

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 8.2  
6月 2016



# 管理者ガイド

Cisco DX70 および DX80

シスコ製品をお選びいただきありがとうございます。

お使いのシスコ製品は、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。

製品マニュアルのこの部分は、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。このガイドについてのご意見、ご感想をお聞かせください。

定期的にシスコの Web 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。

ユーザ マニュアルは次の URL から入手できます。

▶ <http://www.cisco.com/go/dx-docs> [英語]

## 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

はじめに.....	4
ユーザ ドキュメンテーションとソフトウェア .....	5
DX70 および DX80 の概要.....	6
電源オン/オフ .....	7
LED インジケータ .....	8
ビデオ システムの管理方法.....	9
<b>設定 (Configuration) .....</b>	<b>13</b>
ユーザ管理 .....	14
システム バスフリーズの変更.....	15
画面上の [設定 (Settings)] メニューの PIN (暗証番号) コードの設定.....	16
システム設定.....	17
サインイン バナーの追加 .....	18
ビデオ システムのサービス証明書の管理.....	19
信頼できる認証局 (CA) のリストの管理 .....	20
安全な監査ロギングのセットアップ .....	21
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.....	22
CUCM 信頼リストの削除.....	23
永続モードを変更する .....	24
強力なセキュリティ モードの設定.....	25
ビデオ品質の対コール レート比調整.....	26
パケット損失の復元力: ClearPath .....	27
壁紙の選択.....	28
着信音の選択と着信音量の設定.....	29
ローカル連絡先の管理.....	30
<b>周辺機器 .....</b>	<b>31</b>
コンピュータの接続.....	32
<b>メンテナンス.....</b>	<b>33</b>
システム ソフトウェアのアップグレード .....	34
オプション キーの追加 .....	36
システム ステータス .....	37
診断の実行 .....	38
ログ ファイルのダウンロード .....	39
リモート サポート ユーザの作成 .....	40
設定のバックアップまたは復元.....	41
以前使用していたソフトウェア イメージへの復元.....	42
ビデオ システムの工場出荷時設定リセット.....	43
ユーザ インターフェイスのスクリーンショットのキャプチャ .....	46

システム設定.....	47	付録.....	105
システム設定の概要.....	48	ユーザ インターフェイス.....	106
音声設定.....	52	リモート モニタリングのセットアップ.....	107
CallHistory 設定.....	54	Web インターフェイスを使用したコール情報へのアクセス.....	108
会議設定.....	55	Web インターフェイスを使用したコールの発信.....	109
H323 設定.....	59	Web インターフェイスを使用したコンテンツの共有.....	111
ロギングの設定.....	62	ローカル レイアウトの制御.....	112
ネットワーク設定.....	63	相手先 (遠端) カメラの制御.....	113
NetworkServices 設定.....	70	スタートアップ スクリプトの管理.....	114
周辺機器の設定.....	74	ビデオ システムの XML ファイルへのアクセス.....	115
電話帳の設定.....	75	Web インターフェイスからの API コマンドと構成の実行.....	116
プロビジョニング設定.....	76	シリアル インターフェイス.....	117
RoomReset の設定.....	79	技術仕様.....	118
RTP 設定.....	80	サポートされている RFC.....	120
セキュリティ設定.....	81	シスコ Web サイト内のユーザ ドキュメンテーション.....	121
SerialPort 設定.....	83	シスコのお問い合わせ先.....	122
SIP 設定 (SIP settings).....	84		
スタンバイ設定.....	88		
SystemUnit 設定.....	89		
時刻設定.....	90		
UserInterface 設定.....	93		
UserManagement の設定.....	95		
ビデオ設定.....	97		
試験的設定.....	104		

# 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 DX70
- Cisco DX80

コラボレーション ソフトウェア バージョン 8.2 (CE8.2) 以降、すべての DX80 ユニットおよび DX70 ユニットで CE ソフトウェアを実行できます。このソフトウェアは、Cisco TelePresence SX および MX シリーズで動作するソフトウェアと同じものです。

なお、Cisco DX650 は CE ソフトウェアでサポートされておらず、今後のサポート予定もありません。

このガイドには、Cisco Spark に登録されているシステムに関する情報は記載されていません。Cisco Spark ルーム システムの詳細については、以下にアクセスしてください。

▶ <https://help.webex.com/community/cisco-cloud-collab-mgmt> [英語]

### CE ソフトウェアへのソフトウェアの移行

Cisco DX80 と Cisco DX70 は、元々 Android ベースのソフトウェアとともに販売されていました。CE ソフトウェアに移行する前に、変換の要件、および Android ベースのソフトウェアと比較した機能の変更点を注意深く確認することが重要です。この確認を行わないと、導入環境が機能せず、再度変換して前に戻すことが必要になる可能性があります。

詳細については、ソフトウェア リリース ノートと、▶「システム ソフトウェアのアップグレード」の章を参照してください。

### ユーザ ドキュメンテーション

このガイドでは、エンドポイントの管理に必要な情報を提供します。エンドポイントのインストール方法についてはインストール ガイドを、必要な初期設定についてはスタートアップ ガイドを参照してください。

このエンドポイントに関する詳しいガイドは、付録 ▶「シスコ Web サイト内のユーザ ドキュメンテーション」を参照してください。

### ユーザ ドキュメンテーションのダウンロード

次のシスコ Web 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。

▶ <http://www.cisco.com/go/dx-docs> [英語]

### 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 Web サイト [英語] をご覧ください。

▶ <http://www.cisco.com/go/projectworkplace>

### Software

次のシスコ Web 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。

▶ <http://www.cisco.com/cisco/software/navigator.html>

ソフトウェア リリース ノート (CE8) を参照することをお勧めします。

▶ <http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-series-home.html> [英語]

## DX70 および DX80 の概要

Cisco DX70 と DX80 は、ビデオに対応した小型コラボレーション スペース向けに設計されたオールインワン装置です。

これらの装置には、高解像度 (HD) ビデオ、ユニファイド コミュニケーション機能、ラップトップ用の表示、各種拡張機能など高度な機能が搭載されています。

### 機能とメリット

- 専用の常時接続の 1080p 高解像度ビデオ コミュニケーション システム
- スピーカーフォン用の高品位音声システム
- 23 インチ (DX80) または 14 インチ (DX70) の 16:9 画面が、ビデオ通話に魅力的なエクスペリエンスを提供
- 静電容量方式マルチタッチスクリーンの洗練されたパワフルなユーザ インターフェイス
- デバイスの簡単なセルフプロビジョニングで、開封後は即座に使用可能
- 管理者は Cisco Expressway を利用してリモート ワーカーのセキュアな接続を実現
- Cisco Unified Communications Manager (UCM) 、Cisco TelePresence Video Communication Server (VCS) 、および Cisco Spark に登録



Cisco DX70

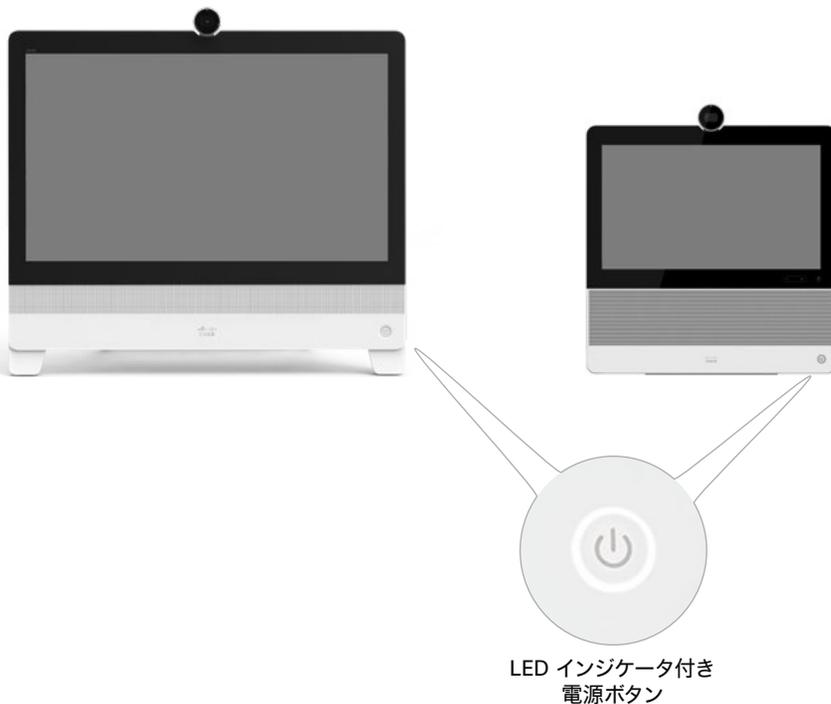


Cisco DX80

## 電源オン/オフ

### 電源ボタンによる電源のオン/オフ

LED インジケータ付きの電源ボタンが、図に示すように前面にあります。



#### スイッチを入れる

ビデオ システムは自動的に起動しません。電源ボタンを軽く押して数秒間押し続けます。

ビデオ システムの起動中は LED が点灯しています。

#### スイッチを切る

電源ボタンを軽く押して消灯するまで押し続けます。

#### スタンバイ モードの開始/終了

電源ボタンを短く押します。装置がスタンバイ状態になるまでに数秒かかります。

### 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

Web 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...)] をクリックして、選択を確定します。

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...)] をクリックして、選択を確定します。

 システムの電源をリモートでオンにすることはできません。

### タッチ インターフェイスを使用した再起動とスタンバイ

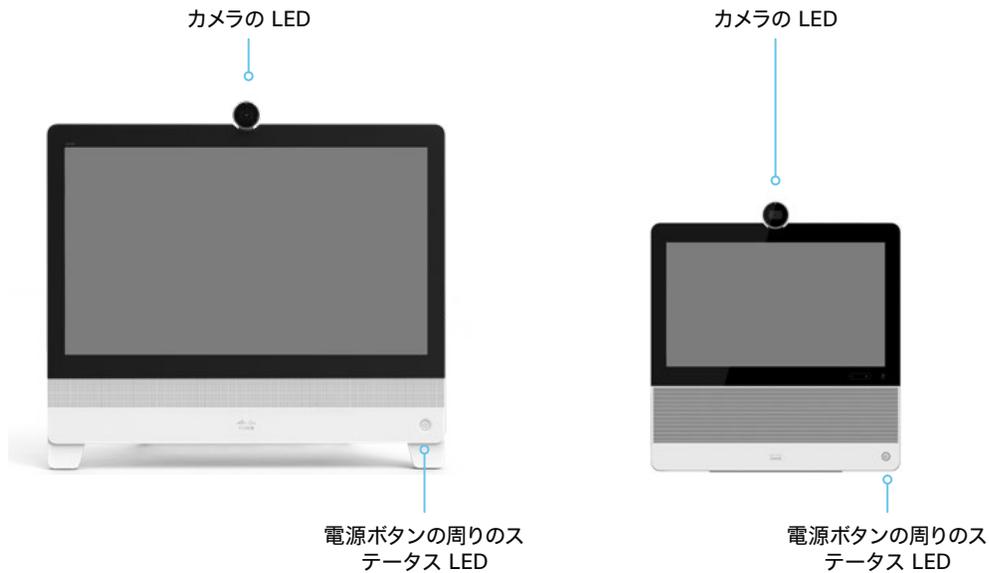
システムを再起動します。

1. ホーム画面で [設定 (settings)] アイコン (歯車の形のアイコン) を選択します。
2. [システム情報 (System Information)] > [再起動 (Restart)] を選択します。
3. 再度 [再起動 (Restart)] を選択して、選択を確定します。

### スタンバイ モードの開始/終了

1. ホーム画面で [設定 (settings)] アイコン (歯車の形のアイコン) を選択します。
2. [スタンバイ (Standby)] を選択します。

## LED インジケータ



### ステータス LED

ステータス LED は、電源ボタンの周りの円形状の部分です。LED の通常の色は白です。赤色のライトは、ハードウェア障害を示します。

通常の動作 (非スタンバイ状態) :

点灯します。

スタンバイ モード時:

LED がゆっくり点滅します。

ネットワーク接続がない場合:

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。

### カメラの LED

カメラの LED はカメラのレンズのすぐ上にあります。

コールの着信時:

LED が点滅します。

コール中:

点灯します。

## ビデオ システムの管理方法

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、Web 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。

あるいは、次のような方法でビデオ システムの API にアクセスすることもできます。

- HTTP または HTTPS (Web インターフェイスでも使用されます)
- SSH
- Telnet
- 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。

### Tip

API で設定またはステータスを使用できる場合、Web インターフェイスの設定またはステータスが次のように API の設定またはステータスに変換されます。

(Web で) `X > Y > Z` を Value に設定することは次と同等です。

`xConfiguration X Y Z:  (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次と同等です。

`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次と同等です。

`xStatus SystemUnit Software Version`

Web 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。

アクセス方式	注	方式を有効/無効にする方法
HTTP/HTTPS	<ul style="list-style-type: none"> <li>• ビデオ システムの Web インターフェイスで使用</li> <li>• 非セキュア (HTTP) 通信またはセキュア (HTTPS) 通信</li> <li>• HTTP: デフォルトで有効</li> <li>• HTTPS: デフォルトで有効</li> </ul>	<p>[ネットワークサービス (NetworkServices)] &gt; [HTTP] &gt; [モード (Mode)]</p> <p>変更を有効にするには、ビデオ システムを再起動します。</p>
Telnet	<ul style="list-style-type: none"> <li>• 非セキュア TCP/IP 接続</li> <li>• デフォルトで無効</li> </ul>	<p>[ネットワークサービス (NetworkServices)] &gt; [Telnet] &gt; [モード (Mode)]</p> <p>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。</p>
SSH	<ul style="list-style-type: none"> <li>• セキュア TCP/IP 接続</li> <li>• デフォルトで有効</li> </ul>	<p>[ネットワークサービス (NetworkServices)] &gt; [SSH] &gt; [モード (Mode)]</p> <p>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。</p>
シリアル インターフェイス (RS-232)	<ul style="list-style-type: none"> <li>• 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。</li> <li>• デフォルトで有効</li> <li>• 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)] &gt; [ログインが必須 (LoginRequired)])</li> </ul>	<p>[シリアル ポート (SerialPort)] &gt; [モード (Mode)]</p> <p>変更を有効にするには、ビデオ システムを再起動します。</p>



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。

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 Web インターフェイス

Web 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:** Web 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)。

Web ブラウザは最新版を使用することを推奨します。

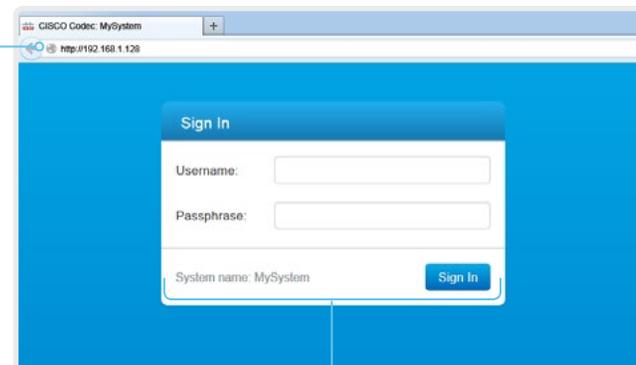
### ビデオ システムへの接続

Web 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. ホーム画面で [設定 (settings)] アイコン (歯車の形のアイコン) を選択します。
2. [システム情報 (System Information)] を選択します。



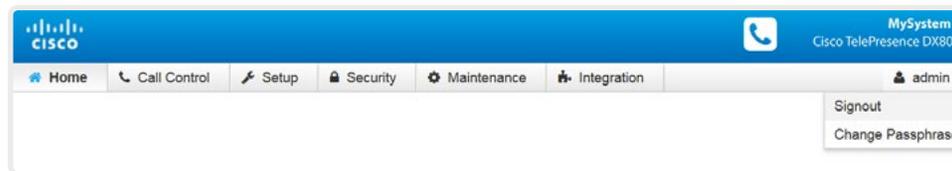
### サインイン

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。



システムには出荷時にデフォルト ユーザ *admin* (パスフレーズなし) が設定されています。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

