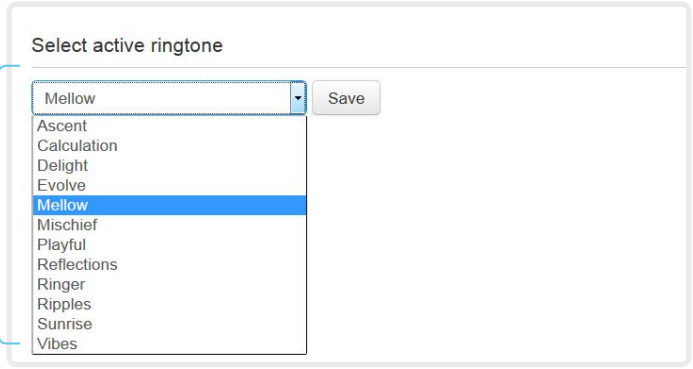
ビデオ システムでブランディング要素がセットアップされている場合は、カスタム壁紙を追加する前に *[ブランディングなしで続行 (Continue without branding) ]* をクリックする必要があります。

# 着信音の選択と着信音量の設定

ウェブ インターフェイスにサインインして、*[セットアップ (Setup) ] > [パーソナライゼーション (Personalization) ]* に移動し、*[着信音 (Ringtones) ]* タブを開きます。

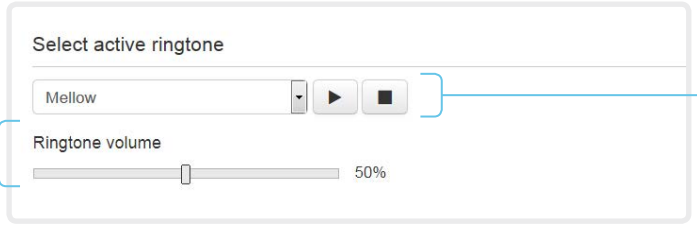
## 呼び出し音の変更

1. ドロップダウン リストから呼び出し音を選択します。
2. *[保存 (Save) ]* をクリックすると、それがアクティブな呼び出し音になります。




## 呼び出し音の音量の設定

呼び出し音の音量を調節するにはスライド バーを使用します。




## 呼び出し音の再生

呼び出し音を再生するには、再生ボタン (▶) をクリックします。

再生を終了するには、停止ボタン ( ■ ) を使用します。

## 着信音について

一連の着信音がビデオ システムにインストールされています。着信音を選択して音量を設定するには、ウェブ インターフェイスを使用します。

ウェブ インターフェイスから、選択した呼び出し音を再生できます。呼び出し音が再生されるのはビデオ システムであり、ウェブ インターフェイスが実行されているコンピュータ上ではないことに注意してください。

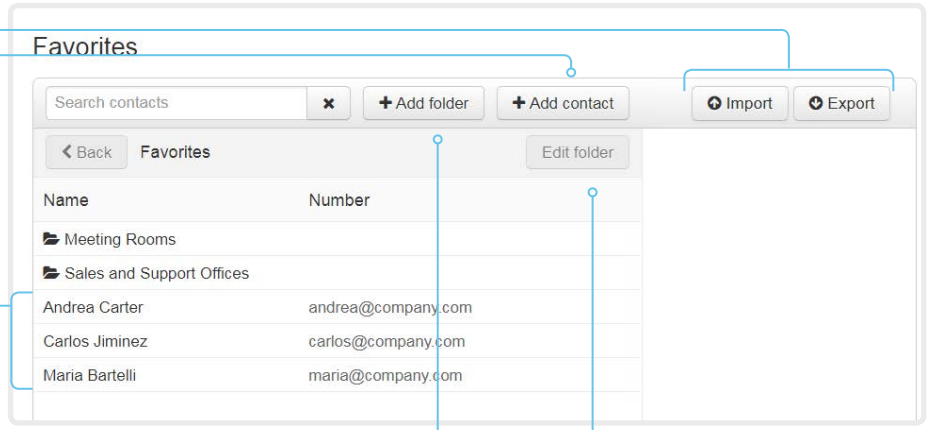
# お気に入りリストの管理

ウェブ インターフェイスにサインインして、*[セットアップ (Setup) ] > [お気に入り (Favorites) ]* に移動します。

## ファイルから連絡先をインポート/エクスポート

ローカルの連絡先をファイルに保存するには *[エクスポート (Export) ]* をクリックし、ファイルから連絡先を取得するには *[インポート (Import) ]* をクリックします。

ファイルから新しい連絡先をインポートすると、現在のすべてのローカル連絡先は破棄されます。




## 連絡先を追加または編集する

1. *[連絡先の追加 (Add contact) ]* をクリックして新しいローカル連絡先を作成するか、連絡先の名前をクリックしてから *[連絡先を編集 (Edit contact) ]* をクリックします。
2. ポップアップ表示されたフォームに値を入力するか、そのフォームを更新します。

   連絡先をサブフォルダに保存するために、フォルダ ドロップダウン リストでフォルダを選択します。

   連絡先に関する複数の連絡方法 (ビデオアドレス、電話番号、携帯番号など) を保存する場合は、*[連絡方法の追加 (Add contact method) ]* をクリックして、新しい入力フィールドに値を入力します。
3. *[保存 (Save) ]* をクリックしてローカル連絡先を保存します。

## コンタクトの削除

1. *[連絡先を編集 (Edit contact) ]* に続いて連絡先の名前をクリックします。
2. *[削除 (Delete) ]* をクリックしてローカル連絡先を削除します。

## サブフォルダを追加または編集する

1. *[フォルダの追加 (Add folder) ]* をクリックして新しいサブフォルダを作成するか、一覧表示されたフォルダの 1 つをクリックしてから *[フォルダの編集 (Edit folder) ]* をクリックします。
2. ポップアップ表示されたフォームに値を入力するか、そのフォームを更新します。
3. *[保存 (Save) ]* をクリックしてフォルダを作成または更新します。

## サブフォルダを削除する

1. フォルダの名前をクリックし、*[フォルダの編集 (Edit folder) ]* をクリックします。
2. フォルダとそのすべてのコンテンツおよびサブ フォルダを削除するには、*[削除 (Delete) ]* をクリックします。ポップアップするダイアログで選択内容を確認します。

## ビデオ システムのユーザ インターフェイスによるお気に入りの管理

### お気に入りリストへの連絡先の追加

1. ホーム画面の *[発信 (Call) ]* を選択します。
2. 追加する連絡先を選択します。
3. *[お気に入りへの追加 (Add to favorites) ]* を選択します。

追加した連絡先は、最上位のフォルダに格納されます。サブフォルダを選択または作成することはできません。

### お気に入りリストからの連絡先の削除

1. ホーム画面の *[発信 (Call) ]* を選択します。
2. *[お気に入り (Favorites) ]* タブを選択します。
3. 削除する連絡先を選択します。
4. *[お気に入りの削除 (Remove favorite) ]* を選択します。

# アクセシビリティ機能のセットアップ

## 着信時のスクリーンの点滅

聴覚に障がいのあるユーザが着信に気付きやすくするために、着信時にスクリーンが赤色と灰色で点滅するようにセットアップできます。

1. ウェブ インターフェイスにサインインして、*[セットアップ (Setup)]* > *[設定 (Configuration)]*に移動します。
2. *[ユーザインターフェイス (UserInterface)]* > *[アクセシビリティ (Accessibility)]* > *[着信コール通知 (IncomingCallNotification)]* に移動して、**[画面表示の強調 (AmplifiedVisuals)]** を選択します。
3. *[Save (保存)]* をクリックします。

第 3 章

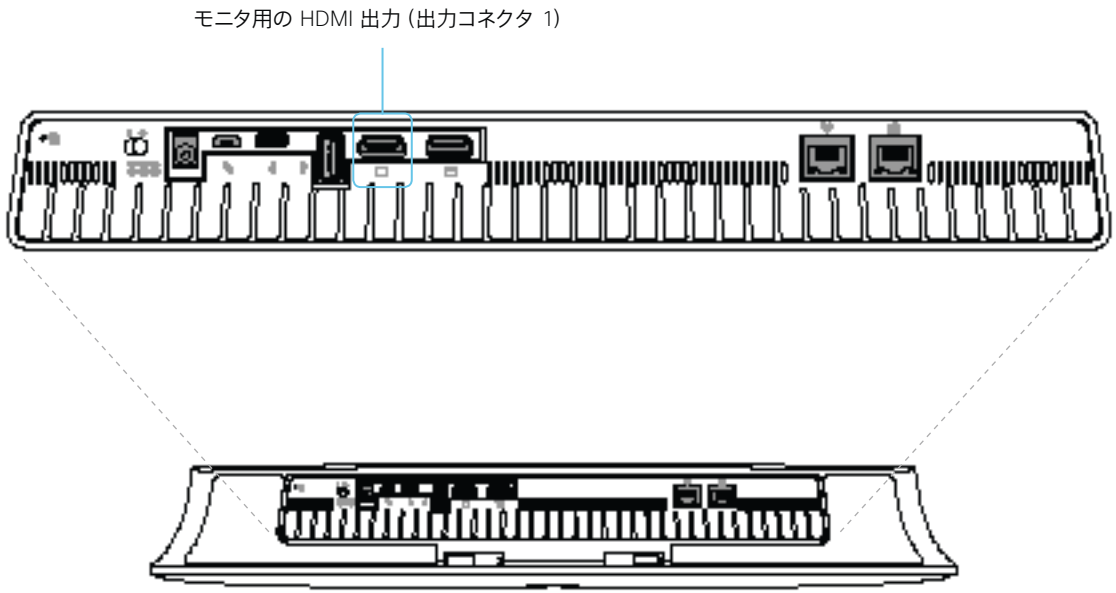
# 周辺機器

# モニタへの接続

ビデオ システムには 1 つの HDMI ビデオ出力があります。

HDMI 出力は、60 fps で最大 3840 × 2160 の解像度をサポートします。高解像度とフレーム レートをサポートするプレミアム HDMI ケーブルが必要です。HDMI 出力には音声はありません。

モニタおよび他の周辺機器の接続時や切断時には、必ず電源を切ってください。



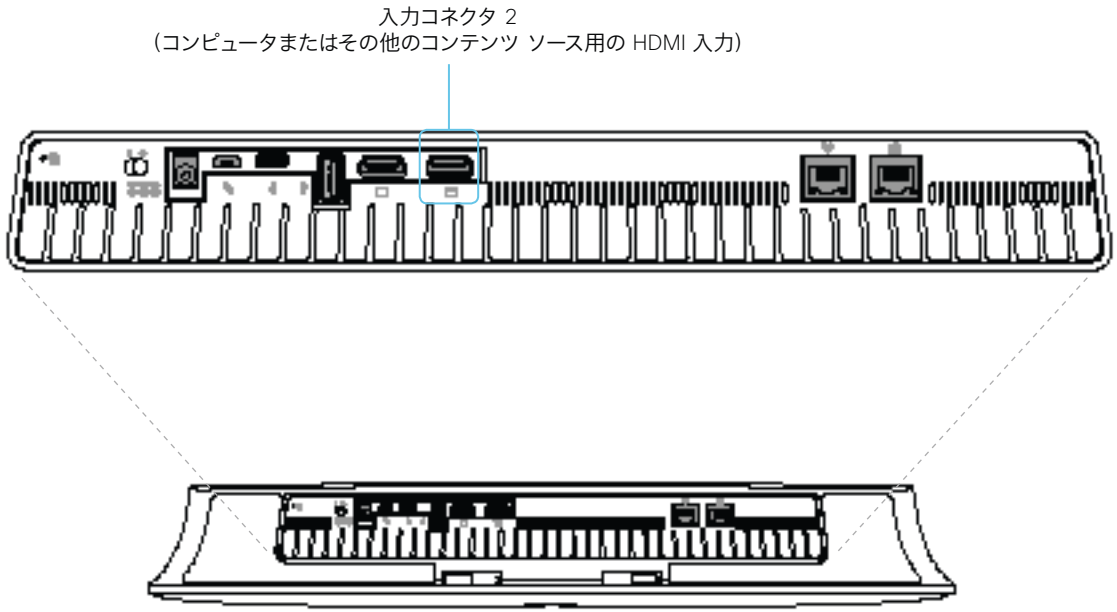
# 入力ソースの接続 (1/2 ページ)

ウェブ インターフェイスにサインインして、*[セットアップ (Setup)] > [設定 (Configuration)]* に移動すると、以下に示す設定が見つかります。

## コンピュータまたはその他のコンテンツ ソースの接続

コンテンツをローカルで、または会議参加者と共有するために、 1 つの入力ソース (パソコン1 台など) を ビデオシステムの HDMI 入力 (入力コネクタ 2) に接続できます。

HDMI 入力は、30 fps で最大 3840 × 2160 の解像度をサポートします。高解像度とフレーム レートをサポートするハイスピード HDMI 1.4b ケーブルが必要です。



# 入力ソースの接続 (2/2 ページ)

## 入力ソースのタイプと名前の設定

入力ソースのタイプと名前を設定することをお勧めします。

- *[ビデオ (Video) ] > [入力 (Input) ] > [コネクタ n (Connector n) ] > [入力ソースタイプ (InputSourceType) ]*
- *[ビデオ (Video) ] > [入力 (Input) ] > [コネクタ n (Connector n) ] > [名前 (Name) ]*

これらの設定によって、ユーザ インターフェイスに表示される名前とアイコンが決まります。分かりやすい名前とアイコンを設定すると、ソースを簡単に選択できるようになります。

入力コネクタ 1 は内蔵カメラであることに注意してください。

## ビデオとコンテンツの品質について

モーションまたは鮮明度に関する品質を最適化するには、*[ビデオ (Video) ] > [入力 (Input) ] > [コネクタ n (Connector n) ] > [品質 (Quality) ]* 設定を使用します。

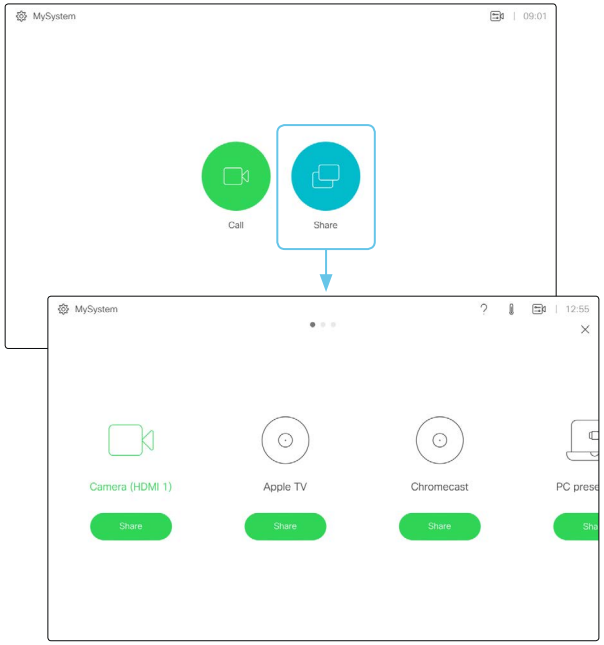
通常、画像の動きが激しい場合は、**[モーション (Motion) ]** を選択する必要があります。高品質で詳細な画像とグラフィックが必要なときは、**[シャープネス (Sharpness) ]** を選択します。

コネクタ 2 のデフォルト値は **[シャープネス (Sharpness) ]**です。

# 入力ソース数の拡大

Cisco のタッチ ユーザ インターフェイスは、サードパーティ製の外部ビデオ スイッチに接続された入力ソースが含まれるようにカスタマイズできます。

ソースは、ビデオ システムに直接接続されている他のビデオと同じように表示されて動作します。




複数の外部入力ソースがあるユーザ インターフェイス (例)

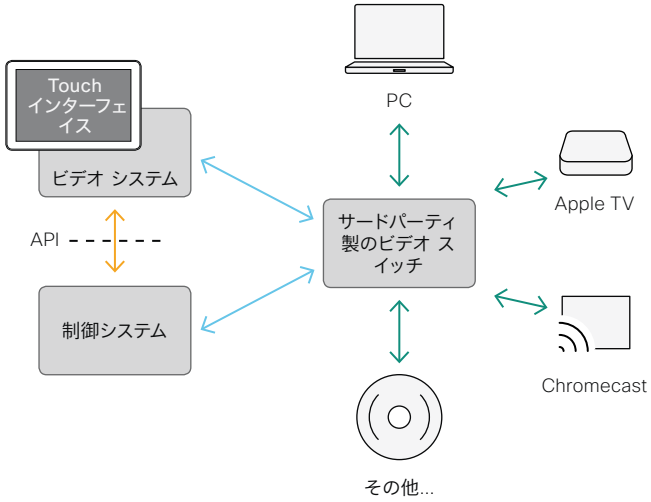
ユーザ インターフェイスを拡張する方法、およびそれをビデオ システムの API を使用してセットアップする方法の詳細については、*カスタマイズ ガイド* を参照してください。次のリンクにアクセスします。

► https://www.cisco.com/go/in-room-control-docs

## アーキテクチャ

タッチ インターフェイスがある Cisco ビデオ システム、サードパーティ製制御システム (Crestron または AMX など) 、およびサードパーティ製ビデオ スイッチが必要です。ビデオ スイッチを制御するのは、ビデオ システムではなく、制御システムです。

制御システムをプログラミングするときには、ビデオ システムの API (イベントとコマンド) * を、ビデオ スイッチや、タッチ インターフェイス上のコントロールと接続するために使用する必要があります。このようにして、ユーザ インターフェイス上に表示されて実行される事柄と、入力ソースの実際の状態とを同期できます。




* 制御システムをプログラミングするときに必要な API コマンドにアクセスするには、RoomControl、Integrator、または admin ユーザ ロールを持つユーザが必要です。

# ディスプレイについて

## リアルタイム通信の要件

Cisco では、ビデオ システムでのカメラからスクリーンへの遅延を最小限にし、また音声コンポーネントとビデオ コンポーネント間全体の遅延を検出してそれを埋め合わせるために、さまざまな取り組みを行ってきました。

コミュニケーションがより自然な感じになるように低遅延のディスプレイを使用することを推奨します。また、多数のディスプレイを注文する前に、サンプルをテストすることも推奨します。

ほとんどのディスプレイによる遅延は多くの場合非常に高い (100 ms より長い) ため、リアルタイム コミュニケーションの品質を損ないます。

次のディスプレイの設定によって、この遅延が低下する可能性があります。

- [ゲーム (Game) ] モード、[PC] モード、あるいは、応答時間 (および通常であれば遅延) を低下させるように設計された同様のモードをアクティブにします。
- 遅延を発生させる、動きを円滑化する機能 (たとえば、[モーション フロー (Motion Flow) ] や [ナチュラル モーション (Natural Motion) ] などのビデオ処理) を非アクティブにします。
- 音響エコー キャンセラの誤動作を発生させる [仮想サラウンド (Virtual Surround) ] 効果や [ダイナミック コンプレッション (Dynamic Compression) ] などの高度な音声処理を非アクティブにします。
- 別の HDMI 入力に変更する。

## Consumer Electronics Control (CEC)

ディスプレイのアクティブなビデオ入力がユーザによって変更されることがあります。アクティブなビデオ入力は、製造元のユーザ インターフェイスから設定されます。

発信すると、ビデオシステムはアクティブなビデオ入力が別の入力に切り替えられたかどうかを検出します。切り替えられている場合、ビデオシステムは入力を切り替え直し、ビデオ システムがアクティブなビデオ入力ソースになります。

ビデオシステムがスタンバイ状態に入るときにアクティブな入力ソースでない場合、ディスプレイはスタンバイ状態に移行しません。

## Cisco が推奨するディスプレイ

最大限のエクスペリエンスと検証済みの互換性のため、次のディスプレイを使用することをお勧めします。このディスプレイの一覧は変更される可能性があるため、CE9 ソフトウェアのリリース ノートで更新を確認してください。

| モデル | LG グローバル ウェブサイト リンク |
|---|---|
| 49″ UHD (49UH5C) | http://www.lg.com/global/business/information-display/digital-signage/lg-49UH5C |
| 55″ UHD (55UH5C) | http://www.lg.com/global/business/information-display/digital-signage/lg-55UH5C |
| 65″ UHD (65UH5C) | http://www.lg.com/global/business/information-display/digital-signage/lg-65UH5C |
| 75″ UHD (75UH5C) | http://www.lg.com/global/business/information-display/digital-signage/lg-75UH5C |
| 86″ UHD (86UH5C) | http://www.lg.com/global/business/information-display/digital-signage/lg-86UH5C |
| 98″ UHD (98UH5C) | http://www.lg.com/global/business/information-display/digital-signage/lg-98LS95D |

| モデル | LG グローバル ウェブサイト リンク |
|---|---|
| QMN シリーズ (43″49″、55″、65″、75″) | https://displaysolutions.samsung.com/digital-signage/detail/1269/QM43N |
| QMH シリーズ (49″55″、65″) | https://displaysolutions.samsung.com/digital-signage/detail/1144/QM49H |
| QBN シリーズ (43″49″、55″、65″、75″) | https://displaysolutions.samsung.com/digital-signage/detail/1274/QB43N |
| QBH シリーズ (65″ 、75″) | https://displaysolutions.samsung.com/digital-signage/detail/1205/QB65H |

# 4K 解像度について

## ディスプレイの接続

システムを初めて起動すると、セットアップ アシスタントが自動的に起動します。ここで、ディスプレイをテストして設定を調整します。画面の指示に従います。

後の段階で設定を調整する必要が生じた場合、ウェブ インターフェイスにサインインして、*[セットアップ (Setup)] > [設定 (Configuration)] > [ビデオ (Video)] > [出力 (Output)] > [コネクタ n (Connector n)] > [解像度 (Resolution)]* に移動し、画面の解像度を調整します。ディスプレイのサポート内容に応じて解像度を設定してください。

スクリーンが黒くなったりちらつく場合は、解像度を低く設定できます。それでも問題が解決しない場合は、Ultra HD をサポートするディスプレイの HDMI ポートに HDMI ケーブルが接続されていることを確認してください。ディスプレイで HDMI Ultra HD の設定がオンになっていることも確認してください。

Cisco では、テスト済みのディスプレイの一覧を提供しています。
▶「Cisco が推奨するディスプレイ」の章を参照してください。

## コンピュータの接続

コンピュータの接続時にエラーが発生すると、スクリーンと Touch 10 コントローラにメッセージが表示されます。

ビデオ入力コネクタのデフォルトの推奨解像度は 1080p60（1920_1080_60）です。コンピュータで 4K 解像度を使用する場合は、ウェブ インターフェイスにサインインし、*[セットアップ (Setup)] > [設定 (Configuration)] > [ビデオ (Video)] > [入力 (Input)] > [コネクタ n (Connector n)] > [推奨解像度 (PreferredResolution)]* に移動して、値を調整します。

また、接続しているコンピュータのオペレーティング システムが提供するディスプレイ/モニタ設定から解像度を上書きすることもできます。

## チェックリスト

確実な動作のために、Cisco に HDMI ケーブルを注文するか、認定 HDMI ケーブルを使用してください。▶「HDMI ケーブルについて」の章を参照してください。

ビデオ システムの入力/出力コネクタが正しく設定されていることを確認してください。

デバイス（TV/ディスプレイ、コンピュータ）が 4K をサポートしており、正しく設定されていることを確認します。

TV/ディスプレイが 4K をサポートしていると製造元が公表していても、TV/ディスプレイをテストして動作を確認する必要があります。

4K の使用では高品質ケーブルの必要性が増します。

- 4kp30 は 1080p60 の約 2 倍のデータレートを使用します。
- 4kp60 は 1080p60 の約 4 倍のデータレートを使用します。

# HDMI ケーブルについて

HDMI ケーブルは、カメラ、ディスプレイ、およびプレゼンテーション ソースとの接続に必要です。

確実な動作のために、Cisco に HDMI ケーブルを注文*するか、認定 HDMI ケーブルを使用することをお勧めします。

## カメラおよびディスプレイ用の HDMI ケーブル

1920X1200@60fps を超える解像度フォーマットには、必ずハイスピード対応の HDMI ケーブルを使用してください。動作が保証されている範囲については、3840×2160 (60fps) で Cisco が事前に選定した HDMI ケーブルを使用するか、またはプレミアム HDMI ケーブル認証プログラムに合格したケーブルを使用します。

## プレゼンテーション ソース用の HDMI ケーブル

プレゼンテーション ソースには、PC/ラップトップ、ドキュメント カメラ、メディア プレーヤー、ホワイトボード、またはその他のデバイスを使用できます。

1920X1080@60fps を超える解像度フォーマットには、必ずハイスピード対応の HDMI ケーブルを使用してください。確実な動作のために、Cisco が提供している HDMI ケーブルを使用するか、高速 HDMI 1.4b カテゴリ 2 仕様準拠のケーブルを使用してください。

HDMI プレゼンテーション ケーブルは Cisco に注文 (HDMI 1.4b カテゴリ 2) することをお勧めします。

HDMI ケーブルの詳細については、▶ http://www.hdmi.org を参照してください。

* Room Kit、Room Kit Plus、Codec Plus、Room 55、および Room 70 は、Cisco の HDMI、ディスプレイ ポート、およびミニ ディスプレイ ポート用プレゼンテーション ケーブル (CAB-HDMI-MULT-9M=) をサポートしていません。

# 最適な概要の機能のセットアップ

ウェブ インターフェイスにサインインして、*[設定 (Configuration) ] > [システム設定 (System Configuration) ]* に移動すると、ここに示す設定が見つかります。

最適な概要機能は自動カメラ フレーミングを使用し、室内の人数に基づいて最適な表示を選択します。

カメラは、デジタル顔検出機能を使用して、室内の個人またはグループを最適に自動表示します。この機能は、室内での参加者の移動や新たな参加者の入室に合わせて、画面にすべてのユーザが含まれるように自動的に調整します。

## 最適な概要の設定

スピーカー トラッキングを設定するには、*[カメラ (Camera) ] > [スピーカー トラック (SpeakerTrack) ]* の設定を使用ます。

*[カメラ (Camera) ] > [スピーカー トラック (SpeakerTrack) ] > [モード (Mode) ]*

**自動**: [ベスト概要 (general general)] が有効になります。システムは室内の人々を検出し自動的に最適なカメラ フレーミングを選択します。このオン/オフは、タッチ コントローラのカメラ制御パネルを使用してすぐに切り替えることができます。

**オフ**: ベスト概要がオフになっています。最適な概要のオン/オフ ボタンがタッチ コントローラに表示されなくなります。

# Touch 10 コントローラの接続 (1/4 ページ)

Touch 10は、ビデオ システムに直接接続するか (このページの説明を参照) 、またはネットワーク (LAN) 経由でビデオ システムとペアリングする (次のページの説明を参照) 必要があります。後者はリモート ペアリングと呼ばれます。

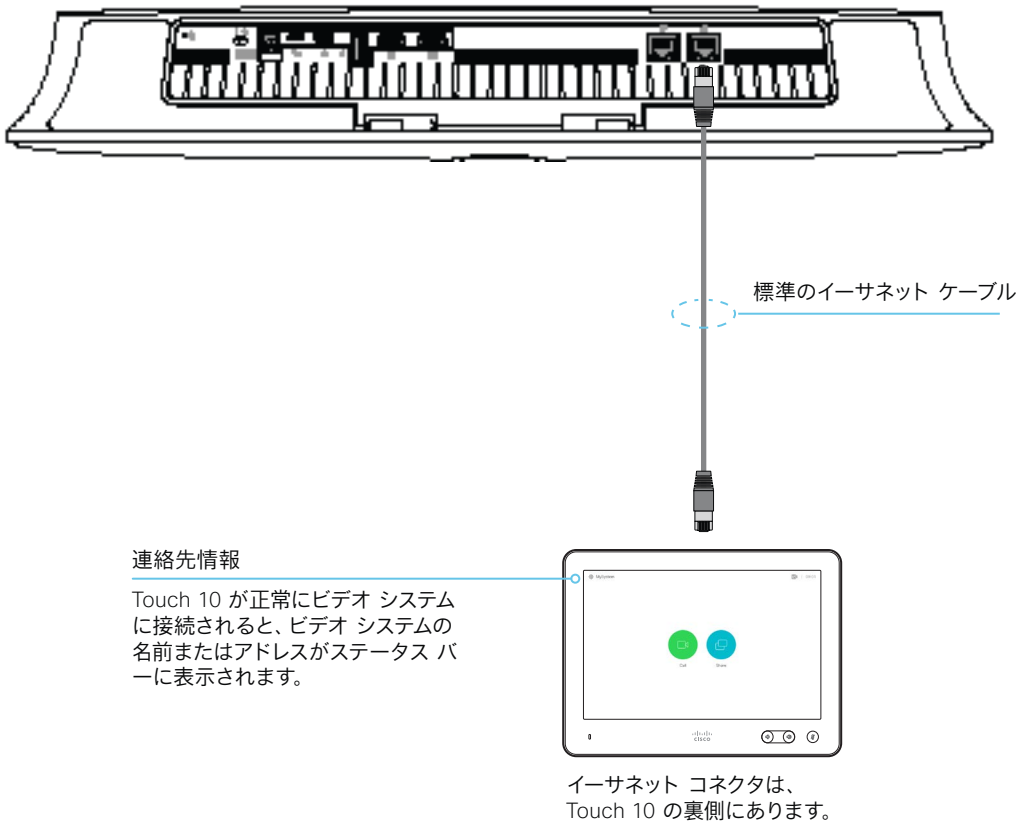
## Touch 10 とビデオ システムの直接接続

図のように、Touch 10 をビデオシステムの Touch 専用 (RJ-45) ポートに接続します。

### Touch 10 の設定

Touch 10 が電源に接続されると、設定手順が始まります。画面に表示される指示に従います。

Touch 10 にソフトウェアのアップグレードが必要な場合は、設定手順の一部で新しいソフトウェアがビデオ システムからダウンロードされ、自動的にユニットにインストールされます。アップグレード後に Touch 10 が再起動します。



# Touch 10 コントローラの接続 (2/4 ページ)

## ネットワーク (LAN) 経由での Touch 10 のビデオ システムへの接続

図のように、Touch 10 とビデオ システムを壁のネットワーク ソケットまたはネットワーク スイッチに接続します。

### Touch 10 の設定

Touch 10 が電源に接続されると、設定手順が始まります。画面に表示される指示に従います。

*[ルーム システムの選択 (Select a room system) ]* 画面が表示されたら、以下の点に注意してください。

- ペアリング可能なシグナリング中ビデオ システムのリストが、画面に表示されます。ペアリングするビデオ システムの名前をタップします。

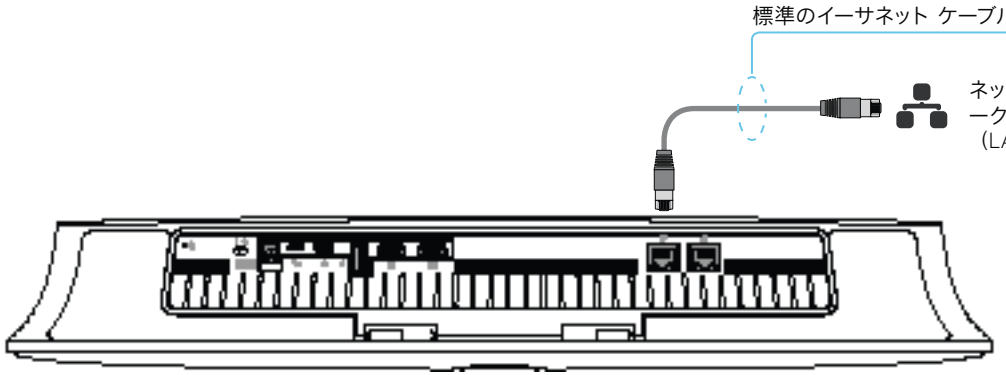
  ビデオ システムをリストに表示するには、次を満たしている必要があることに注意してください。

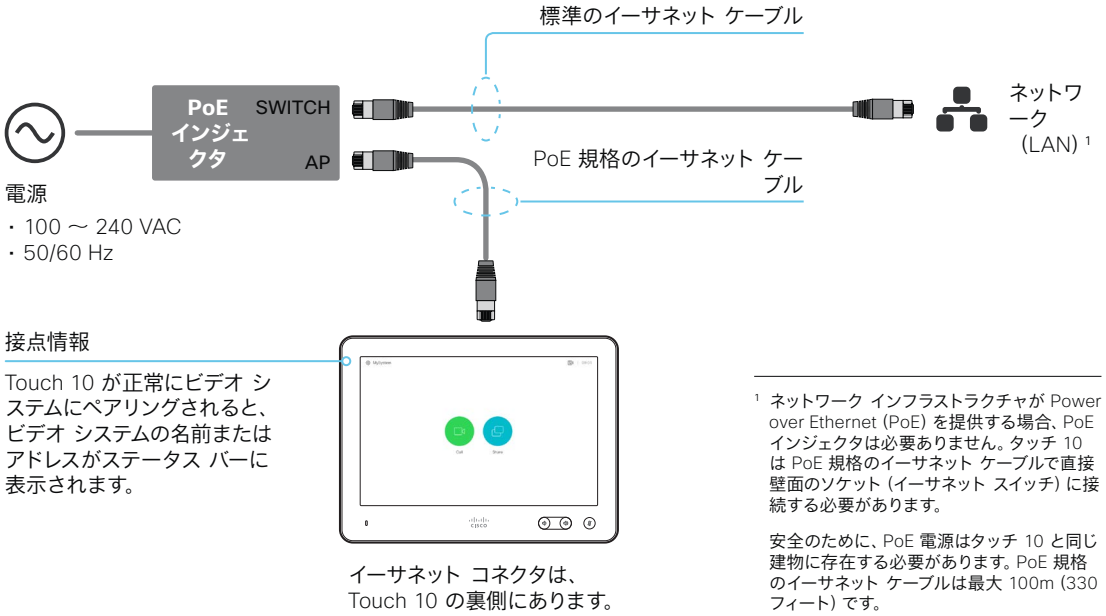
  - ビデオ システムおよびTouch 10 が同じサブネット上にある必要があります。
  - ビデオ システムは、直近の 10 分間に再起動されている必要があります。ビデオ システムがリストに表示されない場合は、再起動してください。
- ビデオ システムが利用可能システムのリストに表示されない場合は、入力フィールドに IP アドレスまたはホスト名を入力します。*[接続 (Connect) ]* をタップします。
- ペアリング プロセスを開始するには、ユーザ名とパスワードを使用してログインする必要があります。[Login] をタップします。

  user ロールを持つユーザであれば十分対応できます。このタスクを実行するために admin ロールは必要ありません。

  ユーザ アカウントを作成してそれにロールを割り当てる方法の詳細については、▶「ユーザ管理」の章を参照してください。

Touch 10 にソフトウェアのアップグレードが必要な場合は、設定手順の一部で新しいソフトウェアがビデオ システムからダウンロードされ、自動的にユニットにインストールされます。アップグレード後に Touch 10 が再起動します。



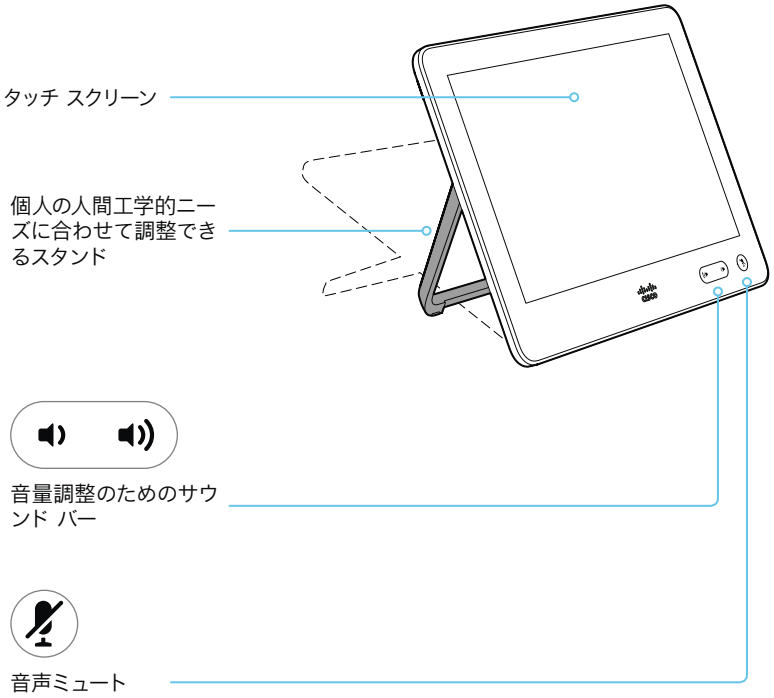

[1] ネットワーク インフラストラクチャが Power over Ethernet (PoE) を提供する場合、PoE インジェクタは必要ありません。タッチ 10 は PoE 規格のイーサネット ケーブルで直接壁面のソケット (イーサネット スイッチ) に接続する必要があります。

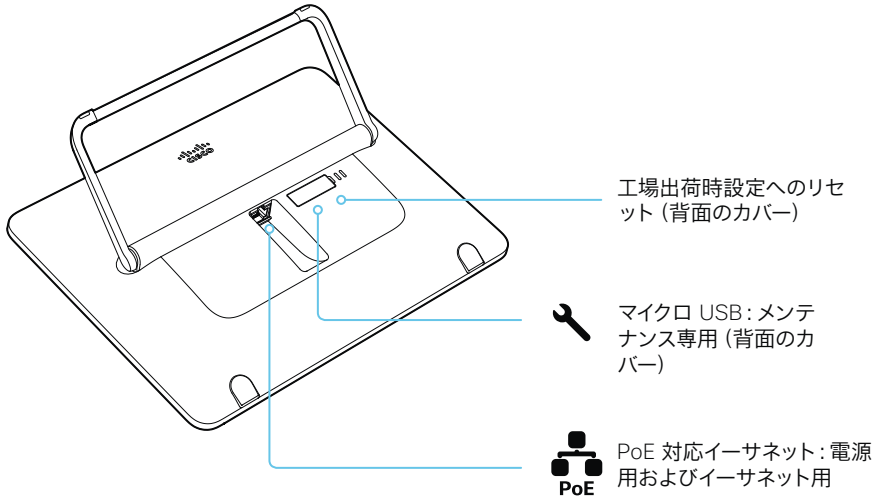
安全のために、PoE 電源はタッチ 10 と同じ建物に存在する必要があります。PoE 規格のイーサネット ケーブルは最大 100m (330 フィート) です。

# Touch 10 コントローラの接続 (4/3 ページ)

## Cisco Touch 10 の物理インターフェイス

これは、2017 年後半に提供が開始された Touch 10 コントローラの新しいバージョンです。以前のバージョンと同じ機能を備えていますが、物理インターフェイスが多少異なります。新しいデバイスは、前面のロゴと、背面のコネクタが少ないことによって識別できます。

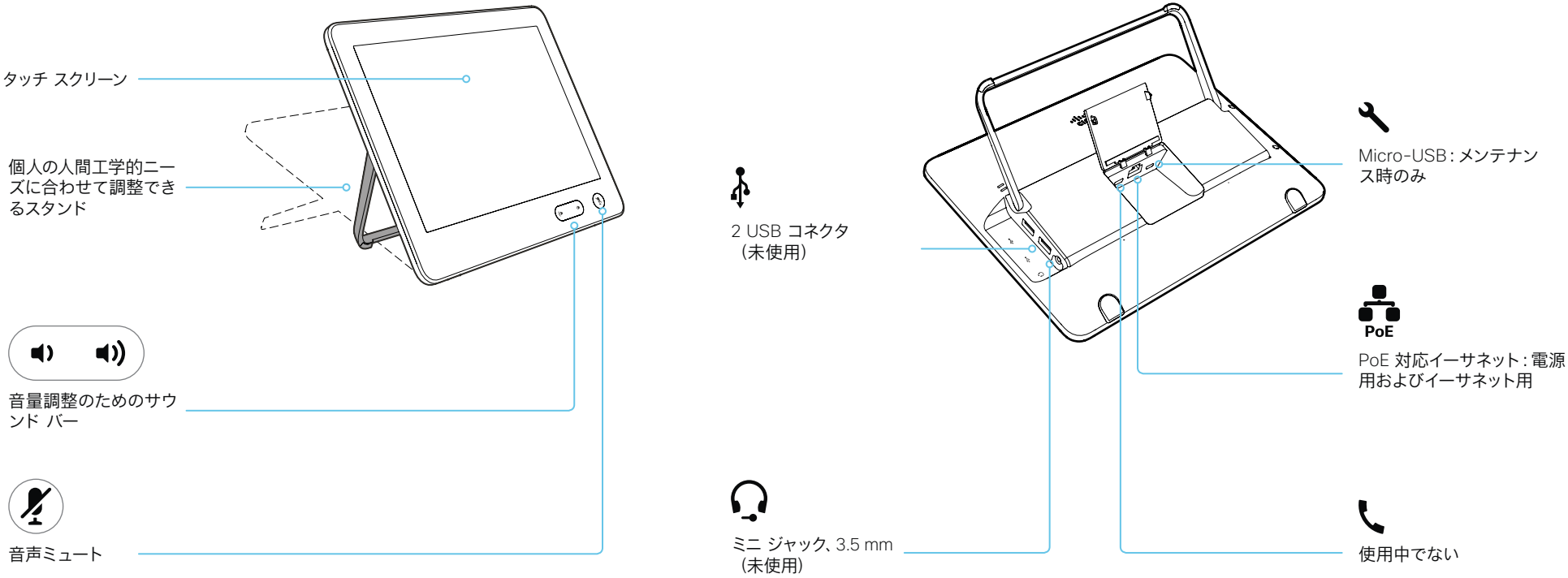


# Touch 10 コントローラの接続 (4/4 ページ)

## Cisco TelePresence Touch 10 の物理インターフェイス

Touch 10 コントローラの新しいバージョンについては、次のページを参照してください。



# ISDN リンクの接続

ISDN リンクは、ビデオ システムが ISDN 回線を使用して接続することを可能にします。また、PSTN (公衆電話交換網) を介したビデオ コールと電話の両方を可能にします。

ISDN リンクは、ISDN BRI、ISDN PRI、および V.35 をサポートしています。ISDN は、SIP または H.323 コール用の通常の IP 接続に加えて使用できます。また、IP インフラストラクチャなしでも使用できます。

ISDN リンクは、ビデオ システムの ウェブ インターフェイスから管理されます。ウェブ インターフェイスにサインインして、*[セットアップ (Setup) ] > [周辺機器 (Peripherals) ]* に移動します。

要件:

- ISDN リンクは、IL1.1.7 以降のソフトウェアを実行している必要があります。
- ビデオ エンドポイントは、ISDN リンクと通信するために、ウェブ インターフェイスまたは API で IPv6 を有効にする必要があります。
- 確実にインストールするために、ISDN リンクのインストール ガイドでネットワーク トポロジを確認してください。
- ビデオ システムおよび ISDN リンクが同じサブネット上にある必要があります。エンドポイントまたは ISDN リンクに新しい IP アドレスが割り当てられている場合は、それらが同じサブネットに保持されている間だけペアリングが維持されます。

制限事項:

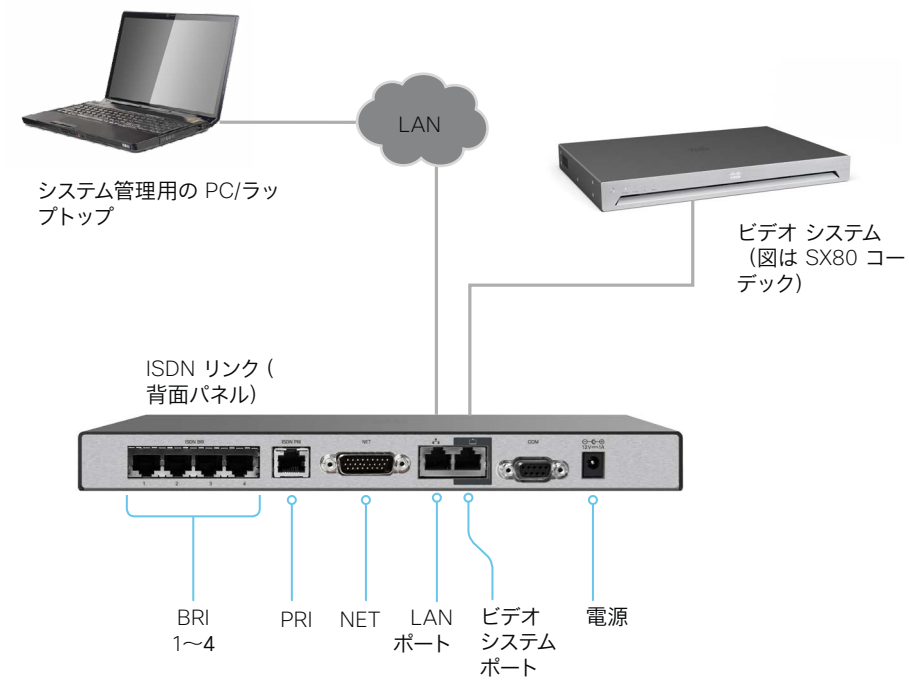
- Cisco Webex クラウド サービスに登録されているビデオ システムでは、ISDN リンクを使用できません。

## セットアップと構成

ISDN リンクの詳細 (リリース ノート、インストール ガイド、管理者ガイド、API ガイド、コンプライアンスおよび安全性ガイド) については、► https://www.cisco.com/go/isdnlink-docs を参照してください。

## LAN およびビデオ システムと ISDN リンクの間の直接接続によるセットアップ

これは推奨されるセットアップです。ただし、その他のオプションもあります。追加の例については、次の ウェブ サイトにあるユーザ マニュアルを参照してください。► https://www.cisco.com/go/isdnlink-docs を参照してください。



第 4 章

# メンテナンス

# システム ソフトウェアのアップグレード

ウェブ インターフェイスにサインインし、*[メンテナンス (Maintenance) ] > [ソフトウェアのアップグレード (Software Upgrade) ]* に移動します。

## 新しいソフトウェアをダウンロードする

各ソフトウェア バージョンに固有のファイル名があります。Cisco Download Software ウェブ ページにアクセスし、お使いの製品のページにアクセスします。▶ https://software.cisco.com/download/home

ファイル名フォーマットは :
“cmterm-s53200ce9_7_x-yyy.k3.cop.sgn”

"x" はドット内のリリース番号、"yyy" は、ソフトウェアの一意の識別子を表します。

## ソフトウェア リリース ノート

新着情報および変更の概要について、ソフトウェア リリース ノート (CE9) を読むことを推奨します。

参照先 : ▶ https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-room-kit-series/tsd-products-support-series-home.html

## 新しいソフトウェアのインストール

適切なソフトウェア パッケージをダウンロードして、コンピュータに保存します。これは .cop.sgn ファイルです。ファイル名は変更しないでください。

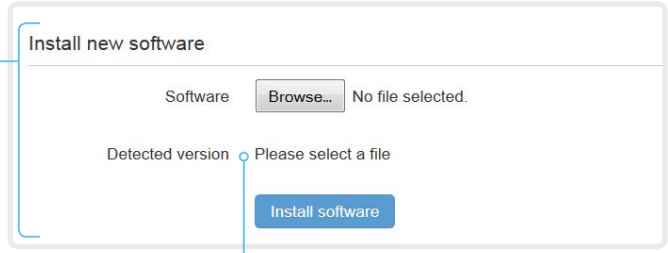
1. *[参照... (Browse...) ]* をクリックして、新しいソフトウェアを含む .cop.sgn ファイルを探します。

   ソフトウェアのバージョンが検出され、表示されます。

2. *[ソフトウェアのインストール (Install Software) ]* をクリックして、インストール プロセスを開始します。

インストールの完了には、通常 15 分以上はかかりません。ウェブ ページから進捗状況を確認できます。インストール後に、ビデオ システムが自動的に再起動します。

再起動後に ウェブ インターフェイスで作業を再開するには、再度サインインする必要があります。




## 新しいソフトウェア バージョンの確認

ファイルを選択すると、ここにソフトウェアのバージョンが表示されます。

## ソフトウェアのダウンロード

Cisco Download Software ウェブ ページにアクセスし、お使いの製品のページにアクセスします。▶ https://software.cisco.com/download/home

Webex Room シリーズは COP ファイルを使用して ウェブ インターフェースからアップグレード可能です。

# オプション キーを追加する

ウェブ インターフェイスにログインし、*[メンテナンス (Maintenance) ] > [オプション キー (Option Keys) ]* に移動します。

すべてのオプション キーのリストと、ビデオ システムにインストールされていないオプション キーのリストが表示されます。

アンインストールされたオプションのオプション キーを取得する方法については、Cisco の担当者にお問い合わせください。

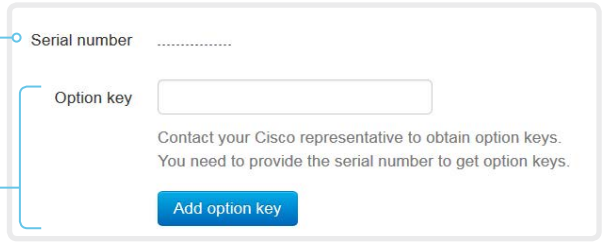
### ビデオ システムのシリアル番号。

オプション キーの注文時にはビデオ システムのシリアル番号が必要です。

### オプション キーの追加

1. テキストの入力フィールドに*オプション キー*を入力します。
2. *[オプション キーの追加 (Add option key) ]* をクリックします。

オプション キーを複数追加する場合は、すべてのキーに対してこの手順を繰り返してください。




## オプション キーについて

ビデオ システムには、1 つ以上のソフトウェア オプションがインストールされている場合、またはインストールされていない場合があります。オプションの機能をアクティブするには、対応する*オプション キー*がビデオ システムに存在する必要があります。

各ビデオ システムには一意のオプション キーがあります。

オプション キーは、ソフトウェアのアップグレードまたは出荷時の状態にリセットしても削除されないため、一度追加するだけで済みます。

# システム ステータス

## システム情報の概要

[システム情報 (System Information) ] ページを表示するには、ウェブ インターフェイスにログインします。

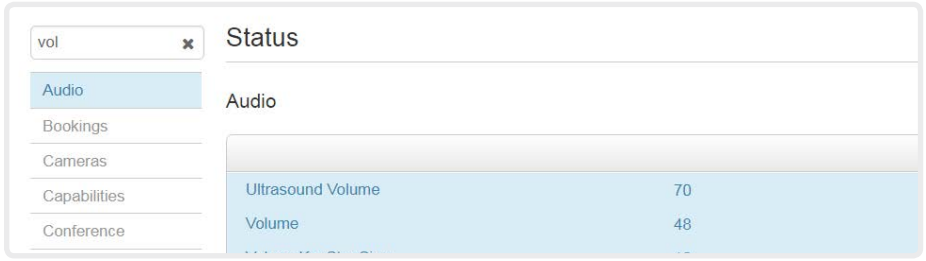
このページには、製品タイプ、システム名、およびハードウェア、ソフトウェア、インストール済みオプション、ネットワーク アドレスに関する基本情報が表示されます。ビデオ ネットワーク (SIP および H.323) の登録ステータスのほか、システムにコールする際に使用する番号および URI も含まれます。

## システム ステータスの詳細

ウェブ インターフェイスにサインインして、*[セットアップ (Setup) ] > [ステータス (Status) ]* に移動し、より詳細なステータス情報*を探します。

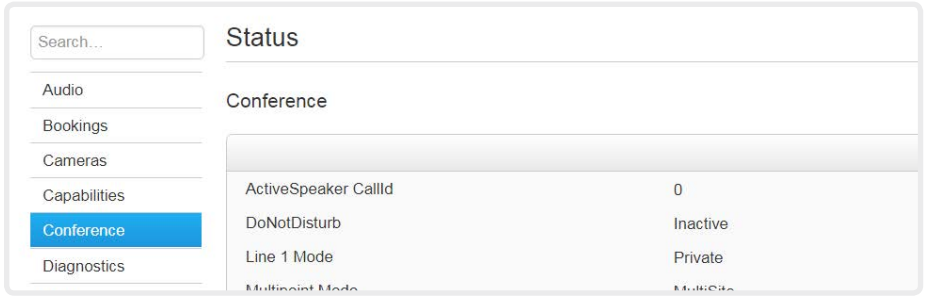
### ステータス エントリを検索する

検索フィールドに必要な数の文字を入力します。これらの文字が含まれているすべてのエントリが右側のペインに表示されます。値スペースにこれらの文字が含まれているエントリも表示されます。




### カテゴリを選択して適切なステータスに移動する

システム ステータスはカテゴリ別にグループ化されます。左側のペインでカテゴリを選択すると、関連するステータスが右側に表示されます。




* 図に示しているステータスは一例です。お使いのシステムのステータスとは異なる場合があります。

# 診断の実行

ウェブ インターフェイスにサインインして、*[メンテナンス (Maintenance) ] > [診断 (Diagnostics) ]* に移動します。

[診断 (Diagnostics) ] ページには、エラーの一般的な原因に関するステータスが示されます*。

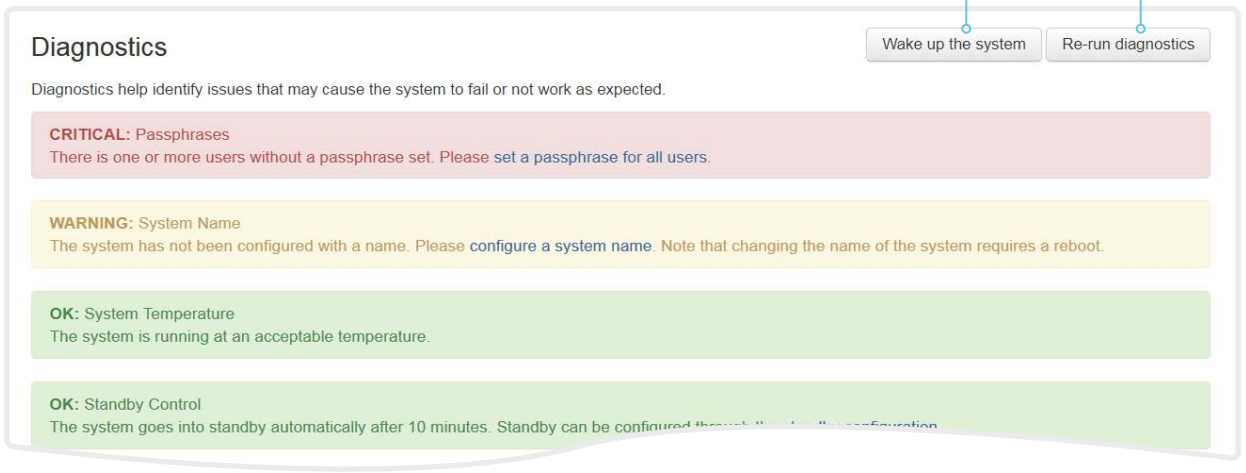
エラーや重大な問題は赤色で目立つように示されます。警告は黄色です。

### 診断の実行

*[診断の再実行 (Re-run diagnostics) ]* をクリックして、リストを最新の状態にします。

### スタンバイ モードを離れる

スタンバイモードのビデオシステムを復帰させるには、*[システムの起動 (Wake up the system) ]* をクリックします。

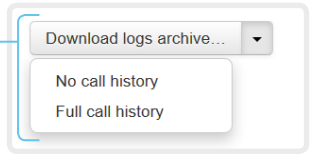



* 図に示しているメッセージは一例ですお使いのシステムでは表示される情報が異なる場合があります。

# ログ ファイルをダウンロードする

ウェブ インターフェイスにサインインして、[*メンテナンス (Maintenance) ] > [システム ログ (System Logs) ]* を選択します。

## すべてのログ ファイルをダウンロードする




*[ログ アーカイブのダウンロード... (Download logs archive...) ]* をクリックして、手順に従います。

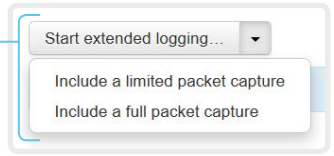
匿名化された通話履歴はログ ファイルにデフォルトで含まれています。

ログ ファイルから通話履歴を除外する場合や、完全な通話履歴 (匿名以外の発信側/着信側) を含める場合は、ドロップダウン リストを使用します。

## 1 つのログファイルを開く/保存

ログ ファイルを開くには ウェブ ブラウザでファイル名をクリックし、ファイルをコンピュータに保存するにはファイル名を右クリックします。


## 拡張ロギングの開始




*[拡張ロギングの開始... (Start extended logging...) ]* をクリックします。.

拡張ロギングは、ネットワーク トラフィックの完全キャプチャが含まれているかどうかによって 3 分から 10 分かかります。

タイムアウトになる前に拡張ロギングを停止するには、*[拡張ロギングの停止 (Stop extended logging) ]* をクリックします。

デフォルトとして、ネットワーク トラフィックはキャプチャされません。ネットワーク トラフィックの一部または全部のキャプチャを含めるには、ドロップダウン メニューを使用します。

## ログ ファイル リストの表示更新

[現在のログ (Current logs) ] または [履歴ログ (Historical logs) ] の更新ボタンをクリックすると、対応するリストの表示が更新されます。

## ログ ファイルについて

ログファイルは、テクニカル サポートが必要な場合に、Cisco のサポートから要求されることがある Cisco 固有のデバッグ ファイルです。

*Current log* ファイルはタイムスタンプ付きのイベント ログ ファイルです。

ビデオ システムを再起動するたびに、現在のログ ファイルはタイムスタンプ付きの*履歴ログ ファイル*にすべてアーカイブされます。履歴ログファイルの最大数に到達すると、最も古いファイルは上書きされます。

## 拡張ロギング モード

拡張ロギング モードをオンにすると、コールのセットアップ中にネットワークの問題の診断に役立つ場合があります。このモードの間は、より多くの情報がログ ファイルに保存されます。

拡張ロギングはビデオ システムのリソースをより多く使用するため、ビデオ システムの動作が標準を下回る場合があります。拡張ロギング モードは、トラブルシューティングのときにのみ使用してください。

# リモート サポート ユーザを作成する

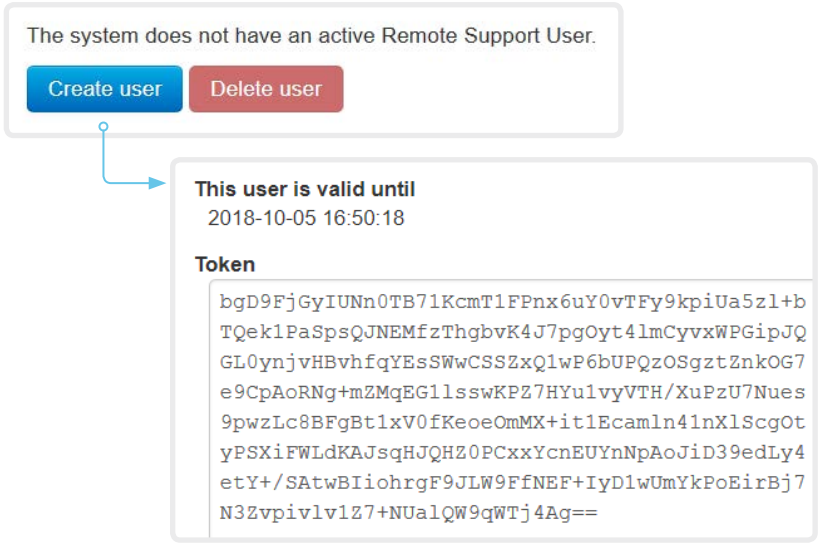
ウェブ インターフェイスにログインし、*[メンテナンス (Maintenance) ] > [システム リカバリ (System Recovery) ]* に移動して、[リモート サポート ユーザ (Remote Support User) ] タブを選択します。

リモート サポート ユーザは、Cisco TAC から指示されたトラブルシューティングを行うためだけに有効にする必要があります。

## リモート サポート ユーザの作成

1. *[ユーザの作成 (Create User) ]* をクリックします。
2. Cisco TAC で案件を開きます。
3. *[トークン (Token) ]* フィールドのテキストをコピーして、Cisco TAC に送信します。
4. Cisco TAC はパスワードを生成します。

リモート サポート ユーザは 7 日間、または削除されるまで有効です。




## リモート サポート ユーザの削除

*[ユーザの削除 (Delete User) ]* をクリックします。

## リモート サポート ユーザについて

ビデオ システムの問題を診断する場合、リモート サポート ユーザを作成できます。

リモート サポート ユーザにはシステムへの読み取りアクセス権が付与され、トラブルシューティングに役立つ限定された一連のコマンドにアクセスできます。

リモート サポート ユーザのパスワードを取得するには、Cisco Technical Assistance Center (TAC) アシスタントが必要です。

# 設定とカスタム要素のバックアップ/復元

ウェブ インターフェイスにサインインして、*[メンテナンス (Maintenance) ] > [バックアップと復元 (Backup and Restore) ]* に移動します。

バックアップ ファイル (zip 形式) には、設定とともにカスタム要素を含めることができます。次の要素からバンドルに含めるものを選択できます。

- ブランディング イメージ
- マクロ
- お気に入り
- サインイン バナー
- 室内制御パネル
- 構成/設定 (すべてまたは一部)

バックアップ ファイルは、ビデオ システムの ウェブ インターフェイスから手動で復元できますが、Cisco UCM または TMS などを使用して複数のビデオ システムにプロビジョニングできるように、バックアップ バンドルを一般化することもできます (**次の章**を参照してください) 。

## バックアップ ファイルの作成

1. *[バックアップの作成 (Create backup) ]* タブを開きます。
2. バックアップ ファイルに含める要素を選択します。

   現在ビデオ システム上に存在しない要素はグレー表示されます。
3. バックアップ ファイルに含める設定 (ある場合) を選択します。次の点に注意してください。
   - デフォルトでは、すべての設定がバックアップ ファイルに含まれます。
   - ウェブ ページの一覧から手動で設定を削除することにより、1 つ以上の設定を手動で削除できます。
   - あるビデオ システムに固有の設定をすべて削除する場合は、*[システム固有の設定の削除 (Remove system-specific configurations) ]* をクリックします。

     これは、他のビデオ システムでバックアップ バンドルを復元する予定がある場合に役立ちます。
4. *[バックアップのダウンロード (Download backup) ]* をクリックして、コンピュータ上の zip ファイルに要素を保存します。

## バックアップ ファイルの復元

1. *[バックアップの復元 (Restore backup) ]* タブを選択します。
2. *[参照... (Browse...) ]* をクリックして、復元するバックアップ ファイルを見つけます。

   バックアップ ファイル内のすべての設定と要素が適用されます。
3. *[ファイルのアップロード (Upload File) ]* をクリックして、バックアップを適用します。

   設定によっては、有効にするためにビデオ システムを再起動する必要があります。

## その他の情報

### マクロの復元

ビデオ システムでマクロを含むバックアップ ファイルを復元する場合、以下の処理が適用されます。

- マクロのランタイムを起動または再起動します。
- マクロは自動的に有効化 (開始) されます。

### ブランド イメージの復元

バックアップバンドルにブランドイメージが含まれている場合、*[ユーザインターフェイス壁紙 (UserInterface Wallpaper) ]* 設定は自動的に **[自動 (Auto) ]** に設定されます。

したがって、ブランド イメージは自動的に表示されます。カスタム壁紙より優先される場合もあります。

### バックアップ ファイル

バックアップ ファイルは、いくつかのファイルを含む zip 形式のファイルです。それらのファイルは zip ファイル内の最上位にあり、フォルダに含まれていないことが重要です。

# カスタム要素の CUCM プロビジョニング

▶ 「構成とカスタム要素のバックアップと復元」の章で説明されているとおり、バックアップ ファイルは、さまざまなビデオシステムの*カスタマイズ テンプレート*として使用できます。

カスタマイズ テンプレート（バックアップ ファイル）は、次のいずれかによってホストされています。

- CUCM TFTP ファイル サービス、または
- HTTP または HTTPS のビデオ システムによって到達可能なカスタム ウェブ サーバ。

ビデオ システムが CUCM (Cisco Unified Communications Manager) からカスタマイズ テンプレートの名前および格納場所に関する情報を取得する際は、ビデオ システムがサーバに接続してファイルをダウンロードし、カスタム要素を復元します。

構成はビデオ システム上では復元されません。これは、構成がカスタマイズ テンプレートとして使用するバックアップ ファイルの一部である場合でも同じです。

## カスタマイズ テンプレートの TFTP ファイル サーバへのアップロード

1. *Cisco Unified OS の管理*にサインインします。
2. *[ソフトウェア アップグレード (Software Upgrades) ] > [TFTP ファイル管理 (TFTP File Management) ]* に移動します。
3. [*Upload File*] をクリックします。入力フィールドにカスタマイズ テンプレートの名前とパスを入力します。
4. [*Upload File*] をクリックします。

## 各ビデオ システムへのカスタマイズ プロビジョニング情報の追加

1. *Cisco Unified CM の管理*にサインインします。
2. *[デバイス (Device) ] > [電話 (Phone) ]* に移動します。
3. 関連するデバイスの製品固有の構成セクション内で、[カスタマイズ プロビジョニング (Customization Provisioning) ] フィールドに以下を入力します。
   - *カスタマイズ ファイル*：カスタマイズ テンプレートのファイル名（backup.zip など）*
   - *カスタマイズ ハッシュの型*：**SHA512**
   - *カスタマイズ ハッシュ*：カスタマイズ テンプレートの SHA512 チェックサム。

   これらのフィールドが存在しない場合は、CUCM に新しいデバイス パッケージをインストールする必要があります。
4. *[保存 (Save) ]* および *[構成の適用 (Apply Config) ]* をクリックし、構成をビデオ システムにプッシュします。

* TFTP サービスを使用しない場合は、カスタマイズ テンプレートの完全な URI：`<hostname>:<portnumber>/<path-and-filename>` を入力する必要があります。

次に例を示します。

- http://host:6970/backup.zip または
- https://host:6971/backup.zip

## SHA512 チェックサム

ヒントウェブ インターフェイスを使用してビデオ システムにファイルを復元することにより、ファイルの SHA512 チェックサムを検索できます。

1. ウェブ インターフェイスにサインインして、*[メンテナンス (Maintenance) ] > [バックアップと復元 (Backup and Restore) ]* に移動します。
2. *[バックアップの復元 (Restore backup) ]* タブを選択します。
3. *[参照 (Browse...) ]* をクリックして、チェックサムを計算したいファイルを検索します。

   ページの下部に SHA512 チェックサムが表示されていることが確認できます。

## CUCM のドキュメンテーション

▶ https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

# カスタム要素の TMS プロビジョニング

► 「構成とカスタム要素のバックアップと復元」の章で説明されているとおり、バックアップ ファイルは、さまざまなビデオシステムの*カスタマイズ テンプレート*として使用できます。

バックアップ ファイルは、HTTP または HTTPS のビデオ システムによって到達可能なカスタム ウェブ サーバ上にホストされる必要があります。

ビデオ システムが TMS (TelePresence Management Suite) からバックアップ ファイルの名前および位置に関する情報を取得する際は、ビデオ システムがサーバに接続してファイルをダウンロードし、カスタム要素を復元します。

## 構成テンプレートの作成と適用

1. 構成テンプレートを作成します。
2. 次の XML 文字列を含むカスタム コマンドを構成テンプレートに追加します。

```
<コマンド>
  <プロビジョニング>
    <サービス>
    <Fetch>
       <URL>web-server-address</URL>
       <Checksum>checksum</Checksum>
       <Origin>origin</Origin>
     </Fetch>
    </サービス>
  </プロビジョニング>
</コマンド>
```

   where

   *web-server-address:* バックアップ ファイルへの URI ( 例 : http://host/backup.zip) 。

   *checksum:* バックアップ ファイルの SHA512 チェックサム。

   *origin:* **Provisioning** *

3. 構成テンプレートをプッシュするビデオ システムを選択し、*[システムのセット (Set on systems) ]*をクリックします。

TMS 構成テンプレートおよびカスタムコマンドの作成方法の詳細については、► Cisco TMS 管理者ガイド を参照してください。

## SHA512 チェックサム

ヒントウェブ インターフェイスを使用してビデオ システムにファイルを復元することにより、ファイルの SHA512 チェックサムを検索できます。

1. ウェブ インターフェイスにサインインして、*[メンテナンス (Maintenance) ] > [バックアップと復元 (Backup and Restore) ]* に移動します。
2. *[バックアップの復元 (Restore backup) ]* タブを選択します。
3. [参照 (Browse...) ] をクリックして、チェックサムを計算したいファイルを検索します。

   ページの下部に SHA512 チェックサムが表示されていることが確認できます。

* このパラメータを **Provisioning** に設定しない場合、バックアップ ファイルの一部である構成もビデオ システムにプッシュされます。バックアップ ファイルに、特定のビデオ システムに固有の構成 (静的 IP アドレス、システム名、連絡先情報など) が含まれている場合、到達不能なビデオ システムで実行される可能性もあります。

# 以前に使用していたソフトウェア イメージに復元する

ウェブ インターフェイスにサインインして、*[メンテナンス (Maintenance) ] > [システム回復 (System Recovery) ]* に移動します。

以前使用していたソフトウェア イメージに交換する前に、ビデオ システムのログ ファイル、構成、およびカスタム要素をバックアップすることをお勧めします。

## ログ ファイル、構成、カスタム要素のバックアップ

1. *[バックアップ (Backup) ]* タブを選択します。
2. *[ログのダウンロード (Download logs) ]* をクリックし、指示に従ってログ ファイルをコンピュータに保存します。
3. *[バックアップのダウンロード (Download Backup) ]* をクリックし、指示に従ってバックアップ バンドルをコンピュータに保存します。

## 以前使用していたソフトウェア イメージに復元する

管理者以外、または、Cisco テクニカル サポートの指示のもとで行う場合以外はこの手順を実行しないでください。

1. [ソフトウェア回復交換 (Software Recovery Swap) ] タブを選択します。
2. *[ソフトウェア：cex.y.z への切り替え... (Switch to software: cex.y.z...) ]* をクリックします。ここで x.y.z はソフトウェア バージョンを示します。
3. *[はい (Yes) ]* をクリックして選択を確定するか、*[キャンセル (Cancel) ]* をクリックして操作を取り消します。

システムがリセットされるまでお待ちください。終了するとシステムは自動的に再起動します。この手順は数分かかることがあります。

## 以前に使用されたソフトウェア イメージについて

ビデオ システムに重大な問題がある場合は、以前使用していたソフトウェア イメージに切り替えることで、問題の解決に役立つ場合があります。

ソフトウェアを最後にアップグレードしてからシステムを工場出荷時設定にリセットしていない場合は、これまで使用していたソフトウェア イメージがシステムに存在しています。ソフトウェアをダウンロードする必要はありません。

# ビデオ システムの工場出荷時設定リセット (1/3 ページ)

ビデオ システムに重大な問題が発生した場合、最後の手段として工場出荷時のデフォルト設定にリセットすることができます。

初期設定にリセットすると元に戻すことはできません。

工場出荷時の状態にリセットする前に以前使用したソフトウェア イメージに戻すことを常に検討してください。多くの場合これでシステムをリカバリします。ソフトウェアのスワップ (切り替え) については、
▶ 「以前使用していたソフトウェア イメージへの復元」の章を参照してください。

ビデオ システムを初期設定の状態へリセットするには、ウェブ インターフェイスまたはユーザ インターフェイスを使用することを推奨します。これらのインターフェイスが利用できない場合は、 pin ホールをリセット (reset pin-hole) を使います。

工場出荷時設定リセットにより、次のような影響が発生します。

- 通話履歴が削除されます。
- パスフレーズがデフォルト設定にリセットされます。
- すべてのシステム パラメータがデフォルト値にリセットされます。
- システムにアップロード済みのファイルが、すべて削除されます。リセットされる内容には、カスタムの壁紙、証明書、およびお気に入りリストが含まれますが、これに限定されません。
- 以前の (非アクティブな) ソフトウェア イメージが削除されます。
- オプション キーは影響を受けません。

工場出荷時設定リセット後、ビデオ システムは自動的に再起動します。これは、以前と同じソフトウェア イメージを使用しています。

**初期設定へのリセットを実行する前に、ビデオ システムのログ ファイル、設定、カスタム要素をバックアップすることをお勧めします。バックアップしない場合は、データが消失する場合があります。**

# ビデオ システムの工場出荷時設定リセット (2/3 ページ)

## ウェブ インターフェイスを使用した初期設定へのリセット

初期設定へのリセットを行う前に、ビデオ システムのログ ファイルと設定をバックアップすることをお勧めします。

ウェブ インターフェイスにサインインして、*[メンテナンス (Maintenance) ] > [システム回復 (System Recovery) ]* に移動します。

1. [初期設定へのリセット (Factory Reset) ] タブを選択して、表示される情報を注意深く読みます。
2. *[初期設定へのリセットの実行 (Perform a factory reset...) ]* クリックします。.
3. *[はい (Yes) ]* をクリックして選択を確定するか、*[キャンセル (Cancel) ]* をクリックして操作を取り消します。
4. ビデオ システムが工場出荷時のデフォルト設定に戻るまで待ちます。終了すると、ビデオ システムは自動的に再起動します。これには数分かかる可能性があります。

   システムが工場出荷時の設定に正常にリセットされると、セットアップ アシスタントが起動し、[ようこそ (Welcome) ] 画面が表示されます。

## ユーザ インターフェイスからの初期設定へのリセット

工場出荷時設定へのリセットを進める前に、ビデオ システムのログ ファイルと設定をバックアップすることをお勧めします。

1. ユーザ インターフェイスの左上隅にある連絡先情報を選択します。
2. *[設定 (Settings) ]* を選択します。
3. *[初期設定へのリセット (Factory Reset) ]* を選択します。
4. 選択を確認するには[リセット (reset) ]を選択し、気が変わったら[戻る (back) ]を選択します。
5. ビデオ システムが工場出荷時のデフォルト設定に戻るまで待ちます。終了すると、ビデオ システムは自動的に再起動します。これには数分かかる可能性があります。

   システムが工場出荷時の設定に正常にリセットされると、セットアップ アシスタントが起動し、*[ようこそ (Welcome) ]* 画面が表示されます。

## ログ ファイル、構成、カスタム要素のバックアップ

ウェブ インターフェイスにサインインして、*[メンテナンス (Maintenance) ] > [システム リカバリ (System Recovery) ]* に移動します。

### ログ ファイル、構成、カスタム要素のバックアップ

1. [バックアップ (Backup) ] タブを選択します。
2. *[ログのダウンロード (Download logs) ]* をクリックし、指示に従ってログ ファイルをコンピュータに保存します。
3. *[バックアップのダウンロード (Download Backup) ]* をクリックし、指示に従ってバックアップ バンドルをコンピュータに保存します。

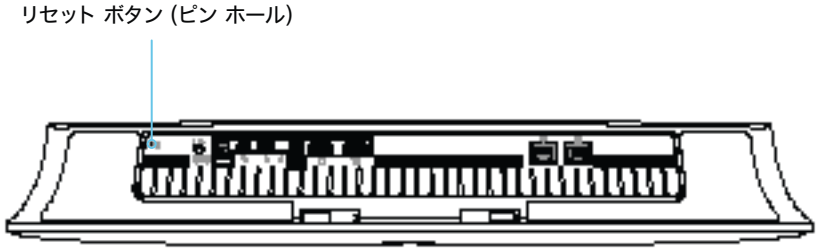
# ビデオ システムの工場出荷時設定リセット (3/3 ページ)

## リセット ボタンを使用して工場出荷時設定にリセットする

工場出荷時設定へのリセットを進める前に、ビデオ システムのログ ファイルと設定をバックアップすることをお勧めします。

1. ユニットを前に傾け、リセット ボタン (ピン ホール) が見えるようにします。
2. ペーパー クリップ (または同等のもの) を使用して、画面が黒くなるまでリセット ボタンを押し続けます (約 10 秒) 。その後、ボタンを離します。
3. ビデオ システムが工場出荷時のデフォルト設定に戻るまで待ちます。終了すると、ビデオ システムは自動的に再起動します。これには数分かかる可能性があります。

   システムが工場出荷時の設定に正常にリセットされると、セットアップ アシスタントが起動し、*[ようこそ (Welcome) ]* 画面が表示されます。



# Cisco Touch 10 の初期設定へのリセット

**この章は、2017 年後半に発売された新しい Touch 10 コントローラ (Cisco Touch 10) に適用されます。** このデバイスは、前面のロゴ、および背面のコネクタが少ないことによって識別されます。

古いバージョンについては、次のページを参照してください。

エラー状態で、接続を再確立するためにタッチ コントローラを工場出荷時設定にリセットすることが必要になる場合があります。その場合は、必ず Cisco のサポート組織に連絡して実行する必要があります。

タッチ コントローラを工場出荷時設定にリセットすると、ペアリング情報が失われ、(ビデオ システムではなく) タッチ自体が工場出荷時の初期状態に戻されます。

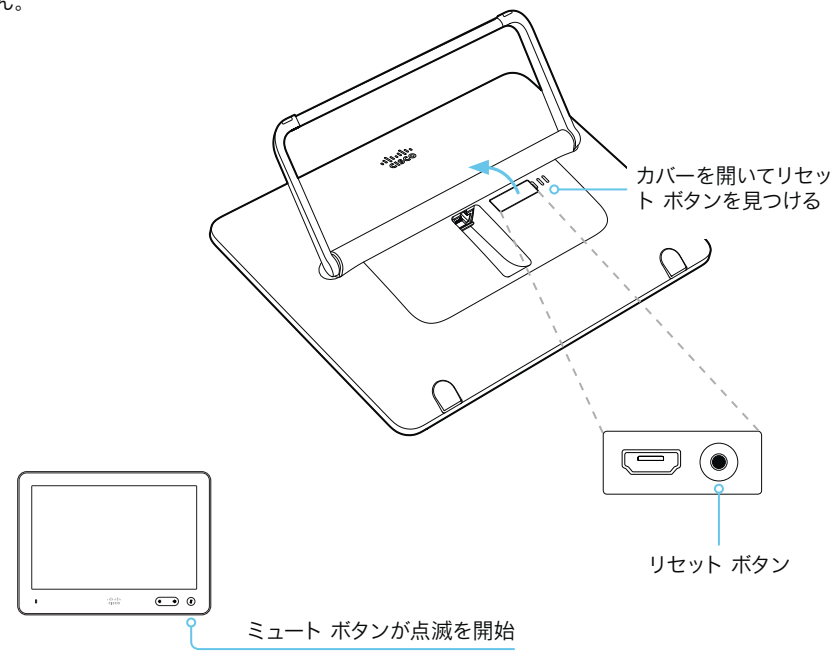
初期設定にリセットすると元に戻すことはできません。

1. 背面の小さなカバーを開き、リセット ボタンを見つけます。
2. 前面のミュート ボタンが点滅し始めるまでリセット ボタンを押し続けます (約 5 秒間)。その後、ボタンを離します。

   Touch 10 が工場出荷時設定へと自動的に戻され、再起動されます。

   Touch 10 がビデオ システムに直接接続されている場合は、新しい設定がビデオ システムから自動的に受信されます。

   Touch 10 が LAN 経由で接続されている場合は、新たにデバイスをビデオ システムにペアリングする必要があります。ペアリングが成功すると、新しい設定がビデオ システムから自動的に受信されます。




## ペアリングについて、およびビデオ システムに Touch 10 を接続する方法について

Touch 10 コントローラを使用するには、Touch 10 をシステムに直接接続するか、LAN 経由でシステムにペアリング (リモート ペアリング) する必要があります。 後者はリモート ペアリングと呼ばれます。

«1»1ペアリング および Touch 10 とビデオ システムの接続方法については、<g id="i1956" >2<g id="i1955" >i1955 ▶「</g>i1955「Touch 10 コントローラの接続」</g>2<g「id="i1957" >3«x1124»x1124</g>3の章を読んでください。

# Cisco TelePresence Touch 10 の初期設定へのリセット

**この章は、最初の Touch 10 コントローラ (Cisco TelePresence Touch 10) に適用されます。** このデバイスには前面のロゴはありません。

2017 年後半に発売された新しいバージョンについては、前のページを参照してください。

エラー状態で、接続を再確立するためにタッチ コントローラを工場出荷時設定にリセットすることが必要になる場合があります。その場合は、必ず Cisco のサポート組織に連絡して実行する必要があります。

タッチ コントローラを工場出荷時設定にリセットすると、ペアリング情報が失われ、(ビデオ システムではなく) タッチ自体が工場出荷時の初期状態に戻されます。

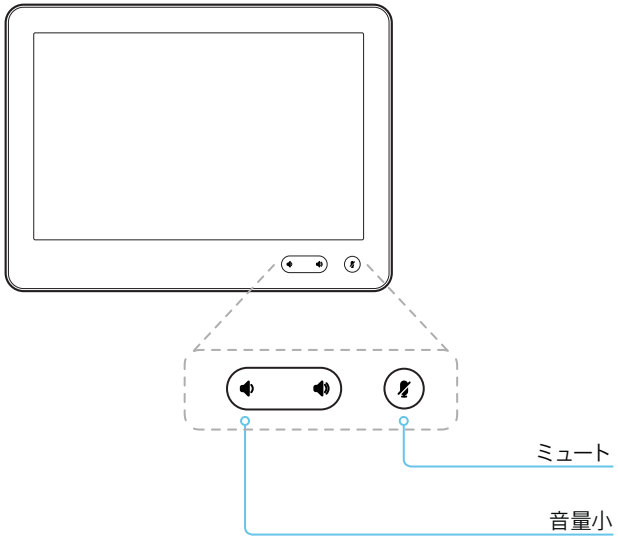
⚠ 初期設定にリセットすると元に戻すことはできません。

1. ミュートおよび音量小ボタンを見つけます。
2. (赤と緑が) 点滅しはじめるまで、ミュート ボタンを押します。約 10 秒かかります。
3. *[音量小 (Volume down) ]* ボタンを 2 回押します。

   Touch 10 が工場出荷時設定へと自動的に戻され、再起動されます。

   Touch 10 がビデオ システムに直接接続されている場合は、新しい設定がビデオ システムから自動的に受信されます。

   Touch 10 が LAN 経由で接続されている場合は、新たにデバイスをビデオ システムにペアリングする必要があります。ペアリングが成功すると、新しい設定がビデオ システムから自動的に受信されます。



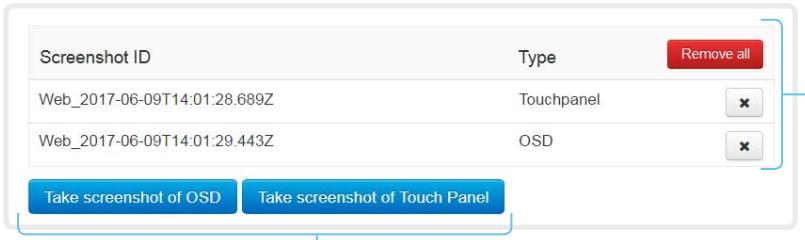

## ペアリングについて、およびビデオ システムに Touch 10 を接続する方法について

Touch 10 コントローラを使用するには、Touch 10 をシステムに直接接続するか、LAN 経由でシステムにペアリング (リモート ペアリング) する必要があります。 後者はリモート ペアリングと呼ばれます。

«1»1ペアリング および Touch 10 とビデオ システムの接続方法については、<g id="i1956" >2<g id="i1955" >i1955 ▶ </g>i1955「Touch 10 コントローラの接続」</g>2<g id="i1957" >3«x1124»x1124</g>3の章を読んでください。

# ユーザ インターイスのスクリーンショットをキャプチャする

ウェブ インターフェイスにサインインして、*[メンテナンス (Maintenance) ] > [ユーザ インターフェイスのスクリーンショット (User Interface Screenshots) ]* に移動します。




## スクリーンショットのキャプチャ

*[タッチ パネルのスクリーンショットを撮る (Take screenshot of Touch Panel) ]* をクリックしてタッチ コントローラのスクリーンショットをキャプチャするか、*[OSD のスクリーンショットを撮る (Take screenshot of OSD) ]* をクリックして画面上の表示のスクリーンショットをキャプチャします。

スクリーンショットはボタンの下のエリアに表示されます。スクリーンショットの準備ができるまで最大 30 秒かかる場合があります。

キャプチャされたすべてのスナップショットはボタンの上のリストに含まれています。イメージを表示するには、スクリーンショット ID をクリックします。

## スクリーンショットを削除する

すべてのスクリーンショットを削除する場合は、*[すべて削除 (Remove all) ]* をクリックします。

1 つのスクリーンショットのみを削除するには、そのスクリーンショットの ✖ ボタンをクリックします。

## ユーザ インタフェースのスクリーンショットについて

ビデオ システムに接続された タッチ コントローラと、画面上の表示 (メイン ディスプレイのメニュー、インジケータ、メッセージ) の両方のスクリーンショットをキャプチャできます。

第 5 章

# システム設定

# システム設定の概要

これ以降のページでは、ウェブ インターフェイス上の [*セットアップ (Setup) ] > [設定 (Configuration) ]* ページで設定されるすべてのシステム設定をリストします。

ウェブ ブラウザを開き、ビデオ システムの IP アドレスを入力して、サインインします。

**IP アドレスの確認方法**

1. ユーザ インターフェイスの左上隅にある連絡先情報を選択します。
2. *[このデバイスについて (About this device) ]*に続き、*[設定 (Settings) ]*を選択します。