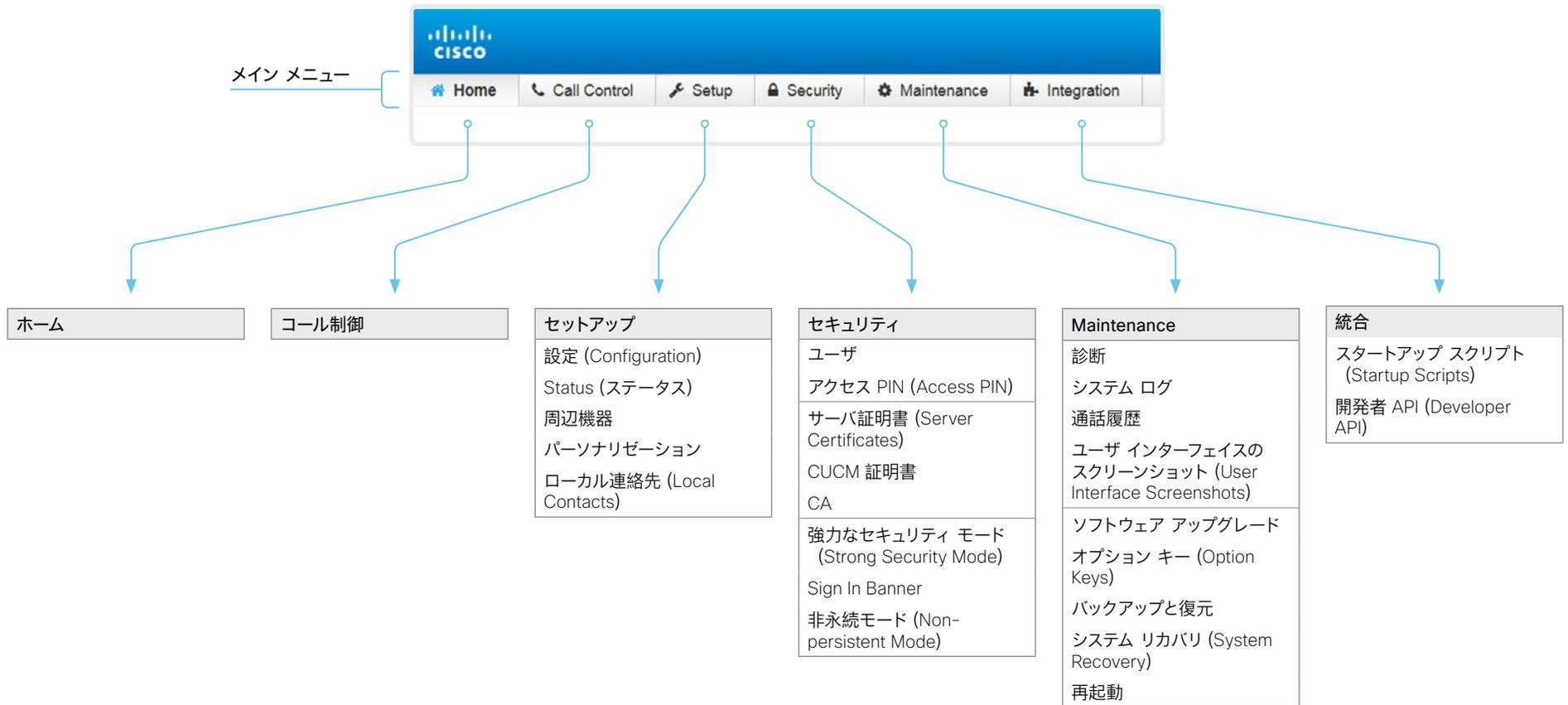
ユーザ名の上にカーソルを移動し、ドロップダウン リストから [サインアウト (Sign out)] を選択します。

ビデオ システムの管理方法 (3/4 ページ)

## Web インターフェイスの構成

Web インターフェイスはサブ ページで構成されています。サインインしているユーザには、そのユーザがアクセス権を持っているページのみが表示されます。

ユーザ管理、ユーザ ロール、およびアクセス権についての詳細は、▶「[ユーザ管理](#)」の章を参照してください。



ビデオ システムの管理方法 (4/4 ページ)

## 画面上で使用可能な設定

画面上で次の情報と設定にアクセスできます。

- ・ システム情報
- ・ 警告とエラー メッセージ
- ・ ビデオ システムの再起動
- ・ 言語、タイムゾーン、ネットワーク、およびプロビジョニング (サービスのアクティベーション) の基本設定
- ・ 拡張ロギング
- ・ 初期設定へのリセット

## システム情報および設定へのアクセス

1. ホーム画面で設定 (歯車) アイコンを選択します。
2. [システム情報 (System Information)] を選択すると、システム情報、潜在的な問題、および [再起動 (Restart)] ボタンが表示されます。
3. 次に [設定 (Settings)] を選択して、システム調整と基本構成を行います。

このメニューを開こうとすると、PIN コードの入力を求められる場合があります。詳細については、「▶ [画面上の設定メニューの PIN コードを設定する](#)」セクションを参照してください。

詳細については、ビデオ システムのスタートアップ ガイドを参照してください。

## 第 2 章

# 設定 (Configuration)

## ユーザ管理

### デフォルトのユーザ アカウント

エンドポイントには初期状態でデフォルトの管理者ユーザ アカウントにフル アクセス権が与えられています。ユーザ名は *admin* で、パスワードは初期設定されていません。

 必ず *admin* ユーザのパスワードを設定する必要があります。

パスワード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 アカウントを作成する

1. Web 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)]、[パスワード (Passphrase)]、[パスワードの確認 (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ワードを変更する必要があります。

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. 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、[自分のパスワード (Your passphrase)] 入力フィールドに自分自身のパスワード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。

\* パスフレーズにより、Web インターフェイスとコマンド ライン インターフェイスが保護されます。

### 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、[パスワード (Your passphrase)] 入力フィールドに確認のため各自のパスワードを入力する必要があります。

#### ユーザ特権を変更する

1. Web 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 ロールを選択して、ステータスを [アクティブ (Active)] または [非アクティブ (Inactive)] に設定し、ユーザが次のサインイン時にパスワード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. [ユーザの更新 (Update 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。

#### パスワードの変更

1. Web 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ワードを入力します。

4. [パスワードの変更 (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 アカウントの削除

1. Web 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. [削除 <ユーザ名>... (Delete <user name>...)] 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 ロールについて

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せん。フル アクセス権を持つユーザ アカウント (デフォルトの *admin* ユーザなど) は、すべてのロールを所有する必要があります。

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。

USER ロールと ADMIN ロールでは権限が重複しています。

**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。

AUDIT ユーザ ロールの権限は、他のロールの権限と重複していません。

## システム パスフレーズの変更

システム パスフレーズは、以下の操作を行うときに必要となります。

- Web インターフェイスへのサインイン
- コマンドライン インターフェイスへのサインインと使用

### 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 アクセス権を持つデフォルトのユーザ アカウントが付属しています。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 システムには多くのユーザ アカウントを作成できます。

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、in the [「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. Web 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、[パスフレーズの変更 (Change passphrase)] 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。

 パスフレーズが現在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。



## 他のユーザのパスフレーズの変更

管理者アクセス権を持っている場合は、任意のユーザのパスワードを変更できます。

1. Web 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。

## 画面上の [設定 (Settings)] メニューの PIN (暗証番号) コードの設定

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、画面上の [設定 (Settings)] メニューに PIN (暗証番号) コードを設定することを推奨します。

### PIN コードの設定

1. Web インターフェイスにサインインし、[セキュリティ (Security)] > [アクセス PIN (Access PIN)] に移動します。
2. PIN (暗証番号) コードを入力フィールドに入力して、[PIN (暗証番号) の設定 (Set PIN)] をクリックします。  
PIN (暗証番号) には数字だけを使用できます。

### PIN (暗証番号) コードの変更

1. Web インターフェイスにサインインし、[セキュリティ (Security)] > [アクセス PIN (Access PIN)] に移動します。
2. [PIN (暗証番号) の (Clear PIN)] をクリックします。

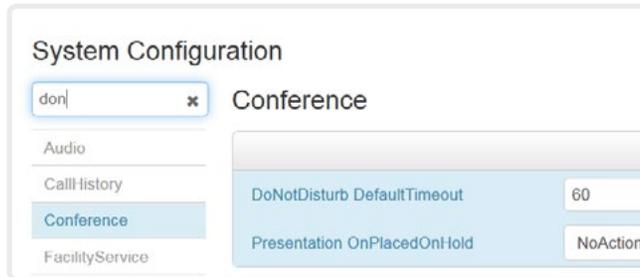
## システム設定

Web 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。

### システム設定の検索

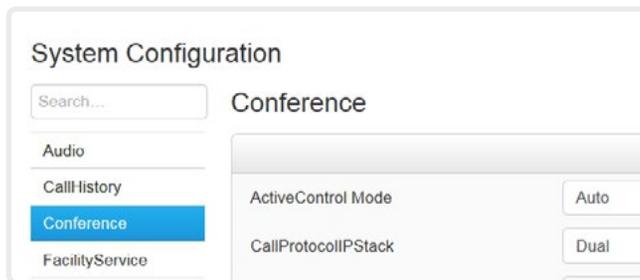
#### 設定の検索

検索フィールドに必要な数の文字を入力します。これらの文字を含む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

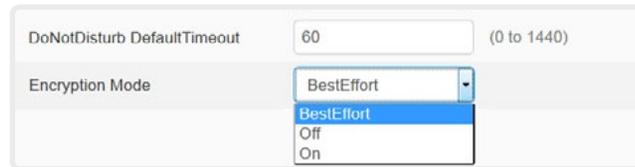
システム設定はカテゴリ別に分類されています。左ペインでカテゴリを選択すると、関連する設定が表示されます。



### システム設定を変更する

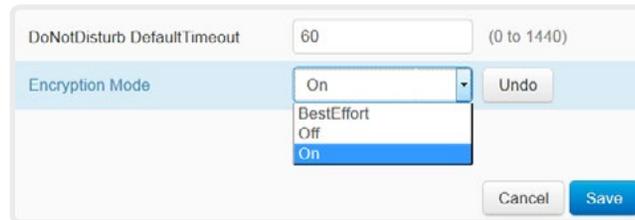
#### 値スペースのチェック

設定の値スペースは、入力フィールドの後のテキストにより、または矢印をクリックして表示されるドロップダウン リストにより指定されます。



#### 値を変更する

- ドロップダウン リストから適切な値を選択するか、入力フィールドに新しいテキストを入力します。
- [保存 (Save)] をクリックして変更を有効にします。  
変更を加えない場合は、[元に戻す (Undo)] または [キャンセル (Cancel)] 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

Web 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」](#)の章で説明しています。

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

Web 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. ユーザがサインインしたとき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。

The image shows a configuration interface for the Sign In Banner. At the top, a box titled "Sign In Banner" contains the text: "The Sign In Banner will be displayed when signing in using SSH, telnet, web and RS 232." Below this is a text input field containing the message: "The information you type here will be shown to all users when they sign in." A blue "Save" button is located below the input field. Arrows point from the "Save" button to a terminal window and a web browser window. The terminal window shows a login prompt: "login as: admin", followed by the banner message, "Using keyboard-interactive authentication.", and "Password:". The web browser window shows the login page with the same banner message displayed above the "Sign In" form, which includes fields for "Username:" and "Passphrase:" and a "Sign In" button. The system name "MySystem" is also visible at the bottom of the login form.

### 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 Web 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。

## ビデオ システムのサービス証明書の管理

Web 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。

### 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。

証明書は、HTTPS サーバ、SIP、IEEE 802.1X、および監査ロギング 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。

### 証明書の有効化、無効化、表示、または削除

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、対応するボタンを使用します。

Certificate	Issuer	HTTPS server	SIP	802.1X	Audit log		
Certificate_A	CertificateAuthority_A	On	Off	Off	Off	Delete...	View Certificate
Certificate_B	CertificateAuthority_B	Off	Off	Off	Off	Delete...	View Certificate

**Add Certificate**

Certificate  No file selected.

Private key (optional)  No file selected.

Passphrase (optional)

This system supports PEM formatted certificate files (.pem). The certificate file may contain the certificate and a RSA or DSA encrypted private key with or without a passphrase. Optionally the private key file may be supplied separately.

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。

### 証明書の追加

1. [参照... (Browse...)] をクリック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. 必要に応じて、[パスフレーズ (Passphrase)] に値を入力します。
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。

## 信頼できる認証局 (CA) のリストの管理

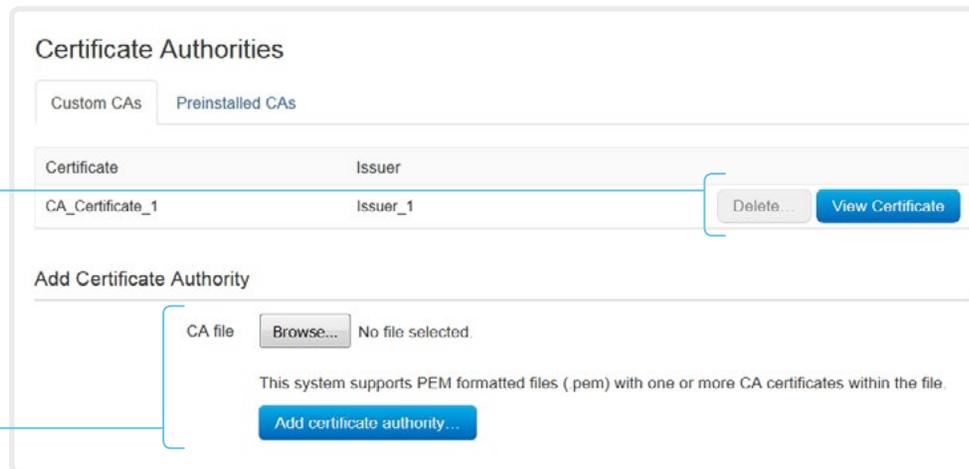
Web インターフェイスにサインインし、[セキュリティ (Security)] > [証明機関 (Certificate Authorities)] に移動して、[カスタム CA (Custom CAs)] タブを開きます。

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)。

### 証明書の表示または削除

証明書を表示または削除するには、対応する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。

### 認証局のリストのアップロード

1. [参照... (Browse...)] をクリックして、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. [証明局の追加... (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。



過去に保存した証明書は自動的に削除されません。

CA 証明書を含む新しいファイルのエントリが既存のリストに追加されます。

### 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 によって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、監査ロギング用および他の接続用に証明書を検証するのに必要なすべての CA が含まれる必要があります。

認証が失敗した場合、接続は確立されません。

## 安全な監査ロギングのセットアップ

Web 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」リストに含まれている必要があります。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)] 設定を見つけ、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。

[保存 (Save)] をクリックして変更を有効にします。

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。

[保存 (Save)] をクリックして変更を有効にします。

The screenshot shows the 'Security' configuration page. Under the 'Audit' section, the 'Logging Mode' dropdown is open, showing options: External, ExternalSecure (selected), Internal, and Off. The 'OnError Action' is set to 'ExternalSecure'. Under the 'Server' section, the 'Address' field is empty, 'Port' is set to 514, and 'PortAssignment' is set to 'Auto'. There are 'Refresh', 'Collapse all', and 'Expand all' buttons at the top right. 'Cancel' and 'Save' buttons are present at the bottom right of each section.

### 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。

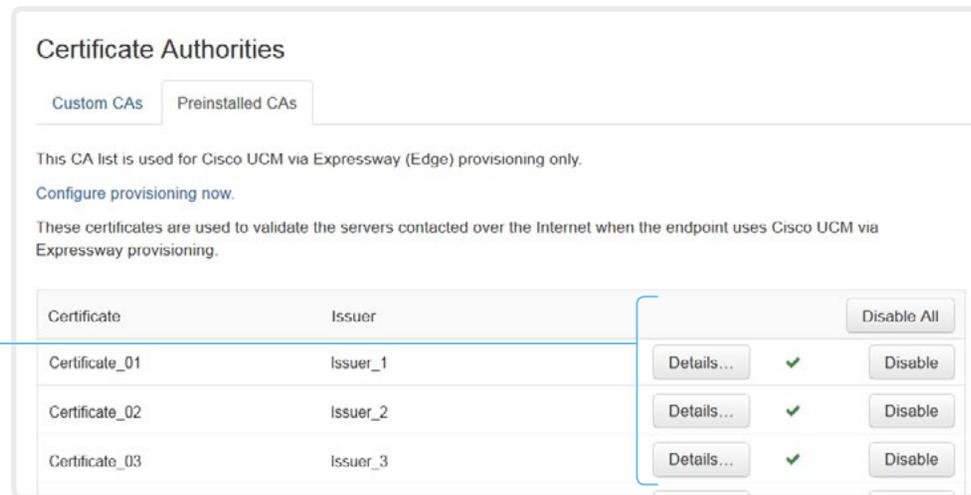
ExternalSecure 監査ログ モードでは、ビデオ システムは暗号化された監査ログを外部監査サーバ (syslog サーバ) に送信します。そのサーバの ID は署名された証明書によって検証される必要があります。

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

監査サーバの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

Web 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。

**i** 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。

### プレインストール済み証明書について

このリスト内のプレインストール済み証明書は、ビデオ システムが Expressway (Edge) 経由で Cisco Unified Communications Manager (CUCM) によって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に照らして検査されます。

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

ビデオ システムを工場出荷時設定にリセットしても、プレインストール済み証明書のリストは削除されません。

## CUCM 信頼リストの削除

この章の情報は、Cisco Unified Communications Manager (CUCM) に登録されているビデオ システムにのみ該当します。

Web 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 信頼リストの削除

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。

ただし、次のケースではこれらを削除する必要があります。

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

### 信頼リストのフィンガープリントと証明書についての概要

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、Web 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つ可能性があります。

### 信頼リストについての詳細情報

CUCM と信頼リストの詳細については、シスコの Web 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

Web 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

ビデオ システムの現在の永続性ステータスは、アクティブ ラジオ ボタンで示されます。

または、[セットアップ (Setup)] > [ステータス (Status)] > [セキュリティ (Security)] > [永続性 (Persistence)] に移動してステータスを確認します。

### 永続設定の変更

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...)] をクリックします。

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



非永続モードへの切り替え前に保存されたログ、設定、その他のデータは消去/削除されません。

### 永続モードについて

デフォルトでは、すべての永続設定は [永続 (Persistent)] に設定されます。つまり、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)、IP 接続情報が通常どおり保存されます。システムを再起動してもこの情報は削除されません。

原則として、永続のデフォルト設定を変更しないことを推奨します。以前のセッションでロギングされたあらゆる情報の表示やトレースをユーザに許可しない場合は、[非永続 (Non-persistent)] モードを使用する必要があります。

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
- ・ 発信または受信されたコールに関する情報 (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内容
- ・ 前回のセッションでのすべての IP 関連情報 (DHCP)



非永続モードに変更する前に保存された情報を消去/削除するには、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。

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

Web 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、その前に [強力なセキュリティ モードの有効化... (Enable Strong Security Mode...)] をクリックして、表示されるダイアログボックスで選択を確認します。

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、パスワードを変更します。新しいパスワードは、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」](#)の章で説明しています。

### 通常モードに戻る

[強力なセキュリティ モードの無効化... (Disable Strong Security Mode...)] をクリックします。ビデオ システムが通常モードに戻ります。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。

#### Strong Security Mode

Strong Security Mode is **not** enabled.

Strong Security Mode is required to adhere to U.S. Department of Defense JITC regulations.

It will introduce the following:

- All users and administrators must change their passphrase and PIN on the next sign in
- New passphrases must meet the following criteria:
  - Minimum 15 characters
  - Minimum 2 uppercase alphabetic characters
  - Minimum 2 lowercase alphabetic characters
  - Minimum 2 numerical characters
  - Minimum 2 non-alphanumeric (special) characters
  - No more than 2 consecutive characters may be the same
  - Must be different from the last 10 previous passphrases used
  - Not more than 2 characters from the previous passphrase can be in the same position
- Passphrases must be changed at least every 60 days
- Passphrases cannot be changed more than once per 24 hours
- 3 failed signins will lock the user account until an administrator re-activates the account

Enable Strong Security Mode.

#### Strong Security Mode

Strong Security Mode is enabled.

Disable Strong Security Mode...

### 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てください。

強力なセキュリティ モードにより、非常に厳格なパスワード要件が設定され、すべてのユーザは次回のサインイン時にパスワードを変更するよう要求されます。

## ビデオ品質の対コール レート比調整

### 最適鮮明度プロファイル

最適鮮明度プロファイルは、ビデオ会議室の照明状態とカメラ (ビデオ入力ソース) の品質を反映します。照明の状態およびカメラの品質が優れているほど、使用するプロファイルは高度になります。良い光の条件では、ビデオ エンコーダは指定のコール レートに一層優れた品質 (高解像度またはフレーム レート) を提供します。

通常は、[中 (Medium)] プロファイルをお勧めします。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。特定のコール レートの解像度を上げるために、高いプロファイルを設定することもできます。

### ビデオ入力品質の設定

最適鮮明度設定を有効にするには、*Video Input Connector n Quality* 設定を **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。

Web 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)] を選択します。

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 (内部カメラ) 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、優先する最適鮮明度プロファイルを選択します。

## 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 はシスコ独自のプロトコルです。CE ソフトウェアを実行するすべてのエンドポイントが ClearPath に対応しています。

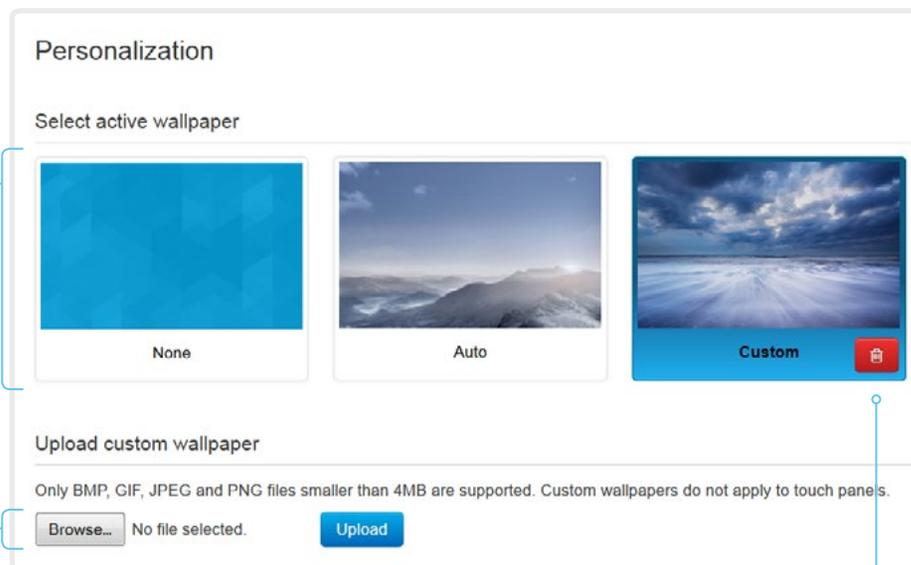
関係するエンドポイントとインフラストラクチャ要素が ClearPath に対応している場合、ポイントツーポイント接続ですべてのパケット損失回復メカニズム (ホスト型会議を含む) が使用されます。

## 壁紙の選択

Web 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)] に移動します。

### 壁紙の選択

リストから壁紙を選択します。  
アクティブな壁紙が強調表示されます。



### 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...)] をクリックして、カスタム壁紙イメージ 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: 4 MB

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。

もう一度使用するには、新たに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

企業ロゴまたは別のカスタム画像をメイン ディスプレイの背景に表示したい場合は、カスタムの壁紙をアップロードして、使用できます。

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。

カスタムの壁紙を使用すると、次の項目がメイン ディスプレイから削除されます。

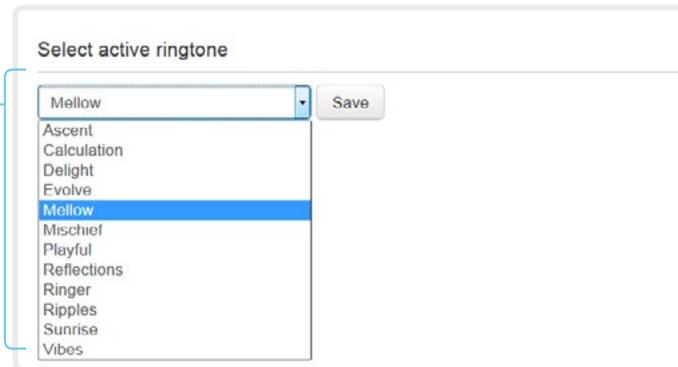
- ・ 時計
- ・ 予定されている会議のリスト

## 着信音の選択と着信音量の設定

Web 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、Web インターフェイスを使用します。

Web 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。呼び出し音は、Web インターフェイスを実行しているコンピュータではなく、ビデオ システム自体で再生されることに注意してください。

## ローカル連絡先の管理

Web インターフェイスにサインインして、[セットアップ (Setup)] > [ローカル連絡先 (Local Contacts)] 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り入れるには [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. 表示されたフォームに値を入力するか、更新します。

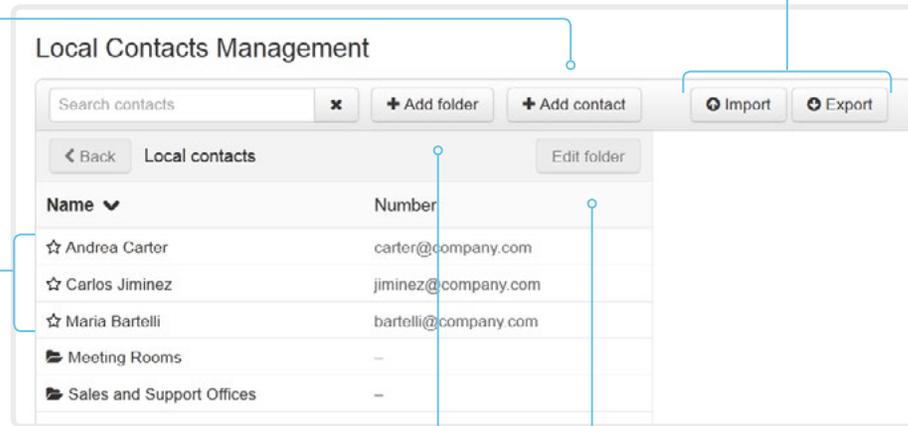
連絡先をサブフォルダに保存するには、フォルダ ドロップダウン リストでフォルダを選択します。

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) を保存するには、[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。



### サブフォルダの追加または編集

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、列挙されたサブフォルダのいずれかをクリックして [フォルダの編集 (Edit folder)] をクリックし、既存のサブフォルダを変更します。
2. 表示されたフォームに値を入力するか、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。

### サブフォルダの削除

1. [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。

## ローカル連絡先の場所

画面上: [発信 (Call)] > [ディレクトリ (Directory)] > [ローカルの連絡先 (Local contacts)] を選択します。ローカルの連絡先は、フォルダの階層を無視してアルファベット順に表示されます。

Web インターフェイス: [コール制御 (Call Control)] をクリックして、[連絡先 (Contacts)] セクションで [ローカル (Local)] タブを開きます。

## お気に入りリスト

[お気に入り (Favorites)] リストは、画面上でのみ使用できます。[お気に入り (Favorites)] リストは、Web インターフェイスでは使用できません。

このリストを見つけるには、[発信 (Call)] > [お気に入り (Favorites)] を選択します。[ローカルの連絡先 (Local contacts)] および他の [ディレクトリ (Directory)] のエントリの両方を [お気に入り (Favorites)] リストに追加できます。

また、お気に入りとマークされたディレクトリ エントリは、[ローカルの連絡先 (Local contacts)] のフォルダに自動的にコピーされます。

## お気に入りリストへの連絡先の追加

画面上: 連絡先を選択してから、\*\*\*を選択します。[お気に入りに設定 (Mark as Favorite)] をクリックします。

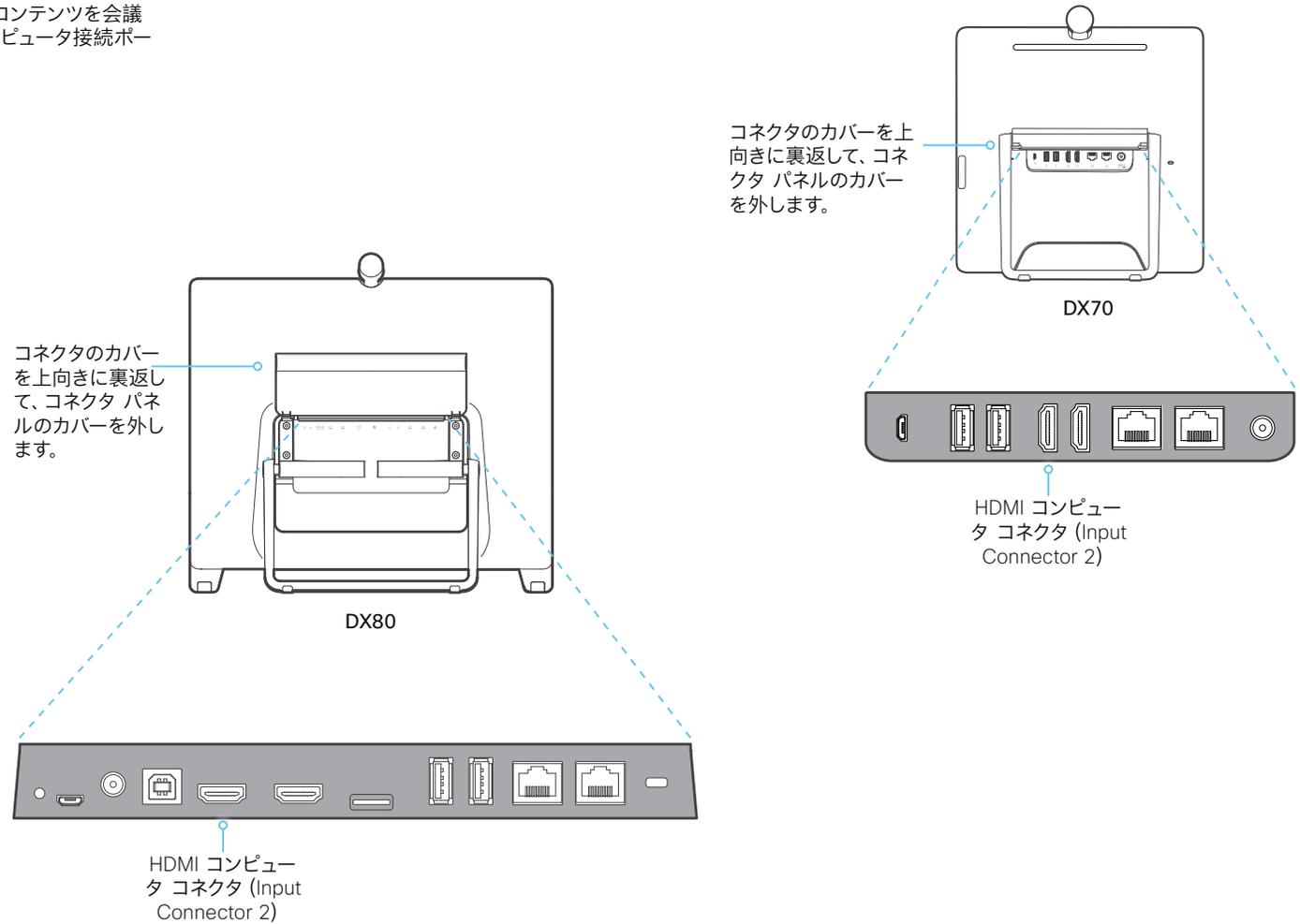
Web インターフェイス: [セットアップ (Setup)] > [ローカル連絡先 (Local Contacts)] に移動します。連絡先の横にある星マークをクリックします。

## 第 3 章

# 周辺機器

## コンピュータの接続

ビデオ システムをコンピュータの画面として使用し、コンテンツを会議の参加者と共有するには、コンピュータを HDMI コンピュータ接続ポートに接続します。



## 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

### Android ベースのソフトウェアと CE ソフトウェアとの間の変換

コラボレーション ソフトウェア バージョン 8.2 (CE8.2) 以降、すべての DX80 ユニットおよび DX70 ユニットで CE ソフトウェアを実行できます。このソフトウェアは、Cisco TelePresence SX および MX シリーズで動作するソフトウェアと同じものです。

Cisco DX80 と Cisco DX70 は、元々 Android ベースのソフトウェアとともに販売されていましたが、近く CE ソフトウェアとともに出荷される予定です。

CE ソフトウェアに変換する前に、変換の要件、および Android ベースのソフトウェアと比較した機能の変化点を注意深く確認することが重要です。

DX デバイス上の CE ソフトウェアでは、CE8.2 の次の機能はサポートされていません。

- ・ ワイヤレス ネットワーク (Wi-Fi)
- ・ Bluetooth ヘッドセット
- ・ サードパーティ製アプリケーションのインストール
- ・ キーボード コントロール、キーボードおよびマウスのリダイレクト
- ・ ボイスメール、エクステンション モビリティ、転送、コール転送、共有回線

詳細については、ソフトウェア リリース ノートを参照してください。

Android ベースのソフトウェアから CE ソフトウェアへの変換、またはその逆の変換の方法の詳細については、[▶http://www.cisco.com/go/dx-docs](http://www.cisco.com/go/dx-docs) [英語] にある「*Install and Upgrade Guides*」で入手できる『Cisco DX70 and DX80 Convert between CE and Android based software』を参照してください。

## システム ソフトウェアをアップグレードする (2/2ページ)

注: 以下の手順では、別の CE ソフトウェアのバージョンへのアップグレード (たとえば、CE8.2.x から CE8.2.y) のみを行います。

Android ベースのソフトウェアと CE ソフトウェアの間で変換したい場合は、前のページを参照してください。

Web インターフェイスにサインインして、[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のダウンロード

ソフトウェアをダウンロードするには、システムのソフトウェア ダウンロード Web ページ (<http://www.cisco.com/cisco/software/navigator.html>) にアクセスします。次に、お使いの製品に移動します。

ファイル名の形式は「s52040ce8\_2\_x.pkg」です。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。

### 新しいソフトウェアのインストール

該当するソフトウェア 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 .pkg ファイルです。

- [参照... (Browse...)] をクリックして、新しいソフトウェアを含む .pkg ファイルを探します。  
ソフトウェア バージョンが検出され、表示されます。
- [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。

通常、インストールは 15 分以内に完了します。Web ページから進捗状況を確認できます。インストール後、ビデオ システムは自動的に再起動します。

再起動後に Web 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。

### 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 (CE8) を読むことを推奨します。

参照先: <http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-series-home.html> [英語]

### ソフトウェア バージョンについて

このビデオ会議システムは CE ソフトウェアを使用しています。このドキュメントに記載されているバージョンは、CE8.2.x です。



### ソフトウェア バージョンの確認

ファイルを選択すると、ソフトウェア バージョンがここに表示されます。

## オプション キーの追加

Web インターフェイスにサインインして、[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、シスコ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. 適切なテキスト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。

Serial number .....