# 音声設定

## Audio DefaultVolume

スピーカーのデフォルト音量を定義します。ビデオ システムのスイッチをオンにするか再起動すると、音量がこの値に設定されます。実行中に音量を変更するには、ユーザ インターフェイスのコントロールを使用します。また、API コマンド (xCommand Audio Volume) を使用して、ビデオ システムの稼働中に音量を変更したり、デフォルト値にリセットしたりすることもできます。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: 50

値スペース: 整数 (0..100)

範囲: 1 ～ 100 の値を選択します。これは、-34.5 dB ～ 15 dB の範囲内の 0.5 dB 単位に相当します。0 に設定すると、音声がオフになります。

## Audio Input HDMI [n] Level

n: 1..1

HDMI 入力コネクタのゲインを設定します。ゲインは、1 db ずつ調整できます。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: 0

値スペース: 整数 (-24..0)

範囲: デシベル (dB) 単位でゲインを選択します。

## Audio Input HDMI [n] Mode

n: 1..1

HDMI 入力コネクタの音声を有効にするかどうかを定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: On

値スペース: Off/On

Off: HDMI 入力で音声を無効にします。

On: HDMI 入力で音声を有効にします。

## Audio Input HDMI [n] VideoAssociation MuteOnInactiveVideo

n: 1..1

この設定を使用して、このプレゼンテーション ソースが現在画面上に表示されていない場合、またはプレゼンテーション ソースが接続されている間常に音声を再生する場合音声再生を停止するかどうかを決定します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: On

値スペース: Off/On

Off: 音声は、プレゼンテーション ソースが接続されている間、ローカルおよび相手先に対して常に再生されます。HDMI 入力ソースを指定する必要はありません。

On: 音声は、接続されているプレゼンテーション ソースが画面上に表示されている間、ローカルおよび相手先に対して再生されます。

## Audio KeyClickDetector Attenuate

ビデオ システム (コーデック) は、キーボードのクリック ノイズを検出し、自動的にマイクの信号を減衰することができます。キー入力のノイズが他の参加者の邪魔をする可能性があるため、会議出席者がキーボードで入力を開始するときにはこの機能が便利です。参加者がキーボードで入力しながら話す場合、マイクの信号は減衰しません。オーディオ キー クリック検出 有効設定が On に設定されている必要があります。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: On

値スペース: Off/On

Off: マイクの信号の減衰は無効です。

On: キーボードのクリック ノイズが検出された場合、システムによりマイクの信号が減衰されます。音声または音声とキーボードのクリックが併せて検出された場合、マイクの信号は減衰されません。

## Audio KeyClickDetector Enabled

ビデオ システム (コーデック) は、キーボードのクリック ノイズを検出し、自動的にマイクの信号を減衰することができます。キー入力のノイズが他の参加者の邪魔をする可能性があるため、会議出席者がキーボードで入力を開始するときにはこの機能が便利です。マイクの信号の減衰を有効にするには、[オーディオ減衰キー クリック検出 (Audio KeyClickDetector Attenuate) ] を On にします。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: Off

値スペース: Off/On

Off: キー クリックの検出は無効です。

On: システムによりキーボードからクリック ノイズが検出されます。

## Audio Microphones Mute Enabled

ビデオ システムでのマイク ミュートの動作を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: True

値スペース: True/InCallOnly

True: 音声ミュートが使用可能になります。

InCallOnly: 音声ミュートはデバイスがコール中の場合にだけ使用できます。アイドル状態のときは、マイクロフォンをミュートにできません。これは、外部の電話サービス/音声システムがコーデックで接続され、コーデックがコール中でないときに使用可能にする場合に便利です。InCallOnly に設定されたとき、音声システムが誤ってミュートにされることを防止できます。

## Audio SoundsAndAlerts RingTone

着信コールに使用する着信音を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: Sunrise

値スペース: Sunrise/Mischief/Ripples/Reflections/Vibes/Delight/Evolve/Playful/Ascent/Calculation/Mellow/Ringer

リストから呼び出し音を選択します。

## Audio SoundsAndAlerts RingVolume

着信コールの着信音量を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER

デフォルト値: 50

値スペース: 整数 (0..100)

範囲: 値は 5 刻みで 0 ～ 100 (-34.5 dB ～ 15 dB) になります。音量 0 = オフです。

## Audio Ultrasound Mode

この設定は、インテリジェント プロキシミティ機能に適用されます。設定はデフォルト値のままにしておいてください。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: Dynamic

値スペース: Dynamic/Static

Dynamic: ビデオ システムによって超音波ボリュームを動的に調整します。ボリュームは、[オーディオ ウルトラサウンド最大音量 (Audio Ultrasound MaxVolume) ] の設定で定義された最大レベルまでさまざまに変化します。

Static: Cisco が助言した場合にのみ使用してください。

## Audio Ultrasound MaxVolume

この設定は、インテリジェント プロキシミティ機能に適用されます。超音波のペアリング メッセージの最大音量を設定します。

必要なユーザ ロール: ADMIN、INTEGRATOR

デフォルト値: 60

値スペース: 整数 (0..60)

指定されている範囲内の値を選択します。0 に設定すると、超音波がオフになります。

# CallHistory 設定

## CallHistory Mode

不在着信や応答されなかったコールを含めて、発着信コールに関する情報を保存するかどうかを決定します（通話履歴）。これにより、ユーザ インターフェイスの Recents リストにコールが表示されるかどうかが決まります。

必要なユーザ ロール：ADMIN、INTEGRATOR

デフォルト値：On

値スペース：Off/On

Off：新しいエントリが通話履歴に追加されません。

On：新しいエントリは通話履歴一覧に保存されます。

# カメラ設定

## Cameras SpeakerTrack Mode

デフォルトとして、カメラは 1 秒あたり 30 フレームを出力します。これにより、通常の帯域と照明条件であってもクローズアップと広い視野両方の画像の品質が良くなります。条件がさらに良い場合、カメラから 1 秒あたり 60 フレームの出力となり、全般的に良い品質となる可能性があります。

必要なユーザ ロール : ADMIN

デフォルト値 : 30

値スペース : 30/60

30 : カメラは、1 秒あたり 30 フレームを出力します。

60 : カメラは、1 秒あたり 60 フレームを出力します。

## Cameras PowerLine Frequency

カメラが電源周波数フリッカー防止をサポートしている場合、カメラは電源からのすべてのフリッカノイズを補うことができます。このカメラ設定はお使いの電源周波数に基づいて設定する必要があります。カメラが電源周波数の自動検出をサポートしている場合、設定で Auto オプションを選択できます。

すべての Cisco Precision カメラはフリッカ防止および電源周波数の自動検出の両方をサポートしています。Auto はデフォルト値であるため、自動検出をサポートしないカメラの場合、この設定を変更する必要があります。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値スペース : 50Hz/60Hz/Auto

50Hz : 電線周波数が 50 Hz の場合、この値を使用します。

60Hz : 電線周波数が 60 Hz の場合、この値を使用します。

Auto : カメラが電源周波数を自動検出できるようにします。

## Cameras Camera Framerate

ビデオシステムは最高の概要機能をサポートしています。最高の概要は自動カメラ フレーミングを使用し、室内の人数に基づいて最適なカメラ表示を選択します。スピーカートラッキングはサポートされていません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/Off

自動: ベスト概要がオンになっています。システムは室内の人々を検出し自動的に最適なカメラ フレーミングを選択します。ユーザは、Touch コントローラのカメラのコントロールパネルで、ベスト概要のオン/オフを即座に切り替えることができますが、その機能は、各コールの後に再度オンになり、システムが次のユーザに対応できるようになります。

オフ: ベスト概要がオフになっています。

# 会議設定

## Conference ActiveControl Mode

アクティブ コントロールは、会議参加者がビデオ システムのインターフェイスを使用して Cisco TelePresence Server または Cisco Meeting Server の会議を管理できるようにする機能です。各ユーザは、参加者リストの表示、ビデオ レイアウトの変更、参加者の接続解除などをインターフェイスから行えます。アクティブ コントロール機能は、インフラストラクチャ (Cisco Unified Communications Manager (CUCM) バージョン 9.1.2 以降、Cisco TelePresence Video Communication Server (VCS) バージョン X8.1 以降、Cisco Media Server (CMS) バージョン 2.1 以降) でサポートされている限り、デフォルトでイネーブルです。アクティブ コントロール機能を無効にするには、この設定を変更します。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/Off

Auto : アクティブ コントロールがインフラストラクチャでサポートされている場合に有効になります。

Off : アクティブ コントロールは無効です。

## Conference AutoAnswer Mode

自動応答モードを定義します。コールに応答する前に数秒間待機する場合は Conference AutoAnswer Delay 設定を使用し、コールに応答するときにマイクをミュートする場合は Conference AutoAnswer Mute 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : タッチ コントローラで [応答 (Answer) ] をタップし、着信コールに手動で応答できます。

On : 通話中でない限り、システムが自動的に着信コールに応答します。常に手動で、通話中の着信コールの応答や拒否が行えます。

## Conference AutoAnswer Mute

着信コールに自動応答する場合にマイクをミュートにするかどうかを定義します。[自動応答モード (AutoAnswer Mode) ] が有効にされている必要があります。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : 着信コールはミュートにされません。

On : 着信コールは自動的に応答されるときミュートにされます。

## Conference AutoAnswer Delay

システムによって自動的に応答される前に着信コールがどれくらい待つ必要があるかを定義します (秒単位)。[自動応答モード (AutoAnswer Mode) ] が有効にされている必要があります。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0..50)

自動応答遅延 (秒単位)。

## Conference CallProtocolIPStack

システムで通信プロトコル (SIP、H323) の IPv4、IPv6、またはデュアル IP スタックを有効にする必要がある場合に選択します。

必要なユーザ ロール : ADMIN

デフォルト値 : Dual

値スペース : Dual/IPv4/IPv6

Dual : 通信プロトコルの IPv4 と IPv6 の両方をイネーブルにします。

IPv4 : [IPv4] に設定すると、通信プロトコルは IPv4 を使用します。

IPv6 : [IPv6] に設定すると、通信プロトコルは IPv6 を使用します。

## Conference DefaultCall Protocol

システムからコールを発信するときに使用されるデフォルトの通信プロトコルを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/H320/H323/Sip/Spark

Auto : 使用可能なプロトコルに基づいた通信プロトコルの自動選択を有効にします。複数のプロトコルが使用可能な場合、優先順位は次の通りです : 1) SIP、2) H323、3) H320。システムが登録を実行できない場合、自動選択により H323 が選択されます。

[H320] : すべてのコールが H.320 コールとしてセットアップされます (Cisco TelePresence ISDN リンクとともに使用している場合のみ) 。

H323 : すべてのコールが H.323 コールとして設定されます。

SIP : すべてのコールが SIP コールとして設定されます。

Spark : Webex 登録済みシステムのために予約されています。使用しません。

## Conference DefaultCall Rate

システムからコールを発信するときに使用するデフォルトのコール レートを定義します。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: 6000

値スペース : 整数 (64..6000)

デフォルト コール レート (kbps) です。

## Conference DoNotDisturb DefaultTimeout

この設定はサイレント セッションのデフォルト期間、つまり着信コールが拒否され、不在履歴として登録される時間を決定します。セッションは、ユーザ インターフェイスを使用して早期に終了できます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: 60

値スペース : 整数 (1..1440)

DoNotDisturb (着信拒否) セッションが自動的にタイム アウトするまでの分数 (最大 1440 分、つまり 24 時間) 。

## Conference Encryption Mode

会議の暗号化モードを定義します。会議が開始されると、数秒間画面に鍵と「Encryption On」または「Encryption Off」という文字が表示されます。

注 : 暗号化オプション キーがビデオ システムにインストールされていない場合、暗号化モードは常に Off になります。

必要なユーザ ロール : ADMIN

デフォルト値 : BestEffort

値スペース : Off/On/BestEffort

Off : システムは、暗号化を使用しません。

On : システムは、暗号化されたコールだけを許可します。

BestEffort : システムは暗号化を可能な限り使用します。

> ポイント ツー ポイント コール : 遠端システムで暗号化 (AES-128) がサポートされている場合、コールは暗号化されます。そうでない場合は、コールは暗号化なしで送信されます。

> MultiSite コール : 暗号化されたマルチサイト会議を実現するためには、すべてのサイトが暗号化をサポートしている必要があります。そうでない場合は、会議は暗号化されません。

## Conference FarEndControl Mode

リモート側 (遠端) にこちら側のビデオ ソースの選択とローカル カメラの制御 (パン、傾斜、ズーム) を許可するかどうか決定できます。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : 遠端はこちら側のビデオ ソースの選択やローカル カメラの制御 (パン、傾斜、ズーム) を許可されません。

On : 遠端にこちら側のビデオ ソースの選択とローカル カメラの制御 (パン、傾斜、ズーム) を許可します。カメラの制御とビデオ ソースの選択は、こちら側でも通常どおり可能です。

## Conference FarEndControl SignalCapability

遠端制御 (H.224) 信号機能モードを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : 遠端制御信号機能をディセーブルにします。

On : 遠端制御信号機能をイネーブルにします。

## Conference FarEndMessage Mode

制御システムまたはマクロと併用するための、ポイントツーポイント通話における 2 種のコーデック間のデータ送信の許可状況を切り替えます。SIP コールでのみ動作します。この設定は、遠隔メッセージ送信コマンドの xCommand のコール使用を有効化または無効化します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : 2 つのコーデック間でメッセージ送信を行うことはできません

On : ポイントツーポイント通話で 2 つのコーデック間のメッセージ送信を行うことができます。

## Conference MaxReceiveCallRate

コールの発信または受信時に使用する最大受信ビット レートを定義します。これは個別のコールの最大ビット レートです。すべての同時アクティブ コールに集約した最大レートを設定するには、Conference MaxTotalReceiveCallRate 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値: 6000

値スペース : 整数 (64..6000)

最大受信帯域 (kbps) 。

## Conference MaxTransmitCallRate

コールの発信または受信時に使用する最大送信ビット レートを定義します。これは個別のコールの最大ビット レートです。すべての同時アクティブ コールに集約した最大レートを設定するには、Conference MaxTotalTransmitCallRate 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値: 6000

値スペース : 整数 (64..6000)

最大送信帯域 (kbps) 。

## Conference MaxTotalReceiveCallRate

この設定は、ビデオ システム内蔵の MultiSite 機能 (オプション) を使用してマルチポイントのビデオ会議をホストする場合に適用されます。

受信全体の最大許容ビット レートを定義します。ビット レートは任意の時点におけるすべてのアクティブ コール間で均等に分割されます。これは、誰かがマルチポイント会議に参加または退出するとき、またはコールが保留 (中断) されるか再開されるときに個々のコールが適切に高速化または低速化されることを意味します。

個々のコールの最大受信ビット レートは、Conference MaxReceiveCallRate 設定により定義されます。

必要なユーザ ロール : ADMIN

デフォルト値: 6000

値スペース : 整数 (64..6000)

最大受信帯域 (kbps) 。

## Conference MaxTotalTransmitCallRate

この設定は、ビデオ システム内蔵の MultiSite 機能 (オプション) を使用してマルチポイントのビデオ会議をホストする場合に適用されます。

送信全体の最大許容ビット レートを定義します。ビット レートは任意の時点におけるすべてのアクティブ コール間で均等に分割されます。これは、誰かがマルチポイント会議に参加または退出するとき、またはコールが保留 (中断) されるか再開されるときに個々のコールが適切に高速化または低速化されることを意味します。

個々のコールの最大送信ビット レートは、Conference MaxTransmitCallRate 設定により定義されます。

必要なユーザ ロール : ADMIN

デフォルト値: 6000

値スペース : 整数 (64..6000)

最大送信帯域 (kbps) 。

## Conference MicUnmuteOnDisconnect Mode

すべてのコールが切断されたときに、マイクを自動的にミュート解除するかどうかを定義します。会議室またはその他の共有リソースでは、このようにして次のユーザのためにシステムを準備する場合があります。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : コール中にミュートにされている場合、コールが切断された後もマイクロフォンをミュートにされたままにします。

On : コールが切断された後にマイクロフォンのミュートを解除します。

## Conference Multipoint Mode

ビデオ システムでマルチパーティ ビデオ会議 (アドホック会議) を処理する方法を定義します。

Cisco TelePresence Video Communication Server (VCS) に登録すると、ビデオ システムで組み込み MultiSite 機能を使用できるようになります。Cisco Unified Communications Manager (CUCM) バージョン 8.6.2 以降にすると、ビデオ システムは、CUCM 会議ブリッジ、または内蔵 MultiSite 機能を使用できます。使用するオプションは CUCM によってセットアップされます。

CUCM 会議ブリッジを使用すれば、多くの参加者との会議をセットアップできます。組み込み MultiSite では、最大 4 人の参加者 (自分自身を含む) が許可されます。

組み込みの MultiSite 機能はオプションであり、すべてのビデオ システムで使用できるわけではありません。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/CUCMMediaResourceGroupList/MultiSite/Off

Auto : マルチポイント方式が自動的に選択されます。マルチポイント方式が使用できない場合は、マルチポイント モードがオフに設定されます。

[CUCMMediaResourceGroupList] : マルチパーティ会議は、CUCM で設定された会議ブリッジによってホストされます。この設定は、CUCM 環境で CUCM によってプロビジョニングされるため、ユーザが手動で設定すべきではありません。

[多地点接続 (MultiSite) ] : 組み込み MultiSite 機能を使用してマルチパーティ会議が設定されます。MultiSite 機能を使用できないときに [多地点接続 (MultiSite) ] が選択された場合、[マルチポイント モード (Multipoint Mode) ] は自動的に [オフ (Off) ] に設定されます。

Off : マルチパーティ会議は許可されません。

## Conference MultiStream Mode

ビデオ システムでは、電話会議のマルチ ストリーム ビデオをサポートしています。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/Off

Auto : 電話会議インフラストラクチャがマルチストリーム機能をサポートしている場合は、マルチストリームが使用されます。必要な最低バージョン : CMS 2.2、CUCM 11.5、VCS X8.7。

Off : マルチストリームが無効になります。

## Conference IncomingMultisiteCall Mode

すでにコール中または会議中の場合に着信コールを許可するかどうかを選択します。

必要なユーザ ロール : ADMIN

デフォルト値 : Allow

値スペース : Allow/Deny

Allow : すでに通話している間に、誰かが電話をかけてきた場合、通知されます。着信コールを受け入れるかどうかは任意です。着信コールに応答している間、進行中のコールを保留しておくこともできますし、それらのコールをマージすることもできます（マルチパーティ ビデオ会議をサポートしている必要があります）。

Deny : すでに通話中の場合、着信コールは拒否されます。着信コールについては通知されません。ただし、コール履歴リストの不在履歴として表示されます。

## Conference Presentation OnPlacedOnHold

リモート サイトで保留状態にされた後、プレゼンテーションを共有し続けるかどうかを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : NoAction

設定可能な値 : NoAction/Stop

NoAction : 保留にされてもビデオ システムはプレゼンテーションの共有を停止しません。保留されている間はプレゼンテーションは共有されませんが、コールが再開されると自動的に継続されます。

Stop : リモート サイトで保留状態にされた後、ビデオ システムはプレゼンテーションの共有を停止します。コールが再開されてもプレゼンテーションは継続されません。

## Conference Presentation RelayQuality

この設定は、内蔵 MultiSite 機能（オプション）を使用してマルチポイント ビデオ会議をホストするときに適用されます。リモート ユーザがプレゼンテーションを共有している場合、ビデオ システムは、プレゼンテーションのトランスコーディングを行い、それをマルチポイント会議の他の参加者に送信します。[リレー品質（RelayQuality）] 設定は、プレゼンテーション ソースに対して、高フレームレートと高解像度のどちらを優先するかを指定します。

必要なユーザ ロール : ADMIN

デフォルト値 : Sharpness

値スペース : Motion/Sharpness

Motion : できるだけ高いフレーム レートにします。高いフレーム レートが必要な場合に使用します（通常、画像の動きが激しい場合）。

Sharpness : できるだけ高い解像度にします。詳細なイメージやグラフィックに高い品質が必要な場合に使用されます。

## Conference VideoBandwidth Mode

会議ビデオ帯域幅モードを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Dynamic

値スペース : Dynamic/Static

Dynamic : ビデオ チャネルの使用可能な送信帯域幅が現在アクティブなチャネル間で分散されます。プレゼンテーションが存在しない場合は、メイン ビデオ チャネルがプレゼンテーション チャネルの帯域幅を使用します。

Static : 使用可能な送信帯域幅が、アクティブでない場合でも各ビデオ チャネルに割り当てられます。

# FacilityService 設定

## FacilityService Service [n] Type

n: 1..5

最大 5 種類のファシリティ サービスを同時にサポートできます。この設定で、どのようなサービスかを選択できます。ファシリティ サービスは、FacilityService Service [n] Name と FacilityService Service [n] Number の両方の設定が正しく設定されていないと使用できません。施設サービスは、ユーザ インターフェイスから利用できます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Helpdesk

値スペース : Catering/Concierge/Emergency/Helpdesk/Security/Transportation/Other

Catering : ケータリング サービスには、このオプションを選択します。

Concierge : コンシェルジュ サービスには、このオプションを選択します。

Emergency : 緊急サービスには、このオプションを選択します。

Helpdesk : ヘルプ デスク サービスには、このオプションを選択します。

Security : セキュリティ サービスには、このオプションを選択します。

Transportation : 転送サービスには、このオプションを選択します。

Other : その他のオプションでカバーされないサービスには、このオプションを選択します。

## FacilityService Service [n] Name

n: 1..5

ファシリティ サービスの名前を定義します。最大 5 種類のファシリティ サービスがサポートされます。ファシリティ サービスは、FacilityService Service [n] Name と FacilityService Service [n] Number の両方の設定が正しく設定されていないと使用できません。名前は、上部バーの疑問符アイコンをタップすると表示されるファシリティ サービス コール ボタンに表示されます。施設サービスは、ユーザ インターフェイスから利用できます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Service 1 : "Live Support" その他のサービス : ""

値スペース : 文字列 (0, 1024)

ファシリティ サービスの名前。

## FacilityService Service [n] Number

n: 1..5

ファシリティ サービスの番号 (URI または電話番号) を定義します。最大 5 種類のファシリティ サービスがサポートされます。ファシリティ サービスは、FacilityService Service [n] Name と FacilityService Service [n] Number の両方の設定が正しく設定されていないと使用できません。施設サービスは、ユーザ インターフェイスから利用できます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: ""

値スペース : 文字列 (0, 1024)

ファシリティ サービスの番号 (URI または電話番号) 。

## FacilityService Service [n] CallType

n: 1..5

各ファシリティ サービスのコール タイプを定義します。最大 5 種類のファシリティ サービスがサポートされます。ファシリティ サービスは、FacilityService Service [n] Name と FacilityService Service [n] Number の両方の設定が正しく設定されていないと使用できません。施設サービスは、ユーザ インターフェイスから利用できます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Video

値スペース : Audio/Video

Audio : オーディオ コールには、このオプションを選択します。

Video : ビデオ コールには、このオプションを選択します。

# H323 設定

## H323 Authentication Mode

H.323 プロファイルの認証モードを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : システムは H.323 ゲートキーパーに対して自身の認証を試行せず、通常の登録を試行します。

On : 認証が必要なことを H.323 ゲートキーパーから示されると、システムはゲートキーパーに対して自身の認証を試みます。コーデックとゲートキーパーの両方で、H323 Authentication LoginName と H323 Authentication Password の設定を定義する必要があります。

## H323 Authentication LoginName

システムは認証のために、H.323 ゲートキーパーに H323 認証ログイン名と H323 認証パスワードを送信します。認証はコーデックから H.323 ゲートキーパーへの単方向の認証です。つまり、システムはゲートキーパーに認証されます。認証が不要であることを H.323 ゲートキーパーが示している場合でも、システムは登録を試行します。H.323 認証モードを有効にする必要があります。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 50)

認証ログイン名。

## H323 Authentication Password

システムは認証のために、H.323 ゲートキーパーに H323 認証ログイン名と H323 認証パスワードを送信します。認証はコーデックから H.323 ゲートキーパーへの単方向の認証です。つまり、システムはゲートキーパーに認証されます。認証が不要であることを H.323 ゲートキーパーが示している場合でも、システムは登録を試行します。H.323 認証モードを有効にする必要があります。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 50)

認証パスワード。

## H323 CallSetup Mode

H.323 コールを確立するときにゲートキーパーとダイレクト コールのどちらを使用するかを定義します。

ダイレクト H.323 コールは、H323 CallSetup Mode が Gatekeeper に設定されている場合も発信できます。

必要なユーザ ロール : ADMIN

デフォルト値 : Gatekeeper

値スペース : Direct/Gatekeeper

Direct : IP アドレスに直接ダイヤルすることによってのみ、H.323 コールを発信できます。

[ゲートキーパー (Gatekeeper) ] : システムは、H.323 コールを発信するためにゲートキーパーを使用します。このオプションを選択する場合は、H323 Gatekeeper Address も設定する必要があります。

## H323 Encryption KeySize

Advanced Encryption Standard (AES) 暗号化キーの確立時に使用する Diffie-Hellman キー交換方式の最小または最大のキー サイズを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Min1024bit

設定可能な値 : Max1024bit/Min1024bit/Min2048bit (最大 1024 ビット/最小 1024 ビット/最小 2048 ビット)

Max1024bit : 最大サイズは 1024 ビットです。

Min1024bit : 最小サイズは 1024 ビットです。

Min2048bit : 最小サイズは 2048 ビットです。

## H323 Gatekeeper Address

ゲートキーパーの IP アドレスを定義します。H323 CallSetup Mode を Gatekeeper に設定する必要があります。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

## H323 H323Alias E164

H.323 エイリアス E.164 は、H.323 ゲートキーパーに設定された番号計画に従ってシステムのアドレスを定義します。E.164 エイリアスは電話番号と同じであり、アクセス コードと結合される場合もあります。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 30)

H.323 エイリアス E.164 アドレス。使用できる文字は、0 ～ 9、*、# です。

## H323 H323Alias ID

H.323 ゲートキーパー上のシステムのアドレス指定に使用され、コール リストに表示される H.323 エイリアス ID を定義します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 49)

H.323 エイリアス ID。例 : "firstname.lastname@company.com", "My H.323 Alias ID"

## H323 NAT Mode

ファイアウォール トラバーサル テクノロジーは、ファイアウォール障壁を通過するセキュアなパスを作成し、外部のビデオ会議システムに接続されたときの音声/ビデオ データの正しい交換を可能にします (IP トラフィックが NAT ルータを通過する場合) 。注 : NAT は、ゲートキーパーとの組み合わせでは動作しません。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Auto/Off/On

Auto : H323 NAT アドレスと実際の IP アドレスのどちらをシグナリングに使用するかをシステムが決定します。これにより、LAN 上のエンドポイント、または WAN のエンドポイントにコールを発信できるようになります。H323 NAT アドレスが間違っているか設定されていない場合、実際の IP アドレスが使用されます。

Off : システムは、実際の IP アドレスをシグナリングします。

On : システムは、Q.931 および H.245 内にある実際の IP アドレスの代わりに、設定された H323 NAT アドレスをシグナリングします。NAT サーバ アドレスは、スタートアップ メニューに [My IP Address: 10.0.2.1] と表示されます。H323 NAT アドレスが間違っているか設定されていない場合、H.323 コールは設定できません。

## H323 NAT Address

NAT 対応ルータの外部/グローバル IP アドレスを定義します。ルータに送信されるパケットは、システムにルーティングされます。ゲートキーパーに登録されている場合は NAT を使用できないことに注意してください。

ルータで、次のポートはシステムの IP アドレスにルーティングする必要があります。

* ポート 1720
* ポート 5555-6555
* ポート 2326-2487

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレスまたは IPv6 アドレス。

## H323 PortAllocation

この設定は、H.323 コール シグナリングに使用される H.245 ポート番号に影響を与えます。

必要なユーザ ロール : ADMIN

デフォルト値 : Dynamic

値スペース : Dynamic/Static

Dynamic : TCP 接続を開くとき、使用するポートをシステムが割り当てます。このようにする理由は、後続のコールで同じポートを使用しないようにするためです。一部のファイアウォールはこれを攻撃の徴候と見なします。Dynamic を選択した場合、使用される H.323 ポートは 11000 ～ 20999 です。20999 に達すると 11000 から再スタートされます。ポートは、特定の範囲内でシステムによって自動的に選択されます。ファイアウォール管理者は、どのポートがいつ使用されるかを推定しようとしてはなりません。指示された範囲内の割り当てスキーマがより詳細な通知なしで変更されることがあるからです。

Static : スタティックに設定すると、スタティックに事前定義された範囲 [5555-6555] 内でポート指定されます。

# HttpClient 設定

## HttpClient モード

HTTP(S) リクエストおよび応答を使用する外部 HTTP(S) サーバとのコミュニケーションを許可または禁止します

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

オフ: ビデオシステムは外部 HTTP(S) サーバと通信できません。

オン: ビデオシステムは外部 HTTP(S) サーバと通信が可能です。

## HttpClient AllowHTTP

HttpClient モード設定は外部 HTTP(S) サーバとの通信の許可または拒否に使用されます。モード設定は HTTP と HTTPS を区別しません。HTTP の使用をさらに許可または禁止するには HttpClient AllowHTTP 設定を使用する必要があります。

必要なユーザ ロール : ADMIN

デフォルト値 : True

値スペース : False/True

偽 : ビデオシステムは HTTPS 経由でのみ通信できます。

真: ビデオシステムは HTTPS と HTTP 経由の両方で通信できます。

## HttpClient AllowInsecureHTTPS

まずサーバ証明書を確認することなく、ビデオシステムが HTTPS 経由でサーバと通信することを許可するかどうか選択できます。

ビデオシステムが証明書検証プロセスをスキップできるとしても、自動的にはスキップしません。証明書検証なしでデータをサーバで交換するには AllowInsecureHTTPS パラメータを各 xCommand HttpClient コマンドで具体的に設定する必要があります。

必要なユーザ ロール : ADMIN

デフォルト値 : False

値スペース : False/True

偽 : ビデオシステムは常に HTTPS サーバに証明書があるかチェックします。証明書検証に失敗したら、サーバとの通信は行われません。

真 : ビデオシステムはサーバとの崇信前に証明書検証プロセスをスキップ可能です。

# ロギングの設定

## Logging Debug Wifi

このオプションが有効であると、ビデオシステムはビデオシステムとアクセス ポイントとの間の Wi-Fi 接続のセットアップやメンテナンスについての詳細な情報を記録します。これは、Wi-Fi接続の問題のトラブルシューティングに役立ちます。Wi-Fi 接続が期待通りに動作している場合は、この設定をオフにすることを推奨します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

オフ : 基本 Wi-Fi 情報だけをロギング。

オン : Wi-Fi 接続についての大量の情報をロギング。

## Logging External Mode

システムログをリモート syslog サーバに保管するかどうかを決定。ロギングモード設定がオフに設定されている場合、この設定には効果がありません。

リモートサーバのアドレスをロギング外部サーバ アドレス設定に入力する必要があります。ロギング外部サーバ ポートセットに記載されていない限り、標準規格 syslog ポートが使用されます。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

オフ : システムログはリモート syslog サーバに保存されません。

オン : システムログはリモート syslog サーバに保存されます。

## Logging External Protocol

リモート ロギング サーバに対して使用するプロトコルを決定します。syslog プロトコル over TLS (Transport Layer Security) 、またはプレーンテキストの syslog プロトコルのいずれかを使用できます。syslog プロトコルの詳細については、RFC 5424 を参照してください。

必要なユーザ ロール : ADMIN

デフォルト値 : SyslogTLS

値スペース : Syslog/SyslogTLS

Syslog : プレーン テキストの syslog プロトコル。

SyslogTLS : syslog プロトコル over TLS。

## Logging External Server Address

リモート syslog サーバの IP アドレス。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

## Logging External Server Port

リモート syslog サーバがメッセージをリッスンするポート。0 に設定されている場合、ビデオ システムで標準の syslog ポートが使用されます。syslog の標準 syslog ポートは 514 で、TLS を使用した syslog の標準 syslog ポートは 6514 です。

必要なユーザ ロール : ADMIN

デフォルト値: 514

値スペース : 整数 (0..65535)

リモート syslog サーバが使用しているポート番号。0 は、ビデオ システムが標準 syslog ポートを使用することを意味します。

## Logging Internal Mode

システムログをビデオシステム（ローカルファイル）に保存するかどうかを決定します。これらは、ログバンドルをビデオシステムからダウンロードした際に得られるファイルです。ロギングモード設定がオフに設定されている場合、この設定には効果がありません。

必要なユーザ ロール：ADMIN

デフォルト値：On

値スペース：Off/On

オフ：システムログはビデオシステムに保存されません。

オン：システムログはビデオシステムに保存されます。

## Logging Mode

ビデオ システムのロギング モードを定義します（syslog サービス）。無効にすると、syslog サービスが起動せず、システムログと監査ログの大部分が生成されません。履歴ログと通話履歴は影響を受けません。

必要なユーザ ロール：ADMIN

デフォルト値：On

値スペース：Off/On

Off：システムのロギング サービスを無効にします。

On：システムのロギング サービスを有効にします。

# マクロ設定

## Macros Mode

マクロを使用して、ビデオ エンドポイントの一部を自動化できる JavaScript コードの一部を記述することができます。このようにしてカスタム動作を作成します。デフォルトではマクロを使用できませんが、初めてマクロ エディタを開くと、コーデックでマクロの使用を有効化するかどうかを尋ねられます。コーデックでのマクロの使用を手動で有効化するか完全に無効化する場合、この設定を使用します。マクロの使用は、マクロ エディター内で無効化できます。ただし、コーデックがマクロをリセットするたびにマクロが自動的に再度有効化されるため、マクロの実行は常時無効にはなりません。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : このビデオ システム上でのマクロの使用を完全に無効にします。

On : このビデオ システム上でのマクロの使用を有効にします。

## Macros AutoStart

すべてのマクロは、マクロ ランタイムに呼び出され、ビデオ エンドポイントにおいてシングル プロセスで実行します。ランタイムは、デフォルトでは実行されているはずですが、手動での停止や開始を選択できます。自動開始が有効化されている場合、ビデオ システムを再起動するときにランタイムは自動的に再度開始します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : ビデオ システムの再起動後、マクロ ランタイムは自動的に開始しません。

On : ビデオ システムの再起動後、マクロ ランタイムが自動的に開始します。

# ネットワーク設定

## Network [n] DNS DNSSEC Mode

n: 1..1

ドメイン ネーム システム セキュリティ拡張 (DNSSEC) は、DNS の拡張セットです。署名されたゾーンの DNS の応答を認証するために使用されます。署名されていないゾーンを引き続き許可します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : ドメイン ネーム システム セキュリティ拡張を無効にします。

On : ドメイン ネーム システム セキュリティ拡張を有効にします。

## Network [n] DNS Domain Name

n: 1..1

DNS ドメイン名は非修飾名に追加されるデフォルトのドメイン名サフィックスです。

例 : DNS ドメイン名が「company.com」で、ルックアップする名前が「MyVideoSystem」の場合、DNS ルックアップ「MyVideoSystem.company.com」になります。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

DNS ドメイン名。

## Network [n] DNS Server [m] Address

n: 1..1

m: 1..3

DNS サーバのネットワーク アドレスを定義します。最大 3 つまでのアドレスを指定できます。ネットワーク アドレスが不明の場合、管理者またはインターネット サービス プロバイダーに問い合わせます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレスまたは IPv6 アドレス。

## Network [n] IEEE8021X Mode

n: 1..1

システムは、イーサネット ネットワークに認証済みネットワーク アクセスを提供するために使用される、ポート ベースのネットワーク アクセス コントロールによって、IEEE 802.1X LAN ネットワークに接続できます。

必要なユーザ ロール : admin、user

デフォルト値 : Off

値スペース : Off/On

Off : 802.1X 認証が無効になります。

On : 802.1X 認証がイネーブルになります。

## Network [n] IEEE8021X TlsVerify

n: 1..1

TLS を使用する場合の、ローカル CA リストの証明書に対する IEEE802.1x 接続のサーバ側証明書の検証です。CA リストはビデオ システムにアップロードする必要があります。これは、ウェブ インターフェイスから実行できます。

この設定は、Network [1] IEEE8021X Eap Tls が有効 (On) の場合にのみ有効です。

必要なユーザ ロール : admin、user

デフォルト値 : Off

値スペース : Off/On

Off : Off に設定する場合、ローカル CA リストに対するサーバ側 X.509 証明書を確認せずに、TLS 接続が許可されます。これは、コーデックに CA リストがアップロードされていない場合、選択する必要があります。

On : On に設定する場合、すべての TLS 接続のローカル CA リストに対して、サーバ側 X.509 証明書が検証されます。有効な証明書を持つサーバだけが許可されます。

## Network [n] IEEE8021X UseClientCertificate

n: 1..1

IEEE802.1x 接続中の、秘密キーと証明書のペアを使用した認証。認証 X.509 証明書は、ビデオ システムにアップロードされている必要があります。これは、ウェブ インターフェイスから実行できます。

必要なユーザ ロール : admin、user

デフォルト値 : Off

値スペース : Off/On

Off : Off に設定した場合、クライアント側の証明書は使用されません (サーバ側のみ) 。

On : On に設定した場合、クライアント (ビデオ システム) はサーバと相互認証 TLS ハンドシェイクを実行します。

## Network [n] IEEE8021X Identity

n: 1..1

802.1X 認証用のユーザ名を定義します。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

802.1 X 認証用のユーザ名。

## Network [n] IEEE8021X Password

n: 1..1

802.1X 認証用のパスワードを定義します。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 50)

802.1X 認証用のパスワード。

## Network [n] IEEE8021X AnonymousIdentity

n: 1..1

802.1X 匿名 ID 文字列は、別のトンネリングされた ID をサポートする EAP-PEAP および EAP-TTLS などの EAP (Extensible Authentication Protocol) タイプとともに、非暗号化 ID として使用されます。設定された場合、匿名 ID は最初の (非暗号化) EAP ID 要求に使用されます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

802.1X 匿名 ID 文字列。

## Network [n] IEEE8021X Eap Md5

n: 1..1

MD5 (メッセージダイジェスト アルゴリズム 5) モードを定義します。これは、共有秘密に依存するチャレンジ ハンドシェイク認証プロトコルです。MD5 は弱いセキュリティです。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : EAP-MD5 プロトコルはディセーブルになります。

On : EAP-MD5 プロトコルが有効になります。

## Network [n] IEEE8021X Eap Ttls

n: 1..1

TTLS (トンネル方式トランスポート層セキュリティ) モードを定義します。クライアント証明書の要件なしで LAN クライアントを認証します。Funk Software および Certicom によって開発されました。通常 Agere Systems、Proxim および Avaya でサポートされます。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : EAP-TTLS プロトコルはディセーブルになります。

On : EAP-TTLS プロトコルが有効になります。

## Network [n] IEEE8021X Eap Tls

n: 1..1

IEEE802.1x 接続用の EAP-TLS (トランスポート層セキュリティ) の使用をイネーブルまたはディセーブルにします。RFC5216 で定義された EAP-TLS プロトコルは最もセキュアな EAP 標準の 1 つと見なされています。LAN クライアントは、クライアント証明書を使用して認証されます。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : EAP-TLS プロトコルはディセーブルになります。

On : EAP-TLS プロトコルが有効になります。

## Network [n] IEEE8021X Eap Peap

n: 1..1

PEAP (Protected Extensible Authentication Protocol) モードを定義します。クライアント証明書の要件なしで LAN クライアントを認証します。Microsoft、Cisco と RSA Security により開発されました。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : EAP-PEAP プロトコルはディセーブルになります。

On : EAP-PEAP プロトコルが有効になります。

## Network [n] IPStack

n: 1..1

システムのネットワーク インターフェイスで IPv4、IPv6、またはデュアル IP スタックを使用する必要がある場合に選択します。注 : この設定を変更した後、反映されるまでに 30 秒間待つ必要があります。

必要なユーザ ロール : admin、user

デフォルト値 : Dual

値スペース : Dual/IPv4/IPv6

Dual : [デュアル (Dual) ] に設定すると、ネットワーク インターフェイスは両方の IP バージョンで同時に動作することができ、また、IPv4 アドレスと IPv6 アドレスの両方を同時に持つことができます。

IPv4 : [IPv4] に設定すると、システムのネットワーク インターフェイスで IPv4 が使用されます。

IPv6 : [IPv6] に設定すると、システムのネットワーク インターフェイスで IPv6 が使用されます。

## Network [n] IPv4 Assignment

n: 1..1

システムが IPv4 アドレス、サブネット マスク、およびゲートウェイ アドレスを取得する方法を定義します。

アドレス割り当てに DHCP を利用する場合は、MAC アドレスによって最後に付加される「01」が、DHCP リクエストでのクライアント識別子として使用されます。

必要なユーザ ロール : admin、user

デフォルト値 : DHCP

値スペース : Static/DHCP

Static : アドレスは、Network IPv4 Address、Network IPv4 Gateway、Network IPv4 SubnetMask の各設定 (静的アドレス) を使用して手動で設定する必要があります。

DHCP : システム アドレスは DHCP サーバによって自動的に割り当てられます。

## Network [n] IPv4 Address

n: 1..1

システムのスタティック IPv4 ネットワーク アドレスを定義します。Network IPv4 Assignment が Static に設定されている場合にのみ適用できます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス。

## Network [n] IPv4 Gateway

n: 1..1

IPv4 ネットワーク ゲートウェイ アドレスを定義します。Network IPv4 Assignment が Static に設定されている場合にのみ適用できます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス。

## Network [n] IPv4 SubnetMask

n: 1..1

IPv4 ネットワークのサブネット マスクを定義します。Network IPv4 Assignment が Static に設定されている場合にのみ適用できます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス。

## Network [n] IPv6 Assignment

n: 1..1

システムが IPv6 アドレスおよびデフォルト ゲートウェイ アドレスを取得する方法を定義します。

アドレス割り当てに DHCPv6 を利用する場合は、MAC アドレスによって最後に付加される「01」が、DHCP リクエストでのクライアント識別子として使用されます。

必要なユーザ ロール : admin、user

デフォルト値 : Autoconf

値スペース : Static/DHCPv6/Autoconf

Static : コーデックおよびゲートウェイの IP アドレスは、Network IPv6 Address および Network IPv6 Gateway の各設定を使用して手動で設定する必要があります。NTP アドレスや DNS サーバ アドレスなどのオプションは、手動で設定するか、または DHCPv6 サーバから取得する必要があります。Network IPv6 DHCPOption 設定は、どの方法を使用するかを決定します。

DHCPv6 : オプションを含むすべての IPv6 アドレスは、DHCPv6 サーバから取得されます。詳細については RFC3315 を参照してください。Network IPv6 DHCPOption 設定は無視されます。