Option key

Contact your Cisco representative to obtain option keys.  
You need to provide the serial number to get option keys.

Add option key

### 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にするには、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。

ビデオ システムごとに一意のオプション キーが割り当てられます。

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

Web インターフェイスにサインインして、[システム情報 (System Information)] ページを表示します。

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

Web 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 エントリの検索

検索フィールドに必要な数の文字を入力します。これらの文字を含む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るエントリも表示されます。

**System Status**

Search: vol  **Audio**

Audio	
Bookings	
Cameras	
Capabilities	

Volume	70
VolumeHandsetUsb	50

#### 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分類されています。左ペインでカテゴリを選択すると、右側に関連ステータスが表示されます。

**System Status**

Search:  **Conference**

Audio	
Bookings	
Cameras	
Capabilities	
Conference	

ActiveSpeaker CallId	0
DoNotDisturb	Inactive
Line 1 Mode	Private
Multinoint Mode	CUCMMediaResourceGroup list

\* 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

Web 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\*。

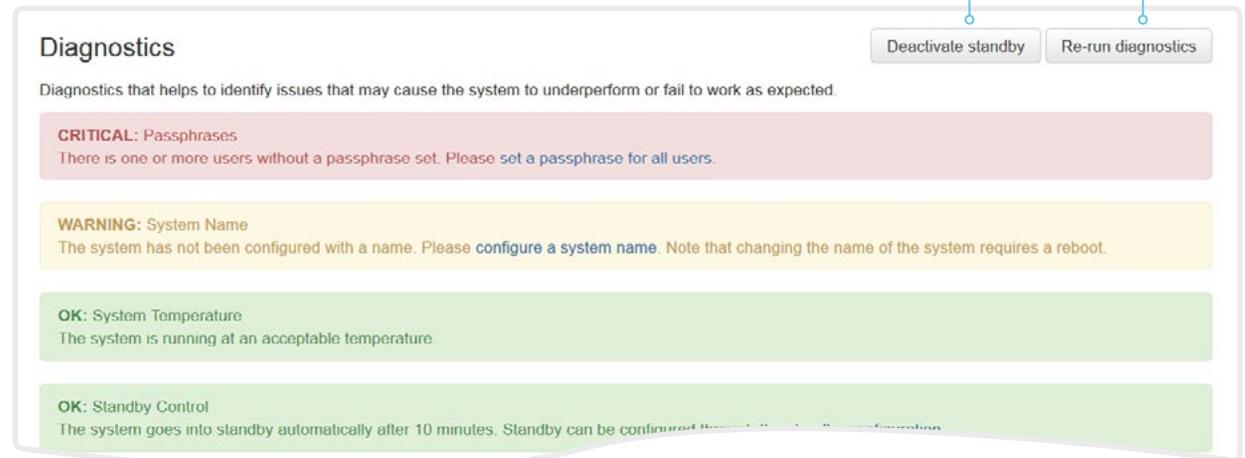
エラーや重大な問題は赤色で目立つように示されます。警告は黄色です。

### 診断の実行

[診断の再実行 (Re-run diagnostics)] をクリックして、リストが最新であることを確認します。

### 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、[スタンバイの非アクティブ化 (Deactivate standby)] 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 ファイルのダウンロード

Web 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)] に移動します。

### すべてのログ ファイルのダウンロード

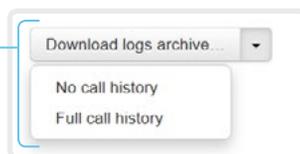
[ログ アーカイブのダウンロード (Download logs archive)] をクリックして、手順に従います。

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せん。

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) を含める場合には、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 Web 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。



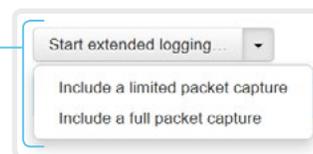
### 拡張ロギングの開始

[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、シスコのサポートから要求されることがあるシスコ固有のデバッグ 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 システムのパフォーマンスが低下する可能性があります。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 ユーザの作成

Web 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 によって指示されたトラブルシューティングを行う場合にのみ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。

The system does not have an active Remote Support User.

Create user

Delete user

This user is valid until  
2015-11-11 08:35:06

#### Token

```
hgD9FjGyIUNn0TB71KcmT1FPnx6uY0vTFy9kpiUa5z1+b
TQek1PaSpsQJNEMfzThgbvK4J7pgoyt4lmCyvxWPGipJQ
GL0ynjvHBvhfqYEsSWwCSSZxQ1wP6bUPQzOSgztZnkOG7
c9CpAoRNng+mZMqEG1lsswKPZ7HYulvyVTH/XuPzU7Nucs
9pwzLc8BFgBt1xV0fKeoeOmMX+it1Ecamln4lnXlScgOt
yPSXiFWLdKAJsQHJQH20PCxxYcnEUYNpAoJiD39edLy4
etY+/SATwBIiohrgF9JLW9FfNEF+IyD1wUmYkPoEirBj7
N3Zvpivlv1Z7+NUalQW9qWTj4Aq==
```

The system has an active Remote Support User.

Create user

Delete user

### 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いくつかの限定的な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。

## 設定のバックアップまたは復元

Web 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。

### 現在の設定の表示

現在の設定を画面上に表示するには、[バックアップのプレビュー (Preview backup)] をクリックします。

### 現在の設定のバックアップ

設定をテキスト ファイルとして保存するには、[バックアップを取る (Take backup)] をクリックします。

### バックアップからの設定の復元

1. [参照... (Browse...)] をクリックして、復元する設定を含むバックアップ ファイルを見つけます。
2. システムをファイルで定義されているとおりに再設定するには、[復元 (Restore)] をクリックします。

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。

### 設定のバックアップについて

[システム設定 (System configuration)] ページで使用可能なすべてのシステム設定を画面に一覧表示することも、バックアップ テキスト ファイルとして保存することもできます。

バックアップ テキスト ファイルをシステムにロードし直して設定を復元することができます。

## 以前使用していたソフトウェア イメージへの復元

Web 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。

注: 以下の手順では、別の CE ソフトウェアのバージョンへの復元 (たとえば、CE8.2.y から CE8.2.x) のみを行えます。

Android ベースのソフトウェアに変換して戻す場合は、▶「[システム ソフトウェアをアップグレードする](#)」の章を参照してください。

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 ファイルと設定をバックアップすることをお勧めします。

### ログ ファイルとシステム設定のバックアップ

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. [設定バックアップのダウンロード (Download Configuration Backup)] をクリックし、指示に従って設定ファイ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

この手順は管理者のみが実行するか、またはシスコ テクニカル サポートと連絡を取っている場合にのみ実行してください。

1. [ソフトウェア リカバリのスワップ (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。この手順には数分かかることがあります。

### 以前使用していたソフトウェア 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以降、システムをまだ工場出荷時設定にリセットしていない場合は、以前に使用したソフトウェア イメージがシステム上に残っています。ソフトウェアを再度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 (1/2 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。



工場出荷時設定リセットは元に戻すことができません。

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。ソフトウェアの交換については、▶ [「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 システムを工場出荷時の状態へリセットするには、Web インターフェイスを使用することを推奨します。Web インターフェイスを使用できない場合は、DX80 ではリセット ボタンを、DX70 ではミュート ボタンと音量ボタンを使用します。

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。

- コール ログが削除されます。
- パスフレーズがデフォルト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されていたファイルは、すべて削除されます。これには、カスタムの壁紙、証明書、ローカルの連絡先、およびお気に入りリストが含まれ、また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。

工場出荷時設定リセットを実行する前に、ビデオ システムのログ ファイルと設定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。

### ログ ファイルとシステム設定のバックアップ

Web 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 ファイルとシステム設定のバックアップ

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. [設定バックアップのダウンロード (Download Configuration Backup)] をクリックし、指示に従って設定 ファイルをコンピュータに保存します。

### Web インターフェイスを使用した工場出荷時設定リセット

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。

Web 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。

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. [初期設定リセットの実行 (Perform a factory reset...)] をクリックします。
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。

ビデオ システムの工場出荷時設定リセットを確認する通知がメイン画面に表示されます。通知は約 10 秒後に非表示になります。

## ビデオ システムの工場出荷時設定リセット (2/3 ページ)

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。

### ミュート ボタンと音量ボタンを使用した DX80 の工場出荷時設定へのリセット

次の手順を実行して、起動時に DX80 を工場出荷時設定にリセットします。ビデオ システムの電源がオンになっている場合、先に進む前に電源ボタンを押して、システムがシャットダウンするまで押し続けます。

1. **ミュート** ボタンと **音量アップ** ボタンを見つけます。
2. 音量アップ ボタンを押したままにして、デバイスの電源をオンにします。
3. ミュート ボタンが赤色に点灯したら、音量アップ ボタンを放し、ミュート ボタンを押します。

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。

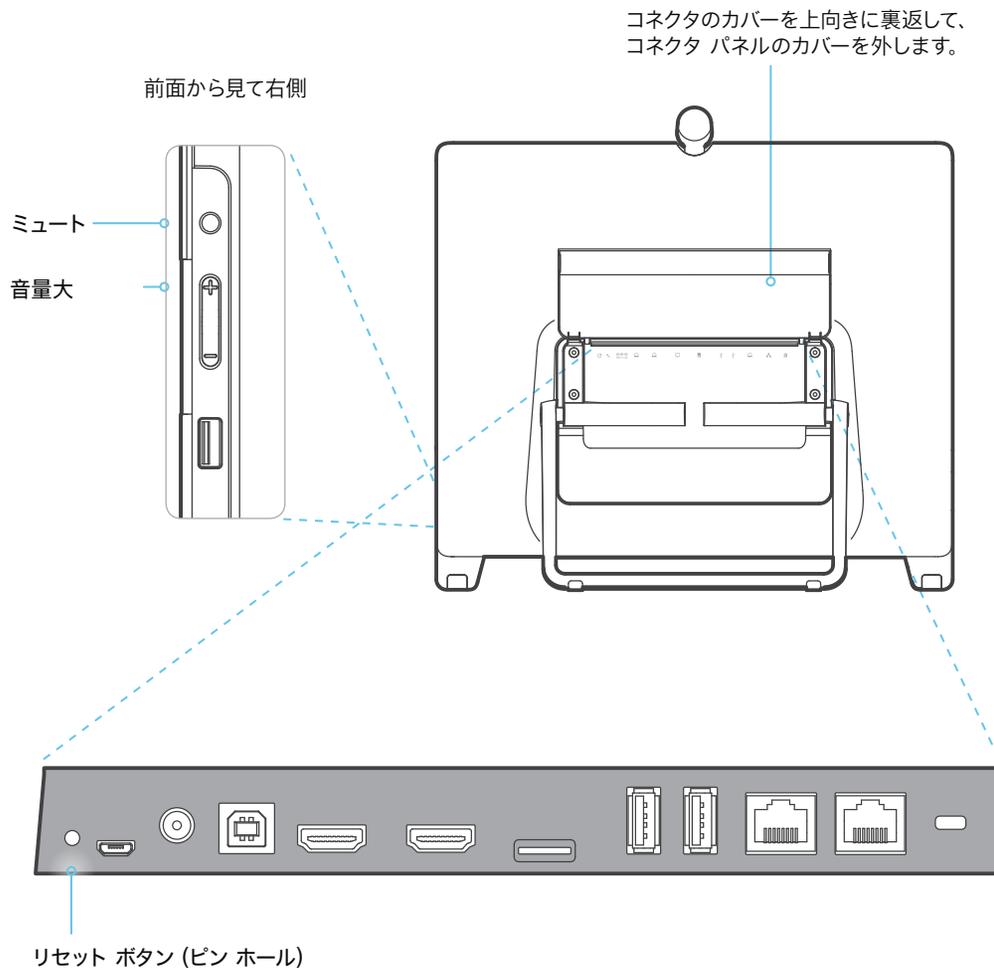
システムが工場出荷時の設定に正常にリセットされると、セットアップ アシスタントが起動し、[ようこそ (Welcome)] 画面が表示されます。詳細については、DX80 のスタートアップガイドを参照してください。

### リセット ボタンを使用した DX80 の工場出荷時設定へのリセット

この方法を使用するには、DX80 が稼動している必要があります。

1. ビデオ システムの背面で、コネクタのカバーを上向きに裏返して、コネクタ パネルのカバーを外します。
2. ペン先 (または同等のもの) を使用して、引っ込んでいるリセット ボタンを押して、[初期設定へのリセットを実行しています (Resetting to factory settings)] という通知が画面に表示されるまで、このボタンを 1 ~ 2 秒間押し続けます。
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。詳細については、DX80 のスタートアップガイドを参照してください。



ボタンは引っ込めて取り付けられているため、使用がかなり難しい場合があります。ボタンを押すと、ボタンが下がる感覚がわかります。

## ビデオ システムの工場出荷時設定リセット (3/3 ページ)

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。

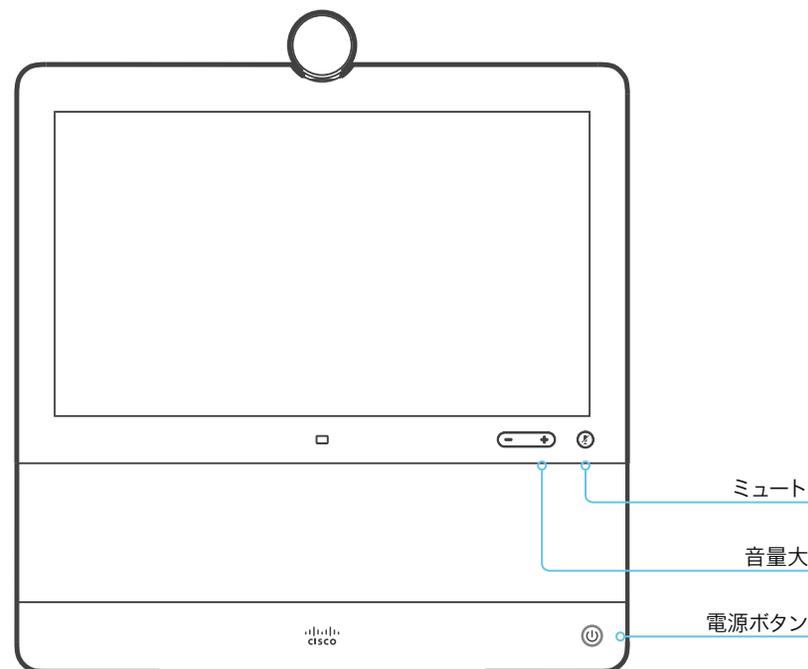
### ミュート ボタンと音量ボタンを使用した DX70 の工場出荷時設定へのリセット

次の手順を実行して、起動時に DX70 を工場出荷時設定にリセットします。ビデオ システムの電源がオンになっている場合、先に進む前に電源ボタンを押して、システムがシャットダウンするまで押し続けます。

1. **ミュート** ボタン (LED) と **音量アップ** ボタン (LED) を見つけます。
2. 電源ボタンを押して、**ミュート** ボタンに注目してください。
3. **ミュート** ボタンが 2 回点滅したら、**音量アップ** ボタンを押し、そのすぐ後に約 4 秒間 **ミュート** ボタンを押し続けます。このプロセス中に、**ミュート** ボタンが数秒間赤になります。

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。詳細については、*DX70 のスタートアップ ガイド* を参照してください。



## ユーザ インターフェイスのスクリーンショットのキャプチャ

Web 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

画面上の表示のスクリーンショットをキャプチャするには、[OSD のスクリーンショットを撮る (Take screenshot of OSD)] をクリックします。

スクリーンショットはボタンの下の領域に表示されます。スクリーンショットの準備ができるまでに最大 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。スクリーンショット ID をクリックするとイメージが表示されます。

### スクリーンショットの削除

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 **X** ボタンをクリックします。

### ユーザ インターフェイスのスクリーンショットについて

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、およびメッセージ) 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、Web 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。

Web 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. ホーム画面で [設定 (settings)] アイコン (歯車の形のアイコン) を選択します。
2. [システム情報 (System Information)] を選択します。

音声設定 .....	52
オーディオ サウンドと着信音 .....	52
オーディオ サウンドと着信音量 .....	52
オーディオのデフォルト音量 .....	52
オーディオ マイク ミュートの有効化 .....	52
オーディオ入力マイクロフォンモード .....	53
通話履歴設定 .....	54
通話履歴モード .....	54
会議設定 .....	55
Conference MaxTotalReceiveCallRate .....	57
会議 アクティブ コントロール .....	55
会議のサイレントセッションのデフォルト期間 .....	56
会議のデフォルト コール レート .....	56
会議の暗号化モード .....	56
会議の最大受信コールレート .....	56
会議の最大転送レート .....	57
会議の遠端制御信号機能 .....	56
会議ビデオ帯域幅プレゼンテーション チャンネルの重み .....	58
会議ビデオ帯域幅モード .....	57
会議保留中のプレゼンテーション .....	57
会議切断時のマイクのミュート解除モード .....	57
会議最大総送信コールレート .....	57
会議 自動応答 ミュート .....	55
会議 自動応答モード .....	55
会議 自動応答 遅延 .....	55
会議 通信プロトコル IP スタック .....	55
会議遠端制御モード .....	56
H323 設定 .....	59
H323 H323エイリアス E164 .....	60
H323 H323エイリアス ID .....	60
H323 NAT アドレス .....	60
H323 NAT モード .....	60
H323 ゲートキーパーのアドレス .....	59
H323 コールセットアップモード .....	59
H323 ポートアロケーション .....	61

H323 暗号化キーサイズ	59	ネットワーク [1] QoS モード	67
H323 認証パスワード	59	ネットワーク [1] VLAN 音声 VlanId	69
H323 認証モード	59	ネットワーク [1] VLAN 音声モード	69
H323 認証ログイン名	59	ネットワーク [1] トラフィック制御モード	69
ロギングの設定	62	ネットワーク [1] リモート アクセス 許可	68
ロギング モード	62	ネットワークサービス設定	70
ロギング 外部サーバのアドレス	62	NetworkServices HTTPS OCSP URL	71
ロギング 外部サーバのポート	62	NetworkServices SSH Mode	73
ロギング外部プロトコル	62	ネットワークサービス CDP モード	70
ロギング外部モード	62	ネットワークサービス H323 モード	70
ネットワーク設定	63	ネットワークサービス HTTPS OCSP モード	71
ネットワーク [1] DNS サーバ [1..3] アドレス	63	ネットワークサービス HTTPS クライアント証明書検証	71
ネットワーク [1] DNS ドメイン名	63	ネットワークサービス HTTPS サーバ証明書検証	70
ネットワーク [1] IEEE8021X Eap Md5	64	ネットワークサービス HTTP モード	70
ネットワーク [1] IEEE8021X Eap Peap	65	ネットワークサービス NTP サーバ [1..3] アドレス	71
ネットワーク [1] IEEE8021X Eap Tls	64	ネットワークサービス NTP モード	71
ネットワーク [1] IEEE8021X Eap Ttls	64	ネットワークサービス SIP モード	71
ネットワーク [1] IEEE8021X Tls検証	63	ネットワーク サービス SNMP コミュニティ名	72
ネットワーク [1] IEEE8021X アイデンティティ	64	ネットワーク サービス SNMP システム ロケーション	72
ネットワーク [1] IEEE8021X クライアント証明書使用	63	ネットワーク サービス SNMP システム接点	72
ネットワーク [1] IEEE8021X パスワード	64	ネットワークサービス SNMP ホスト [1..3] アドレス	72
ネットワーク [1] IEEE8021X モード	63	ネットワークサービス SNMP モード	72
ネットワーク [1] IEEE8021X 匿名のアイデンティティ	64	ネットワーク サービス SSH 公開キー許可	73
ネットワーク [1] IPv4 ゲートウェイ	65	ネットワークサービスTelnetモード	73
ネットワーク [1] IPv4 サブネット マスク	65	ネットワークサービス XMLAPI モード	73
ネットワーク [1] IPv4 モード	65	ネットワークサービス ウェルカムテキスト	73
ネットワーク [1] IPv4 割り当て	65	周辺機器の設定	74
ネットワーク [1] IPv6 DHCP オプション	66	周辺機器ペアリング ウルトラサウンド音量モード	74
ネットワーク [1] IPv6 アドレス	66	周辺機器ペアリング ウルトラサウンド音量最大レベル	74
ネットワーク [1] IPv6 ゲートウェイ	66	電話帳の設定	75
ネットワーク [1] IPv6 割り当て	66	外部電話帳サーバ [1] ID	75
ネットワーク [1] IP スタック	65	外部電話帳サーバ [1] URL	75
ネットワーク [1] MTU	66	外部電話帳サーバ [1] 種類	75
ネットワーク [1] QoS Diffserv ICMPv6	68	プロビジョニング設定	76
ネットワーク [1] QoS Diffserv NTP	68	プロビジョニング HTTP 方式	77
ネットワーク [1] QoS Diffserv オーディオ	67	プロビジョニングの接続性	76
ネットワーク [1] QoS Diffserv シグナリング	68	プロビジョニング パスワード	77
ネットワーク [1] QoS Diffserv データ	67	プロビジョニングモード	76
ネットワーク [1] QoS Diffserv ビデオ	67		

プロビジョニング ログイン名.....	76	SIP パスワード認証.....	84
プロビジョニング 外部マネージャーアドレス.....	77	SIPプロキシ[1..4]アドレス.....	86
プロビジョニング 外部マネージャードメイン.....	78	SIP メールボックス.....	85
プロビジョニング 外部マネージャーパス.....	77	SIP ユーザー名認証.....	84
プロビジョニング 外部マネージャープロトコル.....	77	SIP リッスンポート.....	85
プロビジョニング 外部マネージャー代替アドレス.....	77	SIP 優先IPシグナリング.....	86
RoomReset の設定.....	79	SIP 優先IPメディア.....	86
ルームリセット制御.....	79	SIP 回線.....	85
RTP 設定.....	80	SIP 表示名.....	84
RTP ポート範囲の開始.....	80	スタンバイ設定.....	88
RTP ポート範囲停止.....	80	スタンバイ制御.....	88
セキュリティ設定.....	81	スタンバイ遅延.....	88
セキュリティセッション ユーザーの最大セッション数.....	82	システムユニット設定.....	89
セキュリティセッション 最大総セッション数.....	82	システムユニット名.....	89
セキュリティセッション 最後のログオンを表示.....	82	時刻設定.....	90
セキュリティ監査 エラー処理時.....	81	タイムゾーン.....	91
セキュリティ監査サーバ アドレス.....	81	時刻の日付形式.....	90
セキュリティ監査サーバ ポート.....	82	時間の時刻形式.....	90
セキュリティ監査サーバ ポート割り当て.....	82	ユーザーインターフェース 設定.....	93
セキュリティ監査ロギング モード.....	81	ユーザーインターフェース OSD暗号化インジケータ.....	93
SerialPort 設定.....	83	ユーザーインターフェース キー トーンモード.....	93
シリアルポートモード.....	83	ユーザーインターフェース 言語.....	93
シリアルポート ログイン必須.....	83	ユーザーインターフェース 連絡先情報のタイプ.....	93
SIP 設定 (SIP settings).....	84	ユーザーインターフェイスOSDアウトプット.....	94
SIP ANAT.....	84	ユーザーインターフェイス壁紙.....	94
SIP Ice Tcp候補者の提供.....	85	UserManagement の設定.....	95
SIP Ice デフォルト候補.....	85	ユーザー管理 LDAP サーバー証明書検証.....	96
SIP Ice モード.....	85	ユーザー管理 LDAP サーバアドレス.....	95
SIP Tls検証.....	86	ユーザー管理 LDAP サーバポート.....	95
SIP Turn DropRflx.....	86	ユーザー管理 LDAP モード.....	95
SIP Turn サーバ.....	87	ユーザー管理 LDAP 属性.....	96
SIP Turn パスワード.....	87	ユーザー管理LDAP暗号化.....	95
SIP Turn ユーザ名.....	87	ユーザー管理 LDAP 最小TLSバージョン.....	95
SIP Turn 検出モード.....	86	ユーザー管理 LDAP 管理者グループ.....	96
SIP URI.....	87	ユーザー管理 LDAP 管理者フィルタ.....	96
SIP タイプ.....	87	ビデオ設定.....	97
SIP デフォルトトランスポート.....	84	デオ入力コネクタ [1..2] 名前.....	99

ビデオ アクティブスピーカーのデフォルト PIP ポジション .....	97
ビデオセルフビューオンコールモード .....	103
ビデオセルフビューオンコール時間 .....	103
ビデオセルフビューデフォルトのPIPポジション .....	103
ビデオセルフビューデフォルトフルスクリーンモード .....	102
ビデオセルフビューデフォルトモード .....	102
ビデオ デフォルトのメインソース .....	98
ビデオ デフォルトレイアウトファミリリモート .....	98
ビデオデフォルトレイアウトファミリローカル .....	97
ビデオプレゼンテーション デフォルトソース .....	102
ビデオプレゼンテーション デフォルトのPIPポジション .....	102
ビデオモニター .....	101
ビデオレイアウト 切断されたローカル出力を無効にする .....	101
ビデオ入力コネクタ[1..2] カメラ制御カメラID .....	98
ビデオ入力コネクタ [1..2] カメラ制御モード .....	98
ビデオ入力コネクタ [1..2] 入力ソースタイプ .....	98
ビデオ入力コネクタ [1..2] 最適鮮明度プロファイル .....	99
ビデオ入力コネクタ [1..2] 表示 .....	100
ビデオ入力コネクタ [2] RGB量子化範囲 .....	100
ビデオ入力コネクタ [2] プレゼンテーションの選択 .....	100
ビデオ入力コネクタ [2] 画質 .....	99
ビデオ出力コネクタ[1..2]解像度 .....	101
ビデオ出力コネクタ[1]ホワイトバランスレベル .....	101
ビデオ出力コネクタ[1]輝度 .....	101
ビデオ出力コネクタ[2] CECモード .....	101
ビデオ出力コネクタ [2] RGB量子化範囲 .....	101
ビデオ出力コネクタ [2] オーバースキャンレベル .....	101
ビデオ出力コネクタ [2] ロケーション垂直オフセット .....	101
ビデオ出力コネクタ [2] ロケーション水平オフセット .....	101
モニターロールでのビデオセルフビューのデフォルト .....	102
試験的設定 .....	104

## 音声設定

### オーディオのデフォルト音量

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、ビデオシステム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、デフォルト値にリセットしたり、ビデオシステムの実行中に音量を変更したりすることができます。

必要なユーザ ロール: admin, user

Default value: 50

値スペース: 整数 (0..100)

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、音声オフになります。

### オーディオ マイク ミュートの有効化

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

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。

### オーディオ サウンドと着信音

着信コールに使用する呼び出し音を定義します。

必要なユーザ ロール: admin, 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

リストから着信音を選択します。

### オーディオ サウンドと着信音量

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, USER

Default value: 50

値スペース: 整数 (0..100)

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。

## オーディオ入力マイクロフォンモード

この設定は DX80 にのみ適用されます。

DX80 では両方の脚にマイクが搭載されています。マイクロフォン モードを Focused に設定すると、複数のマイクの感度を中央の音声に集中させることができます。その結果、室内のノイズが聞こえなくなり、ビデオ システムの正面に座った人の声がよく聞こえるようになります。システムの正面に座っていない人の声は聞こえなくなります。

マイクロフォン モードを Wide に設定すると、システムは他のシステムと同様に動作します。横に座っている人の声が聞こえるようになり、また室内のノイズもより聞こえるようになります。

話者が 1 人のみの場合、Focused モードを使用することをお勧めします。システムの前で話している人が複数人いる場合は、Wide モードを使用してください。

必要なユーザ ロール: ADMIN

デフォルト値: Wide

値スペース: Focused/Wide

Focused: 1 点に集中された音の感度。ビデオ システムの真正面にないソースからの音は抑制されます。

Wide: 通常の音の感度によるデフォルトのマイク動作。

## 通話履歴設定

### 通話履歴モード

発信または受信された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)。これには、不在着信と応答されなかったコールが含まれます。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

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: 新しいエントリが通話履歴リストに保存されます。

## 会議設定

### 会議 アクティブ コントロール

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 の会議を管理するためのツールです。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) でサポートされている限り、デフォルトで有効です。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。

### 会議 自動応答モード

自動応答モードを定義します。コールに回答する前に数秒間待機する場合は Conference AutoAnswer Delay 設定を使用し、コールに回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: 着信コールに回答するには、[応答 (Answer)] をタップする必要があります。

On: 通話中でない限り、システムが自動的に着信コールに回答します。通話中の着信コールに対しては、常に手動で応答または拒否する必要があります。

### 会議 自動応答 ミュート

着信コールが自動的に応答する場合にマイクをミュートするかどうか定義します。[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。

### 会議 自動応答 遅延

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

Default value: 0

値スペース: 整数 (0..50)

自動応答遅延 (秒単位)。

### 会議 通信プロトコル IP スタック

システムで通信プロトコル (SIP) 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。

## 会議のデフォルト コール レート

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

Default value: 3072

値スペース: 整数 (64..3072)

デフォルトのコール レート (帯域) (kbps)。

## 会議のサイレントセッションのデフォルト期間

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。デフォルト値は 60 分です。

必要なユーザ ロール: ADMIN

Default value: 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)。

## 会議の暗号化モード

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。

## 会議遠端制御モード

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: 遠端はこちら側のビデオ 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。

## 会議の遠端制御信号機能

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。

## 会議の最大受信コールレート

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

Default value: 3072

値スペース: 整数 (64..3072)

最大受信コール レート (帯域) (kbps)。

## 会議の最大転送レート

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

Default value: 3072

値スペース: 整数 (64..3072)

最大送信コール レート (帯域) (kbps)。

## 会議最大総受信コールレート

受信全体の最大許容ビット レートを定義します。この製品は、同時に複数のコールをサポートしないため、合計送信帯域は 1 つのコールの送信ビット レートと同じになります (参照: Conference MaxReceiveCallRate 設定)。

必要なユーザ ロール: ADMIN

Default value: 3072

値スペース: 整数 (64..3072)

最大受信コール レート (帯域) (kbps)。

## 会議最大総送信コールレート

送信全体の最大許容ビット レートを定義します。この製品は、同時に複数のコールをサポートしないため、合計送信帯域は 1 つのコールの送信ビット レートと同じになります (参照: Conference MaxTotalTransmitCallRate 設定)。

必要なユーザ ロール: ADMIN

Default value: 3072

値スペース: 整数 (64..3072)

最大送信コール レート (帯域) (kbps)。

## 会議切断時のマイクのミュート解除モード

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。

## 会議保留中のプレゼンテーション

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

値スペース: Stop/NoAction

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。

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。

## 会議ビデオ帯域幅モード

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ン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ン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。

## 会議ビデオ帯域幅プレゼンテーション チャンネルの重み

使用可能な送信ビデオ帯域幅が「MainChannel Weight」および「PresentationChannel Weight」に従ってメイン チャンネルおよびプレゼンテーション チャンネルに配信されます。メイン チャンネルの重みが 2 で、プレゼンテーション チャンネルの重みが 1 の場合、メイン チャンネルはプレゼンテーション チャンネルの 2 倍の帯域幅を使用します。

必要なユーザ ロール: ADMIN

Default value: 5

値スペース: 整数 (1..9)

プレゼンテーション チャンネルの帯域幅の重みを設定します。

## H323 設定

### H323 認証モード

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 ゲートキーパーが示している場合、システムはゲートキーパーに対して自身の認証を試行します。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 認証ログイン名

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 認証パスワード

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 コールセットアップモード

H.323 コールの確立時にゲートキーパーまたはダイレクト 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。

Gatekeeper: システムはゲートキーパーを使用して H.323 コールを発信します。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 暗号化キーサイズ

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: Max1024bit

値スペース: Min1024bit/Max1024bit/Min2048bit

Min1024bit: 最小サイズは 1024 ビットです。

Max1024bit: 最大サイズは 1024 ビットです。

Min2048bit: 最小サイズは 2048 ビットです。

### H323 ゲートキーパーのアドレス

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 H323エイリアス 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 H323エイリアス 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 モード

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 アドレス

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。

\* Port 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 ポートアロケーション

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。

## ロギングの設定

### ロギング外部モード

ロギングにリモート syslog サーバを使用す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: Off

値スペース: Off/On

Off: リモート syslog サーバへのロギングを無効にします。

On: リモート syslog サーバへのロギングを有効にします。

### ロギング外部プロトコル

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。TLS (Transport Layer Security) を使用した syslog プロトコル、またはプレーン テキスト形式の syslog プロトコルを使用できます。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。

### ロギング 外部サーバのアドレス

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。

### ロギング 外部サーバのポート

リモート syslog サーバがメッセージをリッスンするポート。デフォルトの 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。標準 syslog ポートは、syslog の場合は 514、syslog over TLS の場合は 6514 です。

必要なユーザ ロール: ADMIN

Default value: 0

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 システムで標準 syslog ポートを使用することを意味します。

### ロギング モード

ビデオ システム (syslog サービス) のロギング モードを定義します。無効にすると、syslog サービスが起動せず、イベント ログの大部分が生成されません。履歴ログとコール ログ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。