Autoconf : IPv6 ネットワーク インターフェイスの IPv6 ステートレス自動設定をイネーブルにします。詳細については RFC4862 を参照してください。NTP アドレスや DNS サーバ アドレスなどのオプションは、手動で設定するか、または DHCPv6 サーバから取得する必要があります。Network IPv6 DHCPOption 設定は、どの方法を使用するかを決定します。

## Network [n] IPv6 Address

n: 1..1

システムのスタティック IPv6 ネットワーク アドレスを定義します。Network IPv6 Assignment が Static に設定されている場合にのみ適用できます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

ネットワーク マスクを含む有効な IPv6 アドレス。例 : 2001:DB8::/48

## Network [n] IPv6 Gateway

n: 1..1

IPv6 ネットワーク ゲートウェイ アドレスを定義します。この設定は、Network IPv6 Assignment が Static に設定されている場合にのみ適用されます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv6 アドレス。

## Network [n] IPv6 DHCPOptions

n: 1..1

DHCPv6 サーバから一連の DHCP オプション (NTP および DNS サーバ アドレスなど) を取得します。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : DHCPv6 サーバからの DHCP オプションの取得を無効にします。

On : 選択した DHCP オプションのセットの DHCPv6 サーバからの取得をイネーブルにします。

## Network [n] MTU

n: 1..1

イーサネット MTU (最大伝送ユニット) サイズを定義します。MTU サイズは、ネットワーク インフラストラクチャでサポートする必要があります。最小サイズは、IPv4 の場合は 576、IPv6 の場合は 1280 です。

必要なユーザ ロール : admin、user

デフォルト値: 1500

値スペース : 整数 (576..1500)

MTU の値を設定します (バイト単位) 。

## Network [n] QoS Mode

n: 1..1

QoS (Quality of Service) は、ネットワーク内のオーディオ、ビデオおよびデータの優先順位を操作するメソッドです。QoS 設定はインフラストラクチャでサポートされている必要があります。DiffServ (ディファレンシエーテッド サービス) は、ネットワーク トラフィックの分類と管理を行い、現代的 IP ネットワークに QoS を提供するためにシンプルかつスケーラブルで粗粒度のメカニズムを指定する、コンピュータ ネットワーキング アーキテクチャです。

必要なユーザ ロール : admin、user

デフォルト値 : Diffserv

値スペース : Off/Diffserv

Off : QoS メソッドは使用されません。

Diffserv : QoS モードを Diffserv に設定すると、Network QoS Diffserv Audio、Network QoS Diffserv Video、Network QoS Diffserv Data、Network QoS Diffserv Signalling、Network QoS Diffserv ICMPv6、および Network QoS Diffserv NTP の各設定を使用してパケットの優先順位が付けられます。

## Network [n] QoS Diffserv Audio

n: 1..1

この設定は、[ネットワーク QoS モード (Network QoS Mode) ] が [Diffserv] に設定されている場合にのみ有効になります。

IP ネットワーク内で音声パケットに持たせる優先順位を定義します。

パケットのプライオリティは、0 ～ 63 です。数字が大きいほど、優先順位が高くなります。音声に推奨されるクラスは、10 進数値 32 と等しい CS4 です。これを確認するには、ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は、パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin、user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでの音声パケットの優先順位を設定します。数値が大きいほど、優先順位が高くなります。0 は「ベスト エフォート」を意味します。

## Network [n] QoS Diffserv Video

n: 1..1

この設定は、[ネットワーク QoS モード (Network QoS Mode) ] が [Diffserv] に設定されている場合にのみ有効になります。

IP ネットワーク内でビデオ パケットに持たせる優先順位を定義します。プレゼンテーション チャネル (共有コンテンツ) 上のパケットも、ビデオ パケットのカテゴリに属します。パケットのプライオリティは、0 ～ 63 です。数字が大きいほど、優先順位が高くなります。ビデオに推奨されるクラスは、10 進数値 32 と等しい CS4 です。これを確認するには、ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は、パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin、user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでのビデオ パケットの優先順位を設定します。数値が大きいほど、優先順位が高くなります。0 は「ベスト エフォート」を意味します。

## Network [n] QoS Diffserv Data

n: 1..1

この設定は、[ネットワーク QoS モード (Network QoS Mode) ] が [Diffserv] に設定されている場合にのみ有効になります。

IP ネットワーク内でデータ パケットに持たせる優先順位を定義します。

パケットのプライオリティは、0 ～ 63 です。数字が大きいほど、優先順位が高くなります。データに対する推奨値は 0 (ベスト エフォート) です。これを確認するには、ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は、パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin、user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでのデータ パケットの優先順位を設定します。数値が大きいほど、優先順位が高くなります。0 は「ベスト エフォート」を意味します。

## Network [n] QoS Diffserv Signalling

n: 1..1

この設定は、[ネットワーク QoS モード (Network QoS Mode) ] が [Diffserv] に設定されている場合にのみ有効になります。

IP ネットワーク内でリアルタイム処理に不可欠 (時間依存) であると考えられるシグナリング パケットに持たせる優先順位を定義します。

パケットのプライオリティは、0 ～ 63 です。数字が大きいほど、優先順位が高くなります。シグナリングに推奨されるクラスは、10 進数値 24 と等しい CS3 です。これを確認するには、ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は、パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin、user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでの信号パケットの優先順位を設定します。数値が大きいほど、優先順位が高くなります。0 は「ベスト エフォート」を意味します。

## Network [n] QoS Diffserv ICMPv6

n: 1..1

この設定は、[ネットワーク QoS モード (Network QoS Mode) ] が [Diffserv] に設定されている場合にのみ有効になります。

IP ネットワーク内で ICMPv6 パケットに持たせる優先順位を定義します。

パケットのプライオリティは、0 ～ 63 です。数字が大きいほど、優先順位が高くなります。ICMPv6 に対する推奨値は 0 (ベスト エフォート) です。これを確認するには、ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は、パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin、user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでの ICMPv6 パケットの優先順位を設定します。数値が大きいほど、優先順位が高くなります。0 は「ベスト エフォート」を意味します。

## Network [n] QoS Diffserv NTP

n: 1..1

この設定は、[ネットワーク QoS モード (Network QoS Mode) ] が [Diffserv] に設定されている場合にのみ有効になります。

IP ネットワーク内で NTP パケットに持たせる優先順位を定義します。

パケットのプライオリティは、0 ～ 63 です。数字が大きいほど、優先順位が高くなります。NTP に対する推奨値は 0 (ベスト エフォート) です。これを確認するには、ネットワーク管理者に問い合わせてください。

ここで設定された優先順位は、パケットがローカル ネットワークの管理者によって制御されるネットワークを出るときに上書きされる可能性があります。

必要なユーザ ロール : admin、user

デフォルト値: 0

値スペース : 整数 (0..63)

IP ネットワークでの NTP パケットの優先順位を設定します。数値が大きいほど、優先順位が高くなります。0 は「ベスト エフォート」を意味します。

## Network [n] RemoteAccess Allow

n: 1..1

リモート アクセスで SSH/HTTP/HTTPS からコーデックに許可する IP アドレス (IPv4/IPv6) を定義します。複数の IP アドレスはスペースで区切られます。

ネットワーク マスク (IP 範囲) は <ip address>/N で指定されます。ここで N は IPv4 では 1 ～ 32 の範囲および IPv6 では 1 ～ 128 の範囲を表します。/N は最初の N ビットがセットされたネットワーク マスクの共通インジケータです。たとえば 192.168.0.0/24 は、192.168.0 で開始するどのアドレスとも一致します。これらはアドレスの最初の 24 ビットだからです。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0..255)

有効な IPv4 アドレスまたは IPv6 アドレス。

## Network [n] Speed

n: 1..1

イーサネット リンクの速度を定義します。デフォルト値では、ネットワークとネゴシエートして自動的に速度が設定されます。このため、デフォルト値は変更しないことをお勧めします。自動ネゴシエーションを使用しない場合、選択した速度を、ネットワーク インフラストラクチャの最も近いスイッチがサポートしているか確認してください。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/10half/10full/100half/100full/1000full

Auto : リンク速度を自動でネゴシエートします。

10half : 10 Mbps 半二重に強制リンクします。

10full : 10 Mbps 全二重に強制リンクします。

100half : 100 Mbps 半二重に強制リンクします。

100full : 100 Mbps 全二重に強制リンクします。

1000full : 1 Gbps 全二重に強制リンクします。

## Network [n] TrafficControl Mode

n: 1..1

ネットワーク トラフィック制御モードを定義して、ビデオ パケットの伝送速度の制御方法を決定します。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : ビデオ パケットをリンク速度で送信します。

On : ビデオ パケットを最大 20 Mbps で送信します。発信ネットワーク トラフィックのバーストを平滑化するために使用できます。

## Network [n] VLAN Voice Mode

n: 1..1

VLAN 音声モードを定義します。Cisco UCM (Cisco Unified Communications Manager) をプロビジョニング インフラストラクチャとして使用している場合、VLAN Voice Mode が Auto に自動的に設定されます。NetworkServices CDP Mode 設定が Off になっている場合は、Auto モードは機能しないことに注意してください。

必要なユーザ ロール : admin、user

デフォルト値 : Auto

値スペース : Auto/Manual/Off

Auto : Cisco Discovery Protocol (CDP) が使用可能な場合は、音声 VLAN に ID を割り当てます。CDP を使用できない場合、VLAN はイネーブルになりません。

Manual : VLAN ID は、Network VLAN Voice VlanId の設定を使用して手動で設定されます。CDP を使用できる場合、手動設定値は、CDP によって割り当てられた値によって却下されます。

Off : VLAN はイネーブルになりません。

## Network [n] VLAN Voice VlanId

n: 1..1

VLAN 音声 ID を定義します。この設定は、ネットワーク VLAN 音声モード が Manual に設定されている場合にだけ有効になります。

必要なユーザ ロール : admin、user

デフォルト値: 1

値スペース : 整数 (1..4094)

VLAN 音声 ID を設定します。

# ネットワークサービス設定

## NetworkServices CDP Mode

CDP (Cisco Discovery Protocol) デーモンをイネーブルまたはディセーブルにします。CDP を有効にすると、エンドポイントは特定の統計情報とデバイス ID を CDP 対応スイッチにレポートします。CDP をディセーブルにする場合、[ネットワーク音声 VLAN モード (Network VLAN Voice Mode) ] : [自動 (Auto) ] 設定は機能しません。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : CDP デーモンは無効です。

On : CDP デーモンは有効です。

## NetworkServices H323 Mode

システムで H.323 コールの発信および受信を可能にするかどうかを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : H.323 コールの発信と受信の可能性をディセーブルにします。

On : H.323 コールの発信と受信の可能性を有効にします。

## NetworkServices HTTP Mode

HTTP または HTTPS (セキュア HTTP) プロトコルによるビデオ システムへのアクセスを許可するか否かを指定します。ビデオ システムの ウェブ インターフェイスは HTTP または HTTPS を使用することに注意してください。この設定を Off にすると、ウェブ インターフェイスを使用できなくなります。

セキュリティの強化 (ウェブ サーバから返されるページと要求の暗号化/暗号化解除) が必要な場合、HTTPS のみを許可します。

注 : 以前のソフトウェア バージョンから CE9.4 (以降) にアップグレードされ、アップグレード後に工場出荷時の設定にリセットされていない状態で提供されるビデオシステムについて、デフォルト値は HTTP + HTTPS となります。

必要なユーザ ロール : ADMIN

デフォルト値 : HTTPS (CE9.4 では HTTP +]HTTPS から HTTPS に変更)

値スペース : Off/HTTP+HTTPS/HTTPS

Off : HTTP や HTTPS によるビデオ システムへのアクセスを禁止します。

HTTP+HTTPS : HTTP と HTTPS の両方によるビデオ システムへのアクセスを許可します。

HTTPS : HTTPS によるビデオ システムへのアクセスを許可し、HTTP によるアクセスを禁止します。

## NetworkServices HTTP Proxy LoginName

これは、HTTP プロキシへの認証に使用されるクレデンシャルのユーザ名部分です。[ネットワーク サービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode) ] が手動に設定されている必要があります。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 80)

認証ログイン名。

## NetworkServices HTTP Proxy Password

これは、HTTP プロキシへの認証に使用されるクレデンシャルのパスワード部分です。[ネットワーク サービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode) ] が手動に設定されている必要があります。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

認証パスワード。

## NetworkServices HTTP Proxy Mode

Cisco Webex の HTTP プロキシを手動でセットアップすることができます。自動設定 (PACUrl) 、完全自動 (WPAD) 、またはオフにしておくことができます。

必要なユーザ ロール : admin、user

デフォルト値 : Off

値スペース : Manual/Off/PACUrl/WPAD

Manual : ネットワーク サービス HTTP プロキシ URL 設定にプロキシ サーバのアドレスを入力します。必要に応じて、ネットワーク サービス HTTP プロキシ ログイン名/パスワード設定に HTTP プロキシのログイン名とパスワードを追加します。

Off : HTTP プロキシ モードがオフになっています。

PACUrl : HTTP プロキシは自動構成です。ネットワーク サービス HTTP プロキシ PACUrl 設定で PAC (プロキシ自動設定) スクリプトの URL を入力する必要があります。

WPAD : WPAD (Web プロキシ自動検出) を使用して、HTTP のプロキシは完全に自動化されかつ自動構成されます。

## NetworkServices HTTP Proxy Url

HTTP プロキシ サーバの URL を設定します。[ネットワーク サービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode) ] が手動に設定されている必要があります。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0..255)

HTTP プロキシ サーバの URL。

## NetworkServices HTTP Proxy PACUrl

PAC (プロキシ自動構成) スクリプトの URL を設定します。[ネットワーク サービス HTTP プロキシ モード (NetworkServices HTTP Proxy Mode) ] が PACUrl に設定されている必要があります。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0..255)

PAC (プロキシ自動構成) スクリプトの URL。

## NetworkServices HTTPS OCSP Mode

OCSP (Online Certificate Status Protocol) レスポンダ サービスのサポートを定義します。OCSP 機能により、証明書失効リスト (CRL) の代わりに OCSP を有効にして、証明書のステータスをチェックできます。

すべての発信 HTTPS 接続に対して、OCSP レスポンダを介してステータスが照会されます。対応する証明書が失効している場合、HTTPS 接続は使用されません。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : OCSP サポートをディセーブルにします。

On : OCSP サポートをイネーブルにします。

## NetworkServices HTTPS OCSP URL

証明書のステータスを調べるために使用される OCSP レスポンダ (サーバ) の URL を定義します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

有効な URL。

## NetworkServices HTTPS Server MinimumTLSVersion

許可する最低バージョンの TLS (Transport Layer Security) プロトコルを設定します。

必要なユーザ ロール : ADMIN

デフォルト値 : TLSv1.1

値スペース : TLSv1.1/TLSv1.2

TLSv1.1 : TLS バージョン 1.1 以降のサポート

TLSv1.2 : TLS バージョン 1.2 以降のサポート

## NetworkServices HTTPS StrictTransportSecurity

HTTP Strict Transport Security ヘッダーにより、ウェブ サイトからブラウザに対して、サイトを HTTP を使用してロードすることを避け、サイトへの HTTP を使用したアクセスはすべて HTTPS リクエストに自動変換する必要があることを通知します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : HTTP Strict Transport Security 機能が無効になります。

On : HTTP Strict Transport Security 機能が有効になります。

## NetworkServices HTTPS VerifyServerCertificate

ビデオ システムが外部 HTTPS サーバ (電話帳サーバや外部マネージャなど) に接続すると、このサーバはビデオ システムに対して自身を識別する証明書を示します。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : サーバ証明書を確認しません。

On : サーバ証明書が信頼できる認証局 (CA) によって署名されていることを確認するようシステムに要求します。これには、信頼できる CA のリストがシステムに事前にアップロードされている必要があります。

## NetworkServices HTTPS VerifyClientCertificate

ビデオ システムが HTTPS クライアント (ウェブ ブラウザなど) に接続すると、クライアントは自分自身を識別するためにビデオ システムに証明書を提示するように要求されることがあります。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : クライアント証明書を確認しません。

On : 信頼できる認証局 (CA) によって署名された証明書を提示するようクライアントに要求します。これには、信頼できる CA のリストがシステムに事前にアップロードされている必要があります。

## NetworkServices NTP Mode

ネットワーク タイム プロトコル (NTP) は、リファレンス タイム サーバにシステムの時刻と日付を同期するために使用されます。時間の更新のために、タイム サーバに定期的に照会します。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/Manual/Off

Auto : システムは時間を参照するために NTP サーバを使用します。デフォルトでは、サーバのアドレスはネットワークの DHCP サーバから取得されます。DHCP サーバを使用しない場合や、DHCP サーバが NTP サーバのアドレスを提供しない場合は、NetworkServices NTP Server [n] Address 設定で指定された NTP サーバ アドレスが使用されます。

Manual : システムは、NetworkServices NTP Server [n] Address 設定で指定された NTP サーバを使って時間を参照します。

Off : システムは NTP サーバを使用しません。NetworkServices NTP Server [n] Address 設定は無視されます。

## NetworkServices NTP Server [n] Address

n: 1..3

NetworkServices NTP Mode が Manual に設定された場合、および NetworkServices NTP Mode が Auto に設定されアドレスが DHCP サーバから提供されない場合に使用される NTP サーバのアドレスです。

必要なユーザ ロール : ADMIN

デフォルト値 : "0.tandberg.pool.ntp.org"

値スペース : 文字列 (0, 255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

## NetworkServices NTP Server [n] Key

n: 1..3

NTP 情報がゼロトラスト 送信元から来ていることを確かめるために、ビデオシステムは NTP 送信元が仕様する ID/キーペアリングを把握する必要があります。キーおよび ID それぞれの設定には、NetworkServices NTP サーバ [n] キーおよび NetworkServices NTP サーバ [n] KeyId 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 2045)

NTP ソースが使用する ID/キーペアの一部であるキー。

## NetworkServices NTP Server [n] KeyId

n: 1..3

NTP 情報がゼロトラスト 送信元から来ていることを確かめるために、ビデオシステムは NTP 送信元が仕様する ID/キーペアリングを把握する必要があります。キーおよび ID それぞれの設定には、NetworkServices NTP サーバ [n] キーおよび NetworkServices NTP サーバ [n] KeyId 設定を使用します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 10)

NTP ソースが使用する ID/キーペアの一部である ID。

## NetworkServices NTP Server [n] KeyAlgorithn

n: 1..3

NTP サーバが使用し、ビデオシステムが時間メッセージを認証するために使用する必要がある、認証ハッシュ機能を選択します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース: None/SHA1/SHA256

なし : NTPサーバはハッシュ機能を使用しません。

SHA1: NTPサーバは SHA-1 ハッシュ機能を使用します。

SHA256: NTP サーバは SHA-256 ハッシュ機能を使用します (ハッシュ機能の SHA-2 群から) 。

## NetworkServices SIP Mode

システムで SIP コールの発信および受信を可能にするかどうかを定義します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : SIP コールの発信と受信の可能性をディセーブルにします。

On : SIP コールの発信と受信の可能性を有効にします。

## NetworkServices SNMP Mode

ネットワーク管理システムでは、管理上の対応を補償する条件についてネットワーク接続デバイス（ルータ、サーバ、スイッチ、プロジェクタなど）をモニタするために SNMP（簡易ネットワーク管理プロトコル）が使用されます。保証の管理上の注意使用されます。SNMP は、システム コンフィギュレーションを説明する管理対象システム変数の形式で管理データを公開します。これらの変数は、その後照会でき（Readonly に設定）、管理アプリケーションによって設定できる場合もあります（ReadWrite に設定）。

必要なユーザ ロール：ADMIN、INTEGRATOR

デフォルト値：ReadOnly

値スペース：Off/ReadOnly/ReadWrite

Off：SNMP ネットワーク サービスをディセーブルにします。

ReadOnly：SNMP ネットワーク サービスを照会のみイネーブルにします。

ReadWrite：SNMP ネットワーク サービスの照会とコマンドの両方をイネーブルにします。

## NetworkServices SNMP Host [n] Address

n: 1..3

最大 3 つの SNMP マネージャのアドレスを定義します。

システムの SNMP エージェント（コーデック内）は、システム ロケーションやシステム接点についてなど、SNMP マネージャ（PC プログラムなど）からのリクエストに応答します。SNMP トラップはサポートされていません。

必要なユーザ ロール：ADMIN、INTEGRATOR

デフォルト値: ""

値スペース：文字列 (0..255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

## NetworkServices SNMP CommunityName

ネットワーク サービス SNMP コミュニティの名前を定義します。SNMP コミュニティ名は SNMP 要求を認証するために使用されます。SNMP 要求は、コーデックの SNMP エージェントから応答を受け取るため、パスワード（大文字と小文字を区別）を持つ必要があります。デフォルトのパスワードは「public」です。Cisco TelePresence Management Suite（TMS）がある場合、同じ SNMP コミュニティがそこで設定されていることを確認する必要があります。注：SNMP コミュニティのパスワードは大文字と小文字が区別されます。

必要なユーザ ロール：ADMIN、INTEGRATOR

デフォルト値: ""

値スペース：文字列 (0, 50)

SNMP コミュニティ名。

## NetworkServices SNMP SystemContact

ネットワーク サービス SNMP システムの連絡先の名前を定義します。

必要なユーザ ロール：ADMIN、INTEGRATOR

デフォルト値: ""

値スペース：文字列 (0, 50)

SNMP システム接点の名前。

## NetworkServices SNMP SystemLocation

ネットワーク サービス SNMP システム ロケーションの名前を定義します。

必要なユーザ ロール：ADMIN、INTEGRATOR

デフォルト値: ""

値スペース：文字列 (0, 50)

SNMP システム ロケーションの名前。

## NetworkServices SSH Mode

SSH (または Secure Shell) プロトコルは、コーデックとローカル コンピュータ間でのセキュアな暗号化通信を提供できます。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : SSH プロトコルはディセーブルになります。

On : SSH プロトコルはイネーブルになります (デフォルト) 。

## NetworkServices SSH HostKeyAlgorithm

SSH ホストキーに使用される暗号化アルゴリズムを選択します。2048 ビットのキーサイズを用いる RSA (リベスト・シャミル・エイドルマンアルゴリズム) 、NIST 曲線の P-384 を用いる ECDSA (楕円曲線デジタル署名アルゴリズム) 、ed25519 署名方式を用いる EdDSA (エドワード曲線デジタル署名アルゴリズム) から選択します。

必要なユーザ ロール : ADMIN

デフォルト値 : RSA

設定可能な値 : ECDSA/RSA/ed25519

ECDSA : ECDSA アルゴリズムを使用します (nist-384p)。

RSA : RSA アルゴリズムを使用します (2048 bits)。

ed25519 : ed25519 アルゴリズムを使用します。

## NetworkServices SSH AllowPublicKey

Secure Shell (SSH) 公開キー認証をコーデックへのアクセスに使用できます。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : SSH 公開キーは許可されません。

On : SSH 公開キーが許可されます。

## NetworkServices UPnP Mode

UPnP (ユニバーサル プラグアンドプレイ) を完全に無効にするか、ビデオ システムがオンになった後または再起動した後に、短時間だけ UPnP を有効にします。

デフォルトでは、ビデオ システムをオンにするか再起動すると、UPnP が有効になります。その後、NetworkServices UPnP Timeout の設定で定義されたタイムアウト時間が経過すると、UPnP は自動的に無効になります。ビデオ システムの ウェブ インターフェイスを使用して、タイムアウトを設定します。

UPnP が有効になると、ビデオ システムはネットワーク上での自身のプレゼンスをアドバタイズします。このアドバタイズによって、タッチ コントローラはビデオ システムを自動的に検出できるようになります。タッチ コントローラとペアリングするために、手動でビデオ システムの IP アドレスを入力する必要はありません。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : UPnP は無効になります。ビデオ システムは自身のプレゼンスをアドバタイズしないため、タッチ コントローラをビデオ システムとペアリングするためにはビデオ システムの IP アドレスを手動で入力する必要があります。

On : UPnP は有効になります。ビデオ システムはタイムアウト期間が経過するまで、自身のプレゼンスをアドバタイズします。

## NetworkServices UPnP Timeout

ビデオ システムがオンになった後または再起動した後、UPnP を有効のままにしておく秒数を定義します。この設定を有効にするには、NetworkServices UPnP Mode を On に設定する必要があります。

必要なユーザ ロール : ADMIN

デフォルト値: 600

値スペース : 整数 (0..3600)

範囲 : 0 ～ 3600 秒の値を選択します。

## NetworkServices Websocket

非セキュアおよびセキュアバージョン (ws および wss) の両方で、ビデオシステムの API に WebSocket プロトコルから相互作用することができます。WebSocket は HTTP に結びついているので、HTTP または HTTPS を有効にしてから WebSockets を使用する必要があります（NetworkServices HTTP モード設定を参照）。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : FollowHTTPService/Off

FollowHTTPService: HTTP または HTTTPS が有効な場合、WebSocket プロトコル経由での通信は許可されます。

オフ : WebSocket プロトコル経由での通信は許可されません。

## NetworkServices WelcomeText

SSH 経由でコーデックにログインする際に、ユーザに表示する情報を選択します。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : ようこそテキストは次のとおりです : ログインに成功しました (Login successfu)

On : ようこそテキストは次のとおりです : <システム名>; ソフトウェア バージョン; ソフトウェアのリリース日; ログインに成功しました (Login successful)

## NetworkServices Wifi Allowed

Wi-Fi アダプタが組み込まれているビデオ システムは、イーサネットまたは Wi-Fi 経由でネットワークに接続できます。イーサネットと Wi-Fi の両方がデフォルトで許可され、ユーザはどちらを使用するかをユーザ インターフェイスから選択できます。この設定を使用して、管理者はユーザ インターフェイスがセットアップできないように Wi-Fi 設定を無効にすることができます。

このシステムは次の標準をサポートします : IEEE 802.11a、IEEE 802.11b、IEEE 802.11g、IEEE 802.11n、and IEEE 802.11ac。システムは次のセキュリティ プロトコルをサポートます : WPA-PSK (AES) 、WPA2-PSK (AES) 、EAP-TLS、EAP-TTLS、EAP-FAST、PEAP、EAP-MSCHAPv2、EAP-GTC、およびオープン ネットワーク (セキュリティ保護なし) 。

ビデオ システムの背面の定格ラベルに記載されている PID （製品 ID) に NR （無線なし) の文字が含まれている場合、システムは Wi-Fi をサポートしていません。

必要なユーザ ロール : admin、user

デフォルト値 : True

値スペース : False/True

False : Wi-Fi は使用できません。イーサネット経由でネットワークに接続する必要があります。

True : イーサネットと Wi-Fi の両方を使用できます。

## NetworkServices Wifi Enabled

ビデオ システムが Wi-Fi 経由でのネットワーク接続を許可されていれば (NetworkServices WIFI Allowed 設定を参照) 、この設定を使用して Wi-Fi を有効および無効にすることができます。

イーサネットと Wi-Fi の両方を同時に使用することはできません。Wi-Fi を設定するときにイーサネット ケーブルが接続されている場合、そのイーサネット ケーブルを抜かないと続行できません。Wi-Fi に接続している最中にイーサネット ケーブルを接続すると、イーサネットが優先されます。イーサネット ケーブルを抜くと、ビデオ システムは、前回接続した Wi-Fi ネットワークが使用可能であれば、そのネットワークに自動的に接続します。

必要なユーザ ロール : admin、user

デフォルト値 : True

値スペース : False/True

False : Wi-Fi は無効になります。

True : Wi-Fi が有効になります。

## NetworkServices XMLAPI Mode

ビデオ システムの XML API をイネーブルまたはディセーブルにします。セキュリティ上の理由からこれを無効にできます。XML API をディセーブルにすると、TMS などとのリモート管理機能が制限され、ビデオ システムに接続できなくなります。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : XML API は無効になります。

On : XML API は有効になります。

# 周辺機器の設定

## Peripherals InputDevice Mode

USB キーボードまたはワイヤレスリモート制御などのサードパーティー入力デバイスの、USB ドングルとの使用を許可するかどうかを定義します。入力デバイスはそれ自体を USB キーボードとしてアドバタイズする必要があります。ご自身で、キークリックに対する応答として行うアクションを定義して実装する必要があります。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

オフ : サードパーティー入力デバイスは許可されません。

オン : サードパーティー USB 入力デバイスはビデオシステムの特定の機能を制御するために使用できます。

## Peripherals Pairing CiscoTouchPanels EmcResilience

多量の電磁雑音が存在する環境でタッチ コントローラを使用すると、誤信号が生じる (例、誰もタップしていないのに、タッチ コントローラがタップされた状態になる) ことがあります。この問題に対処するには、[EMC レジリエンスモード (EMC Resilience Mode) ] を有効にします。

必要なユーザ ロール : ADMIN

デフォルト値 : Off

値スペース : Off/On

Off : EMC レジリエンスモードは無効になります。

On : EMC レジリエンスモードは有効になります。

## Peripherals Profile Cameras

ビデオ システムに接続されることが予想されるタッチ パネルの数を定義します。この情報はビデオ システムの診断サービスで使用します。接続されたカメラの数がこの設定に一致しない場合、診断サービスによって不一致がレポートされます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Minimum1

値スペース : NotSet/Minimum1/0/1/2/3/4/5/6/7

NotSet : カメラ チェックは実行されません。

Minimum1 : 1 台のカメラがビデオ システムに接続されている必要があります。

0 ～ 7 : ビデオ システムへの接続が予想されるカメラの数を選択します。

## Peripherals Profile ControlSystems

サードパーティ製制御システム (Crestron または AMX など) をビデオ システムに接続する予定であれば、定義します。この情報はビデオ システムの診断サービスで使用します。接続された制御システムの数がこの設定に一致しない場合、診断サービスによって不一致がレポートされます。サードパーティ制御システムは 1 つのみサポートされるので注意してください。

1 に設定する場合、xCommand Peripherals Pair コマンドおよび HeartBeat コマンドを使用して、制御システムからビデオ システムにハートビートを送信する必要があります。これが失敗すると、室内制御拡張により、ビデオ システムが制御システムへの接続を失ったことを示す警告が表示されます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : NotSet

値スペース : 1/NotSet

1 : 1 つのサードパーティ製制御システムをビデオ システムに接続する必要があります。

NotSet : サードパーティ製制御システムの検査は実行されません。

## Peripherals Profile TouchPanels

ビデオ システムに接続する予定の Cisco Touch コントローラの数を定義します。この情報はビデオ システムの診断サービスで使用されます。接続されたタッチ コントローラの数がこの設定に一致しない場合、診断サービスによって不一致がレポートされます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Minimum1

値スペース : NotSet/Minimum1/0/1/2/3/4/5

NotSet : タッチ パネル チェックは実行されません。

Minimum1 : 少なくとも 1 台の Cisco Touch コントローラがビデオ システムに接続されている必要があります。

0 ～ 5 : ビデオ システムへの接続が予想されるタッチ コントローラの数を選択します。公式にサポートされる Cisco Touch コントローラは、1 台のみであることに注意してください。

# 電話帳の設定

## Phonebook Server [n] ID

n: 1..1

外部の電話帳の名前を定義します。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0, 64)
外部の電話帳の名前。

## Phonebook Server [n] Pagination

n: 1..1

電話帳サーバがページネーション(ウェルカム ページ) に対応するかどうかを定義します。ページネーションとはサーバが連続検索に対応しているかどうか、さらにこれらの検索がオフセットに関連付けられるかどうかを意味します。これにより、ユーザ インターフェイスは完全な検索結果を得るために必要な可能な限り多くの連続検索を実行できます。

ページネーションが無効の場合、ビデオシステムはシングル検索を行い、最大 100 エントリを検索結果に返します。それ以上の検索結果をさらにスクロールすることはできません。

必要なユーザ ロール : ADMIN
デフォルト値 : Enabled

値スペース : Disabled/Enabled
Disabled : 電話帳サーバはページネーションに対応しません。ビデオシステムはシングル検索を行い、検索結果の最大エントリ数は 100 です。
Enabled : 電話帳サーバはページネーションに対応しています。

## Phonebook Server [n] Type

n: 1..1

電話帳サーバの種類を選択します。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/CUCM/Spark/TMS/VCS
Off : 電話帳を使用しません。
CUCM : 電話帳が Cisco Unified Communications Manager 上に配置されます。
Spark: 電話帳が Cisco Webex クラウドサービス内に配置されます。
TMS : 電話帳が Cisco TelePresence Management Suite サーバ上に配置されます。
VCS : 電話帳が Cisco TelePresence Video Communication Server 上に配置されます。

## Phonebook Server [n] URL

n: 1..1

外部電話帳サーバへのアドレス (URL) を定義します。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0..255)
外部電話帳サーバの有効なアドレス (URL) 。

# プロビジョニング設定

## Provisioning Connectivity

この設定は、プロビジョニング サーバからの内部または外部のコンフィギュレーションを要求するかどうかを、デバイスがどのように検出するか制御します。

必要なユーザ ロール : admin、user

デフォルト値 : Auto

値スペース : Internal/External/Auto

Internal : 内部コンフィギュレーションを要求します。

External : 外部コンフィギュレーションを要求します。

Auto : 内部または外部のコンフィギュレーションを要求するかどうかを自動的に NAPTR クエリーを使用して検出します。NAPTR の応答に「e」フラグがある場合、外部コンフィギュレーションが要求されます。それ以外の場合、内部コンフィギュレーションが要求されます。

## Provisioning ExternalManager Address

外部のマネージャ システムまたはプロビジョニング システムの IP アドレスまたは DNS 名を定義します。

外部マネージャのアドレス (およびパス) が設定されている場合、システムはスタートアップ時にこのアドレスにメッセージを送信します。このメッセージを受信すると、結果として外部マネージャ/プロビジョニング システムはそのユニットにコンフィギュレーション/コマンドを返すことができます。

CUCM または TMS プロビジョニングを使用する場合、外部マネージャ アドレスを自動的に提供するために DHCP サーバをセットアップできます (TMS には DHCP オプション 242、CUCM には DHCP オプション 150) 。プロビジョニング 外部マネージャーアドレス で設定されたアドレスは、DHCP によって提供されるアドレスを上書きします。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

## Provisioning ExternalManager AlternateAddress

エンドポイントが Cisco Unified Communications Manager (CUCM) でプロビジョニングされており、代替 CUCM が冗長性に利用可能な場合にのみ使用できます。代替 CUCM のアドレスを定義します。主な CUCM が使用できない場合、エンドポイントは代替 CUCM でプロビジョニングされます。主な CUCM が再び使用可能になると、エンドポイントはこの CUCM によってプロビジョニングされます。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

## Provisioning ExternalManager Protocol

外部のマネージャ システムまたはプロビジョニング システムに要求を送信する際に、HTTP (非セキュアな通信) または HTTPS (セキュアな通信) のどちらのプロトコルを使用するかを定義します。

選択したプロトコルは、NetworkServices HTTP Mode の設定で有効になっている必要があります。

必要なユーザ ロール : admin、user

デフォルト値 : HTTP

値スペース : HTTPS/HTTP

HTTPS : HTTPS を介してリクエストを送信します。

HTTP : HTTP を介してリクエストを送信します。

## Provisioning ExternalManager Path

外部のマネージャ システムまたはプロビジョニング システムへのパスを定義します。いくつかの管理サービスが同じサーバに存在する、つまり同じ外部マネージャのアドレスを共有する場合、この設定が必要です。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0..255)

外部のマネージャー システムまたはプロビジョニング システムへの有効なパス。

## Provisioning ExternalManager Domain

VCS プロビジョニング サーバの SIP ドメインを定義します。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効なドメイン名。

## Provisioning Mode

プロビジョニング システム (外部マネージャ) を使用してビデオ システムを設定できます。これにより、ビデオ会議のネットワーク管理者は複数のビデオ システムを同時に管理することができます。この設定により、使用するプロビジョニング システムの種類を選択します。プロビジョニングは、オフに切り替えることも可能です。詳細については、プロビジョニング システムのプロバイダー/担当者にお問い合わせください。

必要なユーザ ロール : admin、user

デフォルト値 : Auto

値スペース : Off/Auto/CUCM/Edge/Webex/TMS/VCS

Off : ビデオ システムはプロビジョニング システムによって設定されません。

Auto : DHCP サーバでセットアップされる対象としてプロビジョニング サーバが自動的に選択されます。

CUCM : CUCM (Cisco Unified Communications Manager) からビデオ システムにコンフィギュレーションをプッシュします。

Edge : CUCM (Cisco Unified Communications Manager) からビデオ システムにコンフィギュレーションをプッシュします。システムは Expressway インフラストラクチャを介して CUCM に接続します。Expressway を越えて登録するには、暗号化オプションキーがビデオ システムにインストールされている必要があります。

Webex: Cisco Webex クラウド サービスからビデオ システムに設定をプッシュします。

TMS : TMS (Cisco TelePresence Management System) からビデオ システムにコンフィギュレーションをプッシュします。

VCS : VCS (Cisco TelePresence Video Communication Server) からビデオ システムにコンフィギュレーションをプッシュします。

## Provisioning LoginName

これは、プロビジョニング サーバによるビデオ システムの認証で使用されるクレデンシャルのユーザ名部分です。この設定は、プロビジョニング サーバが要求する場合、使用する必要があります。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 80)

有効なユーザ名。

## Provisioning Password

これは、指定サーバとのビデオ システムの認証に使用されるクレデンシャルのパスワード部分です。この設定は、プロビジョニング サーバが要求する場合、使用する必要があります。

必要なユーザ ロール : admin、user

デフォルト値: ""

値スペース : 文字列 (0, 64)

有効なパスワード。

# プロキシミティの設定

## Proximity Mode

ビデオ システムが超音波ペアリング メッセージを発信するか否かを決定します。

ビデオ システムが超音波を発信すると、プロキシミティ クライアントはビデオ システムが近くにあることを検知できます。クライアントを使用するには、少なくとも 1 つの Proximity サービスをイネーブルにする必要があります (Proximity Services 設定を参照) 。一般的に、すべてのプロキシミティ サービスを有効にすることをお勧めします。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

[オフ (Off) ] : ビデオ システムは超音波を発しないため、Proximity サービスを使用できません。

[オン (On) ] : ビデオ システムが超音波を発し、プロキシミティ クライアントはビデオ システムに近接していることを検出できます。有効になっているプロキシミティ サービスを使用できます。

## Proximity Services CallControl

プロキシミティ クライアントで基本的なコール制御機能を有効または無効にします。この設定を有効にすると、プロキシミティ クライアントを使用してコールを制御できます (ダイヤル、ミュート、音量、コールの終了など) 。このサービスはモバイル デバイス (iOS および Android) でサポートされます。この設定が機能するには、プロキシミティ モードを On にする必要があります。

必要なユーザ ロール : admin、user

デフォルト値 : Disabled

値スペース : Enabled/Disabled

Enabled : プロキシミティ クライアントからのコール制御が有効になります。

Disabled : プロキシミティ クライアントからのコール制御が無効になります。

## Proximity Services ContentShare FromClients

クライアントからのコンテンツ共有を有効または無効にします。この設定を有効にすると、ビデオ システムで無線によってプロキシミティ クライアントからコンテンツを共有できます (ラップトップ画面の共有など) 。このサービスはラップトップ (OS X および Windows) でサポートされます。この設定が機能するには、プロキシミティ モードを On にする必要があります。

必要なユーザ ロール : admin、user

デフォルト値 : Enabled

値スペース : Enabled/Disabled

Enabled : プロキシミティ クライアントからのコンテンツ共有が有効になります。

Disabled : プロキシミティ クライアントからのコンテンツ共有が無効になります。

## Proximity Services ContentShare ToClients

プロキシミティ クライアントに対するコンテンツ共有を有効または無効にします。有効にすると、プロキシミティ クライアントはビデオ システムからプレゼンテーションを受け取ります。詳細を拡大して、以前のコンテンツを表示し、スナップショットを作成できます。このサービスはモバイル デバイス (iOS および Android) でサポートされます。この設定が機能するには、プロキシミティ モードを On にする必要があります。

必要なユーザ ロール : admin、user

デフォルト値 : Disabled

値スペース : Enabled/Disabled

Enabled : プロキシミティ クライアントに対するコンテンツ共有が有効になります。

Disabled : プロキシミティ クライアントに対するコンテンツ共有が無効になります。

# RoomAnalytics 設定

## RoomAnalytics AmbientNoiseEstimation Mode

ビデオシステムは室内の固定周囲ノイズレベル（背景雑音レベル）をレポートできます。結果は RoomAnalytics AmbientNoise レベル dBA ステータスにレポートされます。新しい周囲ノイズレベルが検出されるとステータスが更新されます。

必要なユーザ ロール：ADMIN、INTEGRATOR、USER

デフォルト値：Off

値スペース：Off/On

オン：ビデオシステムは固定周囲ノイズレベルを定期的に予測します。

オフ：ビデオシステムは固定周囲ノイズレベルを定期的に予測しません。

## RoomAnalytics PeopleCountOutOfCall

顔検出を使用して、ビデオ システムが室内にいる人の人数を特定できます。デフォルトでは、システムは通話中のときまたはセルフ ビューに画像を表示したときにのみ人数を数えます。

必要なユーザ ロール：ADMIN、INTEGRATOR、USER

デフォルト値：Off

値スペース：Off/On

Off：ビデオ システムは、システムが通話中のときまたはセルフ ビューがオンのときのみ、人数を数えます。

On：ビデオ システムは、ビデオ システムがスタンバイ モードでない限り、人数を数えます。セルフ ビューがオフであっても、これは非通話中の人数を含みます。

## RoomAnalytics PeoplePresenceDetector

ビデオ システムは、人が室内に存在しているかどうかを確認し、その結果を [室内在室分析（RoomAnalytics PeoplePresence）] のステータスにレポートすることができます。この機能は、超音波に基づいています。室内に人が存在しているかどうかを検出するには最短で 2 分かかり、空室になったあとにステータスを変更するには最長 2 分かかる可能性があります。

必要なユーザ ロール：ADMIN、INTEGRATOR、USER

デフォルト値：Off

値スペース：Off/On

Off：ビデオ システムのステータスに、室内に人が存在しているかどうかは表示されません。

On：ビデオ システムのステータスに、室内に人が存在しているかどうかが表示されます。

# ルームリセットの設定

## RoomReset Control

この設定は、コントロールシステムまたはマクロの使用に対するものです。マクロを使用して、ビデオエンドポイントの一部を自動化できる JavaScript コードの一部を記述することができます。このようにしてカスタム動作を作成します。

ルームが数分に渡って待機状態になると、システムからルームがリセット準備完了状態であると伝えるイベントを送ることができます。

この設定が有効である場合に送られるイベントは次の通りです :