## ネットワーク設定

### ネットワーク [1] DNS ドメイン名

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

デフォルト値: ""

値スペース: 文字列 (0, 64)

DNS ドメイン名。

### ネットワーク [1] DNS サーバ [1..3] アドレス

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

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。

### ネットワーク [1] IEEE8021X モード

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

デフォルト値: Off

値スペース: Off/On

Off: 802.1X 認証がディセーブルになります (デフォルト)。

On: 802.1X 認証がイネーブルになります。

### ネットワーク [1] IEEE8021X Tls検証

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、Web 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) の場合にだけ有効です。

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: 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。

### ネットワーク [1] IEEE8021X クライアント証明書使用

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、Web 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: 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: [オン (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。

## ネットワーク [1] IEEE8021X アイデンティティ

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

デフォルト値: ""

値スペース: 文字列 (0, 64)

802.1X 認証用のユーザ名。

## ネットワーク [1] IEEE8021X パスワード

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

デフォルト値: ""

値スペース: 文字列 (0, 32)

802.1X 認証用のパスワード。

## ネットワーク [1] IEEE8021X 匿名のアイデンティティ

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

デフォルト値: ""

値スペース: 文字列 (0, 64)

802.1X 匿名 ID 文字列。

## ネットワーク [1] IEEE8021X Eap Md5

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

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 プロトコルはイネーブルになります (デフォルト)。

## ネットワーク [1] IEEE8021X Eap Ttls

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

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 プロトコルはイネーブルになります (デフォルト)。

## ネットワーク [1] IEEE8021X Eap Tls

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。RFC 5216 で規定された 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

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 プロトコルはイネーブルになります (デフォルト)。

## ネットワーク [1] IEEE8021X Eap Peap

PEAP (保護拡張認証プロトコル) 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、シスコと RSA Security により開発されました。

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: EAP-PEAP プロトコルはディセーブルになります。

On: EAP-PEAP プロトコルはイネーブルになります (デフォルト)。

## ネットワーク [1] IP スタック

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

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。

## ネットワーク [1] IPv4 割り当て

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。この設定は IPv4 ネットワーク上のシステム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: 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。

## ネットワーク [1] IPv4 モード

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限り適用できます。

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, 64)

有効な IPv4 アドレス。

## ネットワーク [1] IPv4 ゲートウェイ

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限り適用できます。

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, 64)

有効な IPv4 アドレス。

## ネットワーク [1] IPv4 サブネット マスク

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限り適用できます。

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, 64)

有効な IPv4 アドレス。

## ネットワーク [1] IPv6 割り当て

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。この設定は IPv6 ネットワーク上のシステム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: 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 RFC 3315 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 RFC 4862 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。

## ネットワーク [1] IPv6 アドレス

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限り適用できます。

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, 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

## ネットワーク [1] IPv6 ゲートウェイ

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

デフォルト値: ""

値スペース: 文字列 (0, 64)

有効な IPv6 アドレス。

## ネットワーク [1] IPv6 DHCP オプション

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

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。

## ネットワーク [1] MTU

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。IPv4 の場合、最小サイズは 576 で、IPv6 の場合、最小サイズは 1280 です。

必要なユーザ ロール: ADMIN

Default value: 1500

値スペース: 整数 (576..1500)

MTU の値を設定します (バイト単位)。

## ネットワーク [1] QoS モード

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

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。

## ネットワーク [1] QoS Diffserv オーディオ

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。数字が大きいくほど、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

Default value: 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。数字が大きいくほど、優先順位が高くなります。デフォルト値は 0 (ベスト エフォート) です。

## ネットワーク [1] QoS Diffserv ビデオ

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。数字が大きいくほど、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

Default value: 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。数字が大きいくほど、優先順位が高くなります。デフォルト値は 0 (ベスト エフォート) です。

## ネットワーク [1] QoS Diffserv データ

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。数字が大きいくほど、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

Default value: 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。数字が大きいくほど、優先順位が高くなります。デフォルト値は 0 (ベスト エフォート) です。

## ネットワーク [1] QoS Diffserv シグナリング

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。数字が大きいくほど、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

Default value: 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。数値が大きいくほど、優先順位が高くなります。デフォルト値は 0 (ベスト エフォート) です。

## ネットワーク [1] QoS Diffserv ICMPv6

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。数字が大きいくほど、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

Default value: 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。数値が大きいくほど、優先順位が高くなります。デフォルト値は 0 (ベスト エフォート) です。

## ネットワーク [1] QoS Diffserv NTP

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。数字が大きいくほど、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

Default value: 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。数値が大きいくほど、優先順位が高くなります。デフォルト値は 0 (ベスト エフォート) です。

## ネットワーク [1] リモート アクセス 許可

リモート アクセスで SSH/Telnet/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

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。

## ネットワーク [1] トラフィック制御モード

ネットワーク トラフィック制御モードを設定してビデオ パケットの送信レートの制御方法を定義します。

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: 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。

## ネットワーク [1] VLAN 音声モード

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

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。

## ネットワーク [1] VLAN 音声 VlanId

VLAN 音声 ID を定義します。この設定は、Network VLAN Voice Mode 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

Default value: 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

### ネットワークサービス CDP モード

CDP (Cisco Discovery Protocol) デーモンを有効または無効にします。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 を無効にする場合、Network VLAN Voice Mode: 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。

### ネットワークサービス H323 モード

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イネーブルにします (デフォルト)。

### ネットワークサービス HTTP モード

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 Web インターフェイスでは HTTP または HTTPS が使用されることに注意してください。この設定を Off にすると、Web インターフェイスを使用できなくなります。

追加のセキュリティ (リクエストと Web サーバから返されたページの暗号化と復号化) が必要な場合は、HTTPS のみを許可します。

必要なユーザ ロール: ADMIN

デフォルト値: HTTP+HTTPS

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。

### ネットワークサービス HTTPS サーバ証明書検証

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。

## ネットワークサービス HTTPS クライアント証明書検証

ビデオ システムが HTTPS クライアント (Web ブラウザなど) に接続すると、クライアントは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。

## ネットワークサービス HTTPS OCSP モード

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。

## ネットワークサービス 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。

## ネットワークサービス NTP モード

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、NTP 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 サーバを使用し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。

## ネットワークサービス NTP サーバ [1..3] アドレス

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。

## ネットワークサービス SIP モード

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イネーブルにします (デフォルト)。

## ネットワークサービス SNMP モード

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、プロジェクトなど）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

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。

## ネットワークサービス SNMP ホスト [1..3] アドレス

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）からの要求に応答します。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

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。

## ネットワーク サービス SNMP コミュニティ名

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 管理スイート（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

デフォルト値: ""

値スペース: 文字列 (0, 50)

SNMP コミュニティ名。

## ネットワーク サービス SNMP システム接点

ネットワーク サービス SNMP システム接点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, 50)

SNMP システムの連絡先の名前。

## ネットワーク サービス SNMP システム ロケーション

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

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。

## ネットワークサービスSSHモード

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)。

## ネットワーク サービス SSH 公開キー許可

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。

## ネットワークサービスTelnetモード

Telnet は、インターネットまたはローカル エリア ネットワーク (LAN) 接続で使用されるネットワーク プロトコルです。

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: Telnet プロトコルはディセーブルになります。これが出荷時の設定です。

On: Telnet プロトコルはイネーブルになります。

## ネットワークサービス ウェルカムテキスト

Telnet/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)

## ネットワークサービス XMLAPI モード

ビデオ システムの XML API を有効または無効にします。セキュリティ上の理由からこれを無効にできます。XML API を無効にすると、TMS など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 (デフォルト)。

## 周辺機器の設定

周辺機器ペアリング ウルトラサウンド音量モード  
なし。

周辺機器ペアリング ウルトラサウンド音量最大レベル  
なし。

## 電話帳の設定

### 外部電話帳サーバ [1] ID

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)

外部電話帳の名前。

### 外部電話帳サーバ [1] 種類

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 Spark 上に配置されます。

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。

### 外部電話帳サーバ [1] URL

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

### プロビジョニングの接続性

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。

### プロビジョニングモード

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/Spark/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: プロビジョニング サーバを自動的に選択します。

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 Collaboration Edge インフラストラクチャを介して CUCM に接続します。

Spark: Spark 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。

### プロビジョニング ログイン名

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。

## プロビジョニング パスワード

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。

## プロビジョニング HTTP 方式

HTTP 方式をプロビジョニングに使用する場合に選択します。

必要なユーザ ロール: admin, user

デフォルト値: POST

値スペース: GET/POST

GET: プロビジョニングサーバが GET をサポートする場合、GET を選択します。

POST: プロビジョニングサーバが POST をサポートする場合、POST を選択します。

## プロビジョニング 外部マネージャーアドレス

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)。Provisioning ExternalManager Address 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。

## プロビジョニング 外部マネージャー代替アドレス

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。

## プロビジョニング 外部マネージャープロトコル

リクエストを外部マネージャ/プロビジョニングシステムに送信するときに HTTP (非セキュア通信) プロトコルを使用するか、HTTPS (セキュア通信) 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: 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 により要求を送信します。

## プロビジョニング 外部マネージャーパス

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 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。

## プロビジョニング 外部マネージャードメイン

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。

## ルームリセットの設定

### ルームリセット制御

なし。

## RTP 設定

### RTP ポート範囲の開始

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 ~ 2487 の範囲の UDP ポートを使用します。各メディア チャンネルは RTP および RTCP に 2 つの隣接ポートを使用します。UDP ポート範囲に必要なポートの数は、エンドポイントで対応できる同時コールの数に基づいています。

注: 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

Default value: 2326

値スペース: 整数 (1024..65438)

RTP ポート範囲の最初のポートを設定します。

### RTP ポート範囲停止

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 UDP ポートを使用します。各メディア チャンネルは RTP および RTCP に 2 つの隣接ポートを使用します。UDP ポート範囲に必要なポートの数は、エンドポイントで対応できる同時コールの数に基づいています。

注: 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

Default value: 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。

## セキュリティ設定

### セキュリティ監査ロギング モード

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。External/ExternalSecure モードを使用し、[セキュリティ監査サーバ ポート割り当て (Security Audit Server PortAssignment)] 設定でポート割り当てを [手動 (Manual)] に設定する場合は、[セキュリティ監査サーバ アドレス (Security Audit Server Address)] と [セキュリティ監査サーバのポート (Security Audit Server Port)] の設定で監査サーバのアドレスとポート番号も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: Off

値スペース: Off/Internal/External/ExternalSecure

Off: 監査ロギングは実行されません。

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。

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: 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、Web インターフェイスを使用してコーデック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 アドレスと一致する必要があります、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。

### セキュリティ監査 エラー処理時

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 コーデックはリポートし、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。

### セキュリティ監査サーバ アドレス

監査ログは syslog サーバに送信されます。syslog サーバの IP アドレスを定義します。有効な IPv4 または IPv6 のアドレス形式のみが受け入れられます。ホスト名はサポートされていません。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 アドレスまたは IPv6 アドレス。

## セキュリティ監査サーバ ポート

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

Default value: 514

値スペース: 整数 (0..65535)

監査サーバ ポートを設定します。

## セキュリティ監査サーバ ポート割り当て

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、[セキュリティ監査サーバのポート (Security Audit Server Port)] 状態をチェックできます。Web インターフェイスで [設定 (Configuration)] > [システム ステータス (System 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 InactivityTimeout

ユーザが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

Default value: 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。

## セキュリティセッション ユーザーの最大セッション数

ユーザ 1 人あたりの最大同時セッション数。デフォルト値の 0 は、ハード リミットなしを意味します。セッションはリソースを消費するため、いくつかの制限がありますが、制限はさまざまな条件に基づいて異なるものになります。

必要なユーザ ロール: ADMIN

Default value: 0

値スペース: 整数 (0..100)

ユーザ 1 人あたりの最大セッション数。0 は、ハード リミットがないことを意味します。

## セキュリティセッション 最大総セッション数

合計の同時セッションの最大数。デフォルト値の 0 は、ハード リミットなしを意味します。セッションはリソースを消費するため、いくつかの制限がありますが、制限はさまざまな条件に基づいて異なるものになります。

必要なユーザ ロール: ADMIN

Default value: 0

値スペース: 整数 (0..100)

合計の最大セッション数。0 は、ハード リミットなしを意味します。

## セキュリティセッション 最後のログオンを表示

SSH または Telnet 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 UserId、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

### シリアルポートモード

シリアルポート (Micro USB から USB ケーブルへの接続を介して) を有効または無効にします。シリアルポートは 115200 bps、8 データ ビット、パリティなし、1 ストップ ビットを使用します。

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: 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。

### シリアルポート ログイン必須

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 settings)

### 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 ユーザー名認証

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ー名部分です。

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)

有効なユーザー名。

### SIP パスワード認証

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 デフォルトトランスポート

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: TCP/UDP/Tls/Auto

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 表示名

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 モード

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。このため、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 サーバが提供されている場合は ICE は有効、そうでない場合は ICE は無効になります。

Off: ICE が無効になります。

On: ICE が有効になります。

## SIP Ice デフォルト候補

ICE プロトコルは、使用するメディアルートについて結論に達するまで少しの時間を必要とします (最长で発信の最初の 5 秒)。この期間中に、ビデオシステムのメディアは、この設定の定義に従って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 アドレスに送信します。

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せん。

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 Tcp候補者の提供

ビデオシステムで TCP 接続を使用したメディアの送受信をサポート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: ビデオシステムで TCP 接続を使用したメディアを使用不可にします。

On: ビデオシステムで TCP 接続を使用したメディアを使用可能にします。

## SIP 回線

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 (デフォルト)。

## SIP リッスンポート

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。この設定はデフォルト値のまま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

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 メールボックス

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 優先IPメディア

メディア (音声、ビデオ、データ) を送受信するための優先 IP バージョンを定義します。[Network IPStack] および [Conference CallProtocolIPStack] の両方が [デュアル (Dual)] に設定されている場合、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。

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: メディアの優先 IP バージョンは IPv4 です。

IPv6: メディアの優先 IP バージョンは IPv6 です。

## SIP 優先IPシグナリング

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プロキシ[1..4]アドレス

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 Tls検証

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、Web 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、コードックに 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 検出モード

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 サーバ

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 ユーザ名

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 パスワード

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 タイプ

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 および Broadsoft 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

### スタンバイ制御

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

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。

### スタンバイ遅延

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

Default value: 10

値スペース: 整数 (1..480)

スタンバイ遅延 (分) を設定します。

## システムユニット設定

### システムユニット名

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。

## 時刻設定

### 時間の時刻形式

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。

### 時刻の日付形式

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。

## タイムゾーン

ビデオ システムの地理的な場所のタイム ゾーンを定義します。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, user

デフォルト値: Etc/UTC

値スペース: Africa/Abidjan, Africa/Accra, Africa/Addis\_Ababa, Africa/Algiers, Africa/Asmara, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar\_es\_Salaam, Africa/Djibouti, Africa/Douala, Africa/EL\_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Juba, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao\_Tome, Africa/Timbuktu, Africa/Tripoli, Africa/Tunis, Africa/Windhoek, America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Araguaina, America/Argentina/Buenos\_Aires, America/Argentina/Catamarca, America/Argentina/ComodRivadavia, America/Argentina/Cordoba, America/Argentina/Jujuy, America/Argentina/La\_Rioja, America/Argentina/Mendoza, America/Argentina/Rio\_Gallegos, America/Argentina/Salta, America/Argentina/San\_Juan, America/Argentina/San\_Luis, America/Argentina/Tucuman, America/Argentina/Ushuaia, America/Aruba, America/Asuncion, America/Atikokan, America/Atka, America/Bahia, America/Bahia\_Banderas, America/Barbados, America/Belem, America/Belize, America/Blanc-Sablon, America/Boa\_Vista, America/Bogota, America/Boise, America/Buenos\_Aires, America/Cambridge\_Bay, America/Campo\_Grande, America/Cancun, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Chihuahua, America/Coral\_Harbour, America/Cordoba, America/Costa\_Rica, America/Creston, America/Cuiaba, America/Curacao, America/Danmarkshavn, America/Dawson, America/Dawson\_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/Eirunepe, America/EI\_Salvador, America/Ensenada, America/Fort\_Nelson, America/Fort\_Wayne, America/Fortaleza, America/Glace\_Bay, America/Godthab, America/Goose\_Bay, America/Grand\_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Hermosillo, America/Indiana/Indianapolis, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Petersburg, America/Indiana/Tell\_City, America/Indiana/Vevay, America/Indiana/Vincennes, America/Indiana/Winamac, America/Indianapolis, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/Kentucky/Louisville, America/Kentucky/Monticello, America/Knox\_IN, America/Kralendijk, America/La\_Paz, America/Lima, America/Los\_Angeles, America/Louisville, America/Lower\_Princes, America/Maceio, America/Managua, America/