*e RoomReset SecondsToReset: 30

** end

*e RoomReset Reset

** end

必要なユーザ ロール : ADMIN

デフォルト値 : On

設定可能な値: CameraPositionsOnly/Off/On (カメラポジションのみ/オフ/オン)

CameraPositionsOnly (カメラポジションのみ) : 適用されません。

Off : ルームリセットイベントは送られません。

On : ルームリセット制御が有効になっており、ルームリセットイベントが送信されます。

# RTP 設定

## RTP Ports Range Start

RTP ポート範囲の最初のポートを定義します。

デフォルトで、RTP および RTCP メディア データに 2326 ～ 2486 の範囲のポートを使用します。RTP ビデオ ポート範囲を無効にしたときの最小範囲は 100、RTP ビデオ ポート範囲を有効にしたときの最小範囲は 20 です。

RTP ビデオ ポート範囲が有効な場合、オーディオは RTP ポート範囲設定で定義された範囲を使用し、その他のメディア データは RTP ビデオ ポート範囲設定で定義された範囲を使用します。2 つの範囲は重ならない必要があります。

設定の変更内容は、次回の発信から有効になります。

必要なユーザ ロール : ADMIN

デフォルト値: 2326

値スペース : 整数 (1024..65438)

RTP ポート範囲内で最初のポートを設定します。

## RTP Ports Range Stop

RTP ポート範囲の最後のポートを定義します。

デフォルトで、RTP および RTCP メディア データに 2326 ～ 2487 の範囲のポートを使用します。RTP ビデオ ポート範囲が有効な場合、システムは 1024 ～ 65436 の範囲のポートを使用します。RTP ビデオ ポート範囲を無効にしたときの最小範囲は 100、RTP ビデオ ポート範囲を有効にしたときの最小範囲は 20 です。

RTP ビデオ ポート範囲が有効な場合、オーディオは RTP ポート範囲設定で定義された範囲を使用し、その他のメディア データは RTP ビデオ ポート範囲設定で定義された範囲を使用します。2 つの範囲は重ならない必要があります。

設定の変更内容は、次回の発信から有効になります。

必要なユーザ ロール : ADMIN

デフォルト値: 2486

値スペース : 整数 (1120..65535)

RTP ポート範囲内で最後のポートを設定します。

## RTP Video Ports Range Start

RTP ビデオ ポート範囲の最初のポートを定義します。

開始と終了の値の両方が 0 に設定されている場合、RTP ビデオ ポートの範囲は無効です。有効にするには、最初のポートを 1024 から 65454 までの値に設定し、最後のポートを 1024 から 65535 までの値に設定します。最小範囲は 80 です。

RTP ビデオ ポート範囲が有効な場合、オーディオは RTP ポート範囲設定で定義された範囲を使用し、その他のメディア データは RTP ビデオ ポート範囲設定で定義された範囲を使用します。2 つの範囲は重ならない必要があります。

設定の変更内容は、次回の発信から有効になります。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0、1024..65454)

RTP ビデオ ポート範囲の最初のポートを設定します。

## RTP Video Ports Range Stop

RTP ビデオ ポート範囲の最後のポートを定義します。

開始と終了の値の両方が 0 に設定されている場合、RTP ビデオ ポートの範囲は無効です。有効にするには、最初のポートを 1024 から 65454 までの値に設定し、最後のポートを 1024 から 65535 までの値に設定します。最小範囲は 80 です。

RTP ビデオ ポート範囲が有効な場合、オーディオは RTP ポート範囲設定で定義された範囲を使用し、その他のメディア データは RTP ビデオ ポート範囲設定で定義された範囲を使用します。2 つの範囲は重ならない必要があります。

設定の変更内容は、次回の発信から有効になります。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0、1024..65535)

RTP ビデオ ポート範囲の最後のポートを設定します。

# セキュリティ設定

## Security Audit Logging Mode

監査ログを記録または送信する場所を定義します。監査ログは syslog サーバに送信されます。ロギングモード設定がオフに設定されている場合、この設定には効果がありません。

External モードまたは ExternalSecure モードを使用する場合は、セキュリティ監査サーバアドレス 設定に監査サーバのアドレスを入力する必要があります。

必要なユーザ ロール : AUDIT

デフォルト値 : Internal

設定可能な値 : External/ExternalSecure/Internal/Off （外部/安全な外部/内部/オフ）

External : システムは外部監査 syslog サーバに監査ログを送信します。syslog サーバでは UDP をサポートする必要があります。

ExternalSecure : ビデオシステムは監査 CA リストの証明書で検証された外部 syslog サーバに暗号化された監査ログを送信します。監査 CA リスト ファイルは、ウェブ インターフェイスを使用してビデオシステムにアップロードする必要があります。CA のリストの証明書の common_name パラメータは syslog サーバの IP アドレスまたは DNS 名と一致する必要があり、セキュア TCP サーバでセキュア (TLS) TCP syslog メッセージをリッスンするように設定される必要があります。

Internal : システムは内部ログに監査ログを記録し、いっぱいになった場合はログをローテーションします。

Off : 監査ロギングは実行されません。

## Security Audit OnError Action

syslog サーバへの接続が失われた場合の動作を定義します。この設定は、Security Audit Logging Mode が ExternalSecure に設定されている場合のみ関連します。

必要なユーザ ロール : AUDIT

デフォルト値 : Ignore

値スペース : Halt/Ignore

Halt : 停止状態が検出された場合、システム コーデックはリブートし、停止状態が過ぎ去るまではオーディタだけが装置の操作を許可されます。停止状態が過ぎ去ると、監査ログは syslog サーバに再スプールされます。ネットワークの違反 (物理リンクなし) 、動作中の外 Syslog サーバが存在しない (または syslog への間違ったアドレスまたはポート) 、TLS 認証が失敗した (使用中の場合) 、ローカル バックアップ (再スプール) ログがいっぱいになった、などの停止状態があります。

Ignore : システムは、通常の動作を続行し、いっぱいになった場合は内部ログをローテーションします。接続が復元されると syslog サーバに再度監査ログを送信します。

## Security Audit Server Address

監査ログの送信先である syslog サーバの IP アドレスまたは DNS 名を設定します。この設定は、Security Audit Logging Mode が External または ExternalSecure に設定されている場合のみ関連します。

必要なユーザ ロール : AUDIT

デフォルト値: ""

値スペース : 文字列 (0..255)

有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

## Security Audit Server Port

監査ログは syslog サーバに送信されます。システムが監査ログを送信する syslog サーバのポートを定義します。この設定は、Security Audit PortAssignment が Manual に設定されている場合にのみ関連します。

必要なユーザ ロール : AUDIT

デフォルト値: 514

値スペース : 整数 (0..65535)

監査サーバのポートを設定します。

## Security Audit Server PortAssignment

監査ログは syslog サーバに送信されます。外部 syslog サーバのポート番号の割り当て方法を定義できます。この設定は、Security Audit Logging Mode が External または ExternalSecure に設定されている場合のみ関連します。使用しているポート番号を確認するために、Security Audit Server Port 状態をチェックできます。ウェブ インターフェイスで [セットアップ (Setup) ] > [ステータス (Status) ] に移動するか、コマンドライン インターフェイスの場合はコマンド xStatus Security Audit Server Port を実行します。

必要なユーザ ロール : AUDIT

デフォルト値 : Auto

値スペース : Auto/Manual

Auto : [セキュリティ監査ロギング モード (Security Audit Logging Mode) ] が [外部 (External) ] にセットされている場合、UDP ポート番号 514 を使用します。Security Audit Logging Mode が ExternalSecure にセットされている場合、TCP ポート番号 6514 を使用します。

Manual : [セキュリティ監査サーバのポート (Security Audit Server Port) ] 設定で定義されたポート値を使用します。

## Security Session FailedLoginsLockoutTime

ユーザが Web または SSH セッションのログインに失敗したあと、システムがユーザをロックアウトする時間を定義します。

この設定への変更を反映させるには、システムを再起動します。

必要なユーザ ロール : ADMIN

デフォルト値: 60

値スペース : 整数 (0..10000)

ロックアウト時間 (分) を設定します。

## Security Session InactivityTimeout

ユーザが Web または SSH セッションから自動的にログ アウトする前に、システムがユーザの非アクティブ状態をどれくらいの時間受け入れるかを定義します。

この設定への変更を反映させるには、システムを再起動します。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0..10000)

非アクティブ タイムアウト (分単位) を設定します。非アクティブな状態でも強制的に自動ログアウトしない場合は、0 を選択します。

## Security Session MaxFailedLogins

Web または SSH セッションにログイン試行を失敗できるユーザ 1 人あたりの最大数を定義します。ユーザが試行の最大数を超えた場合、ユーザはロックアウトされます。0 は、失敗できるログインの回数に制限がないことを意味します。

この設定への変更を反映させるには、システムを再起動します。

必要なユーザ ロール : ADMIN

デフォルト値: 0

値スペース : 整数 (0..10)

ユーザ 1 人あたりの失敗できるログイン試行の最高回数を設定します。

## Security Session MaxSessionsPerUser

ユーザ 1 人あたりの最大同時セッション数は 20 セッションです。

必要なユーザ ロール : ADMIN

デフォルト値: 20

値スペース : 整数 (1..20)

ユーザ 1 人あたりの最大同時セッション数を設定します。

## Security Session MaxTotalSessions

同時セッションの合計最大数は 20 セッションです。

必要なユーザ ロール : ADMIN
デフォルト値: 20

値スペース : 整数 (1..20)
同時セッションの合計最大数を設定します。

## Security Session ShowLastLogon

SSH を使用してシステムにログインしたとき、前回ログインに成功したセッションのユーザ ID、時刻および日付が表示されます。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
On : 最後のセッションに関する情報を表示します。
Off : 最後のセッションに関する情報を表示しません。

# SerialPort 設定

## SerialPort Mode

シリアル ポートを有効/無効にします。

必要なユーザ ロール : ADMIN、INTEGRATOR
デフォルト値 : On

値スペース : Off/On
Off : シリアル ポートをディセーブルにします。
On : シリアル ポートをイネーブルにします。

## SerialPort BaudRate

シリアル ポートに、ボー レート (データ送信レート、ビット/秒) を設定します。
シリアル ポートの他の接続パラメータは次のとおりです。データ ビット : 8。パリティ : なし。ストップ ビット : 1。フロー制御 : なし。

必要なユーザ ロール : ADMIN、INTEGRATOR
デフォルト値: 115200

値スペース : 115200
リストされているボー レート (bps) からボー レートを選択します。

## SerialPort LoginRequired

シリアル ポートに接続するときにログインが必要かどうかを定義します。

必要なユーザ ロール : ADMIN
デフォルト値 : On

値スペース : Off/On
Off : ユーザはログインせずに、シリアル ポート経由でコーデックにアクセスできます。
On : シリアル ポート経由でコーデックに接続するときに、ログインが必要です。

# SIP 設定

## SIP ANAT

ANAT (Alternative Network Address Types) は RFC 4091 で規定されている複数のアドレスとアドレス タイプのメディア ネゴシエーションを有効にします。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
Off : ANAT を無効にします。
On : ANAT を有効にします。

## SIP Authentication UserName

これは、SIP プロキシへの認証に使用されるクレデンシャルのユーザ名部分です。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0, 128)
有効なユーザ名。

## SIP Authentication Password

これは、SIP プロキシへの認証に使用されるクレデンシャルのパスワード部分です。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0, 128)
有効なパスワード。

## SIP DefaultTransport

LAN で使用するトランスポート プロトコルを選択します。

必要なユーザ ロール : ADMIN
デフォルト値 : Auto

値スペース : Auto/TCP/Tls/UDP
TCP : システムはデフォルトの転送方法として常に TCP を使用します。
UDP : システムはデフォルトの転送方法として常に UDP を使用します。
Tls : システムはデフォルトの転送方法として常に TLS を使用します。TLS 接続の場合、SIP CA リストをビデオ システムにアップロードできます。このような CA リストがシステムにない場合は匿名の Diffie Hellman が使用されます。
Auto : システムは、TLS、TCP、UDP の順序でトランスポート プロトコルを使用して接続を試みます。

## SIP DisplayName

設定されたとき、着信コールは SIP URI ではなく、表示名を報告します。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0, 550)
SIP URI の代わりに表示する名前。

## SIP Ice DefaultCandidate

ICE プロトコルには、使用するメディア ルートを決定するまでの時間（最大で通話開始から 5 秒間）が必要となります。この時間内に、この設定に従って、ビデオ システムのメディアが、デフォルトの候補に送信されます。

必要なユーザ ロール：ADMIN

デフォルト値：Host

値スペース：Host/Rflx/Relay

Host：メディアをビデオ システムのプライベート IP アドレスへ送信します。

Rflx：TURN サーバから見えるビデオ システムのパブリック IP アドレスにメディアを送信します。

Relay：TURN サーバで割り当てられた IP アドレスおよびポートにメディアを送信します。

## SIP Ice Mode

ICE (Interactive Connectivity Establishment、RFC 5245) は、最適化されたメディア パスの検出にビデオ システムで使用できる NAT トラバーサル ソリューションです。そのため、音声とビデオの最短ルートがビデオ システム間で常に確保されます。

必要なユーザ ロール：ADMIN

デフォルト値：Auto

値スペース：Auto/Off/On

Auto：TURN サーバを指定した場合は、ICE が有効になります。それ以外の場合は、ICE が無効になります。

Off：ICE が無効になります。

On：ICE が有効になります。

## SIP Line

Cisco Unified Communications Manager (CUCM) に登録すると、エンドポイントを共有回線の一部にできます。これは、複数のデバイスが同じディレクトリ番号を共有することを意味します。RFC 4235 で規定されているように、同じ番号を共有する各デバイスは、ライン上のもう一方のアピアランスからステータスを受け取ります。

共有回線はエンドポイントではなく CUCM によって設定されることに注意してください。そのため、手動でこの設定を変更しないでください。CUCM は必要に応じてこの情報をエンドポイントにプッシュします。

必要なユーザ ロール：ADMIN

デフォルト値：Private

値スペース：Private/Shared

Shared：システムは共有回線の一部であるため、ディレクトリ番号を他のデバイスと共有します。

Private：このシステムは共有回線の一部ではありません。

## SIP ListenPort

SIP TCP/UDP ポートでの着信接続のリッスンをオンまたはオフにします。オフにした場合、エンドポイントは SIP レジストラ (CUCM または VCS) を介してのみ到達可能になります。セキュリティ対策として、エンドポイントが SIP プロキシに設定されている場合は SIP ListenPort をオフにすべきです。

必要なユーザ ロール：ADMIN

デフォルト値：On

値スペース：Off/On

Off：SIP TCP/UDP ポートでの着信接続のリッスンをオフにします。

On：SIP TCP/UDP ポートでの着信接続のリッスンをオンにします。

## SIP Mailbox

Cisco Unified Communications Manager (CUCM) に登録すると、個人用ボイス メールボックスを所有するオプションが与えられます。

必要なユーザ ロール：ADMIN

デフォルト値: ""

値スペース：文字列 (0, 255)

有効な番号またはアドレス。ボイス メールボックスがない場合は、文字列を空のままにしておきます。

## SIP MinimumTLSVersion

許可する最低バージョンの TLS (Transport Layer Security) プロトコルを設定します。

必要なユーザ ロール : ADMIN
デフォルト値 : TLSv1.0

値スペース : TLSv1.0/TLSv1.1/TLSv1.2
TLSv1.0 : TLS バージョン 1.0 以上をサポートします。
TLSv1.1 : TLS バージョン 1.1 以上をサポートします。
TLSv1.2 : TLS バージョン 1.2 以上をサポートします。

## SIP PreferredIPSignaling

シグナリングの優先 IP バージョンを定義します (音声、ビデオ、データ) 。Network IPStack および Conference CallProtocolIPStack の両方が Dual に設定されていて、ネットワークに優先 IP バージョンを選択するメカニズムがない場合にのみ使用可能です。また、優先 IP バージョンが登録に使用されるように、DNS で A/AAAA ルックアップのプライオリティを指定します。

必要なユーザ ロール : ADMIN
デフォルト値 : IPv4

値スペース : IPv4/IPv6
IPv4 : シグナリングの優先 IP バージョンは IPv4 です。
IPv6 : シグナリングの優先 IP バージョンは IPv6 です。

## SIP Proxy [n] Address

n: 1..4

プロキシ アドレスは発信プロキシに手動で設定されたアドレスです。完全修飾ドメイン名、または IP アドレスを使用することが可能です。デフォルト ポートは、TCP および UDP の場合は 5060 ですが、もう 1 ポート準備できます。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0..255)
有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

## SIP TlsVerify

TLS 接続の場合、SIP CA リストをビデオ システムにアップロードできます。これは、ウェブ インターフェイスから実行できます。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
Off : 検証せずに TLS 接続を許可するには、Off に設定します。TLS 接続は、サーバから受信した x.509 証明書をローカル CA リストと確認せずにセットアップできます。これは通常、コーデックに SIP CA リストがアップロードされていない場合、選択する必要があります。
On : TLS 接続を確認するには、On に設定します。x.509 証明書が CA リストで検証された、サーバへの TLS 接続だけが許可されます。

## SIP Turn DiscoverMode

検出モードを定義し、DNS で利用可能な TURN サーバの検索に対してアプリケーションを有効/無効にします。コールを発信する前に、システムはポート割り当てが可能かどうかを確認します。

必要なユーザ ロール : ADMIN
デフォルト値 : On

値スペース : Off/On
Off : 検出モードを無効にします。
On : DNS で利用可能な TURN サーバを検索し、コールを発信する前にポート割り当てが可能かどうかをテストします。

## SIP Turn DropRflx

DropRflx は、リモート エンドポイントが同じネットワークにない場合に限り、TURN リレー経由でエンドポイントにメディアを強制させます。

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
Off : DropRflx を無効にします。
On : リモート エンドポイントが別のネットワークにある場合、TURN リレー経由でメディアを強制します。

## SIP Turn Server

TURN (Traversal Using Relay NAT) サーバのアドレスを定義します。これはメディア リレー フォールバックとして使用され、また、エンドポイント固有のパブリック IP アドレスを検出するためにも使用されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

推奨する形式は DNS SRV レコード (例 : _turn._udp.<ドメイン>) ですが、有効な IPv4 または IPv6 アドレスも指定できます。

## SIP Turn UserName

TURN サーバへのアクセスに必要なユーザ名を定義します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 128)

有効なユーザ名。

## SIP Turn Password

TURN サーバへのアクセスに必要なパスワードを定義します。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 128)

有効なパスワード。

## SIP Type

ベンダーまたはプロバイダーに対する SIP 拡張および特別な動作を有効にします。

必要なユーザ ロール : ADMIN

デフォルト値 : Standard

値スペース : Standard/Cisco

Standard : 標準 SIP プロキシに登録する場合はこれを使用します (Cisco TelePresence VCS でテスト済み) 。

Cisco : Cisco Unified Communications Manager に登録する場合はこれを使用します。

## SIP URI

SIP URI (Uniform Resource Identifier) は、ビデオ システムの識別に使用されるアドレスです。URI が登録され、SIP サービスによりシステムへの着信コールのルーティングに使用されます。SIP URI 構文は RFC 3261 で定義されています。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

SIP URI 構文に準拠したアドレス (URI) 。

# スタンバイ設定

## Standby BootAction

コーデックの再起動後のカメラの位置を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER
デフォルト値: DefaultCameraPosition

値スペース: None/DefaultCameraPosition/RestoreCameraPosition
None: アクションはありません。
RestoreCameraPosition: ビデオ システムを再起動すると、カメラは再起動前の位置に戻ります。
DefaultCameraPosition: ビデオ システムを再起動すると、カメラは工場出荷時のデフォルトの位置に移動します。

## Standby Control

システムがスタンバイ モードに移行するか否かを定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR
デフォルト値: On

値スペース: Off/On
Off: システムはスタンバイ モードを開始しません。
On: Standby Delay がタイム アウトになると、システムはスタンバイ モードになります。Standby Delay を適切な値に設定する必要があります。

## Standby Delay

スタンバイ モードに入る前に、システムがアイドル モードのまま経過する時間の長さ (分単位) を定義します。[スタンバイ制御 (Standby Control) ] が有効である必要があります。

必要なユーザ ロール: ADMIN、INTEGRATOR
デフォルト値: 10

値スペース: 整数 (1..480)
スタンバイ遅延 (分) を設定します。

## Standby StandbyAction

スタンバイ モードに入るときのカメラ位置を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR
デフォルト値: PrivacyPosition

値スペース: None/PrivacyPosition
None: アクションはありません。
PrivacyPosition: ビデオ システムがスタンバイになると、プライバシー保護のためカメラは横向きになります。

## Standby WakeupAction

スタンバイ モードを抜けるときのカメラ位置を定義します。

必要なユーザ ロール: ADMIN、INTEGRATOR、USER
デフォルト値: RestoreCameraPosition

値スペース: None/RestoreCameraPosition/DefaultCameraPosition
None: アクションはありません。
RestoreCameraPosition: ビデオ システムがスタンバイではなくなると、カメラはスタンバイ前の位置に戻ります。
DefaultCameraPosition: ビデオ システムがスタンバイではなくなると、カメラは工場出荷時のデフォルトの位置に移動します。

## Standby WakeupOnMotionDetection

動体検知自動ウェイク アップは、人が室内に入ってきたときに検知する機能です。この機能は、超音波検出に基づいています。

必要なユーザ ロール: ADMIN、INTEGRATOR
デフォルト値: On

値スペース: Off/On
Off: 動体検知ウェイクアップは無効です。
On: 人が部屋に入ってくると、システムが自動的にスタンバイからウェイクアップします。

# SystemUnit 設定

## SystemUnit Name

システム名を定義します。コーデックが SNMP エージェントとして機能している場合に、システム名は DHCP リクエストでホスト名として送信されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 50)

システム名を定義します。

## SystemUnit CrashReporting Advanced

ビデオ システム （コーデック) がクラッシュすると、システムは解析のために [Cisco Automatic Crash Report ツール (Cisco Automatic Crash Report tool) ] （ACR) ヘログを自動的に送信できます。ACR ツールは、Cisco の内部使用のみであり、お客様は利用できません。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : ACR ツールは標準的なログ解析を実行します。

On : ACR ツールは高度なログ解析を実行します。

## SystemUnit CrashReporting Mode

ビデオ システム （コーデック) がクラッシュすると、システムは解析のために [Cisco Automatic Crash Report ツール (Cisco Automatic Crash Report tool) ] （ACR) ヘログを自動的に送信できます。ACR ツールは、Cisco の内部使用のみであり、お客様は利用できません。

必要なユーザ ロール : ADMIN

デフォルト値 : On

値スペース : Off/On

Off : ACR ツールにログは送信されません。

On : ACR ツールにログは自動的に送信されます。

## SystemUnit CrashReporting Url

ビデオ システム （コーデック) がクラッシュすると、システムは解析のために [Cisco Automatic Crash Reportツール (Cisco Automatic Crash Report tool) ] （ACR) ヘログを自動的に送信できます。ACR ツールは、Cisco の内部使用のみであり、お客様は利用できません。

必要なユーザ ロール : ADMIN

デフォルト値 : "acr.cisco.com"

値スペース : 文字列 (0..255)

[Cisco Automatic Crash Report ツール (Cisco Automatic Crash Report tool) ] の URL。

# 時刻設定

## Time TimeFormat

時刻形式を定義します。

必要なユーザ ロール : admin、user
デフォルト値 : 24H

値スペース : 24H/12H
24H : 24 時間の時間フォーマットを設定します。
12H : 12 時間 (AM/PM) の時間フォーマットを設定します。

## Time DateFormat

日付形式を定義します。

必要なユーザ ロール : admin、user
デフォルト値 : DD_MM_YY

値スペース : DD_MM_YY/MM_DD_YY/YY_MM_DD
DD_MM_YY : 2010 年 1 月 30 日は「30.01.10」と表示されます。
MM_DD_YY : 2010 年 1 月 30 日は「01.30.10」と表示されます。
YY_MM_DD : 2010 年 1 月 30 日は「10.01.30」と表示されます。

## Time Zone

ビデオ システムが物理的に存在する地域のタイム ゾーンを設定します。値スペースの情報は、tz データベース（別名：IANA タイムゾーン データベース）から取得しています。

必要なユーザ ロール： ADMIN、INTEGRATOR、USER

デフォルト値：Etc/UTC

設定可能な値：アフリカ/アビジャン、アフリカ/アクラ、アフリカ/アディスアベバ、アフリカ/アルジェ、アフリカ/アスマラ、アフリカ/アスメラ、アフリカ/バマコ、アフリカ/バンギ、アフリカ/バンジュール、アフリカ/ビサウ、アフリカ/ブランタイア、アフリカ/ブラザビル、アフリカ/ブジュンブラ、アフリカ/カイロ、アフリカ/カサブランカ、アフリカ/セウタ、アフリカ/コナクリ、アフリカ/ダカール、アフリカ/ダルエスサラーム、アフリカ/ジブチ、アフリカ/ドゥアラ、アフリカ/アイウン、アフリカ/フリータウン、アフリカ/ガボローネ、アフリカ/ハラーレ、アフリカ/ヨハネスブルク、アフリカ/ジュバ、アフリカ/カンパラ、アフリカ/ハルツーム、アフリカ/キガリ、アフリカ/キンシャサ、アフリカ/ラゴス、アフリカ/リーブルビル、アフリカ/ロメ、アフリカ/ルアンダ、アフリカ/ルブンバシ、アフリカ/ルサカ、アフリカ/マラボ、アフリカ/マプト、アフリカ/マセール、アフリカ/ムババーネ、アフリカ/モガディシュ、アフリカ/モンロヴィア、アフリカ/ナイロビ、アフリカ/ンジャメナ、アフリカ/ニアメイ、アフリカ/ヌアクショット、アフリカ/ワガドゥグ、アフリカ/ポルトノボ、アフリカ/サントメ・プリンシペ、アフリカ/ティンブクトゥ、アフリカ/トリポリ、アフリカ/チュニス、アフリカ/ウィントフック、アメリカ/アダック、アメリカ/アンカレッジ、アメリカ/アンギラ、アメリカ/アンティグア、アメリカ/アラグァイーナ、アメリカ/アルゼンチン/ブエノスアイレス、アメリカ/アルゼンチン/カタマルカ、アメリカ/アルゼンチン/コモドーロ・リバダビア、アメリカ/アルゼンチン/コルドバ、アメリカ/アルゼンチン/フフイ、アメリカ/アルゼンチン/ラ・リオージャ、アメリカ/アルゼンチン/メンドーサ、アメリカ/アルゼンチン/リオ・ガレゴス、アメリカ/アルゼンチン/サルタ、アメリカ/アルゼンチン/サンファン、アメリカ/アルゼンチン/サンルイス、アメリカ/アルゼンチン/トゥクマン、アメリカ/アルゼンチン/ウシュアイア、アメリカ/アルバ、アメリカ/アスンシオン、アメリカ/アティコーカン、アメリカ/アトーチャ、アメリカ/バヒア、アメリカ/バヒあ・バンデラス、アメリカ/バルバドス、アメリカ/ベレン、アメリカ/ベリーズ、アメリカ/ブランサルトン、アメリカ/ボア・ビスタ、アメリカ/ボゴタ、アメリカ/ボイシ、アメリカ/ブエノスアイレス、アメリカ/ケンブリッジベイ、アメリカ/カンポグランデ、アメリカ/カンクーン、アメリカ/カラカス、アメリカ/カタマルカ、アメリカ/カイエン、アメリカ/ケイマン、アメリカ/シカゴ、アメリカ/チワワ、アメリカ/コーラル・ハーバー、アメリカ/コルドバ、アメリカ/コスタリカ、アメリカ/クレストン、アメリカ/クイアバ、アメリカ/キュラソー、アメリカ/デンマルクション、アメリカ/ドーソン、アメリカ/ドーソンクリーク、アメリカ/デンバー、アメリカ/デトロイト、アメリカ/ドミニカ、アメリカ/エドモントン、アメリカ/エイルネペ、アメリカ/エルサルバドル、アメリカ/エンセナダ、アメリカ/フォート・ネルソン、アメリカ/フォート・ウェイン、アメリカ/フォルタレザ、アメリカ/グレース・米、アメリカ/ゴットホープ、アメリカ/グース・ベイ、アメリカ/グランドターク、アメリカ/グレナダ、アメリカ/グアダルーペ、アメリカ/グアテマラ、アメリカ/グアヤキル、アメリカ/ガイアナ、アメリカ/ハリファクス、アメリカ/ハバナ、アメリカ/エルモシージョ、アメリカ/インディアナ/インディアナポリス、アメリカ/インディアナ/ノックス、アメリカ/インディアナ/マレンゴ、アメリカ/インディアナ/ピータースバーグ、アメリカ/インディアナ/テルシティ、アメリカ/インディアナ/ヴィベイ、アメリカ/インディアナ/ヴァンセンヌ、アメリカ/インディアナ/ウィナマク、アメリカ/インディアナポリス、アメリカ/イヌヴィック、アメリカ/イカルイト、アメリカ/ジャマイカ、アメリカ/フフイ、アメリカ/ジュノー、アメリカ/ケンタッキー/ルイビル、アメリカ/ケンタッキー/モンティチェロ、アメリカ/ノックス、アメリカ/クラレンダイク、アメリカ/ラパス、アメリカ/リマ、アメリカ/ロサンゼルス、アメリカ/ルイビル、アメリカ/ローワー・プリンシズ、アメリカ/マセイオ、アメリカ/マナグア、アメリカ/マナウス、アメリカ/マリゴ、アメリカ/マルティニーク、アメリカ/マタモロス、アメリカ/マサトラン、アメリカ/メンドーサ、アメリカ/メノミニー、アメリカ/メリダ、アメリカ/メトラカトラ、アメリカ/メキシコシティ、アメリカ/ミクロン島、アメリカ/モンクトン、アメリカ/モントレー、アメリカ/モンテビデオ、アメリカ/モントリオール、アメリカ/モンセラート、アメリカ/ナッソー、アメリカ/ニューヨーク、アメリカ/ニピゴン、アメリカ/ノーム、アメリカ/ノローニャ、アメリカ/ノースダコタ/ビューラ、アメリカ/ノースダコタ/センター、アメリカ/ノースダコタ/ニュー・セーラム、アメリカ/オジナガ、アメリカ/パナマ、アメリカ/パングナータング、アメリカ/パラマリボ、アメリカ/フェニックス、アメリカ/ポルトープランス、アメリカ/ポートオブスペイン、アメリカ/ポルト・アクレ、アメリカ/ポルト・ヴェーリョ、アメリカ/プエルトリコ、アメリカ/レイニーリバー、アメリカ/ランキン・インレット、アメリカ/レシフェ、アメリカ/レジーナ、アメリカ/レゾリュート、アメリカ/リオ・ブランコ、アメリカ/ロサリオ、アメリカ/サンタイザベル、アメリカ/サンタレム、アメリカ/サンチアゴ、アメリカ/サントドミンゴ、アメリカ/サンパウロ、アメリカ/スコールスビーサンド、アメリカ/シップロック、アメリカ/氏とか、アメリカ/サン・バルテルミー島、アメリカ/セント・ジョーンズ、アメリカ/セントクリストファー・ネイビス、アメリカ/セントルシア、アメリカ/セント・トーマス、アメリカ/サン・ヴィンセント、アメリカ/スウィフトカレント、アメリカ/テグシガルパ、アメリカ/スーリー、アメリカ/サンダーベイ、アメリカ/ティファナ、アメリカ/トロント、アメリカ/トルトラ、アメリカ/バンクーバー、アメリカ/バージン、アメリカ/ホワイトハウス、アメリカ/ウィニペグ、アメリカ/ヤクタート、アメリカ/イエローナイフ、南極/ケーシー、南極/デービス、南極/デュモン・デュルヴィル、南極/マックォーリー、南極/モーソン、南極/マクマルド、南極/パーマー、南極/ロゼラ、南極/南極点、南極/昭和、南極/トロール、南極/ボストーク、北極/ロングイェールビーン、アジア/アデン、アジア/アルマトイ、アジア/あんまん、アジア/アナディル、アジア/アクタウ、アジア/アクトベ、アジア/アシガバート、アジア/アシガバート、アジア/バグダッド、アジア/バーレーン、アジア/バクー、アジア/バンコク、アジア/バルナウル、アジア/ベイルート、アジア/ビシュケク、アジア/ブルネイ、アジア/カルカッタ、アジア/チタ、アジア/チョイバルサン、アジア/重慶、アジア/重慶、アジア/コロンボ、アジア/ダッカ、アジア/ダマスカス、アジア/ダッカ、アジア/ディリ、アジア/ドバイ、アジア/ドゥシャンベ、アジア/ガザ、アジア/ハルビン、アジア/ヘブロン、アジア/ホーチミンシティ、アジア/香港、アジア/ホブド、アジア/イルクーツク、アジア/イスタンブール、アジア/ジャカルタ、アジア/ジャヤプラ、アジア/エルサレム、アジア/カブール、アジア/カムチャッカ、アジア/カラチ、アジア/カシュガル、アジア/カトマンズ、アジア/カトマンズ、アジア/ハンドゥイガ、アジア/コルカタ、アジア/クラスノヤルスク、アジア/クアラルンプール、アジア/クチン、アジア/クウェート、アジア/マカオ、アジア/マカオ、アジア/マガダン、アジア/マカッサル、アジア/マニラ、アジア/マスカット、アジア/ニコシア、アジア/ノヴォクズネツク、アジア/ノヴォシビルスク、アジア/オムスク、アジア/オラル、アジア/プノンペン、アジア/ポンティアナック、アジア/平壌、アジア/カタール、アジア/クズロルダ、アジア/ラングーン、アジア/リャド、アジア/サイゴン、アジア/サハリン、アジア/サマルカンド、アジア/ソウル、アジア/上海、アジア/シンガポール、アジア/スレドネコリムスク、アジア/台北、アジア/タシケント、アジア/トビリシ、アジア/テヘラン、アジア/テルアビブ、アジア/ティンプー、アジア/ティンプー、アジア/東京、アジア/トムスク、アジア/ウジュンパンダン、アジア/ウランバートル、アジア/ウランバートル、アジア/ウルムチ、アジア/ウスチ＝ネラ、アジア/ヴィエンチャン、アジア/ウラジオストク、アジア/ヤクーツク、アジア/エカテリンブルク、アジア/エレバン、大西洋/アゾレス諸島、大西洋/バミューダ諸島、大西洋/カナリア諸島、大西洋/カーボベルデ、大西洋/フェロー諸島、大西洋/フェロー諸島、大西洋/ヤンマイエン島、大西洋/マデイラ島、大西洋/レイキャビク、大西洋/南ジョージア、大西洋/セントヘレナ、大西洋/スタンレー、オーストラリア/ACT、オーストラリア/アデレード、オーストラリア/ブリスベン、オーストラリア/ブロークンヒル、オーストラリア/キャンベラ、オーストラリア/カリー、オーストラリア/ダーウィン、オーストラリア/ユークラ、オーストラリア/ホバート、オーストラリア/LHI、オーストラリア/リンデマン、オーストラリア/ロード・ハウ、オーストラリア/メルボルン、オーストラリア/NSW、オーストラリア/ノース、オーストラリア/パース、オーストラリア/クイーンズランド、オーストラリア/サウス、オーストラリア/シドニー、オーストラリア/タスマニア、オーストラリア/ヴィ

クトリア、オーストラリア/ウエスト、オーストラリア/ヤンコウィナ、ブラジル/アクレ、ブラジル/デ・ノローニャ、ブラジル/イースト、CET、CST6CDT、カナダ/アトランティック、カナダ/セントラル、カナダ/イーストサスカチュワン、カナダ/イースタン、カナダ/マウンテン、カナダ/ニューファンドランド、カナダ/パシフィック、カナダ/サスカチュワン、カナダ/ユーコン、チリ/コンチネンタル、チリ/イースター島、キューバ、EET、EST、EST5EDT、エジプト、Eire、その他/GMT、その他/GMT+0、その他/GMT+1、その他/GMT+10、その他/GMT+11、その他/GMT+12、その他/GMT+2、その他/GMT+3、その他/GMT+4、その他/GMT+5、その他/GMT+6、その他/GMT+7、その他/GMT+8、その他/GMT+9、その他/GMT-0、その他/GMT-1、その他/GMT-10、その他/GMT-11、その他/GMT-12、その他/GMT-13、その他/GMT-14、その他/GMT-2、その他/GMT-3、その他/GMT-4、その他/GMT-5、その他/GMT-6、その他/GMT-7、その他/GMT-8、その他/GMT-9、その他/GMT0、その他/グリニッジ、その他/UCT、その他/UTC、その他/ユニバーサル、その他/ズールー、ヨーロッパ/アムステルダム、ヨーロッパ/アンドラ、ヨーロッパ/アストラハン、ヨーロッパ/アテナ、ヨーロッパ/ベルファスト、ヨーロッパ/ベルグラード、ヨーロッパ/ベルリン、ヨーロッパ/ブラティスラヴァ、ヨーロッパ/ブリュッセル、ヨーロッパ/ブカレスト、ヨーロッパ/ブダペスト、ヨーロッパ/ビュージンゲン、ヨーロッパ/キシナウ、ヨーロッパ/コペンハーゲン、ヨーロッパ/ダブリン、ヨーロッパ/ジブラルタル、ヨーロッパ/ガーンジー、ヨーロッパ/ヘルシンキ、ヨーロッパ/マン島、ヨーロッパ/イスタンブール、ヨーロッパ/ジャージー、ヨーロッパ/カリーニングラード、ヨーロッパ/キエフ、ヨーロッパ/キロフ、ヨーロッパ/リスボン、ヨーロッパ/リュブリャナ、ヨーロッパ/ロンドン、ヨーロッパ/ルクセンブルク、ヨーロッパ/マドリード、ヨーロッパ/マルタ、ヨーロッパ/マリエハムン、ヨーロッパ/ミンスク、ヨーロッパ/モナコ、ヨーロッパ/モスクワ、ヨーロッパ/ニコシア、ヨーロッパ/おスロー、ヨーロッパ/パリ、ヨーロッパ/ポドゴリツァ、ヨーロッパ/プラハ、ヨーロッパ/リガ、ヨーロッパ/ローマ、ヨーロッパ/サマラ、ヨーロッパ/サンマリノ、ヨーロッパ/サラエボ、ヨーロッパ/シンフェロポリ、ヨーロッパ/スコピエ、ヨーロッパ/ソフィア、ヨーロッパ/ストックホルム、ヨーロッパ/タリン、ヨーロッパ/ティラーナ、ヨーロッパ/ティラスポリ、ヨーロッパ/ウリヤノフスク、ヨーロッパ/ウージュホロド、ヨーロッパ/ファドゥーツ、ヨーロッパ/バチカン、ヨーロッパ/ウィーン、ヨーロッパ/ヴィリニュス、ヨーロッパ/ヴォルゴグラード、ヨーロッパ/ワルシャワ、ヨーロッパ/ザグレブ、ヨーロッパ/ザポリージャ、ヨーロッパ/チューリッヒ、英国、英国エア、GMT、GMT+0、GMT-0、GMT0、グリニッジ、HST、香港、アイスランド、インド洋/アンタナナリボ、インド洋/チャゴス、インド洋/クリスマス諸島、インド洋/ココス、インド洋/コモロ諸島、インド洋/ケルゲレン諸島、インド洋/マヘ島、インド洋/モルディブ、インド洋/モーリシャス諸島、インド洋/マヨット、インド洋/レユニオン、イラン、イスラエル、ジャマイカ、日本、クェゼリン、リビア、MET、MST、MST7MDT、メキシコ/バハノルテ、メキシコ/バハスル、メキシコ/一般、NZ、NZ-CHAT、ナバホ、PRC、PST8PDT、太平洋/アピア、太平洋/オークランド、太平洋/ブーゲンビル、太平洋/チャタム、太平洋/チューク諸島、太平洋/イースター島、太平洋/エファテ島、太平洋/エンダーベリー島、太平洋/ファカオフォ島、太平洋/フィジー、太平洋/フナフティ島、太平洋/ガラパゴス諸島、太平洋/ガンビア、太平洋/ガダルカナル、太平洋/グアム、太平洋/ホノルル、太平洋/ジョンストン、太平洋/キリスィマスィ、太平洋/コスラエ、太平洋/クェゼリン、太平洋/マジュロ、太平洋/マルキーズ諸島、太平洋/ミッドウェー島、太平洋/ナウル、太平洋/ニウエ、太平洋/ノーフォーク、太平洋/ヌメア、太平洋/パゴパゴ、太平洋/パラオ、太平洋/ピトケアン、太平洋/ポンペイ、太平洋/ポナペ、太平洋/ポートモレスビー、太平洋/ラロトンガ、太平洋/サイパン、太平洋/サモア、太平洋/タヒチ、太平洋/タラワ、太平洋/トンガタプ、太平洋/トラック、太平洋/ウェーキ、太平洋/ウォリス、太平洋/ヤップ、ポーランド、ポルトガル、ROC、ROK、シンガポール、トルコ、UCT、米国/アラスカ、米国/アリューシャン、米国/アリゾナ、米国/セントラル、米国/東インディアナ、米国/イースタン、米国/ハワイ、米国/インディアナスターク、米国/ミシガン、米国/マウンテン、米国/パシフィック、米国/パシフィックニュー、米国/サモア、UTC、ユニバーサル、W-SU、WET、ズールー

リストからタイム ゾーンを選択します。

# UserInterface 設定

## UserInterface Accessibility IncomingCallNotification

画面表示を強調した着信コールの通知を利用できます。画面と Touch 10 は約 1 秒ごと (1.75 Hz) に赤と白に点滅し、聴覚が不自由なユーザが着信コールに気づきやすくするようにしています。システムが通話中の場合、進行中の通話の妨げになるため画面は点滅しません、その代わり、通常の通知が画面とタッチパネルに表示されます。

必要なユーザ ロール : ADMIN、INTEGRATOR、USER

デフォルト値 : Default

値スペース : AmplifiedVisuals/Default

AmplifiedVisuals : ビデオ システムが着信したときに画面とタッチパネル上での画面表示の強調を有効にします。

Default : スクリーンとタッチパネル上での通知を使用したデフォルトの動作を有効にします。

## UserInterface Branding AwakeBranding Colors

ビデオシステムがブランドカスタマイズによりセットアップされている場合、この設定は、ビデオシステムが起動している時に表示されるロゴの色に影響します。ロゴをフルカラーで表示するか、あるいはバックグラウンドや画面上のその他の要素と自然になじむように、ロゴの不透明度を低減するかどうか選択できます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値スペース : 自動/ネイティブ

自動 : ロゴの不透明度は低減されます。

ネイティブ : ロゴはフルカラーです。

## UserInterface ContactInfo Type

ユーザ インターフェイスで表示する連絡先の種類を選択します。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/DisplayName/E164Alias/H320Number/H323Id/IPv4/IPv6/None/SipUri/SystemName

Auto : 他のシステムがこのシステムに到達するためにダイヤルする必要があるアドレスを表示します。アドレスはデフォルトのコール プロトコルおよびシステム登録によって異なります。

None : どのようなコンタクト情報も表示しません。

IPv4 : システムの IPv4 アドレスを示します。

IPv6 : システムの IPv6 アドレスを示します。

H323Id : システムの H.323 ID を表示します (H323 H323Alias ID の設定を参照) 。

H320Number : 連絡先情報としてシステムの H.320 番号を表示します (Cisco TelePresence ISDN リンクを使用している場合のみサポート) 。

E164Alias : 連絡先情報としてシステムの H.323 E164 エイリアスを表示します (H323 H323Alias E164 の設定を参照) 。

SipUri : システムの SIP URI を表示します (SIP URI の設定を参照) 。

SystemName : システム名を表示します (SystemUnit Name の設定を参照) 。

DisplayName : システムの表示名を表示します (SIP DisplayName の設定を参照) 。

## UserInterface CustomMessage

アウェイク モードのとき、スクリーンの下部左側にカスタム メッセージを表示することができます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: ""

値スペース : 文字列 (0, 128)

カスタム メッセージを追加します。カスタム メッセージを削除するには空の文字列を追加します。

## UserInterface KeyTones Mode

テキストまたは数値を入力する際に、キーボード クリック効果音 (キー トーン) が鳴るようにシステムを設定できます。

必要なユーザ ロール : admin、user

デフォルト値 : On

値スペース : Off/On

Off : キー トーンは再生されません。

On : キー トーンがオンになります。

## UserInterface Features Call Start

ユーザインターフェイスからデフォルトの通話終了ボタンを削除するかどうかを選択します。設定はボタンだけを削除し、機能などは削除しません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値のスペース: 自動/非表示

自動: デフォルトボタンをユーザ インターフェイスに表示します。

非表示 : デフォルトボタンをユーザ インターフェイスから削除します。

## ユーザーインターフェース機能コールの MidCallControls

ユーザインターフェイスからデフォルトの保留、転送、および通話再開ボタンを削除するかどうかを選択します。設定はボタンだけを削除し、機能などは削除しません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値のスペース: 自動/非表示

自動: デフォルトボタンをユーザ インターフェイスに表示します。

非表示 : ユーザ インターフェイスからデフォルトボタンを削除します。

## ユーザーインターフェース機能コール開始

ユーザーインターフェイスから、デフォルトの通話ボタン (ディレクトリ、お気に入り、および直近の通話リスト) 、さらにデフォルトの着信追加参加者ボタンを削除するかどうかを選択します。設定はボタンだけを削除し、機能などは削除しません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値のスペース: 自動/非表示

自動: デフォルトボタンをユーザ インターフェイスに表示します。

非表示 : ユーザ インターフェイスからデフォルトボタンを削除します。

## UserInterface Features Call VideoMute

ユーザーインターフェイスにデフォルトの[ビデオをオフにする]ボタンを表示するかどうかを選択します。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値のスペース: 自動/非表示

自動 : この機能が継続的な通話でサポートされている場合、ユーザーインターフェイスに[ビデオをオフにする]ボタンが表示されます。

非表示 : [ビデオをオフにする]ボタンはユーザーインターフェイスに表示されません。

## UserInterface Features HideAll

ユーザ インターフェイスからデフォルトボタンを削除するかどうかを選択します。設定はボタンだけを削除し、機能などは削除しません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : False

値スペース : False/True

偽: すべてのデフォルトボタンをユーザ インターフェイスに表示します。

真: すべてのデフォルトボタンをユーザ インターフェイスから削除します。

## UserInterface Features Share Start

ユーザ インターフェイスから、デフォルトボタンおよび、通話中と通話中以外両方のコンテンツの共有とプレビュー用もその他の UI 要素を削除するかどうかを選択します。設定はボタンと UI 要素だけを削除し、機能などは削除しません。Proximity または Cisco Webex Teams アプリを使ってコンテンツの共有は可能です。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値のスペース: 自動/非表示

自動: デフォルトボタンと UI 要素をユーザ インターフェイスに表示します。

非表示: デフォルトボタンと UI 要素をユーザ インターフェイスから削除します。

## UserInterface Language

ユーザ インターフェイスで使用される言語を選択します。該当する言語がサポートされていない場合、デフォルトの言語 (英語) が使用されます。

必要なユーザ ロール : admin、user

デフォルト値 : English

値スペース : Arabic/Catalan/ChineseSimplified/ChineseTraditional/Czech/Danish/Dutch/English/EnglishUK/Finnish/French/FrenchCanadian/German/Hebrew/Hungarian/Italian/Japanese/Korean/Norwegian/Polish/Portuguese/PortugueseBrazilian/Russian/Spanish/SpanishLatin/Swedish/Turkish

リストから言語を選択します。

## UserInterface OSD EncryptionIndicator

暗号化インジケータが画面に表示される時間の長さを定義します。暗号化された通話のアイコンは、ロックされた南京錠です。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/AlwaysOn/AlwaysOff

Auto : コールが暗号化されている場合は、「コールは暗号化されています (Call is encrypted) 」という通知が 5 秒間表示されます。その後、通話の残りの部分では暗号化インジケータ アイコンが表示されます。

コールが暗号化されていない場合は、「コールは暗号化されていません (Call is not encrypted) 」という通知が 5 秒間表示されます。暗号化インジケータ アイコンは表示されません。

AlwaysOn : 「コールは暗号化されています (Call is encrypted) 」という通知が 5 秒間表示されます。その後、通話の残りの部分では暗号化インジケータ アイコンが表示されます。

AlwaysOff : 暗号化インジケータは画面上に表示されません。

## UserInterface OSD HalfwakeMessage

カスタム メッセージは、システムが起動中の状態のとき、メインスクリーンの中央に表示できます。カスタム メッセージは、ビデオ システムの使用開始方法の指示を与えるデフォルト メッセージに置き換えられます。カスタム メッセージを追加せずにデフォルト メッセージを削除することもできます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 128)

カスタム メッセージ。空の文字列 : デフォルト メッセージを復元します。空白のみ : メッセージは一切表示されません。

## UserInterface OSD Output

オンスクリーン用の情報とインジケータ (OSD) を表示するモニタを定義します。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値スペース : Auto

自動 : オンスクリーン用の情報とインジケータをシステムの画面に送信します。

## ユーザーインターフェース電話帳モード

この設定は、ユーザーが連絡先をディレクトリに追加または変更したり、お気に入りリストをビデオシステムのユーザ インターフェイスに追加または変更可能かどうかを決定します。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : [読み取り/書き込み (Read-write) ]

値スペース : ReadOnly/ReadWrite

読み取り専用 : 連絡先をお気に入りリストに追加したり、お気に入りリストの連絡先を編集したりできません。また、通話前にディレクトリやお気に入りリストから連絡先を編集することはできません。

読み取り/書き込み : 連絡先をお気に入りリストに追加したり、お気に入りリストの連絡先を編集したりできます。また、通話前にディレクトリやお気に入りリストから連絡先を編集することができます。

## UserInterface Security Mode

この設定では、重要なシステム情報 (例、ビデオ システムの連絡先情報や IP アドレス、タッチ コントローラ、および UCM/VCS レジストラ) がユーザ インターフェイス (ドロップダウン メニューと設定パネル) で公開されるのを防ぐことができます。設定パネルに移動するとこのような情報は非表示になっていないので注意してください。

管理者権限を持たない人に連絡先情報、IP アドレス、MAC アドレス、シリアル番号およびソフトウェアのバージョンを絶対に公開しない場合は、[ユーザ インターフェイス設定メニュー モード (UserInterface SettingsMenu Mode) ] を [ロック (Locked) ] に設定します。また、管理者権限を持つすべてのユーザ アカウントにパスフレーズを設定することも必要です。

必要なユーザ ロール : ADMIN

デフォルト値 : Normal

値スペース : Normal/Strong

Normal : IP アドレスやその他のシステムの情報がユーザ インターフェイスに表示されます。

Strong : 連絡先情報および IP アドレスは、ユーザ インターフェイス (ドロップ ダウン メニューと設定パネル) に表示されません。

## UserInterface SettingsMenu Mode

ビデオ システムの管理者パスワードによって、ユーザ インターフェイス (Touch 10 または画面) の設定パネルを保護することができます。このパスワードが空白の場合、誰でも設定パネルの設定にアクセスできます (例、システムを初期設定へリセット) 。認証を有効にすると、認証を必要とするすべての設定に南京錠のアイコンが表示されます。設定を選択するときに、管理者のユーザ名とパスフレーズを入力するよう求められます。認証が必須でない設定には、南京錠のアイコンが表示されません。

必要なユーザ ロール : ADMIN

デフォルト値 : Unlocked

値スペース : Locked/Unlocked

Locked : 管理者のユーザ名とパスフレーズによる認証が必要です。

Unlocked : 認証は必要ありません。

## UserInterface SettingsMenu Visibility

システム名 (または連絡先情報) と、関連のあるドロップダウンメニューや設定パネルをユーザインターフェイスの左上隅に表示するかどうかを選択します。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値のスペース: 自動/非表示

自動 : システム名をロップダウンメニューと設定パネルと共に、ユーザ インターフェイスの左上隅に表示します。

非表示 : システム名をロップダウンメニューと設定パネルと共に、ユーザ インターフェイスの左上隅に表示しません。

## UserInterface Sounds Mode

このバージョンでは適用されません。

必要なユーザ ロール : ADMIN、USER

## UserInterface Wallpaper

アイドル状態のときのビデオ画面の背景画像（壁紙）を選択します。

ウェブ インターフェイスを使用してビデオシステムにカスタムの壁紙をアップロードできます。サポートされるファイル形式は BMP、GIF、JPEG、PNG です。最大ファイル サイズは 4 MByte です。カスタム壁紙を使用すると、予定されている会議のクロックおよび一覧がメイン ディスプレイから削除されます。

必要なユーザ ロール： ADMIN、INTEGRATOR、USER

デフォルト値：Auto

値スペース：Auto/Custom/None

[自動（Auto）]：デフォルトの壁紙を使用します。

None：画面に背景イメージはありません。

Custom：画面の背景画像としてカスタムの壁紙を使用します。カスタム壁紙がシステムにアップロードされていない場合、設定がデフォルト値に戻ります。

## UserInterface UsbPromotion

USB カメラとしてビデオシステムを使用できることを知らせるテキストを、ハーフウェイク画面に表示するかどうかを選択します。

必要なユーザ ロール：ADMIN

デフォルト値：Off

値スペース：Off/On

オフ：USB カメラの情報テキストは表示されません。

オン：USB カメラの情報テキストが表示されます。

## UserInterface WebcamOnlyMode

このビデオシステムは web カメラとして、通常のビデオシステムとして使用できます。オンプレミスまたはクラウドコールサービス（CUCM、VCS、Webex など）に登録されていない場合でも、web カメラとして使用できます。

この設定では、ビデオシステムが登録されていないシナリオの場合に、ユーザインターフェイスを web カメラのみのシナリオに適応させるかどうかを決定します。

必要なユーザ ロール：ADMIN

デフォルト値：Auto

値スペース：Auto/Off

自動：ビデオシステムがコールサービスに登録されている場合、完全なユーザインターフェイスが表示されます。ビデオシステムが登録されていないためにコールに使用できない場合、無関係のユーザインターフェイス要素は削除されます。

オフ：システムには常に完全なユーザインターフェイスが表示されます。

# UserManagement の設定

## UserManagement LDAP Admin Filter

LDAP フィルタは、管理者権限が付与されるユーザを判別するために使用します。

LDAP 管理者グループまたは LDAP 管理者フィルタをつねに設定する必要があります。ユーザーー管理 LDAP 管理者フィルタが設定されている LDAP Admin フィルタ優先、その場合、UserManagement LDAP Admin グループの設定は無視されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0, 1024)

この文字列の構文については、LDAP の仕様を参照してください。例 : "(| (memberof CN admin group、OU = company grouips、DC = company、DC = com) (sAMAccountName=username))」

## UserManagement LDAP Admin Group

この AD (Active Directory) グループのメンバーには、管理者権限が付与されます。この設定は、memberOf:1.2.840.113556.1.4.1941:=<group name> の短縮形です。

LDAP 管理者グループまたは LDAP 管理者フィルタをつねに設定する必要があります。ユーザーー管理 LDAP 管理者フィルタが設定されている LDAP Admin フィルタ優先、その場合、UserManagement LDAP Admin グループの設定は無視されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

AD グループの識別名。例 : "CN=admin group, OU=company groups, DC=company, DC=com"

## UserManagement LDAP Attribute

提供されるユーザ名へのマッピングに使用される属性。設定しない場合は、sAMAccountName が使用されます。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

属性名。

## UserManagement LDAP BaseDN

検索を開始するエントリの識別名 (ベース) 。

必要なユーザ ロール : ADMIN

デフォルト値: ""

値スペース : 文字列 (0..255)

ベースの識別名。例 : "DC=company, DC=com"

## UserManagement LDAP Encryption

ビデオ システムと LDAP サーバとの間の通信を保護する方法を定義します。ポート番号は、UserManagement LDAP Server Port 設定を使用してポート番号をオーバーライドできます。

必要なユーザ ロール : ADMIN

デフォルト値 : LDAPS

値スペース : LDAPS/None/STARTTLS

LDAPS : ポート 636 over TLS (Transport Layer Security) 上の LDAP サーバに接続します。

None : ポート 389 上の LDAP サーバに接続します (暗号化なし) 。

STARTTLS : ポート 389 上の LDAP サーバに接続し、次に STARTTLS を送信して TLS 暗号化を有効にします。

## UserManagement LDAP MinimumTLSVersion

許可する最低バージョンの TLS (Transport Layer Security) プロトコルを設定します。

必要なユーザ ロール : ADMIN
デフォルト値 : TLSv1.2

値スペース : TLSv1.0/TLSv1.1/TLSv1.2
TLSv1.0 : TLS バージョン 1.0 以上をサポートします。
TLSv1.1 : TLS バージョン 1.1 以上をサポートします。
TLSv1.2 : TLS バージョン 1.2 以上をサポートします。

## UserManagement LDAP Mode

ビデオ システムは、LDAP (Lightweight Directory Access Protocol) サーバを、ユーザ名とパスワードを一元的に保存および検証する場所として使用することをサポートします。この設定を使用して、LDAP 認証を使用するかどうか設定します。実装は、Microsoft Active Directory (AD) サービスでテスト済みです。

LDAP モードでスイッチする場合、設定に合わせたユーザ管理 LDAP 設定の構成を確認してください。いくつかの例を示します。

例 1 :

- ユーザ管理 LDAP モード : On
- ユーザ管理 LDAP アドレス : "192.0.2.20"
- ユーザ管理 LDAP ベース DN : "DC=company, DC=com"
- ユーザ管理 LDAP 管理グループ : "CN admin group、OU = company grouips、DC = company、DC = com"

例 2 :

- ユーザ管理 LDAP モード : On
- ユーザ管理 LDAP アドレス : "192.0.2.20"
- ユーザ管理 LDAP ベース DN : "DC=company, DC=com"
- ユーザ管理 LDAP 管理フィルタ : "(| (memberof CN admin group、OU = company grouips、DC = company、DC = com)(sAMAccountName=username))」

必要なユーザ ロール : ADMIN
デフォルト値 : Off

値スペース : Off/On
Off : LDAP 認証は許可されません。
On: LDAP 認証は許可されます。

## UserManagement LDAP Server Address

LDAP サーバの IP アドレスまたはホスト名を設定します。

必要なユーザ ロール : ADMIN
デフォルト値: ""

値スペース : 文字列 (0..255)
有効な IPv4 アドレス、IPv6 アドレス、またはホスト名。

## UserManagement LDAP Server Port

LDAP サーバに接続するポートをオンに設定します。0 に設定した場合は、選択したプロトコルのデフォルトを使用します (「UserManagement LDAP Encryption 設定」を参照) 。

必要なユーザ ロール : ADMIN
デフォルト値: 0

値スペース : 整数 (0..65535)
LDAP サーバのポート番号。

## UserManagement LDAP VerifyServerCertificate

ビデオ システムを LDAP サーバに接続すると、サーバはビデオ システムに証明書を提示して身元を示します。この設定は、ビデオ システムがサーバの証明書を確認するかどうかを決定するために使用します。

必要なユーザ ロール : ADMIN
デフォルト値 : On

値スペース : Off/On
Off : ビデオ システムは LDAP サーバの証明書を検証しません。
On : ビデオ システムは、LDAP サーバの証明書が信頼できる認証局 (CA) によって署名されているか必ず検証します。システムにアップロードする信頼できる CA の一覧に、その CA を事前に追加する必要があります。ビデオ システムの ウェブ インターフェイスを使用して、信頼できる CA の一覧を管理します (詳細については、管理者ガイドを参照) 。

# ビデオ設定

## Video ActiveSpeaker DefaultPIPPosition

通話中のスピーカーを示すピクチャインピクチャ (PiP) の画面上の位置を定義します。この設定は、通話中のスピーカーを PiP 表示するビデオ レイアウト (オーバーレイ レイアウト) を使用している場合にのみ有効です。また、場合によっては、カスタム レイアウトでも有効です (「Video DefaultLayoutFamily Local の設定」を参照) 。この設定は、次回以降のコールで有効になります。コール中に変更された場合、現在のコールへの影響はありません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Current

値スペース : Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current : 通話中のスピーカーの PiP の位置はコール終了後にも変更されません。

UpperLeft : 通話中のスピーカーの PiP が画面の左上隅に表示されます。

UpperCenter : 通話中のスピーカーの PiP が画面の上部中央に表示されます。

UpperRight : 通話中のスピーカーの PiP が画面の右上隅に表示されます。

CenterLeft : 通話中のスピーカーの PiP が画面の左中央に表示されます。

CenterRight : 通話中のスピーカーの PiP が画面の右中央に表示されます。

LowerLeft : 通話中のスピーカーの PiP が画面の左下隅に表示されます。

LowerRight : 通話中のスピーカーの PiP が画面の右下隅に表示されます。

## Video DefaultLayoutFamily Local

ローカルで使用するビデオ レイアウト ファミリを選択します。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/Equal/Prominent/Overlay/Single

Auto : システムによって提供されるローカル レイアウト データベースに指定されたデフォルト レイアウト ファミリがローカル レイアウトとして使用されます。

Equal : Equal レイアウト ファミリがローカル レイアウトとして使用されます。画面上に十分なスペースがある限り、すべてのビデオのサイズは等しくなります。

Prominent : [対象拡大表示 (Prominent) ] レイアウト ファミリがローカル レイアウトとして使用されます。通話中のスピーカー、または (存在する場合) プレゼンテーションは大きい画像となり、他の参加者は小さい画像となります。通話中のスピーカーが遷移するとき、音声が切り替えられます。

Overlay : [オーバーレイ (Overlay) ] レイアウト ファミリがローカル レイアウトとして使用されます。通話中のスピーカー、または (存在する場合) プレゼンテーションは全画面表示となり、他の参加者は小さいピクチャ イン ピクチャ (PiP) となります。通話中のスピーカーが遷移するとき、音声が切り替えられます。

Single : 通話中のスピーカー、または (存在する場合) プレゼンテーションは全画面表示となります。他の参加者は表示されません。通話中のスピーカーが遷移するとき、音声が切り替えられます。

## Video DefaultLayoutFamily Remote

リモート参加者 (遠く) に送信されるストリーミングで使用するビデオ レイアウト ファミリを選択します。この設定は、ビデオ システム内蔵の MultiSite 機能 (オプション) を使用してマルチポイントのビデオ会議をホストする場合にのみ適用されます。

必要なユーザ ロール : ADMIN

デフォルト値 : Auto

値スペース : Auto/Equal/Prominent/Overlay/Single

Auto : ローカル レイアウト データベースによって指定される、デフォルト レイアウト ファミリが、リモート レイアウトとして使用されます。

Equal : Equal レイアウト ファミリがリモート レイアウトとして使用されます。画面上に十分なスペースがある限り、すべてのビデオのサイズは等しくなります。

Prominent : Prominent レイアウト ファミリがリモート レイアウトとして使用されます。通話中のスピーカー、または (存在する場合) プレゼンテーションは大きい画像となり、他の参加者は小さい画像となります。通話中のスピーカーが遷移するとき、音声が切り替えられます。

Overlay : [オーバーレイ (Overlay) ] レイアウト ファミリがリモート レイアウトとして使用されます。通話中のスピーカー、または (存在する場合) プレゼンテーションは全画面表示となり、他の参加者は小さいピクチャ イン ピクチャ (PiP) となります。通話中のスピーカーが遷移するとき、音声が切り替えられます。

Single : 通話中のスピーカー、または (存在する場合) プレゼンテーションは全画面表示となります。他の参加者は表示されません。通話中のスピーカーが遷移するとき、音声が切り替えられます。

## Video DefaultMainSource

発信を開始する際にデフォルトのメイン ビデオ ソースとして使用されるビデオ入力ソースを定義します。

必要なユーザ ロール : admin、user

デフォルト値: 1

値スペース : 1

デフォルトのメイン ビデオ ソースとして使用されるソース。

## Video Input Connector [n] CameraControl CameraId

n: 1..2

カメラ ID は、このビデオ入力に接続されているカメラの一意の ID です。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Connector n: 1 (コネクタ n : 1)

設定可能な値: Connector n: 1 (コネクタ n : 1)

カメラ ID は固定されており、変更できません。

## Video Input Connector [n] CameraControl Mode

n: 1..2

このビデオ入力コネクタに接続されているカメラを制御するかどうかを定義します。

カメラ制御はコネクタ 2 (HDMI) では使用できないことに注意してください。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Connector 1 : On Connector 2 : Off

値スペース : Connector 1 : Off/On Connector 2 : Off

Off : カメラ制御をディセーブルにします。

On : カメラ制御をイネーブルにします。

## Video Input Connector [n] CEC Mode

n: 2..2

ビデオ入力 (HDMI) は、Consumer Electronics Control (CEC) をサポートします。この設定を有効にすると、接続デバイスの情報 (デバイスの種類やデバイス名) がビデオ システム ステータスで使用可能になります (ビデオ入力コネクタ [n] 接続デバイス CEC [n]) 。ただし、接続デバイスは CEC もサポートすることが条件となります。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : On

設定可能な値: Connector n: Off/On

Off : CEC が無効になります。

On : CEC が有効になります。

## Video Input Connector [n] InputSourceType

n: 1..2

ビデオ入力に接続された入力ソースのタイプを選択します。
コネクタ 1 はシステムの内蔵カメラであることに注意してください。

必要なユーザ ロール : ADMIN、INTEGRATOR
デフォルト値 : Connector 1 : camera Connector 2 : PC

値スペース : Connector 1 : camera Connector 2 : PC/camera/document_camera/mediaplayer/whiteboard/other

PC : コンピュータがビデオ入力に接続されている場合に使用します。
camera : カメラがビデオ入力に接続されている場合に使用します。
document_camera : ドキュメント カメラがビデオ入力に接続されている場合に使用します。
mediaplayer : メディア プレーヤーがビデオ入力に接続されている場合に使用します。
whiteboard : ホワイトボード カメラがビデオ入力に接続されている場合に使用します。
other : 他のオプションが当てはまらない場合に使用します。

## Video Input Connector [n] Name

n: 1..2

ビデオ入力コネクタの名前を定義します。

必要なユーザ ロール : ADMIN、INTEGRATOR
デフォルト値 : Connector 1 : "Camera" Connector 2 : PC

値スペース : 文字列 (0, 50)
ビデオ入力コネクタの名前。

## Video Input Connector [n] OptimalDefinition Profile

n: 1..2

この設定は、対応する Video Input Connector [n] Quality 設定が Sharpness に設定されている場合には無効です。

最適鮮明度プロファイルは、ビデオ会議室の照明状態とカメラと品質を反映します。光の条件およびカメラの品質が優れているほど、プロファイルが高くなります。通常、Norma] または Medium プロファイルが推奨されます。ただし、光の条件が良い場合、特定のコール率の解像度を大きくするために、High プロファイルを設定できます。解像度は、発呼側と着信側の両方のシステムでサポートされている必要があります。

必要なユーザ ロール : ADMIN、INTEGRATOR
デフォルト値 : Medium

値スペース : Normal/Medium/High

Normal : 照明が通常から不良の環境には、このプロファイルを使用します。解像度は控えめに設定されます。
Medium : 安定した光条件および高品質なビデオ入力が必要です。一部のコール レートの場合、これは高解像度へ移動できます。
High : 優れた全体的なエクスペリエンスを実現するには、理想に近いビデオ会議の光の状態および高品質なビデオ入力が必要です。相当高い解像度が使用されます。

## Video Input Connector [n] PreferredResolution

n: 2..2

ビデオ システムに HDMI 経由でシステムに接続したソース デバイス (例 : ラップトップ) の推奨解像度として通知されている画面の解像度とリフレッシュ レートを定義します。送信元デバイス (ラップトップのディスプレイ設定ソフトウェア) によって手動で上書きされない限り、解像度とリフレッシュ レートはソース側の解像度の選択に関するロジックによって自動的に選択されます。

2560_1440_60 と 3840_2160_30 のフォーマットは、1920_1080_60 フォーマットと比較すると約 2 倍の量のデータを使用し、HDMI 1.4b データレート以上に対応したプレゼンテーション ケーブル (またはアダプタ) を必要とします。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Connector n : 1920_1080_60

設定可能な値: Connector n: 1920_1080_60/2560_1440_60/3840_2160_30

1920_1080_60 : 解像度は 1920 X 1080、リフレッシュ レートは 60 Hz です。

2560_1440_60 : 解像度は 2560 X 1440、リフレッシュ レートは 60 Hz です。

3840_2160_30 : 解像度は 3840 X 2160、リフレッシュ レートは 30 Hz です。

## Video Input Connector [n] PresentationSelection

n: 2..2

ビデオ入力にプレゼンテーション ソースを接続するときの、ビデオ システムの動作を定義します。

ビデオ システムがスタンバイ モードである場合、プレゼンテーション ソースを接続すると起動します。遠端とプレゼンテーションを共有するには、この設定が AutoShare に設定されていなければ、追加操作 (ユーザ インターフェイスで [共有 (Share) ] を選択) が必要です。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: Connector n: OnConnect

設定可能な値: Connector n: AutoShare/Desktop/Manual/OnConnect （自動共有/デスクトップ/手動/接続上）

AutoShare : 通話時に、ビデオ入力のコンテンツは、ケーブルを接続するかまたはソースが有効になると (たとえば接続されているコンピュータがスリープ モードから復帰するなど) 、自動的に遠端とローカル画面に表示されます。ユーザ インターフェイス上で [共有 (Share) ] を選択する必要はありません。コールの発信時または応答時にプレゼンテーション ソースがすでに接続されている場合は、ユーザ インターフェイス上で [共有 (Share) ] を手動で選択する必要があります。

Desktop : ビデオ入力のコンテンツは、ケーブルを接続するかまたはソースが有効になると (たとえば接続されているコンピュータがスリープ モードから復帰するなど) 、画面に表示されます。これは、アイドル状態のときと通話中のときの両方に適用されます。また、ビデオ入力のコンテンツは、通話の終了時にアクティブ入力であれば、画面に表示されたままとなります。

Manual : ユーザ インターフェイスで [共有 (Share) ] を選択するまでビデオ入力の内容は画面に表示されません。

OnConnect : ビデオ入力のコンテンツは、ケーブルを接続するかまたはソースが起動すると (たとえば接続されているコンピュータがスリープ モードから復帰するなど) 、画面に表示されます。それ以外の場合は、Manual モードと同じ動作です。

## Video Input Connector [n] Quality

n: 2..2

ビデオのエンコーディングと送信のときには、高解像度と高フレーム レートとの間にトレード オフが存在します。一部のビデオ ソースでは、高フレーム レートが高解像度より重要である場合や、逆の場合もあります。この設定で、高フレーム レートと高解像度のどちらを優先するかを指定します。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: Connector n: Sharpness

設定可能な値: Connector n: Motion/Sharpness

Motion : できるだけ高いフレーム レートにします。通常、多数の参加者がいる場合や画像の動きが激しい場合など、高フレーム レートが必要なときに使用されます。

Sharpness : できるだけ高い解像度にします。詳細なイメージやグラフィックに高い品質が必要な場合に使用されます。

## Video Input Connector [n] RGBQuantizationRange

n: 2..2

ビデオ入力に接続されたデバイスは CEA-861 で規定されている RGB ビデオ量子化範囲の規則に従う必要があります。残念ながら、一部のデバイスは規格に準拠していません。その場合、ソースの完全なイメージを取得するために、この設定を使用して設定を上書きできます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Auto

値スペース : Auto/Full/Limited

Auto : RGB 量子化範囲は CEA-861-E に従ったビデオ形式に基づいて自動的に選択されます。CE ビデオ形式は、限定された量子化範囲レベルを使用します。IT ビデオ形式は、完全な量子化範囲レベルを使用します。

Full : 完全な量子化の範囲。R、G、B の量子化範囲にはすべてのコード値 (0 ～ 255) が含まれます。これは CEA-861-E で規定されています。

Limited : 限定された量子化の範囲。極端なコード値を除いた R、G、B の量子化範囲 (16 ～ 235) 。これは CEA-861-E で規定されています。

## Video Input Connector [n] Visibility

n: 1..2

ユーザ インターフェイスのメニューにあるビデオ入力コネクタの表示を定義します。

コネクタ 1 はシステムの内蔵カメラであり、プレゼンテーション ソースとして使用できないことに注意してください。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Connector 1: Never Connector 2: Always

値スペース : Connector 1: Never Connector 2: Always/IfSignal/Never

Always : ビデオ入力コネクタ用メニュー選択は、ユーザ インターフェイスに常に表示されます。

IfSignal : ビデオ入力コネクタ用メニュー選択は、ビデオ入力に何か接続されている場合のみ表示されます。

Never : 入力の送信元はプレゼンテーション ソースとして使用されないため、ユーザ インターフェイスに表示されません。

## Video Output Connector [n] CEC Mode

n: 1..1

ビデオ出力 (HDMI) は、Consumer Electronics Control (CEC) をサポートします。

この設定が [オン (On) ] の場合、システムはシステム自体がスタンバイに移行する際、画面をスタンバイ状態に設定するために CEC を使用します。同様に、システムがスタンバイから復帰するとき、システム自身が画面を起動します。

画面のアクティブなビデオ入力がユーザによって変更されることがあります。発信が開始されると、ビデオ システムはアクティブなビデオ入力が画面の別の入力に切り替えられたかどうかを検出します。すると、ビデオ システムは入力を切り戻すため、ビデオ システムがアクティブなビデオ入力ソースになります。ビデオ システムがスタンバイ状態に入るときにビデオ システムがアクティブな入力ソースでない場合、画面はスタンバイに設定されません。

出力に接続した画面に CEC 互換性があること、および CEC が画面上で有効であることが必須条件です。

CEC については、製造業者によって異なるマーケティング名称が使用されていることに注意してください。例 : Anynet+ (Samsung) 、Aquos Link (シャープ) 、BRAVIA Sync (Sony) 、HDMI-CEC (日立) 、Kuro Link (パイオニア) 、CE-Link および Regza Link (東芝) 、RIHD (オンキョー) 、HDAVI Control、EZ-Sync、VIERA Link (Panasonic) 、EasyLink (Philips) 、NetCommand for HDMI (三菱) 。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : On

値スペース : Off/On

Off : CEC が無効になります。

On : CEC が有効になります。

## Video Output Connector [n] MonitorRole

n: 1..1

適用なし

## Video Output Connector [n] Resolution

n: 1..1

接続している画面の解像度とリフレッシュ レートを定義します。

1920_1200_60 より大きなフォーマットには、高品質なディスプレイ ケーブルを使用する必要があります。動作を保証するには、3840_2160_60 で使用するように Cisco によってあらかじめ認定されたディスプレイ ケーブルを使用するか、「プレミアム HDMI 認定」プログラムに合格したケーブルをご使用ください。

UHD テレビおよび画面には、3840_2160_30 (30 Hz) のみしか使用できないものもありますが、3840_2160_60 (60 Hz) はデフォルト設定ではありません。このような場合、テレビと画面の関連設定で、ビデオ システムが接続されている HDMI 入力として 3840_2160_60 を許可するように再設定する必要があります。

必要なユーザ ロール : ADMIN、INTEGRATOR、USER

デフォルト値 : Connector n: Auto

値スペース : Auto/1920_1080_50/1920_1080_60/1920_1200_50/1920_1200_60/2560_1440_60/3840_2160_30/3840_2160_60

Auto : システムは接続されたモニタのネゴシエーションに基づいて自動的に最適な解像度の設定を試行します。

1920_1080_50 : 解像度は 1920 X 1080、リフレッシュ レートは 50 Hz です。

1920_1080_60 : 解像度は 1920 X 1080、リフレッシュ レートは 60 Hz です。

1920_1200_50 : 解像度は 1920 X 1200、リフレッシュ レートは 50 Hz です。

1920_1200_60 : 解像度は 1920 X 1200、リフレッシュ レートは 60 Hz です。

2560_1440_60 : 解像度は 2560 X 1440、リフレッシュ レートは 60 Hz です。

3840_2160_30 : 解像度は 3840 X 2160、リフレッシュ レートは 30 Hz です。

3840_2160_60 : 解像度は 3840 X 2160、リフレッシュ レートは 60 Hz です。

## Video Output Connector [n] RGBQuantizationRange

n: 1..1

HDMI 出力に接続されたデバイスは CEA-861 で規定されている RGB ビデオ量子化範囲の規則に従う必要があります。残念ながら、一部のデバイスは規格に準拠していません。その場合、ディスプレイの完全なイメージを取得するために、この設定を使用して設定を上書きできます。ほとんどの HDMI ディスプレイはフルの量子化範囲を想定しています。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Full

値スペース : Auto/Full/Limited

Auto : RGB の量子化の範囲は、AVI インフォフレームの RGB 量子化範囲ビット (Q0、Q1) に基づいて自動的に選択されます。AVI インフォフレームが使用できない場合、RGB 量子化範囲は CEA-861-E に従ったビデオ形式に基づいて選択されます。

Full : 完全な量子化の範囲。R、G、B の量子化範囲にはすべてのコード値 (0 ～ 255) が含まれます。これは CEA-861-E で規定されています。

Limited : 限定された量子化の範囲。極端なコード値を除いた R、G、B の量子化範囲 (16 ～ 235) 。これは CEA-861-E で規定されています。

## Video Presentation DefaultPIPPosition

プレゼンテーションのピクチャインピクチャ (PiP) の画面上の位置を定義します。この設定は、たとえばユーザ インターフェイスを使用して、プレゼンテーションが明示的に PiP に縮小された場合にのみ有効です。この設定は、次回以降のコールで有効になります。コール中に変更された場合、現在のコールへの影響はありません。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Current

値スペース : Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current : プレゼンテーション PiP の位置はコール終了後にも変更されません。

UpperLeft : プレゼンテーション PiP が画面の左上隅に表示されます。

UpperCenter : プレゼンテーション PiP が画面の上部中央に表示されます。

UpperRight : プレゼンテーション PiP が画面の右上隅に表示されます。

CenterLeft : プレゼンテーション PiP が画面の左中央に表示されます。

CenterRight : プレゼンテーション PiP が画面の右中央に表示されます。

LowerLeft : プレゼンテーション PiP が画面の左下隅に表示されます。

LowerRight : プレゼンテーション PiP が画面の右下隅に表示されます。

## Video Presentation DefaultSource

デフォルトのプレゼンテーション ソースとして使用するビデオ入力ソースを定義します。この設定は、API およびサード パーティのユーザ インターフェイスで使用できます。Cisco が提供するユーザ インターフェイスの使用時には関係ありません。

必要なユーザ ロール : admin、user

デフォルト値 : 2

値スペース : 1/2

デフォルトのプレゼンテーション ソースとして使用するビデオ入力ソース。

## Video Presentation Priority

帯域幅がメインビデオチャネルとプレゼンテーションチャネル間で分散される方法を決定します。

必要なユーザ ロール : ADMIN

デフォルト値: 等しい

値スペース: 等しい/高/低

利用可能なビデオ伝送帯域幅がメイン チャネルとプレゼンテーション チャネルの間で分散されます。

高 : プレゼンテーションチャネルは、メインビデオチャネルを犠牲にして、利用可能な帯域の大部分に割り当てられます。

低 : メインビデオチャネルは、プレゼンテーションチャネルを犠牲にして、利用可能な帯域の大部分に割り当てられます。

## Video Selfview Default FullscreenMode

コール終了後に、メイン ビデオ ソース (セルフビュー) を全画面表示するか、小さいピクチャインピクチャ (PiP) として表示するかを定義します。この設定はセルフビューがオンになっている場合にのみ有効です (Video Selfview Default Mode の設定を参照) 。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Current

値スペース : Off/Current/On

Off : セルフビューは PiP として表示されます。

Current : セルフビューの画像のサイズはコール終了時に未変更の状態に保たれます。つまりコール中に PiP であった場合はコール終了後にも PiP のままであり、コール中に全画面であった場合はコール終了後にも全画面のままです。

On : セルフビューの画像は全画面表示されます。

## Video Selfview Default Mode

コール終了後にメイン ビデオ ソース (セルフビュー) を画面に表示するかどうかを定義します。セルフビュー ウィンドウの位置とサイズはそれぞれ、Video Selfview Default PIPPosition と Video Selfview Default FullscreenMode の設定によって決まります。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Current

値スペース : Off/Current/On

Off : セルフビューはコール退出時にオフにされます。

Current : セルフビューはそのままの状態で残ります。つまりコール中にオンであった場合はコール終了後にもオンのままであり、コール中にオフであった場合はコール終了後にもオフのままです。

On : セルフビューはコール退出時にオンにされます。

## Video Selfview Default OnMonitorRole

コールの後にメイン ビデオ ソース (セルフビュー) を表示する画面/出力を設定します。この値は、異なる出力用に設定された Video Output Connector [n] MonitorRole 設定のモニタ ロールを反映します。

この設定は、セルフ ビューが全画面で表示されたとき、およびセルフビューがピクチャインピクチャ (PiP) で表示されたときの両方に適用されます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Current

値スペース : Current/First/Second

Current : コールを中止すると、セルフビュー画像がコール中と同じ出力上に維持されます。

First : セルフビュー画像は、Video Output Connector [n] MonitorRole が First に設定された出力上に表示されます。

Second : セルフビュー画像は、Video Output Connector [n] MonitorRole が Second に設定された出力上に表示されます。

## Video Selfview Default PIPPosition

コール終了後に小さいセルフビュー ピクチャインピクチャ (PiP) を表示する画面上の位置を定義します。この設定は、セルフビューがオンになっており (Video Selfview Default Mode 設定を参照) 、全画面表示がオフになっている場合 (Video Selfview Default FullscreenMode 設定を参照) にのみ有効です。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : Current

値スペース : Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current : セルフビュー PiP の位置はコール終了後にも変更されません。

UpperLeft : セルフビュー PiP が画面の左上隅に表示されます。

UpperCenter : セルフビュー PiP が画面の上部中央に表示されます。

UpperRight : セルフビュー PiP が画面の右上隅に表示されます。

CenterLeft : セルフビュー PiP が画面の左中央に表示されます。

CenterRight : セルフビュー PiP が画面の右中央に表示されます。

LowerLeft : セルフビュー PiP が画面の左下隅に表示されます。

LowerRight : セルフビュー PiP が画面の右下隅に表示されます。

## Video Selfview OnCall Mode

コールをセットアップする短い間、この設定を使用してセルフ ビューがオンにされます。セルフビューをオンのままにしておく時間の長さは、Video Selfview OnCall Duration 設定で定義します。これは一般にセルフ ビューがオフの場合に適用されます。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値 : On

値スペース : Off/On

Off : セルフ ビューはコール セットアップ中に自動的に表示されません。

On : セルフ ビューはコール セットアップ中に自動的に表示されます。

## Video Selfview OnCall Duration

この設定は Video Selfview OnCall Mode 設定がオンになっている場合にのみ有効です。この場合、ここで設定された秒数により、自動的にオフにされる前にセルフ ビューが表示される期間が決まります。

必要なユーザ ロール : ADMIN、INTEGRATOR

デフォルト値: 10

値スペース : 整数 (1..60)

範囲 : セルフ ビューをオンにする期間を選択します。有効な範囲は、1 ～ 60 秒です。

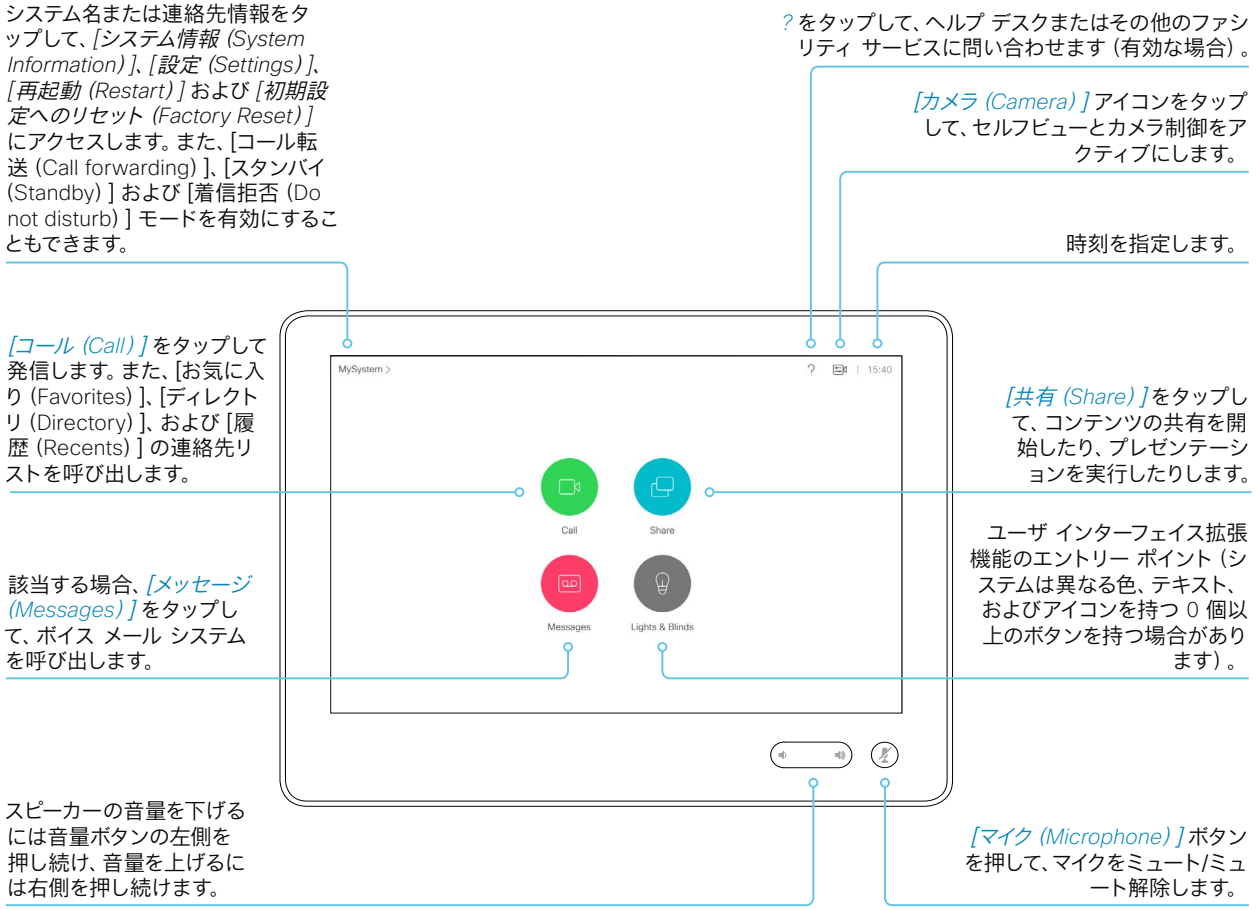
# 試験的設定

試験的設定は、テストのためだけのもので、Cisco と同意したのでない限り使用できません。これらの設定は記載されておらず、以降のリリースで変更されます。

# 付録

# Touch 10 の使用方法

Touch 10 ユーザ インターフェイスとその使用方法の詳細については、ビデオ システムのユーザ ガイドを参照してください。



# USB カメラとしての Room Kit Mini の使用

ビデオシステムが USB カメラとして使用されている可能性があります。このモードでは、次の用途が使用します。

- ビデオシステムのカメラ
- ビデオシステムのマイク
- ビデオシステムのラウドスピーカー
- 必要に応じて、ビデオシステムに接続されている画面
- サードパーティクライアント*を使用しているコンピュータ