Manaus, America/Marigot, America/Martinique, America/Matamoros, America/Mazatlan, America/Mendoza, America/Menominee, America/Merida, America/Metlakatla, America/Mexico\_City, America/Miquelon, America/Moncton, America/Monterrey, America/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New\_York, America/Nipigon, America/Nome, America/Noronha, America/North\_Dakota/Beulah, America/North\_Dakota/Center, America/North\_Dakota/New\_Salem, America/Ojinaga, America/Panama, America/Pangnirtung, America/Paramaribo, America/Phoenix, America/Port-au-Prince, America/Port\_of\_Spain, America/Porto\_Acre, America/Porto\_Velho, America/Puerto\_Rico, America/Rainy\_River, America/Rankin\_Inlet, America/Recife, America/Regina, America/Resolute, America/Rio\_Branco, America/Rosario, America/Santa\_Isabel, America/Santarem, America/Santiago, America/Santo\_Domingo, America/Sao\_Paulo, America/Scoresbysund, America/Shiprock, America/Sitka, America/St\_Barthlemy, America/St\_Johns, America/St\_Kitts, America/St\_Lucia, America/St\_Thomas, America/St\_Vincent, America/Swift\_Current, America/Tegucigalpa, America/Thule, America/Thunder\_Bay, America/Tijuana, America/Toronto, America/Tortola, America/Vancouver, America/Virgin, America/Whitehorse, America/Winnipeg, America/Yakutat, America/Yellowknife, Antarctica/Casey, Antarctica/Davis, Antarctica/DumontDUrville, Antarctica/Macquarie, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/Palmer, Antarctica/Rothera, Antarctica/South\_Pole, Antarctica/Syowa, Antarctica/Troll, Antarctica/Vostok, Arctic/Longyearbyen, Asia/Aden, Asia/Almaty, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe, Asia/Ashgabat, Asia/Ashkhabad, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/Barnaul, Asia/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, Asia/Chita, Asia/Choibalsan, Asia/Chongqing, Asia/Chungking, Asia/Colombo, Asia/Dacca, Asia/Damascus, Asia/Dhaka, Asia/Dili, Asia/Dubai, Asia/Dushanbe, Asia/Gaza, Asia/Harbin, Asia/Hebron, Asia/Ho\_Chi\_Min, Asia/Hong\_Kong, Asia/Hovd, Asia/Irkutsk, Asia/Istanbul, Asia/Jakarta, Asia/Jayapura, Asia/Jerusalem, Asia/Kabul, Asia/Kamchatka, Asia/Karachi, Asia/Kashgar, Asia/Kathmandu, Asia/Katmandu, Asia/Khandyga, Asia/Kolkata, Asia/Krasnoyarsk, Asia/Kuala\_Lumpur, Asia/Kuching, Asia/Kuwait, Asia/Macao, Asia/Macau, Asia/Magadan, Asia/Makassar, Asia/Manila, Asia/Muscat, Asia/Nicosia, Asia/Novokuznetsk, Asia/Novosibirsk, Asia/Omsk, Asia/Oral, Asia/Phnom\_Penh, Asia/Pontianak, Asia/Pyeongyang, Asia/Qatar, Asia/Qyzylorda, Asia/Rangoon, Asia/Riyadh, Asia/Saigon, Asia/Sakhalin, Asia/Samarkand, Asia/Seoul, Asia/Shanghai, Asia/Singapore, Asia/Srednekolymsk, Asia/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Tel\_Aviv, Asia/Thimbu, Asia/Thimphu, Asia/Tokyo, Asia/Tomsk, Asia/Ujung\_Pandang, Asia/Ulaanbaatar, Asia/Ulan\_Bator, Asia/Urumqi, Asia/Ust-Nera, Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yekaterinburg, Asia/Yerevan, Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape\_Verde, Atlantic/Faeroe, Atlantic/Faroe, Atlantic/Jan\_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South\_Georgia, Atlantic/St\_Helena, Atlantic/Stanley, Australia/ACT, Australia/Adelaide, Australia/Brisbane, Australia/Broken\_Hill, Australia/Canberra, Australia/Currie, Australia/Darwin, Australia/Eucla, Australia/Hobart, Australia/LHI, Australia/Lindeman, Australia/Lord\_Howe, Australia/Melbourne, Australia/NSW, Australia/North, Australia/Perth, Australia/Queensland, Australia/South, Australia/Sydney, Australia/

Tasmania, Australia/Victoria, Australia/West, Australia/Yancowinna, Brazil/Acre, Brazil/DeNoronha, Brazil/East, Brazil/West, CET, CST6CDT, Canada/Atlantic, Canada/Central, Canada/East-Saskatchewan, Canada/Eastern, Canada/Mountain, Canada/Newfoundland, Canada/Pacific, Canada/Saskatchewan, Canada/Yukon, Chile/Continental, Chile/EasterIsland, Cuba, EET, EST, EST5EDT, Egypt, Eire, Etc/GMT, Etc/GMT+0, Etc/GMT+1, Etc/GMT+10, Etc/GMT+11, Etc/GMT+12, Etc/GMT+2, Etc/GMT+3, Etc/GMT+4, Etc/GMT+5, Etc/GMT+6, Etc/GMT+7, Etc/GMT+8, Etc/GMT+9, Etc/GMT-0, Etc/GMT-1, Etc/GMT-10, Etc/GMT-11, Etc/GMT-12, Etc/GMT-13, Etc/GMT-14, Etc/GMT-2, Etc/GMT-3, Etc/GMT-4, Etc/GMT-5, Etc/GMT-6, Etc/GMT-7, Etc/GMT-8, Etc/GMT-9, Etc/GMT0, Etc/Greenwich, Etc/UCT, Etc/UTC, Etc/Universal, Etc/Zulu, Europe/Amsterdam, Europe/Andorra, Europe/Astrakhan, Europe/Athens, Europe/Belfast, Europe/Belgrade, Europe/Berlin, Europe/Bratislava, Europe/Brussels, Europe/Bucharest, Europe/Budapest, Europe/Busingen, Europe/Chisinau, Europe/Copenhagen, Europe/Dublin, Europe/Gibraltar, Europe/Guernsey, Europe/Helsinki, Europe/Isle\_of\_Man, Europe/Istanbul, Europe/Jersey, Europe/Kaliningrad, Europe/Kiev, Europe/Kirov, Europe/Lisbon, Europe/Ljubljana, Europe/London, Europe/Luxembourg, Europe/Madrid, Europe/Malta, Europe/Mariehamn, Europe/Minsk, Europe/Monaco, Europe/Moscow, Europe/Nicosia, Europe/Oslo, Europe/Paris, Europe/Podgorica, Europe/Prague, Europe/Riga, Europe/Rome, Europe/Samara, Europe/San\_Marino, Europe/Sarajevo, Europe/Simferopol, Europe/Skopje, Europe/Sofia, Europe/Stockholm, Europe/Tallinn, Europe/Tirane, Europe/Tiraspol, Europe/Ulyanovsk, Europe/Uzhgorod, Europe/Vaduz, Europe/Vatican, Europe/Vienna, Europe/Vilnius, Europe/Volgograd, Europe/Warsaw, Europe/Zagreb, Europe/Zaporozhye, Europe/Zurich, GB, GB-Eire, GMT, GMT+0, GMT-0, GMT0, Greenwich, HST, Hongkong, Iceland, Indian/Antananarivo, Indian/Chagos, Indian/Christmas, Indian/Cocos, Indian/Comoro, Indian/Kerguelen, Indian/Mahe, Indian/Maldives, Indian/Mauritius, Indian/Mayotte, Indian/Reunion, Iran, Israel, Jamaica, Japan, Kwajalein, Libya, MET, MST, MST7MDT, Mexico/BajaNorte, Mexico/BajaSur, Mexico/General, NZ, NZ-CHAT, Navajo, PRC, PST8PDT, Pacific/Apia, Pacific/Auckland, Pacific/Bougainville, Pacific/Chatham, Pacific/Chuuk, Pacific/Easter, Pacific/Efate, Pacific/Enderbury, Pacific/Fakaofu, Pacific/Fiji, Pacific/Funafuti, Pacific/Galapagos, Pacific/Gambier, Pacific/Guadalcanal, Pacific/Guam, Pacific/Honolulu, Pacific/Johnston, Pacific/Kiritimati, Pacific/Kosrae, Pacific/Kwajalein, Pacific/Majuro, Pacific/Marquesas, Pacific/Midway, Pacific/Nauru, Pacific/Niue, Pacific/Norfolk, Pacific/Noumea, Pacific/Pago\_Pago, Pacific/Palau, Pacific/Pitcairn, Pacific/Pohnpei, Pacific/Ponape, Pacific/Port\_Moresby, Pacific/Rarotonga, Pacific/Saipan, Pacific/Samoa, Pacific/Tahiti, Pacific/Tarawa, Pacific/Tongatapu, Pacific/Truk, Pacific/Wake, Pacific/Wallis, Pacific/Yap, Poland, Portugal, ROC, ROK, Singapore, Turkey, UCT, US/Alaska, US/Aleutian, US/Arizona, US/Central, US/East-Indiana, US/Eastern, US/Hawaii, US/Indiana-Starke, US/Michigan, US/Mountain, US/Pacific, US/Pacific-New, US/Samoa, UTC, Universal, W-SU, WET, Zulu

リストからタイムゾーンを選択します。

## ユーザーインターフェース 設定

### ユーザーインターフェース 連絡先情報のタイプ

ホーム画面に表示される連絡先情報のタイプと、[設定 (Settings)] アイコンをタップしたときに表示される連絡先情報のタイプを選択します。

必要なユーザ ロール: ADMIN

デフォルト値: Auto

値スペース: Auto/None/IPv4/IPv6/SipUri/SystemName/DisplayName

Auto: このシステムに到達するために別のシステムがダイヤルできるアドレスを示します。アドレスは、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 アドレスを表示します。

IPv6: システムの IPv6 アドレスを表示します。

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)。

### ユーザーインターフェース キー トーンモード

テキストや数字を入力しているときに、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: Off

値スペース: Off/On

Off: キー トーンによる効果音はありません。

On: キー トーンによる効果音がオンになります。

### ユーザーインターフェース 言語

画面のメニューとメッセージで使用する言語を選択します。

必要なユーザ ロール: ADMIN, USER

デフォルト値: English

値スペース: English/ChineseSimplified/ChineseTraditional/Catalan/Czech/Danish/Dutch/Finnish/French/FrenchCanadian/German/Hungarian/Italian/Japanese/Korean/Norwegian/Polish/PortugueseBrazilian/Russian/Spanish/Swedish/Turkish/Arabic/Hebrew

リストから言語を選択します。

### ユーザーインターフェース OSD暗号化インジケータ

暗号化インジケータ (鍵) が画面に表示される時間の長さを定義します。暗号化されたコールはロックされた鍵のアイコンで示され、暗号化されていないコールはバツ印の付いたロックされた鍵のアイコンで示されます。

必要なユーザ ロール: ADMIN

デフォルト値: Auto

値スペース: Auto/AlwaysOn/AlwaysOffAuto: 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、コール中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。また、暗号化インジケータ アイコンは 5 秒後に画面から消えます。

AlwaysOn: 暗号化インジケータはコール全体にわたり画面上に表示されます。

AlwaysOff: 暗号化インジケータは画面上に表示されません。

## ユーザーインターフェイスOSDアウトプット

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

Default value: 1

値スペース: Auto/1/2/3

Auto: オンスクリーン用の情報とインジケータをシステムの内蔵ディスプレイに送信します。

範囲 1 ~ 3: 情報とインジケータを指定された出力に送信します。画面表示の情報とインジケータを内蔵ディスプレイに送信する場合は 1 を選択し、システムの HDMI 出力に接続されたディスプレイに OSD を送信する場合は 2 または 3 を選択します。

## ユーザーインターフェイス壁紙

アイドル状態のときのビデオ画面の背景イメージ (壁紙) を選択します。

Web 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、クロックと予定されている会議のリストは、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、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。

## ユーザー管理設定

### ユーザー管理 LDAP モード

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を設定します。実装は、Microsoft Active Directory (AD) サービスでテスト済みです。

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: LDAP 認証は許可されません。

On: LDAP 認証を使用します。

### ユーザー管理 LDAP サーバアドレス

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。

### ユーザー管理 LDAP サーバポート

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

Default value: 0

値スペース: 整数 (0..65535)

LDAP サーバ ポート番号。

### ユーザー管理LDAP暗号化

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: 暗号化なしでポート 389 で LDAP サーバに接続します。

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。

### ユーザー管理 LDAP 最小TLSバージョン

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 以降をサポートします。

TLSv1.1: TLS バージョン 1.1 以降をサポートします。

TLSv1.2: TLS バージョン 1.2 以降をサポートします。

## ユーザー管理 LDAP サーバー証明書検証

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 サーバの証明書を確認しません。

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。信頼できる CA のリストを管理するには、ビデオ システムの Web インターフェイスを使用します (詳細については『管理者ガイド』を参照)。

## ユーザー管理 LDAP 管理者フィルタ

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。設定したら、この設定は UserManagement LDAP Admin Group 設定よりも優先されるようになります。

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, 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: 「(CN=adminuser)」

## ユーザー管理 LDAP 管理者グループ

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。UserManagement LDAP Admin Filter が設定されている場合、こ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」

## ユーザー管理 LDAP 属性

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。

## ビデオ設定

### ビデオ アクティブスピーカーのデフォルト PIP ポジション

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

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。

### ビデオデフォルトレイアウトファミリローカル

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、音声は切り替えられます。

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せん。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、音声は切り替えられます。

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、音声は切り替えられます。

## ビデオ デフォルトレイアウトファミリリモート

リモート参加者が使用するビデオ 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: 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ず。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、音声切り替えられます。

## ビデオ デフォルトのメインソース

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

Default value: 1

値スペース: 1

メイン ビデオ ソースとして使用されるソースを設定します。

## ビデオ入力コネクタ [1..2] カメラ制御モード

カメラを制御できるかどうかを定義します。この値は、Connector 1 (内蔵カメラ) と Connector 2 (HDMI) の両方で固定されており、変更できません。

必要なユーザ ロール: ADMIN

デフォルト値: Off

値スペース: Off

Off: カメラ制御をディセーブルにします。

## ビデオ入力コネクタ[1..2] カメラ制御カメラID

カメラ ID は、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

Default value: 1

値スペース: 1

カメラ ID は固定されており、変更できません。

## ビデオ入力コネクタ [1..2] 入力ソースタイプ

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

デフォルト値: Connector 1: camera Connector 2: desktop

値スペース: Connector 1: camera Connector 2: camera/desktop/document\_camera/mediaplayer/PC/whiteboard/other

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。

desktop: ビデオ システムのモニタが、この入力に接続されている PC/ラップトップのメインスクリーンである場合、これを使用します。Video Input Connector [n] PresentationSelection 設定も desktop に設定する必要があります。

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。

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。

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: 他のオプションに該当しない場合に使用します。

## ビデオ入力コネクタ [1..2] 名前

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

デフォルト値: ""

値スペース: 文字列 (0, 50)

ビデオ入力コネクタの名前。

## ビデオ入力コネクタ [2] 画質

ビデオをエンコードして送信する場合は、高解像度と高フレーム レートとの間でトレード オフが生じます。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。この設定は、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。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。

## ビデオ入力コネクタ [1..2] 最適鮮明度プロファイル

この設定は、対応する Video Input Connector [n] Quality が Motion に設定されている場合のみ有効になります。

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。良い光の条件では、ビデオ エンコーダは指定のコール レートに一層優れた品質 (高解像度またはフレーム レート) を提供します。通常、[標準 (Normal)] または [中 (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、[高 (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

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。

## ビデオ入力コネクタ [2] プレゼンテーションの選択

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

デフォルト値: Desktop

値スペース: AutoShare/Desktop/Manual/OnConnect

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 インターフェイスで [共有 (Share)] を選択する必要はありません。通話実行時または通話への応答時にプレゼンテーション ソースが既に接続されている場合、ユーザ インターフェイスで [共有 (Share)] を手動で選択する必要があります。

Desktop: ケーブルを接続すると、またはソースがアクティブ化されると (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と)、ビデオ入力のコンテンツが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、通話を終了しても、終了時にビデオ入力にアクティブ入力である場合は、そのビデオ入力のコンテンツが画面に引き続き表示されます。

Manual: ユーザ インターフェイスで [共有 (Share)] を選択するまで、ビデオ入力のコンテンツは画面に表示されません。

OnConnect: ケーブルを接続すると、またはソースがアクティブ化されると (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と)、ビデオ入力のコンテンツが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。

## ビデオ入力コネクタ [2] RGB量子化範囲

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

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。

## ビデオ入力コネクタ [1..2] 表示

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。

Video Input Connector 2 Visibility (HDMI コネクタ) のデフォルト値は IfSignal です。

必要なユーザ ロール: ADMIN

デフォルト値: Connector 1: Never Connector 2: Always Connector 3: OnConnect

値スペース: Connector 1: Never Connector 2, 3: Never/Always/IfSignal

Never: 入力ソースがプレゼンテーション ソースとして使用される見込みがない場合、[なし (Never)] に設定します。

Always: [常時 (Always)] に設定すると、ビデオ入力コネクタ用メニュー選択はグラフィカル ユーザ インターフェイスに常に表示されます。

IfSignal: [シグナルがある場合 (IfSignal)] に設定すると、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。