ビデオシステムがコールサービス (クラウドまたはオンプレミス) に登録されている場合、システムは通常のビデオシステムとして、および USB カメラとしての両方で使用できます。システム自体が、何が接続されているかに基づいて、どのモードになるかを決定します。

ビデオシステムがコールサービスに*登録されていない*場合でも、システムを USB カメラとして使用できます。

## セットアップと構成

管理者は、特別な設定を行わなくても、ビデオシステムを USB カメラとしてセットアップすることができます。

ただし、次のように一部のカスタマイズと*USBカメラのみ*のセットアップに対する適用を行うことができます。

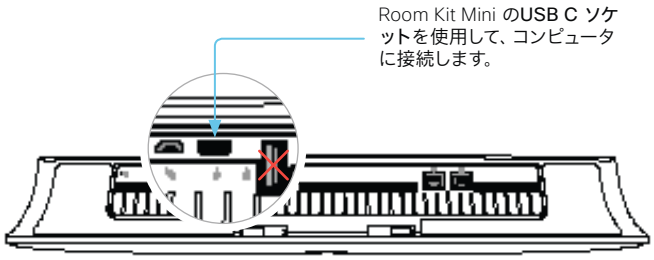
- 初回のセットアップウィザードには、ビデオシステムを USB デバイスとしてのみ使用するオプションが用意されています。このオプションを選択するときは、コールサービス (クラウドまたはオンプレミス) の登録を省略します。
- ビデオシステムがコールサービスに登録されていない場合は、*UserInterface > WebcamOnlyMode* 設定を使用して、ユーザインターフェイスを USB カメラのみのシナリオに適応させることができます。

  Touch 10 に対して完全なユーザインターフェイスを保持するか、またはコールサービスに登録されていない場合に不適切な要素を削除するかを選択できます。

* たとえば、Microsoft Teams、Skype for Business、Slack、Zoom などがあります。Cisco は製品の発売前にこれらのクライアントを正常にテストしています。異なるソフトウェアバージョン間の互換性は、定期的にはテストされません。

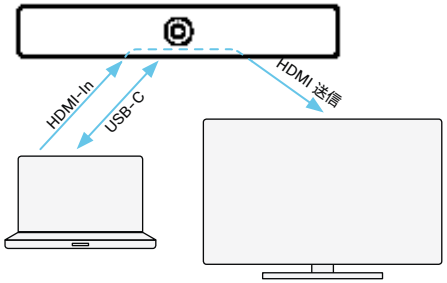
## USB-C に接続する

USB カメラとして使用するには、次に示すように、システムがコンピューターに接続されていて、接続がアクティブになっている必要があります (コンピュータはスリープモードではいけません)。




Touch 10 からカメラと音量を制御できます。その他の機能は、使用しているコンピュータ上のサードパーティクライアントによって制御されます。

### ビデオシステムに接続されている画面を使用します。




**USB-C**

- ビデオシステムのカメラおよびマイクからのビデオとオーディオをコンピュータークライアントへ
- コンピュータクライアントからの音声をビデオシステムのスピーカーへ

**HDMI インおよび HDMI 送信:**

- ビデオシステムを介してコンピュータクライアント (far end) から画面にビデオを再生します。

## ビデオ解像度

サポートされるビデオ解像度

- 720p
- 1080p

## 最小要件

最小 USB バージョン:

- USB 2.0

最小のコンピュータオペレーティングシステム:

- Windows 7
- OS X 10.6

# リモート モニタリングのセットアップ

要件:

- *RemoteMonitoring* オプション

リモート モニタリングは別の場所からビデオ システムを制御する場合に便利です。

入力ソースからのスナップショットが ウェブ インターフェイスに表示されるため、部屋にいなくてもカメラ ビューをチェックしてカメラを制御できます。

有効にすると、スナップショットは約 5 秒おきに自動的に更新されます。


## ビデオ システムに *RemoteMonitoring* オプションがあるかどうかを確認する

1. ウェブ インターフェイスにログインします。
2. [ホーム (Home) ] ページで、インストールされているオプションのリストに *RemoteMonitoring* が含まれているかどうかを確認します。

   リストにない場合、リモート モニタリングは使用できません。

## リモート モニタリングを有効にする

*RemoteMonitoring* オプション キーをインストールします。オプション キーのインストール方法については、►「オプション キーを追加する」の章で説明しています。

リモート モニタリング オプションを有効にする場合は、プライバシーに関する地域の法律および規制を遵守する必要があります。また、システム管理者がカメラや画面を監視および制御する場合があることを、システムのユーザに適切な方法で通知してください。システムの使用時にプライバシー規制を遵守するのはお客様の責任であり、Cisco はこの機能の違法な使用について一切の責任を否認します。

## スナップショットについて

### ローカル入力ソース

ビデオ システムのローカル入力ソースのスナップショットは [コール制御 (Call Control) ] ページに表示されます。

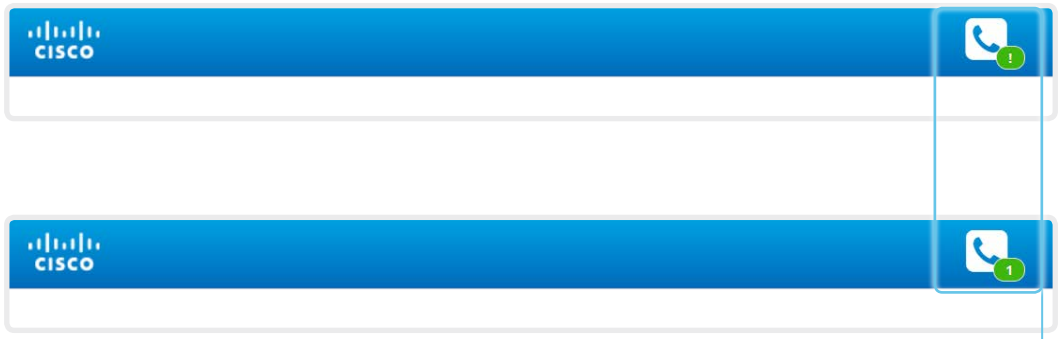
スナップショットは、ビデオ システムがアイドル状態のときにも、通話中にも表示されます。

### 遠端のスナップショット

通話中の場合、遠端カメラからのスナップショットも表示できます。遠端ビデオ システムに [リモート モニタリング (RemoteMonitoring) ] オプションがあるかどうかは問題ではありません。

遠端スナップショットは、コールが暗号化されていると表示されません。

# ウェブ インターフェイスを使用したコール情報へのアクセスとコール応答



## 着信通知

*[コールインジケーター (Call indicator)]* をクリックし、コールの応答と拒否を行う *[コール操作 (Call Control)]* ページを開きます。

## システムが通話中

バッジはアクティブ コール数を示します。

## コールインジケーター

コールインジケーターでは着信の通知表示と、システムが通話中になる時を表示します。

システムが待機状態の場合、コールインジケーターは表示されません。

## コールの操作

*[コール操作 (Call Control)]* ページでは、コール操作に関係する操作ボタンが表示されます。各ボタンを使用して次のことを実行します。

- コールの詳細を表示する
- コールを保留にする
- 通話に応答します。
- コールを切断する

# ウェブ インターフェイスを使用してコールをかける (1/2 ページ)

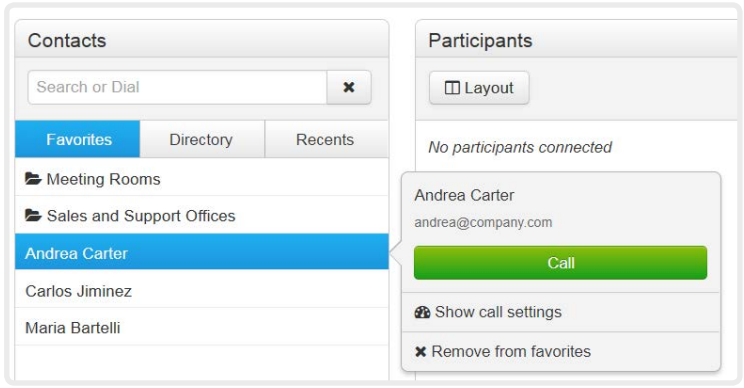
ウェブ インターフェイスにログインし、*[コール制御 (Call Control) ]* に移動します。

## コールの発信

ウェブ インターフェイスを使ってコールを開始した場合でも、コールに使用されるのはビデオ システム (ディスプレイ、マイクおよびスピーカー) であり、ウェブ インターフェイスを実行する PC ではありません。

1. 正しいエントリを見つけるには、*[お気に入り (Favorites) ]* リスト、*[ディレクトリ (Directory) ]* リスト、または *[発着信履歴 (Recents) ]* リストに移動するか、あるいは [検索またはダイヤル (*Search or Dial*) ] フィールドに 1 文字以上を入力します*。該当する連絡先名をクリックします。
2. 連絡先カードで *[コール (Call) ]* をクリックします。

または、[検索して発信 (Search and Dial) ] フィールドに完全な URI または番号を入力します。次に、URI または番号の横に表示される *[コール (Call) ]* ボタンをクリックします。




* 検索時には、入力内容に応じて、[お気に入り (Favorites) ]、[ディレクトリ (Directory) ]、および [履歴 (Recents) ] リストの一致するエントリが表示されます。

### DTMF トーンの送信

アプリケーションが DTMF (デュアルトーン多重周波数) シグナリングを必要とする場合は、クリックしてキー パッドを開きます。


### コールの詳細の表示/非表示

情報ボタンをクリックすると、コールの詳細情報が表示されます。

もう一度ボタンをクリックすると情報が非表示になります。

### コールの保留および復帰

参加者を保留にするには、その名前の横にある ⏸ ボタンを使用します。

コールを再開するには、保留中の参加者に表示される ▶ ボタンを使用します。

### コールの終了

コールまたは会議を終了するには、*[全通話切断 (Disconnect all) ]* をクリックします。表示されるダイアログで選択内容を確認します。

1 人の参加者のみコールを終了するには、その参加者の 📞 ボタン をクリックします。

# ウェブ インターフェイスを使用してコールをかける (2/2 ページ)

ウェブ インターフェイスにログインし、*[コール制御 (Call Control) ]* に移動します。

## 複数の相手に発信

ポイントツーポイントのビデオ コール (2 者間限定のコール) を拡張して、音声専用でもう 1 人の参加者を増やすことができます。

オプションの組み込み MultiSite 機能をシステムで使用している場合は、本人も含めて最大 4 人までがビデオ コール (会議) に参加できます。 最初の参加者を呼び出したときと同じ手順で、次の会議参加者を呼び出してください。

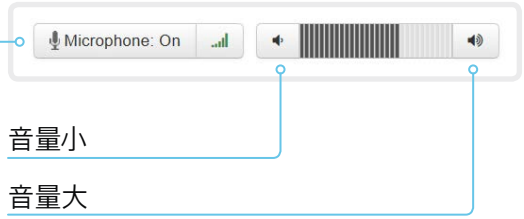
会議ブリッジを使用した複数のコール (CUCM のアドホック会議) は、ビデオ システムでサポートされていても ウェブ インターフェイスではサポートされません。

## 音量の調整

### マイクをミュートにする

*[マイク: オン (Microphone: On) ]* をクリックして、マイクをミュートにします。すると、テキストが *[マイク: オフ (Microphone: Off) ]* に変わります。

ミュートを解除するには、*[マイク: オフ (Microphone: Off) ]* をクリックします。



# ウェブ インターフェイスを使用してコンテンツを共有する

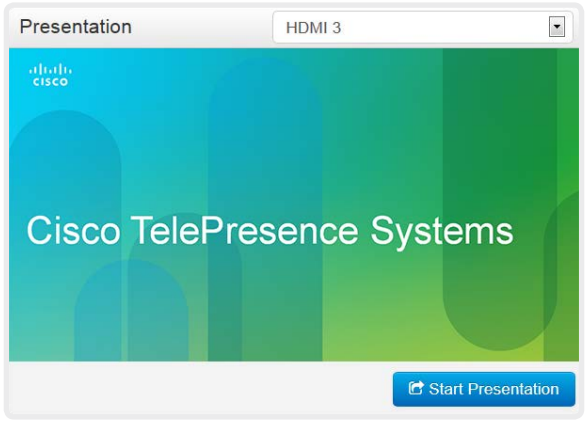
ウェブ インターフェイスにログインし、*[コール制御 (Call Control)]* に移動します。

## コンテンツの共有

1. *[プレゼンテーションの開始 (Start Presentation)]* をクリックします。すると、テキストが *[プレゼンテーションの停止 (Stop Presentation)]* に変わります。

**コンテンツ共有の停止：**

共有している間に表示される *[プレゼンテーションを中止 (Stop Presentation)]* ボタンをクリックします。




### スナップショット領域

選択されたプレゼンテーション ソースのスナップショットが表示されます。

*リモート モニタリング* オプションがあるビデオシステムでのみ利用できます。

## コンテンツ シェアリング (共有) について

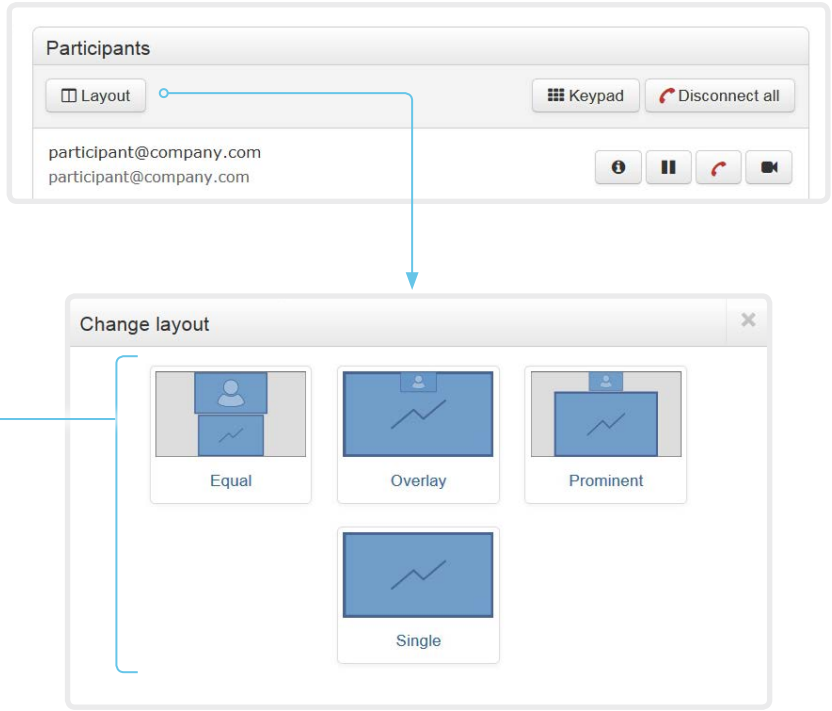
プレゼンテーション ソースは、ビデオ入力またはお使いのビデオ システムに接続することができます。プレゼンテーション ソースとして最も多く使用されるのは PC ですが、システムの設定によってはその他のオプションを使用できる場合があります。

通話中に、他の参加者 (相手先) とコンテンツを共有できます。

コール (通話) 中でない場合は、コンテンツはローカルに表示されます。

# ローカル レイアウトの制御

ウェブ インターフェイスにログインし、*[コール制御 (Call Control) ]* に移動します。




## レイアウトの変更

*[レイアウト (Layout) ]* をクリックし、表示されるウィンドウで望ましいレイアウトを選択します。

選択するレイアウトのセットは、システム設定によって異なります。

レイアウトは、アイドル中でも通話中でも変更可能です。

## レイアウトについて

ここでいうレイアウトとは、プレゼンテーションとビデオを画面に表示するさまざまな方法のことです。会議の種類によって、レイアウトを変える必要があります。

通話や会議の参加者の数は、選択肢に反映されます。

# ローカル カメラの制御

ウェブ インターフェイスにログインし、*[コール制御 (Call Control) ]* に移動します。

## 前提条件

- *[ビデオ (Video) ] > [入力 (Input) ] > [コネクタ n (Connector n) ] > [カメラ制御 (CameraControl) ] > [モード (Mode) ]* 設定が **[オン (On) ]** になっている。
- カメラにパン、チルト、またはズーム機能が付いている。
- スピーカーのトラッキングはオフです。

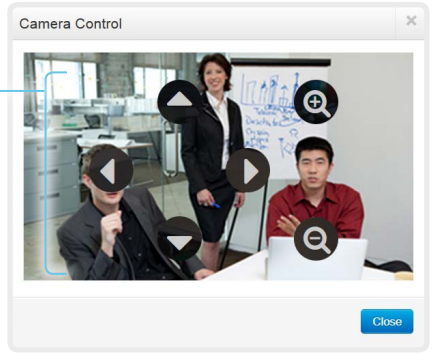
## スナップショット領域

メイン入力ソースのスナップショットが表示されます。

*リモート モニタリング* オプションがあるビデオ システムでのみ利用できます。

## スナップショットを自動更新する


## パン/チルト/ズーム コントロールを使用したカメラの移動




最高概要をオンにすると、カメラ制御は使用できません。

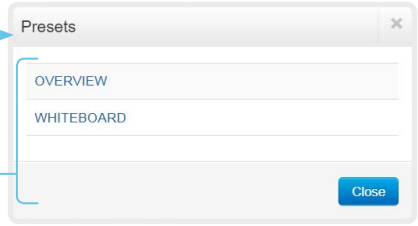
1. カメラ アイコンをクリックして、カメラ制御ウィンドウを開きます。

   部屋からのビデオ スナップショットは、*リモート モニタリング* オプションがあるビデオシステムにのみ表示されます。

2. カメラのパンには左右の矢印キー、チルトには上下の矢印キー、ズームインとズームアウトには + および - を使用します。

   関連するコントロールのみがウィンドウに表示されます。

3. *[Close]* をクリックして、ウィンドウを閉じます。




## カメラのプリセット位置への移動

1. *[プリセット... (Presets...) ]* をクリックして、使用可能なプリセットのリストを開きます。

   プリセットが定義されていない場合は、ボタンが無効になり、[プリセットなし (No presets) ] と表記されます。

2. プリセットの名前をクリックすると、カメラがそのプリセット位置に移動します。

3. *[Close]* をクリックして、ウィンドウを閉じます。

ウェブ インターフェイスを使用してプリセットは定義できません。タッチ コントローラを使用する必要があります。

プリセットを選択すると、最高概要は自動的にオフになります。

# 相手先カメラの制御

ウェブ インターフェイスにログインし、*[コール制御 (Call Control) ]* に移動します。

## 前提条件

以下の条件において、通話中にリモート参加者のカメラ (相手先) を制御できます。

- 遠端ビデオ システムで *[会議 (Conference) ] > [遠端制御 (FarEndControl) ] > [モード (Mode) ]* 設定が **[オン (On) ]** になっている。
- 遠端カメラにパン、チルト、ズーム機能がある。関連する制御のみ表示される。
- 遠端カメラではスピーカーのトラッキングはオンになっていない。
- ローカル ビデオ システムにリモート モニタリング オプションがある。


## リモート参加者のカメラを制御

1. リモート カメラ制御ウィンドウを開くには、カメラのアイコンをクリックします。
2. カメラのパンには左右の矢印キー、チルトには上下の矢印キー、ズームインとズームアウトには + および - を使用します。

   遠端カメラの制御が許可されていない場合は、画面にコントロールが表示されません。

   コールが暗号化されている場合、制御の背後の遠端スナップショットは表示されません。

# パケット損失の復元力：ClearPath

ClearPath により、高度なパケット損失復元メカニズムを導入できます。これらのメカニズムは、エラーを起こしやすい環境でビデオ システムを使用した場合の品質を向上させます。

ClearPath は Cisco 独自のプロトコルです。CE ソフトウェアが実行されているすべてのエンドポイントが ClearPath に対応しています。

関係するエンドポイントとインフラストラクチャ要素が ClearPath に対応している場合、ポイントツーポイント接続（ホストされた会議を含む）ですべてのパケット損失復元メカニズムが使用されます。MultiSite 会議でサポートされるのは、これらのメカニズムの一部だけです。

# ルーム分析 (1/2 ページ)

ルーム分析機能は、会議室からのいくつかの変数を使用します。また、それらの変数を再利用して、時間経過やコールのたびに部屋の使用率を分析します。

## 人の存在の検出

ビデオ システムは、人が室内にいるかどうかを見つける機能を備えています。室内に人がいるかどうかを検知するには最低 2 分かかります。部屋が空室になった後、ステータスを変更するまで最大 2 分かかることがあります。

この機能は、超音波に基づいています。室内にいた人物の記録を保持することはなく、人が部屋にいたかどうかだけを検知します。

ウェブ インターフェイスから人の存在の検出をオンまたはオフにできます。ウェブ インターフェイスにサインインして、*[セットアップ (Setup)] > [設定 (Configuration)] > [ルーム分析 (RoomAnalytics)] > [人の存在の検出 (PeoplePresenceDetector)]* に移動します。

## 人数のカウント

顔検出を使用して、ビデオ システムが室内にいる人の人数を特定できます。室内にいた人物の記録を保持することはなく、顔の平均数だけを検知します。カメラに顔を向けていない人はカウントされません。室内に物体や写真がある場合、これらも顔として検知され、カウントされる可能性があります。

信頼性の高い平均数を得るために、コール時間の長さは最低 2 分必要です。2 分未満のコールと人数のカウントが無効にされたコールでは、通話履歴を取得すると「N/A」が表示されます。

デフォルトでは、ビデオ システムは通話中のときまたはセルフ ビューに画像を表示したときにのみ人数をカウントします。

非通話中の人をカウントするように選択できます。有効にすると、ビデオ システムはビデオ システムがスタンバイ モードでない限り、人数を数えます。セルフ ビューがオフであっても、これは非通話中の人数を含みます。ウェブ インターフェイスにサインインして、*[セットアップ (Setup)] > [設定 (Configuration)] > [ルーム分析 (RoomAnalytics)] > [非通話中の人をカウント (PeopleCountOutOfCall)]* に移動します。

## Status (ステータス)

人の存在および人のカウントに関する特定の瞬間のステータスを確認することができます。ウェブ インターフェイスにサインインして、*[セットアップ (Setup)] > [ステータス (Status)] > [ルーム分析 (RoomAnalytics)]* に移動します。

## 診断

Touch 10 コントローラから SpeakerTrack 診断モードを有効にすると、画面上で実況される人数のカウンタを見ることができます。セルフ ビューをオンにしてタッチ コントローラの左上隅にある連絡先情報をタップし、*[設定 (Settings)]* メニューを開きます。*[問題と診断 (Issues & diagnostics)]* をタップし、*[SpeakerTrack の診断 (SpeakerTrack diagnostics)]* をオンにします。

## 通話履歴コマンド

コール後に、通話履歴コマンドから人々の平均数の値を抽出できます。

- `xCommand CallHistory Get DetailLevel: Full`

通話履歴コマンドは、API (Application Programming Interface) から使用できます。詳細については、お使いの製品の API リファレンス ガイドを参照してください。

▶ https://www.cisco.com/go/room-docs

# Room 分析 (2/2 ページ)

## 周囲ノイズレポート

ビデオシステムは室内の固定周囲ノイズレベルをレポートできます。レポートされた値はA荷重デシベル値(dBA)で、人間の耳の応答に反響します。この機能に関連するすべてのシグナリング処理はローカルで、転送されるデータは算出されたノイズレベルだけです。

この値はノイズレベルの異常な変化の検出に使用できます。このような変化は、室内で作業している人にとってはじゃあmであるノイズを引き起こす場合があります。施設管理はこの問題をトラブルシューティングするために迅速に介入できます。

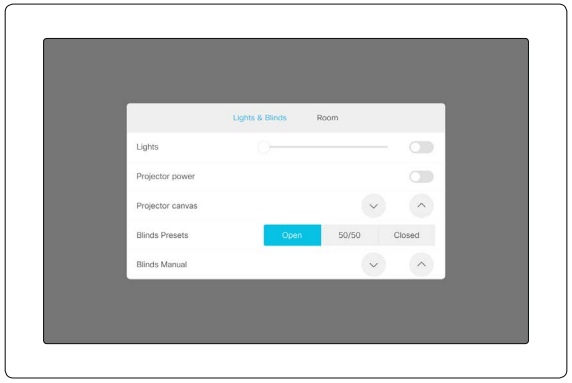
ウェブ インターフェイスから周囲ノイズの検出をオンまたはオフにできます。ウェブ インターフェイスにサインインして、*[セットアップ (Setup) ] > [設定 (Configuration) ] > [ルーム分析 (RoomAnalytics) ] > [周囲ノイズ予測 (AmbientNoiseEstimationI) ] > [モード]* に移動します。

カスタマイゼーション

# ビデオ システムの Touch 10 ユーザ インターフェイスをカスタマイズ (1/2 ページ)

照明やブラインドなど、会議室内の周辺機器の制御を許可するようにユーザ インターフェイスをカスタマイズすることができます。また、マクロをトリガーすることによってビデオ システムの動作を変更します。

これにより、制御システムの機能とビデオ システムのユーザ フレンドリーなユーザ インターフェイスとの強力な組み合わせが可能になります（Touch 10）。




室内制御パネルの例

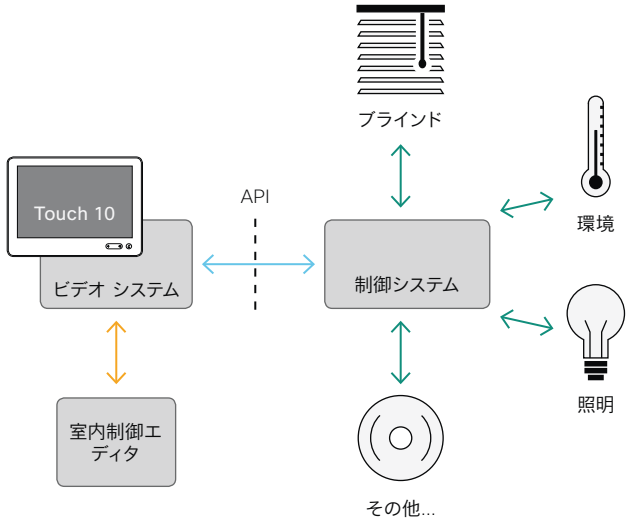
室内制御エディタを使用してカスタム ユーザ インターフェイス パネル（室内制御パネル）を設計する方法、およびビデオ システムの API を使用して室内制御をプログラミングする方法の詳細については、『*カスタマイズ ガイド*』を参照してください。次のリンクにアクセスします。

► https://www.cisco.com/go/in-room-control-docs

## 室内制御アーキテクチャ

Touch 10 コントローラおよび制御システムでは、Cisco のビデオ システムが必要です。制御システムは、ハードウェア ドライブや周辺機器を備えた Crestron や AMX などの他社製システムである場合もあります。これはビデオ システムではなく、周辺機器を制御する制御システムです。

制御システムをプログラミングする場合、ビデオ システムのユーザ インターフェイス上のコントロールを接続するために、ビデオ システムの API（イベントとコマンド）を使用する必要があります。




室内制御の概略図

ビデオ システムのマクロ フレームワークは、制御システムとしても役立つことがあります。この場合、制御システムはビデオ システムの API を使用して、短縮ダイヤル、言語の選択、カスタマイズされたシステムのリセットなど、あらゆる種類のローカル機能をトリガーすることができます。

カスタマイゼーション

# ビデオ システムの Touch 10 ユーザ インターフェイスをカスタマイズ (2/2 ページ)

## 室内制御エディタ

### 無料のエディタ

ビデオ システムのソフトウェアには、無料の使いやすいドラッグアンドドロップ エディタが付属しています。カスタム ユーザ インターフェイス パネル (室内制御パネル) の構成にはこれを使用してください。

ウェブ インターフェイスにサインイン*して、*[統合 (Integration)] > [室内制御 (In-Room Control)]* に移動します。

- *[エディタの起動 (Launch Editor)]* をクリックして、エディタをビデオ システムの ウェブ インターフェイスから直接起動します。

  新しい室内制御パネルをビデオ システムにプッシュすることができます。結果はタッチ コントローラ上に即座に表示されます。
- *[エディタをダウンロード (Download Editor)]* をクリックして、お使いのハード ドライブからブラウザでローカルに実行できるスタンドアロン バージョンをダウンロードします。

  これにより、ビデオ システムに接続せずにカスタム インターフェイスを構成できます。後でファイルをエクスポートおよびインポートして、ローカル バージョンとビデオ システム間で作業を移動することができます。

### プレビュー機能

エディタは、カスタム インターフェイスがどのようにユーザ インターフェイスに表示されるか確認するためのプレビュー機能も提供します。

プレビュー機能はお使いのカスタム (室内制御) パネルの完全なソフトウェア バージョンでもあるため、制御をクリックすると、実際の Touch 10 ユーザ インターフェイスで選択されるのと同じ動作が発生します。

したがって、実際の Touch 10 ユーザ インターフェイスで有効にすることなく、プレビュー機能を使用してお使いの統合をテストできます。離れた場所からビデオ システムの室内制御を使用することもできます。

## ルーム シミュレータ

ルーム シミュレータを使用して、Touch 10 ユーザ インターフェイスの室内制御により、室内の状態がどのように変更されたかを可視化することができます。

ビデオ システムのシミュレータ設定をエクスポートする前に、すべての既存の室内の設定をバックアップします。シミュレータ設定は、ビデオ システム上の既存の設定を置き換えます。

ウェブ インターフェイスにサインインして、*[統合 (Integration)] > [室内制御 (In-Room Control)]* に移動します。

- *[シミュレータの起動 (Launch Simulator)]* をクリックして、ルーム シミュレータをブラウザで開きます。

  ルーム シミュレータには、ビデオ システムにエクスポート可能な定義済みの室内制御設定が含まれます。つまり、実際の Touch 10 ユーザ インターフェイスから、シミュレータの仮想会議室を制御することができます。
- *[シミュレータ設定のロード (Load simulator config)]* をクリックして、ビデオ システムのシミュレータ設定をエクスポートします。

* 制御システムをプログラミングするときに必要な室内制御エディタおよび API コマンドにアクセスするには、ROOMCONTROL、INTEGRATOR、または ADMIN ユーザ ロールを持つユーザが必要です。

カスタマイゼーション

# マクロを使用したビデオ システムの動作のカスタマイズ

マクロにより、ビデオ システム上で実行するコードの独自のスニペットを作成できます。言語は、arrow functions、promises および classes などの機能をサポートする JavaScript/ECMAScript 6 です。

マクロ フレームワークを利用して、インテグレータはビデオ システムの動作を個別の顧客要件に応じて調整するスクリプトを作成することができます。インテグレータが行える作業には、独自の機能または機能のバリエーションの実装、特定の設定または再設定の自動化、機能のカスタム テストやモニタリングの作成などがあります。

マクロの使用とカスタム ユーザ インターフェイス（以前は室内制御パネルと呼ばれた）の作成を組み合わせることで、ユーザ インターフェイス（Touch 10）を修正して、カスタマイズされたローカル機能をトリガーできます。以下に例を示します。

- 短縮ダイヤルボタンの追加
- すべての設定を好みのデフォルト セットアップに戻すためのルーム リセットボタンの追加

マクロについての詳細およびビデオ システムの組み込みマクロエディタの使用方法については、 *カスタマイズ ガイド* を参照してください。次のリンクにアクセスします。

► https://www.cisco.com/go/in-room-control-docs

## ビデオ システムでのマクロの使用の許可

ウェブ インターフェイスにサインインして、*[セットアップ (Setup) ] > [設定 (Configuration) ]* に移動します。

- *[マクロ (Macros) ] > [モード (Mode) ]* を [オン (On) ] に設定します。

  この設定が [オフ (Off) ] の場合にマクロ エディタを起動しようとすると、ポップアップ メッセージが表示されます。*[マクロの有効化 (Enable Macros) ]* をタップして応答した場合は [*マクロ (Macros) ] > [モード (Mode) ]* 設定が自動的に [オン (On) ] に変更され 、エディタが起動します。

## マクロ エディタの起動

ウェブ インターフェイスにサインイン * して、*[統合 (Integration) ] > [マクロ エディタ (Macro Editor) ]* に移動します。

オフラインで使用可能なエディタのスタンドアロン バージョンは提供されていません。

## マクロ エディタ

マクロ エディタは、以下のことができる強力なツールです。

- 変更したり、そのまま使用したり、または自身のマクロを記述する際のヒントとして使用したりするコードの例をロードできます。
- 詳細なマクロ記述チュートリアルを用意しているので、参照してください。コードの例についても、より詳しく説明しています。
- 独自のマクロを記述し、ビデオ システムにアップロードできます。
- マクロは、個別に有効または無効にできます。
- マクロを実行したときの動作は、組み込みのログ コンソールで確認できます。

* マクロ エディタにアクセスするには、ADMIN ユーザ ロールを保持しているユーザが必要です。

カスタマイゼーション

# ユーザ インターフェイスからデフォルトボタンを削除する

*通話* または *共有*などのデフォルトボタンを使用しない使用例もあります。このような使用しないボタンは混乱を引き起こす場合があります。このような場合、使用しないボタンを from the ユーザ インターフェイスから削除できます。カスタムイン-ルームコントロールパネルはまだ表示されています。カスタムボタンを追加しながら、デフォルトボタンを削除すると、ユーザ インターフェイスを完全にカスタマイズできます。

例えば、誰もビデオシステムからコンテンツや通話を共有しないのであれば、*通話* や *共有* ボタンを削除できます。代わりに、実行されるタスク向けのカスタムボタン (In-Room 制御) を追加します。

## 構成

以下の設定を使ってデフォルトボタンをユーザ インターフェイスから削除します。設定はビデオシステムの ウェブ インターフェイス、および API で利用できます。

- *ユーザーインターフェイス > 機能 > 通話 > 開始*: デフォルト *通話* ボタンを削除 (ディレクトリ、お気に入り、最近の通話リストを含む) 。さらに、通話中に参加者ボタンを*追加*します。
- *ユーザーインターフェイス > 機能 > 通話 > ビデオミュート*: デフォルト *ビデオをオフにする* ボタンを削除します。
- *ユーザーインターフェイス > 機能 > 共有 > 開始*: 通話中および通話中以外の両方で、コンテンツの共有およびプレビュー用のデフォルトユーザ インターフェイスを削除します。
- *ユーザーインターフェイス > 機能 > すべて非表示*: すべてのデフォルトボタンを削除します。In-Room Control パネルは削除されません。
- *ユーザーインターフェイス > 機能 > 通話 > 終了*: *通話終了* ボタンを削除します。
- *ユーザーインターフェイス > 機能 > 通話 > MidCallControls*: *保留*、*再開*、および *転送* 通話中ボタンを削除します。

設定はボタンだけを削除し、機能などは削除しません。*共有* ボタンをユーザーインターフェイスから削除しても、Proximity を使用してコンテンツを共有できます。

## 解説場所

ボタンの削除方法およびユーザインターフェイスのカスタマイズi方法については *カスタマイズガイド*を参照してください。 次のリンクにアクセスします。

► https://www.cisco.com/go/in-room-control-docs

カスタマイゼーション

# サードパーティ USB 入力デバイスの使用

サードパーティー USB 入力デバイスを使用してビデオシステムの特定の機能を制御できます。USB ドングルや USB キーボードでの Bluetooth リモート制御はこのような入力デバイスの一例です。

この機能は、Touch 10 または DX ユーザ インターフェイス、いずれか便利な方の機能の補正を意味しています。Touch 10とDXのユーザ インターフェイスを交換するという意味ではありません。

適用例

- 教室や授業中では、小型リモート制御を使用してビデオシステムをスタンバイモードから起動するのに使用します。また、表示する入力ソースを選択するためにリモート制御を使用するのも便利です。
- Touch 10 を使用できない状況でのカメラビュー（パン、チルト、ズーム）の制御例えば、病院の手術室。

## 機能の概要

USB 入力デバイスのボタンを押すと、イベントが API に生成されます。マクロあmたはサードパーティーの制御デバイスはこのようなイベントをリッスンし、応答することが可能です。この挙動は、In-Room Control ボタンの挙動に似ています。ウェブフックを使って、直接SSH セッションでイベントをリッスンすることも可能です。

アクション選択からすぐに利用できるアクションのライブラリはありません。ご自身で、イベントに対する応答として行うアクションを定義して実装する必要があります。次に例を示します。

- [音量アップ]キーが押されたら、ビデオシステムの音量を上げます。
- [スリープ]キーが押されたら、ビデオシステムをスタンバイモードにします。

## 設定、イベント、およびステータス

USB 入力デバイスのサポートはデフォルトで無効になっています。*周辺機器 > InputDevice > モード* を **オン**に設定することで明示的に有効にします。

ボタンを押してから離すと、押されたおよびリリースされたイベントが作成されます：

```
*e UserInterface InputDevice Key アクションキー: <キーの名前>
*e UserInterface InputDevice Key アクションコード: <キーの ID>
*e ユーザーインターフェイス InputDevice Key アクションタイプ:押された
** end
*e UserInterface InputDevice Key アクションキー: <キーの名前>
*e UserInterface InputDevice Key アクションキー: <キーの ID>
*e ユーザーインターフェイス InputDevice Key アクションタイプ:リリースされた
** end
```

イベントをリッスンするには、InputDevice イベントからのフィードバックを登録する必要があります。

```
xFeedback Register /event/UserInterface/InputDevice
** end
```

ルームデバイスがサードパーティー入力デバイスを検出すると、入力デバイスはルームデバイス *ユーザーインターフェイス > 周辺機器 > ConnectedDevice* ステータスにリストされます。入力デバイスは複数のデバイスとして報告される場合があります。

## 必要な工具

- Cisco Webex Room Series または DX シリーズからのシステム
- 自体を USB キーボードとしてアドバタイズするサードパーティー入力デバイス。例えば、USB ドングル付きの Bluetooth リモート制御。

## 解説場所

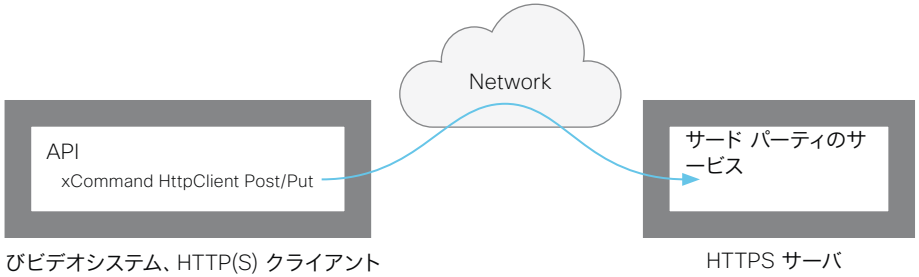
サードパーティー入力デバイスの利用についての詳細は、 *カスタマイズガイド*をご覧ください。 次のリンクにアクセスします。

► https://www.cisco.com/go/in-room-control-docs

Cisco support (TAC) はマクロを含む、サードパーティーコードのデバッグに対応していません。マクロやサードパーティーコードについてのヘルプは、►Cisco Collaboration Developer コミュニティ を確認してください。

カスタマイゼーション

# HTTPs Post および Put 要求の送信




この機能は任意の HTTP(S) ポストおよびプットリクエストをビデオシステムから HTTP(S) サーバに送信することができます。

マクロを使用することで、いつでもデータを HTTP(S) サーバに送信できます。送信するデータを選択して、お好きなように構築することが可能です。このようにすれば、データをすでに確立されているサービスに適用できます。

セキュリティ対策：

- このHTTP(S) ポスト/プット機能はデフォルトで無効に設定されています。システム管理者は *HttpClient > モード* を オンに設定することでこの機能を明示的に有効にする必要があります。
- システム管理者は *HttpClient > AllowHTTP* を 偽に設定することで HTTP の使用を防ぐことができます。
- システム管理者は、デバイスがデータを送信可能な先であるHTTP(S) サーバのリストを指定できます。
- 同時に行えるポストとプットリクエストの数は制限されています。

## 許容されている HTTP(S) サーバのリスト

システム管理者はコマンドを使用して最大 10 の許容されている HTTP(S) サーバ (ホスト)のリストを設定し維持できます：

- `xCommand HttpClient` はホスト名追加表現を許容します：`<HTTP(S)` サーバのホスト名または `IP` アドレスに一致する正規表現`>`
- `xCommand HttpClient` はホスト名の消去を許容します
- `xCommand HttpClient` はホスト名リストを許容します
- `xCommand HttpClient` はホスト名削除 `ID` を許容します：`<`リスト内のエントリーの `ID>`

リストが空でない場合、HTTP(S) リクエストをリスト内のサーバにだけ送信できます。リストが空の場合、リクエストを任意の HTTP(S) サーバに送信できます。

許容されているサーバのリストに対するチェックは、非セキュア (HTTP) およびセキュア (HTTPS) なデータ転送の両方で実行されます。

## 証明書検証なしの HTTPS の許可

リクエストを HTTPS 経由で送信する場合、ビデオシステムはデフォルトにより HTTPS サーバの証明書をチェックします。HTTPS サーバ証明書が有効でない場合、 エラーメッセージが表示されます。ビデオシステムはサーバにデータを送信しません。

HTTPS は証明書検証とともに使用することを推奨します。これが不可能な場合は、システム管理者は *HttpClient > AllowInsecureHTTPS* を オンに設定します。これにより、HTTPS の使用がサーバ証明書を検証しなくても可能になります。

## HTTP(S) 要求の送信

HTTP(S) クライアントポスト機能が有効になると、以下のコマンドを使用して Post および Put リクエストを HTTP(S) サーバに送信できます：

- `xCommand HttpClient Post [AllowInsecureHTTPS:` `<`真/偽`>] [`ヘッダー：`<`ヘッダーテキスト`>]`
  `Url:` `<`リクエストの送信先の `URL>`
- `xCommand HttpClient Post [AllowInsecureHTTPS:` `<`真/偽`>] [`ヘッダー：`<`ヘッダーテキスト`>]`
  `Url:` `<`リクエストの送信先の `URL>`

複数行コマンドがありますAPI ガイドを読んで、複数行コマンドの使用方法、さらにコマンドパラメータの詳細説明を理解してください。

## 解説場所

HTTP(S) Post リクエストについての詳細情報は *カスタマイズガイド*にあります。 次のリンクにアクセスします。

► https://www.cisco.com/go/in-room-control-docs

# 入力ソースの構成 (1/2 ページ)

ビデオ システムの API を使用すると、単一の主要なビデオ ストリームで最大 4 つの入力ソースを結合できます。

入力ソースの最大数は、ビデオ システムによって*異なります*。

| ビデオ システム | 組み合わすことができる異なる入力ソースの最大数 |
|---|---|
| Room Kit、Room Kit Mini、SX20、MX200 G2, MX300 G2 | 2 |
| Codec Plus、Room 55、Room 55 Dual、Room 70 | 3 |
| SX80、MX700、MX800 Codec Pro、Room 70 G2 | 4 |
| SX10、DX70、DX80 | 利用不可 |

## ソース構成

### 構成レイアウト

3 つのレイアウトから選択できます。

- 等しい
- Prominent
- PIP (2 つの入力ソースを構成するときにのみ使用可能)

PIP 位置をコーナーの一つに変更できます。PIP のサイズは通常でも大型でも可能です。

構成とレイアウトは、コールとコール外の両方でいつでも変更できます。

### 自画面

自画面は、遠端に送信されるのと同じ構成イメージを示します。

### 個別カメラ制御

API コマンド (`xCommand Camera *`) を使用して、個々のカメラを制御することができますが、ユーザ インターフェイス上の制御は使用できません。

ユーザ インターフェイスでカメラを選択すると、メインのビデオ ストリームが構成されたビデオ ストリームから、選択されたカメラからの単一のストリームに切り替えられます。

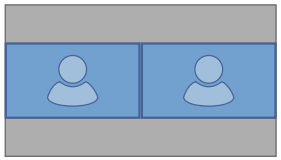
### オン デマンドによる構成およびレイアウトの変更

入力ソース構成は API コマンドを使用してのみ利用可能です。専用のユーザ インターフェイスは提供されません。

構成とレイアウトをオン デマンドで簡単に変更できるようにするには、マクロを使用してカスタム ユーザ インターフェイス パネル (室内制御パネル) を作成することをお勧めします。

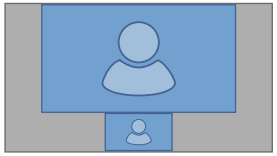
## レイアウト

### 等しい



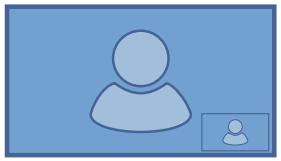
ソースの数 : 2

### Prominent



ソースの数 : 2

### ピクチャインピクチャ *(PIP)*



右下隅

右下済、大型 PIP

# 入力ソースの構成 (2/2 ページ)

## API コマンド

```
xCommand ビデオ入力 SetMainVideoSource
    ConnectorId: <1..n> SourceId: <1..m>
    Layout: <Equal, PIP, Prominent>
    PIPPosition <左下、右下、左上、右上>
    PIPSize <自動、大型>
```

**値は次のとおりです。**

入力ソースは、(ConnectorId) に接続されている物理コネクタか、論理ソース識別子 (SourceId) のいずれかによって識別できます。同じコマンド内で異なる識別子を混合することはできません。ConnectorId または SourceId のいずれかを使用してください。これらの識別子は、*[ビデオ入力コネクタ (Video Input Connector) ]* および *[ビデオ入力ソース (Video Input Source) ]* のステータスで見つけることができます。

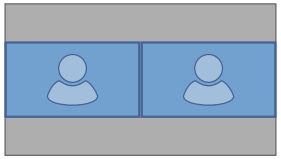
Equal と PIP、さらにプロミネント (**レイアウト**) の違いは、サイドバーに表示されます。

PIP 位置をコーナーの一つに変更できます。PIP のサイズは通常 (自動) でも大型でも可能です。

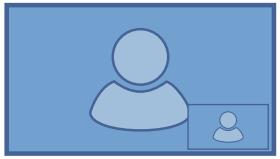
詳細については、API ガイドを参照してください。

### 例

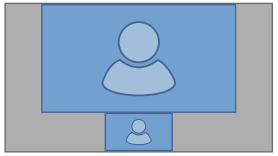
```
xCommand Video Input SetMainVideoSource ConnectorId: 1 ConnectorId: 2 Layout: Equal
```



```
xCommand Video Input SetMainVideoSource SourceId: 1 SourceId: 2 Layout: PIP PIPPosition: LowerRight PIPSize: Large
```



```
xCommand Video Input SetMainVideoSource SourceId: 1 SourceId: 2 Layout: Prominent
```



# プレゼンテーションソースの構成 (1/2 ページ)

ビデオ システムの API を使用すると、単一のビデオ ストリームで最大 4 つのプレゼンテーションソースを組み合わせることができます。

プレゼンテーションソースの最大数は、ビデオ システムによって*異なります*。

| ビデオ システム | プレゼンテーションソースの最大組み合わせ可能数 |
|---|---|
| Room Kit、Room Kit Mini、SX20、MX200 G2、MX300 G2 | 2 |
| Codec Plus、Room 55、Room 55 Dual、Room 70 | 3 |
| SX80、MX700、MX800、Codec Pro、Room 70 G2 | 4 |
| SX10、DX70、DX80 | 利用不可 |

ケーブル (DVI、VGA、HDMIなど) 経由で共有されているソースのみ共有できます。

## ソース構成

### 構成レイアウト

2 つのレイアウトから選択できます。

- 等しい
- Prominent

ソースの数は、コール時と非コール時どちらであっても、いつでも変更できます。画像サイズは修正できません。

ソースが画面に表示される順序は、コマンド内の順番に従います。表示は左上から始まり、右下が最後になります。

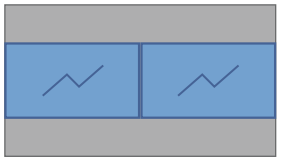
### オン デマンドによる構成およびレイアウトの変更

プレゼンテーションソース構成は API コマンドを使用してのみ利用可能です。専用のユーザ インターフェイスは提供されません。

構成とレイアウトをオン デマンドで簡単に変更できるようにするには、マクロを使用してカスタム ユーザ インターフェイス パネル (室内制御パネル) を作成することをお勧めします。

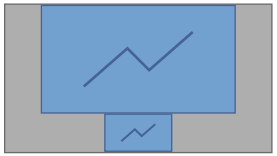
## レイアウト

### 等しい



ソースの数 : 2

### Prominent



ソースの数 : 2

# プレゼンテーションソースの構成 (2/2 ページ)

## API コマンド

```
xCommand Presentation Start
    xCommand Presentation Start
    ConnectorId: <1..n>
    PresentationSource: <1..m>
    Instance: <新規, 1..n>
    Layout: <Equal, Prominent>SendingMode:
    <LocalRemote, LocalOnly>
```

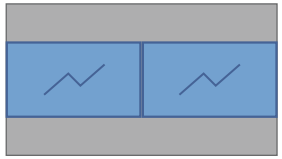
**値は次のとおりです。**

入力ソースは、接続されている物理コネクタ (ConnectorId) 、または論理ソース識別子 (PresentationSource) のどちらかによって識別可能です。同じコマンド内で異なる識別子を使うことはできません。ConnectorId または PresentationSource のうち片方のみを使用してください。これらの識別子は、*[ビデオ入力コネクタ (Video Input Connector) ]* および *[ビデオ入力ソース (Video Input Source) ]* のステータスで見つけることができます。

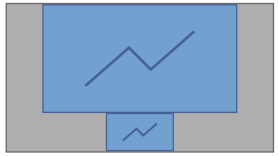
詳細については、API ガイドを参照してください。

## 例

```
xCommand Presentation Start PresentationSource: 1 PresentationSource: 2 Layout: Equal
```

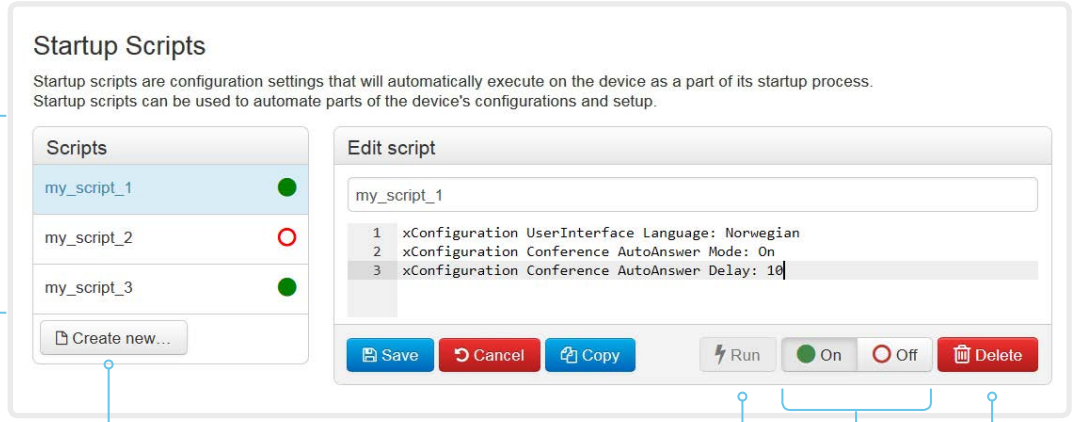


```
xCommand Presentation Start ConnectorId: 1 ConnectorId: 2 Layout: Prominent
```



# スタートアップ スクリプトを管理する

ウェブ インターフェイスにサインインして、*[統合 (Integration) ] > [スタートアップ スクリプト (Startup Scripts) ]* を選択します。




図に示しているスクリプト名と設定は一例です。独自のスクリプトを作成できます。

## スタートアップ スクリプトのリスト

1 つ以上のスタートアップ スクリプトを作成できます。*

緑色のドットがアクティブなスタートアップ スクリプトの横に、赤色の丸が非アクティブなスタートアップ スクリプトの横に表示されます。

複数のスタートアップ スクリプトがある場合は、リストの上から下に順番に実行されます。

## スタートアップ スクリプトを作成する

1. *[新規作成 (Create new...) ]* をクリックします。.
2. タイトル入力フィールドにスタートアップ スクリプトの名前を入力します。
3. コマンド入力エリアにコマンド（xConfiguration または xCommand）を入力します。新しい行で各コマンドを開始します。
4. *[Save (保存) ]* をクリックします。
5. *[オン (On) ]* をクリックして、スタートアップ スクリプトをアクティブにします。

既存のスクリプトを編集の開始点として使用する場合は、そのスクリプトを選択して *[コピー (Copy) ]* をクリックします。

## 起動スクリプトをすぐに実行する

1. リストからスタートアップ スクリプトを選択します。
2. *[実行 (Run) ]* をクリックします。

   アクティブなスタートアップ スクリプトと非アクティブなスタートアップ スクリプトの両方をすぐに実行できます。

## スタートアップ スクリプトをアクティブ化または非アクティブ化する

1. リストからスタートアップ スクリプトを選択します。
2. スクリプトをアクティブにする場合は *[オン (On) ]* を、非アクティブにする場合は *[オフ (Off) ]* をクリックします。

   アクティブなスタートアップ スクリプトは、ビデオ システムが起動するたびに呼び出されます。

## スタートアップ スクリプトを削除する

1. リストからスタートアップ スクリプトを選択します。
2. *[削除 (Delete)* をクリックします。

## スタートアップ スクリプトについて

スタートアップ スクリプトには起動手順の一部として実行されるコマンド (xCommand) および構成 (xConfiguration) が含まれます。

`xCommand SystemUnit Boot` など、いくつかのコマンドとコンフィギュレーションはスタートアップ スクリプトに含めることができません。不正なコマンドや設定が含まれたスクリプトは保存できません。

xCommand および xConfiguration の構文とセマンティックは、製品の API ガイドに説明されています。

# ビデオ システムの XML ファイルにアクセスする

ウェブ インターフェイスにサインインして、*[統合 (Integration) ] > [開発者 API (Developer API) ]* を選択します。

XML ファイルはビデオ システムの API の一部です。システムに関する情報が階層で構成されています。

- *Configuration.xml* には現在のシステム設定 (コンフィギュレーション) が含まれます。これらの設定は、ウェブ インターフェイスまたは API (アプリケーション プログラミング インターフェイス) から制御されます。
- *status.xml* 内の情報は常にビデオ システムによって更新され、システムおよびプロセスの変更が反映されます。ステータス情報は、ウェブ インターフェイスまたは API からモニタします。
- *Command.xml* にはアクションの実行をシステムに指示するために使用できるコマンドの概要が含まれます。コマンドは、API から発行されます。
- *Valuespace.xml* には、システム設定、ステータス情報、およびコマンドのすべての値スペースの概要が含まれています。

## XML ファイルを開く

XML ファイルを開くにはファイル名をクリックします。

## API について

アプリケーション プログラミング インターフェイス (API) は、ビデオ システムを使用する統合技術者や開発者を対象としたツールです。API に関する詳細は、ビデオ システムの API ガイドで説明されています。

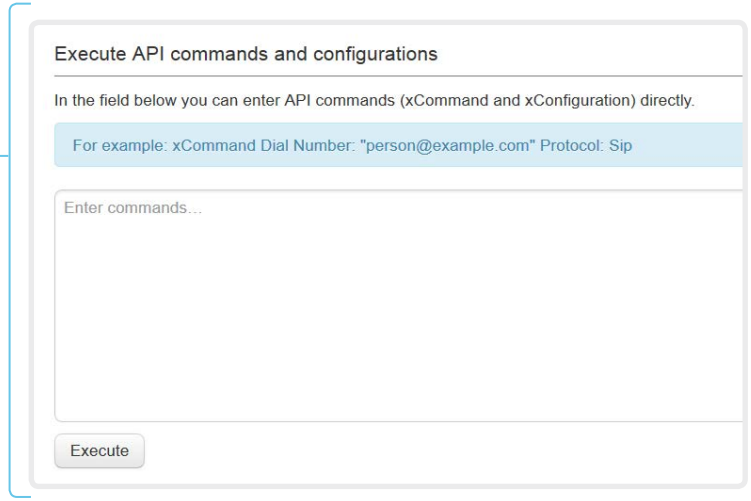
# ウェブ インターフェイスからの API コマンドとコンフィギュレーションの実行

ウェブ インターフェイスにサインインして、*[統合 (Integration) ] > [開発者 API (Developer API) ]* を選択します。

コマンド (xCommand) および設定 (xConfiguration) は、ウェブ インターフェイスから実行できます。構文とセマンティックについては、ビデオ システムの API ガイドで説明されています。

## API コマンドとコンフィギュレーションの実行

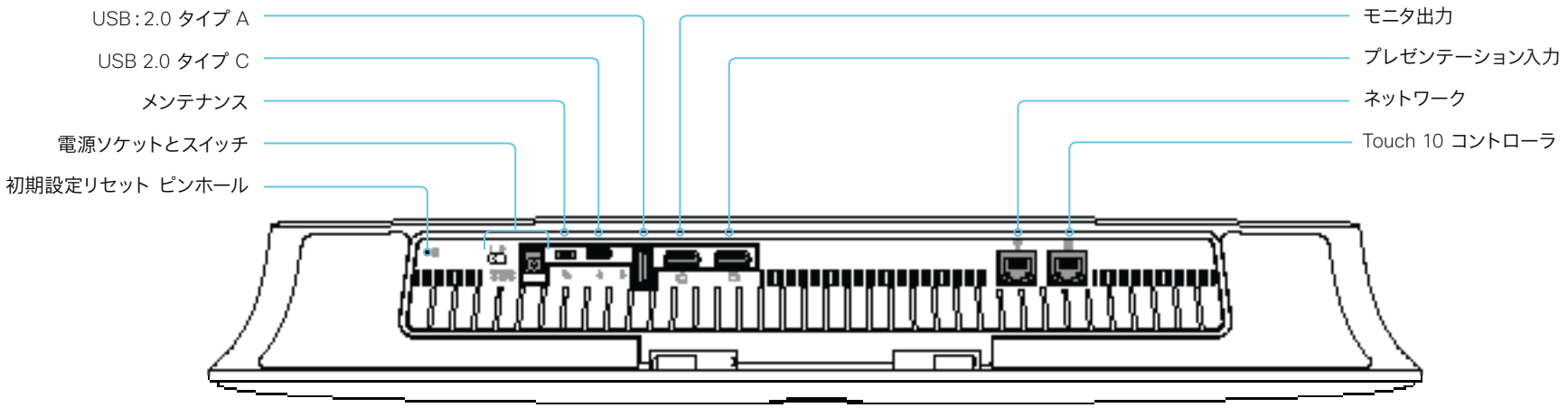
1. テキスト領域に、コマンド (xCommand または xConfiguration) またはコマンド シーケンスを入力します。
2. *[実行 (Execute) ]* をクリックしてコマンドを発行します。




## API について

アプリケーション プログラミング インターフェイス (API) は、ビデオ システムを使用する統合技術者や開発者を対象としたツールです。API に関する詳細は、ビデオ システムの API ガイドで説明されています。

# コネクタ パネル




## 初期設定リセット ピンホール

ピンホールは最後の手段として使用してください。初期設定へのリセットは、Touch ユーザ インターフェイスまたは ウェブ インターフェイスから実行することをお勧めします。

## 電源

必ず付属の電源を使用してください。電源スイッチがオンの位置にある場合、システムは自動的に電源が入ります。

## メンテナンス

ビデオ システムとのシリアル通信には、マイクロ USB コネクタを使用します。

## USB

- USB : 2.0 タイプ A
- USB 2.0 タイプ C

## モニタ出力

HDMI バージョン 2.0、最大解像度は 60 fps で 3840 × 2160。これらの出力には音声がありません。高解像度とフレーム レートをサポートするプレミアム HDMI ケーブルが必要です。Cisco 認定ディスプレイ ケーブルをお勧めします。

## プレゼンテーション入力

HDMI バージョン 1.4b、最大解像度はコンピューターでは 30 fps で 3840 × 2160。高解像度とフレーム レートをサポートするハイスピード HDMI 1.4b ケーブルが必要です。Cisco 認定プレゼンテーション ケーブルをお勧めします。

## ネットワーク

イーサネット インターフェイス、10 Mb/100 Mb/1 Gb のイーサネット LAN インターフェイス (RJ45) 。

## Touch 10 コントローラ

Touch 10 は、このソケットでは提供されていないイーサネット経由で電源供給されています。

# イーサネットポートについて

## メインネットワークポート

メイン ネットワーク ポート - ネットワーク ポート 1 - は常に LAN 接続用に予約されています。これはすべてのビデオ システムに適用されます。

ビデオ システムによっては、ネットワーク ポート 1 に番号 1 とネットワーク シンボル (品) のいずれか、または両方が付いています。

## 補助ネットワークポート

ビデオ システムの一部には複数のネットワーク ポートが備わっています。追加のポートは、カメラ、Touch 10、サードパーティー製制御システムなどの周辺機器に使用できます。

このようなネットワークポートに接続されているデバイスはコーデックからローカル IP アドレスを取得するため、企業ネットワークには接続されていません。パケットをメインネットワークポート (LAN) と補助ネットワークポート (リンク-ローカル) の間で移動させることはできません。

- Cisco 周辺デバイスには、169.254.1.41 から 169.254.1.240 の範囲 (DHCP) でのダイナミック IP アドレスが割り当てられます。
- Cisco 以外のデバイスには、ダイナミック IP アドレス (DHCP) : 169.254.1.30 を割り当てることができます。

  注 : Cisco 以外のデバイスでダイナミック IP アドレスを取得できるのは、一度に 1 つだけです。
- さらに、Cisco 以外のデバイスには、169.254.1.241 ～ 169.254.1.254 の範囲の静的 IP アドレスを割り当てることもできます。

この方法は、SSH を使用してコーデックに接続する場合にも使用できます。このケースでは、IP アドレス 169.254.1.1 を使用できます。

## Power over Ethernet (PoE)

補助ネットワークポートには Power over Ethernet (PoE) を提供するものもあります。これらのポートは Touch 10 コントローラなどの周辺機器に電源を供給します。

| 製品 | 補助ネットワークポートの数 | PoE 付きの補助ネットワークポートの数 |
|---|---|---|
| Room Kit | 1 | 0 |
| Room Kit Mini | 1 | 1 ( ) |
| Room 55 | 1 | 1 ( ) |
| Room 70 / Room 55 Dual | 2 | 1 ( ) |
| Room 70 G2 | 4 | 2 ( 、PoE) |
| Codec Plus | 2 | 1 ( ) |
| Codec Pro | 4 | 2 ( 、PoE) |
| SX10 | 0 | 0 |
| SX20 | 0 | 0 |
| SX80 | 2 | 0 |
| MX200 G2 / MX300 G2 | 2 | 0 |
| MX700 / MX800 | 2 | 0* |
| DX70 / DX80 | 1 | 0 |

* これらの製品には個別の PoE インジェクタがあり、補助ネットワークポートの 1 つに接続されます。PoE インジェクタは Touch 10 コントローラに使用されます。

# メンテナンス用のシリアル インターフェイス

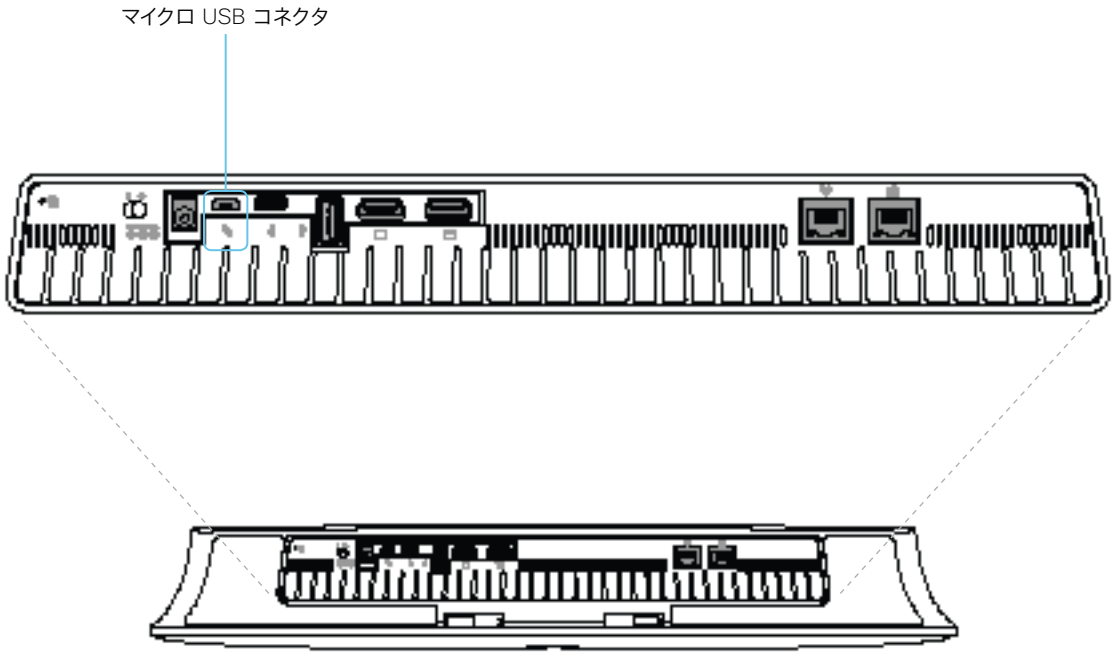
ビデオ システムとの直接通信には、マイクロ USB コネクタを使用します[1]. マイクロ USB to USB ケーブルが必要です。コンピュータによりシリアル ポート ドライバが自動インストールされない場合には、手動でコンピュータにインストールする必要があります [2]。

シリアル インターフェイスに接続するには、ターミナル エミュレータ（SSH クライアント）を使用します。最も一般的なコンピュータ タイプ (PC、MAC) およびオペレーティング システムでは、PuTTY または Tera Term は機能します。

シリアル接続は、IP アドレス、DNS、またはネットワークなしでも使用できます。

パラメータ :

- ボー レート : 115200 bps
- データ ビット : 8
- パリティ : なし
- ストップ ビット : 1
- ハードウェア フロー制御 : オフ


## ビデオ システムの設定値

シリアル通信はデフォルトでイネーブルになっています。動作を変更するには、次の設定を使用します。

*[シリアルポート (SerialPort) ] > [モード (Mode) ]*

セキュリティ上の理由から、シリアル インターフェイスを使用する前にサインインするように求められます。動作を変更するには、次の設定を使用します。

*[シリアルポート (SerialPort) ] > [ログインが必須 (LoginRequired) ]*

ビデオ システムが CUCM によりプロビジョニングされる場合、シリアル ポート設定は CUCM から設定する必要があります。

[1] マイクロ USB ポートはメンテナンス用途で使います。シリアル接続経由でビデオ システムの API にアクセスする場合は、USB ポート ( タイプ A) に接続します。詳細については、API ガイドを参照してください。

[2] UART ブリッジ仮想 COM ポート (VCP) ドライバには、CP210x USB が必要です。次の内容を参照してください。▶ http://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers

# TCP ポートの開放

コーデック内の ウェブ サーバでは、非セキュアまたは不必要なポート、プロトコル、モジュール、またはサービスの使用が禁止または制限されています。いくつかのポートは、デフォルトで開放されているか、閉じられています。

## TCP 22 : SSH

SSH モード設定を [オフ (Off) ] にすることで、ポートを閉じることができます。

```
NetworkServices SSH Mode: Off/On
```

## TCP 80 : HTTP

HTTP モードを [オフ (Off) ] にするか、[HTTPS (HTTPS) ] にすることで、ポートを閉じることができます。

```
NetworkServices HTTP Mode: HTTP+HTTPS/HTTPS/Off
```

## TCP 443 : HTTP

HTTP モード設定を [オフ (Off) ] にすることで、ポートを閉じることができます。

```
NetworkServices HTTP Mode: HTTP+HTTPS/HTTPS/Off
```

## TCP 4043 : リモート ペアリング ソフトウェアのダウンロード

Touch パネルとのリモート ペアリングを [オフ (Off) ] に設定することでポートを閉じることができます。

```
Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On
```

## TCP 4045 : リモート ペアリング バージョン情報

Touch パネルとのリモート ペアリングを [オフ (Off) ] に設定することでポートを閉じることができます。

```
Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On
```

## TCP 4051 : リモート ペアリング セッション接続

このポートは、Touch パネルがビデオ システムとリモート ペアリングされている場合にのみ使用可能 (オープン) です。Touch パネルとのリモート ペアリングを [オフ (Off) ] に設定することでポートを閉じることができます。

```
Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On
```

## TCP 4052 : リモート ペアリングおよび転送

このポートは、Touch パネルがビデオ システムとリモート ペアリングされている場合にのみ使用可能 (オープン) です。Touch パネルとのリモート ペアリングを [オフ (Off) ] に設定することでポートを閉じることができます。

```
Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On
```

## TCP 4053 : リモート ペアリング ポート

Touch パネルとのリモート ペアリングを [オフ (Off) ] に設定することでポートを閉じることができます。

```
Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On
```

## TCP 5060/5061 : SIP リッスン ポート

SIP リッスン ポートはデフォルトで開放されています。SIP リッスン ポートは、Cisco UCM (Unified Communication Manager) によって無効にされています。SIP リッスン ポートを [オフ (Off) ] にすることで、ポートを閉じることができます。

```
SIP ListenPort: Off/On
```

システム設定は、ウェブ インターフェイスの *[セットアップ (Setup) ] > [構成 (Configuration) ]* ページから設定します。ウェブ ブラウザを開き、ビデオ システムの IP アドレスを入力して、サインインします。

# TMS からの HTTPFeedback アドレス

ビデオ システムが Cisco TelePresence Management Suite (TMS) に追加されると、TMS に情報 (イベント) を送り返すように自動的に設定されます。ビデオ システムは、これらのイベントが TMS から送信されるようにアドレスを受信します (HTTPFeedback address) 。このアドレスが存在しないか、または正しく設定されていない場合、ビデオ システムは TMS にイベントを送信できません。

## 失われたイベントへの応答

ビデオ システムがイベントへの応答を受信しない場合、間隔を増やしながら最大 6 回、HTTPFeedback アドレスに送信を再試行します。

ビデオ システムが再試行でも応答を受信しない場合、エンドポイントは HTTPFeedback アドレスを削除し、TMS にイベントを送信できなくなります。HTTPFeedback ステータスは、失敗したことを示します。障害のタイプを示す診断メッセージがあります。

メッセージの再送を試みる際、TMS での通話詳細記録 (CDR) の紛失が生じます。

## TMS からの新しい HTTPFeedback アドレスの取得

イベントを送信するための新しいアドレスを取得するには、ビデオ システムを再起動して、TMS から次の管理アドレスがプッシュされるのを待つ必要があります (予定されているか、TMS 管理者によってトリガーされる) 。

# サポートされている RFC

RFC (Request For Comments) シリーズには、Internet Engineering Task Force (IETF) によって作成される技術仕様およびポリシー文書など、インターネットに関する技術および組織のドキュメントが含まれます。

CE ソフトウェアは、以下を含む RFC の範囲をサポートしています。

- RFC 2782『DNS RR for specifying the location of services (DNS SRV)』
- RFC 3261 SIP『Session Initiation Protocol』
- RFC 3263『Locating SIP Servers』
- RFC 3361『DHCP Option for SIP Servers』
- RFC 3550 RTP『RTP: A Transport Protocol for Real-Time Applications』
- RFC 3711『The Secure Real-time Transport Protocol (SRTP)』
- RFC 4091『The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework』
- RFC 4092『Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)』
- RFC 4582『The Binary Floor Control Protocol』

  draft-ietf-bfcpbis-rfc4582bis-00『Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport』
- RFC 4733『RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals』
- RFC 5245『Interactive Connectivity Establishment (ICE)』: A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
- RFC 5589『SIP Call Control Transfer』
- RFC 5766『Traversal Using Relays around NAT (TURN)』: Relay Extensions to Session Traversal Utilities for NAT (STUN)
- RFC 5905『Network Time Protocol Version 4: Protocol and Algorithms Specification』

# 技術仕様 (1/2 ページ)

### ソフトウェアの互換性
- Cisco Collaboration Endpoint Software Version 9.6 以降
- RoomOS

### 帯域幅
- ポイントツーポイントで最大 6 Mbps

### ファイアウォール トラバーサル
- Cisco TelePresence Expressway テクノロジー
- H.460.18 および H.460.19 ファイアウォール トラバーサル

### ビデオ標準
- H.264
- H.265 (SIP)

### ビデオ入力
- 1 つの HDMI 入力により*、HD1080p60 を含め最大 4K (3840 X 2160/30 fps) のフォーマットをサポート
- Consumer Electronics Control (CEC) 2.0

### ビデオ出力
- 60 fps で最大 3840 × 2160 (4Kp60) のフォーマットをサポートする 1 つの HDMI 出力 *
- 30 fps または 60 fps で最大 1920 × 1080 (HD1080p) のライブ ビデオ解像度 (エンコードおよびデコード)
- Consumer Electronics Control (CEC) 2.0

### USB パススルー
- 接続されたコンピュータで、1 つの USB ケーブルでビデオ、マイク、およびスピーカーを使用可能
- ビデオ解像度 720p

### 音声標準
- AAC-LD
- G.722
- G.722.1
- G.711
- G.729
- Opus

### 音声機能
- ハイクオリティ 20kHz オーディオ
- オートゲイン コントロール (AGC)
- オート ノイズ リダクション
- アクティブ リップ シンク

### 音声入力
- HDMI からのオーディオ入力 1 個
- 内部マイクロフォン

### スピーカー (統合)
- 平衡型構成の高品質スピーカー 3 個
- 周波数特性 : 70Hz ～ 20kHz
- 増幅器用電源 : 24W
- 最大出力レベル : 85dB SPL

### MULTISITE
- H.239 デュアル ストリーム (H.323)
- BFCP デュアル ストリーム (SIP)
- 5fps で最大 3840 × 2160 の解像度のサポート

### DUAL ストリーム
- 1 つの HDMI 入力により、HD1080p60 を含め最大 4K (3840 X 2160/30 fps) のフォーマットをサポート
- Consumer Electronics Control (CEC) 2.0

### ワイヤレス共有
- Cisco Webex Teams アプリケーション (最大 3840 X 2160/5 fps)
- Cisco Webex Meetings アプリケーション (最大 3840 X 2160/5 fps)
- Cisco Intelligent Proximity クライアント (5 fps で 最大 1920 × 1080)

### マルチポイント サポート
- マルチサイト オプションで組み込み 4-way SIP/H.323 会議機能

### マルチサイト機能 (組み込みマルチポイント) 、オプションのアップグレード
- 適応型 SIP/H.323 マルチサイト :
  - **3 ウェイ: コンテンツのない 1080p30 までの解像度。解像度は最大 720 p 30 で、1080p15 までのコンテンツ**
  - **4 ウェイ: 最大 720p30 まで、最大 1080p15 までの解像度。**
- 完全個別音声および映像トランスコーディング
- 同一会議で H.323、SIP、VoIP が混在可能
- 5 fps で最大 3840 × 2160 の解像度で、任意の参加者からのプレゼンテーション (H.239/BFCP) をサポート
- ベスト インプレッション機能 (自動連続表示レイアウト)
- 任意のサイトからの暗号化およびデュアル ストリーム

### プロトコル
- H.323
- SIP
- Cisco WebEx

### 組み込み暗号化
- H.323 および SIP ポイントツーポイント
- 規格準拠 : H.235 v3 および Advanced Encryption Standard (AES)
- キーの自動生成と交換

### IP ネットワーク機能
- サービス設定での DNS ルックアップ
- 差別化サービス (QoS)
- IP 帯域幅最適化コントロール (フロー制御を含む)
- 自動ゲートキーパー検出
- ダイナミック再生およびリップシンクのバッファリング
- H.323 の H.245 DTMF トーン
- SIP の RFC 4733 DTMF トーン
- NTP による日時のサポート
- メディア適合およびレジリエンス
- URI ダイヤル
- DHCP (ダイナミック ホスト コンフィギュレーション プロトコル)
- IEEE 802.1x ネットワーク認証
- IEEE 802.1q VLAN
- IEEE 802.1p QoS および Class of Service (CoS)

### IPV6 ネットワークのサポート
- H.323 および SIP に対する単一コール スタックのサポート
- DHCP、SSH、HTTP、HTTPS、DNS、および DiffServ に対するデュアル スタックの IPv4 および IPv6
- スタティックと自動 IP 設定 (ステートレス アドレス自動設定) の両方をサポート

### CISCO UNIFIED COMMUNICATIONS MANAGER
- Cisco Unified Communications Manager (CUCM) のネイティブ登録
- CUCM バージョン 9.1.2 以降と Cisco Webex Room Kit Mini のデバイス パックが必要

### セキュリティ機能
- HTTPS および SSH を使用して管理
- IP 管理パスワード
- 管理メニューのパスワード
- IP サービスの無効
- ネットワーク設定の保護
- プライバシー カバー

### ネットワーク インターフェイス
- LAN 用イーサネット (RJ-45) X 1、10/100/1000 Mbps
- Cisco Touch 10 用イーサネット (RJ-45) X 1
- Wi-Fi : IEEE 802.11a/b/g/n/ac 2.4GHz、5GHz、2x2 MIMO

### その他のインターフェイス
- USB 2.0 ポート Type-A X 1
- USB 2.0 ポート Type-C X 1
- 1 つのマイクロ USB ポート
- 初期設定リセット ピンホール

### オプションのハードウェア コンポーネント
- HDMI プレゼンテーションケーブル 8 m/26.2 フィート
- USB パススルー機能用 4 m/13 フィート USB ケーブル
- 画面取り付けキット

# 技術仕様 (2/2 ページ)

**カメラの概要**
- 4K Ultra HD カメラ
- 最大 60 fps をサポート (ベスト オーバービュー適用時には最大 30 fps)
- 8 メガピクセルイメージセンサー
- 1/1.4 CMOS
- 2 倍ズーム
- f/1.4 開口
- 水平視野角 120°
- 自動フレーミング (顔検出)
- 自動フォーカス、輝度およびホワイト バランス
- 焦点距離 : 1 m ～無限遠

**電源**
- 100-240 VAC、50/60 Hz、12 $V_{DC}$入力
- 平均 20 W、ピーク時 70 W
- 電源 FSP FSP070-AHAN2 または AcBel ADF019 を使用する必要あり

**動作温度および湿度**
- 周囲温度 : 0 ～ 40 °C (32 ～ 104°F)
- 相対湿度 (RH) : 10 ～ 90%

**保管および輸送の温度**
- RH 10 ～ 90% では -20 ～ 60°C (-4 ～ 60°F) (結露しないこと)

**寸法**
- 幅: 500 mm/19.7
- 高さ : 781 mm (30.7 インチ)
- 深さ:77 mm/3 in
- 重量 : 18+ kg (40 ポンド)

**認定および適合規格**
- 指令 2014/35/EU (低電圧指令)
- 指令 2014/30/EU (EMC 指令) : クラス A
- 指令 2014/53/EU (無線機器指令)
- 指令 2011/65/EU (RoHS)
- 指令 2002/96/EC (WEEE)

- NRTL 認定 (製品の安全性)
- FCC CFR 47 Part 15B (EMC) : クラス A
- FCC CFR 47 Part 15C (RF)
- FCC CFR 47 Part 15E (RF)
- FCC Listed (無線機器)

各国の認定書類については、Product Approval Status Database (製品認定ステータス データベース) www.ciscofax.com を参照してください。

すべての仕様は予告なしに変更される場合があります。システム仕様は異なる場合があります。

これらのドキュメントの画像はすべて説明目的でのみ使用され、実際の製品とは異なる場合があります。



2019 年 4 月

# Cisco ウェブ サイト内のユーザ ドキュメンテーション

次の短いリンクを使用して、CE ソフトウェアを実行する製品シリーズのマニュアルを検索します。

Room シリーズ:

► https://www.cisco.com/go/room-docs

MX シリーズ:

► https://www.cisco.com/go/mx-docs

SX シリーズ:

► https://www.cisco.com/go/sx-docs

DX シリーズ:

► https://www.cisco.com/go/dx-docs

通常、すべての Cisco Collaboration エンドポイントのユーザ マニュアルはこちらから検索できます。
► https://www.cisco.com/go/telepresence/docs

マニュアルは以下のカテゴリに整理されています。一部のマニュアルはすべての製品で利用できません。

**インストールとアップグレード > インストールとアップグレード ガイド**

- *インストレーション ガイド*:製品のインストール方法
- *スタートアップ ガイド*:システムを稼働させるために必要な初期設定
- *RCSI ガイド*:法規制の遵守および安全に関する情報

**保守と運用 > メンテナンスとオペレーション ガイド**

- *スタートアップ ガイド*:システムを稼働させるために必要な初期設定
- *管理者ガイド*:製品の管理に必要な情報
- *『Deployment guide for TelePresence endpoints on CUCM』*:ビデオ システムを Cisco Unified Communications Manager (CUCM) とともに使用開始するために実行するタスク
- *スペア部品の概要、スペア部品の交換ガイド、ケーブル スキーマ*:スペア部品を交換するときに役立つ情報

**保守と運用 > エンドユーザ ガイド**

- *ユーザ ガイド*:製品の使用方法
- *クイック リファレンス ガイド*:製品の使用方法
- *物理インターフェイス ガイド*:コネクタのパネルと LED など、コーデックの物理インターフェイスに関する詳細

**リファレンス ガイド > コマンド リファレンス**

- *『API リファレンス ガイド』*:Application Programmer Interface (API) のリファレンス ガイド

**リファレンス ガイド > テクニカル リファレンス**

- *CAD 図面*:測定値付き 2D CAD 図面

**[設定 (Configure) ] > [設定ガイド (Configuration Guides) ]**

- *カスタマイズ ガイド*:ユーザ インターフェイスのカスタマイズ方法、ビデオ システムの API を使用した室内操作のプログラムする方法、マクロの作成方法、オーディオ コンソールを用いた高度な音声セットアップの構成方法

**設計 > 設計ガイド**

- *ビデオ会議室に関するガイドライン*:会議室の設計とベストプラクティスに関する一般的なガイドライン
- *ビデオ会議室のガイドライン*:音質を向上させるための対策

**ソフトウェア ダウンロード、リリースと一般情報 > ライセンス情報**

- *オープン ソース ドキュメンテーション*:この製品で使用されるオープン ソース ソフトウェアのライセンスおよび通知

**[ソフトウェア ダウンロード、リリースと一般情報 (Software Downloads, Release and General Information) ] > [リリース ノート (Release Notes) ]**

- *ソフトウェア リリース ノート*

# Cisco のお問い合わせ先

Cisco の ウェブ サイトでは、Cisco の世界各地のお問い合わせ先を確認できます。

参照先 : ► https://www.cisco.com/go/offices

本社
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA

## Intellectual property rights

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。

Cisco が導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校 (UCB) により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムに適応したものです。

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。Cisco 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、Cisco およびその供給者は、このマニュアルに適用できるまたは適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 Cisco またはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

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

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

Cisco は世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号については、Cisco の ウェブサイトをご覧ください www.cisco.com/go/offices。

Cisco および Cisco ロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。Cisco の商標の一覧については、www.cisco.com/go/trademarks をご覧ください。掲載されている第三者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。(1110R)

## Cisco 製品のセキュリティの概要

この製品には、輸入、輸出、譲渡、使用を規制する米国またはその他の国の法律の対象となる暗号化機能が含まれています。Cisco の暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、http://www.bis.doc.gov/policiesandregulations/ear/index.htm で参照できます。