## ビデオレイアウト 切断されたローカル出力を無効にする

この設定は、On に固定されています。

デフォルト値: On

値スペース: On

On: 組み込みのレイアウト エンジンにモニタを接続するローカル出力のみレイアウトを設定します。

## ビデオモニター

モニタ レイアウト モードを定義して、空間のセットアップに必要な各種レイアウトの数を反映させます。2 番目のモニタがプレゼンテーション用に確保できることに注意してください。

必要なユーザ ロール: ADMIN

デフォルト値: Auto

値スペース: Auto/Single/Dual/DualPresentationOnly

Auto: レイアウトは、ビデオ システムの内蔵モニタに表示されます。追加のモニタはサポートされません。

Single: 適用されません。

Dual: 適用されません。

DualPresentationOnly: 適用されません。

## ビデオ出力コネクタ[1]輝度

ビデオ システムの内蔵ディスプレイの明るさレベルを定義します。

必要なユーザ ロール: admin, user

Default value: 80

値スペース: 整数 (0..100)

範囲: 値は 0 ~ 100 である必要があります。

## ビデオ出力コネクタ[2] CECモード

HDMI 出力 (Output Connector 2) は将来の使用に備えるものです。

## ビデオ出力コネクタ [2] ロケーション水平オフセット

HDMI 出力 (Output Connector 2) は将来の使用に備えるものです。

## ビデオ出力コネクタ [2] ロケーション垂直オフセット

HDMI 出力 (Output Connector 2) は将来の使用に備えるものです。

## ビデオ出力コネクタ [2]オーバースキャンレベル

HDMI 出力 (Output Connector 2) は将来の使用に備えるものです。

## ビデオ出力コネクタ[1..2]解像度

Connector 1: 内蔵ディスプレイの解像度とリフレッシュ レートです。この値は固定されており、変更できません。

Connector 2: HDMI 出力 (Output Connector 2) は将来の使用に備えるものです。

デフォルト値: Connector 1: 1920\_1080\_60

値スペース: Connector 1: 1920\_1080\_60

1920\_1080\_60: 解像度は 1920 x 1080、更新間隔は 60 Hz です。

## ビデオ出力コネクタ [2] RGB量子化範囲

HDMI 出力 (Output Connector 2) は将来の使用に備えるものです。

## ビデオ出力コネクタ[1]ホワイトバランスレベル

内蔵ディスプレイの色温度 (ホワイト バランス) は、4000 K (暖色) ~ 9000 K (寒色) で調整できます。

必要なユーザ ロール: admin, user

Default value: 6500

値スペース: 整数 (4000..9000)

ケルビン単位の色温度。

## ビデオプレゼンテーション デフォルトのPiPポジション

プレゼンテーション 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

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。

## ビデオプレゼンテーション デフォルトソース

デフォルト 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。シスコが提供するユーザ 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: 2

デフォルト 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。

## ビデオセルフビューデフォルトモード

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 設定と Video Selfview Default FullscreenMode 設定によって決定されます。

必要なユーザ ロール: ADMIN

デフォルト値: Current

値スペース: Off/Current/On

[オフ (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が残ります。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もオフのままです。

[オン (On)]: セルフビューはコール退出時にオンにされます。

## ビデオセルフビューデフォルトフルスクリーンモード

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である場合にのみ有効です (Video Selfview Default Mode 設定を参照)。

必要なユーザ ロール: ADMIN

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。

## モニターロールでのビデオセルフビューのデフォルト

なし。

## ビデオセルフビューデフォルトのPIPポジション

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であり (Video Selfview Default Mode 設定を参照)、フルスクリーン ビューがオフである場合 (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

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。

## ビデオセルフビューオンコールモード

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

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。

## ビデオセルフビューオンコール時間

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

Default value: 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、シスコと同意したのでは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

## ユーザ インターフェイス

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。

[システム情報 (System information)] と [設定 (Settings)] メニューへのアクセス、ビデオ システムの [再起動 (Restart)]、[スタンバイ (Standby)] モードと [応答不可 (Do not disturb)] モードのアクティブ化と非アクティブ化、画面の明るさの調節

システム名または連絡先情報

[発信 (Call)] をタップすると、[お気に入り (Favorites)] リスト、[ディレクトリ (Directory)] リスト、[発信履歴 (Recents)] リストなどの連絡先を呼び出したり、[検索またはダイヤル (Search or Dial)] フィールドを開いたりできます

[システム情報 (System information)] と [設定 (Settings)] メニューへのアクセス、ビデオ システムの [再起動 (Restart)]、[スタンバイ (Standby)] モードと [応答不可 (Do not disturb)] モードのアクティブ化と非アクティブ化、画面の明るさの調節

システム名または連絡先情報

[発信 (Call)] をタップすると、[お気に入り (Favorites)] リスト、[ディレクトリ (Directory)] リスト、[発信履歴 (Recents)] リストなどの連絡先を呼び出したり、[検索またはダイヤル (Search or Dial)] フィールドを開いたりできます



## リモート モニタリングのセットアップ

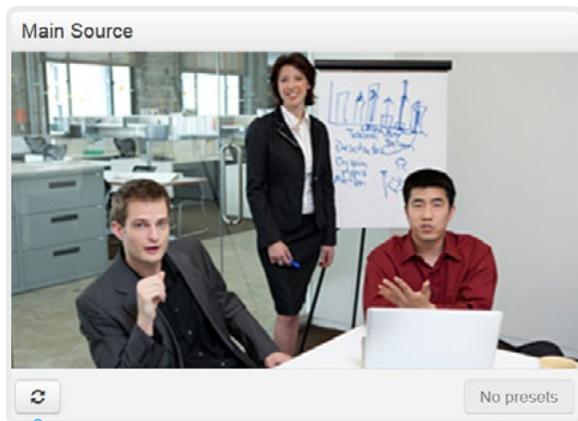
要件:

- 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役立ちます。

入力ソースからのスナップショットが Web 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 ビューを確認したり、カメラを制御したりできます。

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。



スナップショットを自動更新する

ビデオ システムに *RemoteMonitoring* オプションがあるかどうかの確認

- Web インターフェイスにサインインします。
- [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 モニタリングの有効化

*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 キーの追加](#)」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可能性があることを、システムの利用者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、シスコ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が [コール制御 (Call Control)] ページに表示されます。

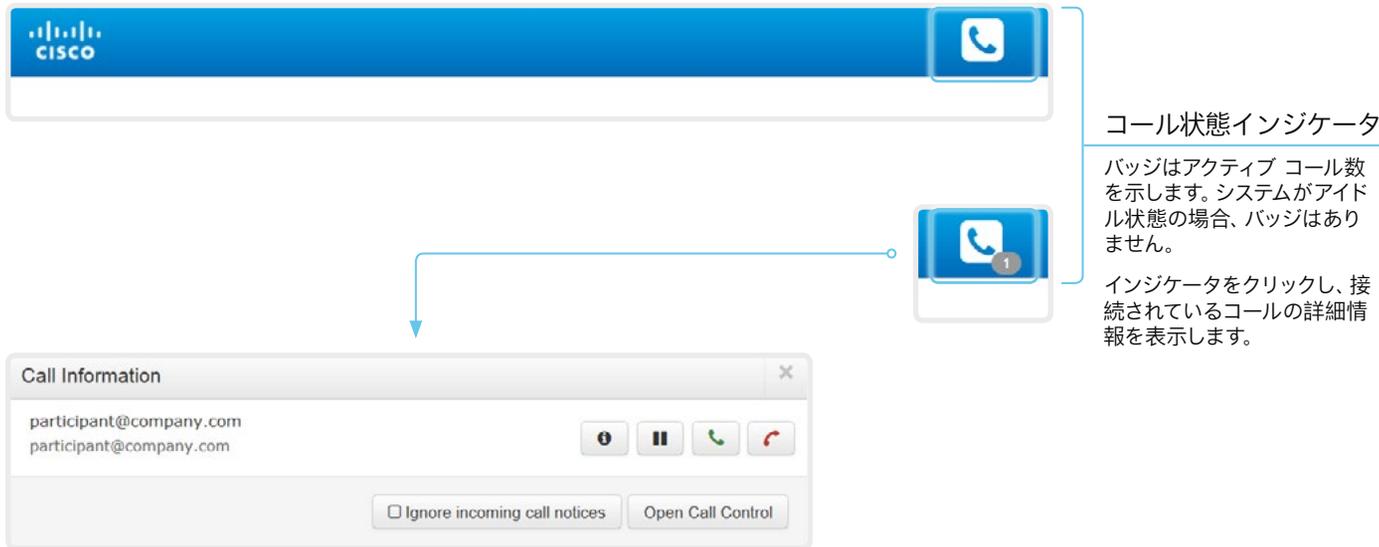
スナップショットは、ビデオ システムがアイドル中でも通話中でも表示されます。

遠端のスナップショット

通話中に、遠端カメラからのスナップショットを表示することもできます。この場合、遠端ビデオ システムに *RemoteMonitoring* オプションがあるかどうかは関係ありません。

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。

## Web インターフェイスを使用したコール情報へのアクセス



### コール状態インジケータ

バッジはアクティブ コール数を示します。システムがアイドル状態の場合、バッジはありません。

インジケータをクリックし、接続されているコールの詳細情報を表示します。

### コール状態インジケータについて

コール状態インジケータは、システムが通話中であるかどうかを示します。着信コールについてユーザに通知することもできます。

コール状態インジケータは [コール制御 (Call Control)] ページ以外のすべてのページで使用できます。

### [コール情報 (Call Information)] ウィンドウの表示

[コール情報 (Call Information)] ウィンドウを手動で開くには、**コール状態インジケータ**をクリックします。

デフォルトでは、ビデオ システムがコールを受信すると [コール情報 (Call Information)] ウィンドウが自動的に表示されます。

### 着信コール通知のオン/オフの切り替え

[着信コール通知を無視する (Ignore incoming call notices)] をクリックすると、ビデオ システムがコールを受信したときに [コール情報 (Call Information)] ウィンドウを自動的に表示するかどうかを決定できます。

このチェックボックスをオンにした場合は、[コール情報 (Call Information)] ウィンドウが自動的に開きません。

### [コール制御 (Call Control)] ページの表示

[コール制御 (Call Control)] ページに直接移動するには、[コール制御を開く (Open Call Control)] をクリックします。

### コールの制御

関連する制御ボタンが [コール情報 (Call Information)] ウィンドウに表示されます。ボタンの用途は次のとおりです。

-  コールの詳細を表示する
-  コールを保留にする
-  コールに応答する
-  コールを切断する

## Web インターフェイスを使用したコールの発信

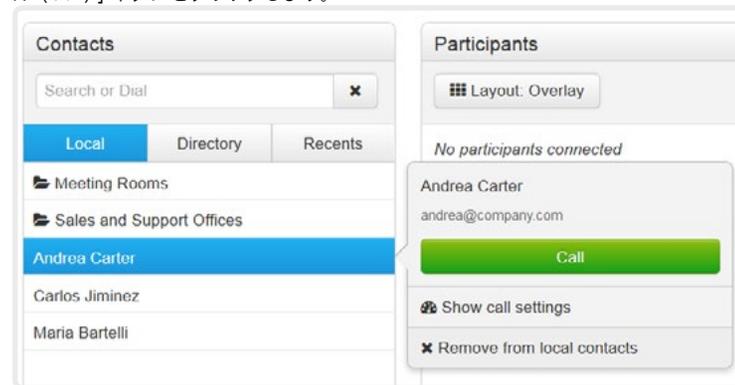
Web インターフェイスにサインインして、[コール制御 (Call Control)] に移動します。

### コールの発信

**i** Web 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、Web インターフェイスを実行する PC ではありません。

1. [ローカル (Local) ]、[ディレクトリ (Directory) ]、または [履歴 (Recents) ] リストに移動して該当するエントリを探すか、[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。



#### コールの詳細の表示/非表示

[情報ボタン (information button) ] 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、その参加者の名前の横にある [ ] 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

コールを終了するには、[全通話切断 (Disconnect all) ] または [ ] ボタンをクリックします。

\* 検索時には、入力内容に応じて、[ローカル (Local) ]、[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。

## Web インターフェイスを使用したコールの発信 (2/2 ページ)

Web インターフェイスにサインインして、[コール制御 (Call Control)] に移動します。

### 複数の相手に発信

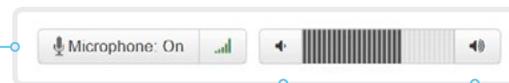
会議ブリッジを使用した複数のコール (CUCM のアドホック会議) は、ビデオ システムでサポートされていても Web インターフェイスではサポートされません。

### ボリュームを調整する

#### マイクのミュート

[マイク: オン (Microphone: On)] をクリックすると、マイクがミュートになります。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。



音量小

音量大

## Web インターフェイスを使用したコンテンツの共有

Web インターフェイスにサインインして、[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。これにより、テキストが [プレゼンテーションを中止 (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

選択し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

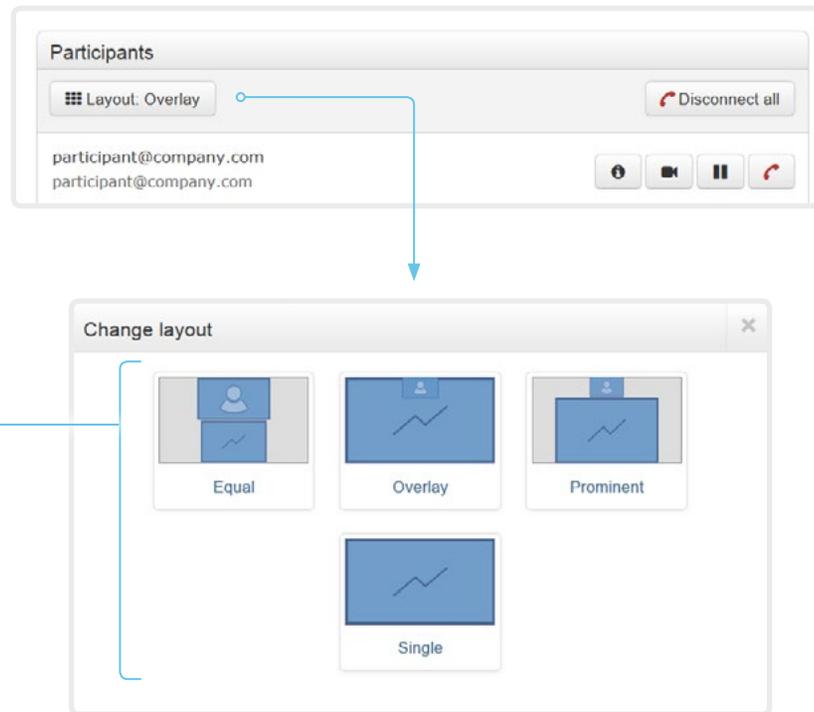
プレゼンテーション ソース (最も多いのは PC) は、ビデオ システムの背面にあるコンピュータ用の HDMI コネクタに接続できます。

コールの間、コールの他の参加者 (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

Web インターフェイスにサインインして、[コール制御 (Call Control)] に移動します。



### レイアウトの変更

[レイアウトの変更 (Change layout)] をクリックし、表示されるウィンドウで優先する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、ビデオとプレゼンテーション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。

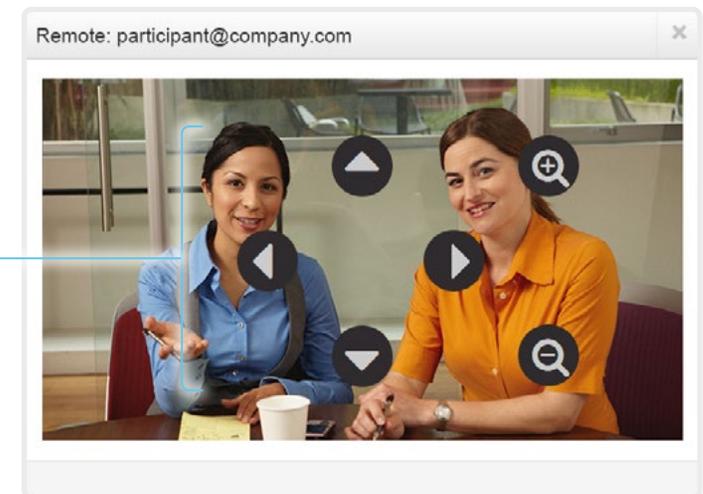
## 相手先 (遠端) カメラの制御

Web インターフェイスにサインインして、[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。
- 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

- 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。
- 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。

## スタートアップ スクリプトの管理

Web 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)] に移動します。

### 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。

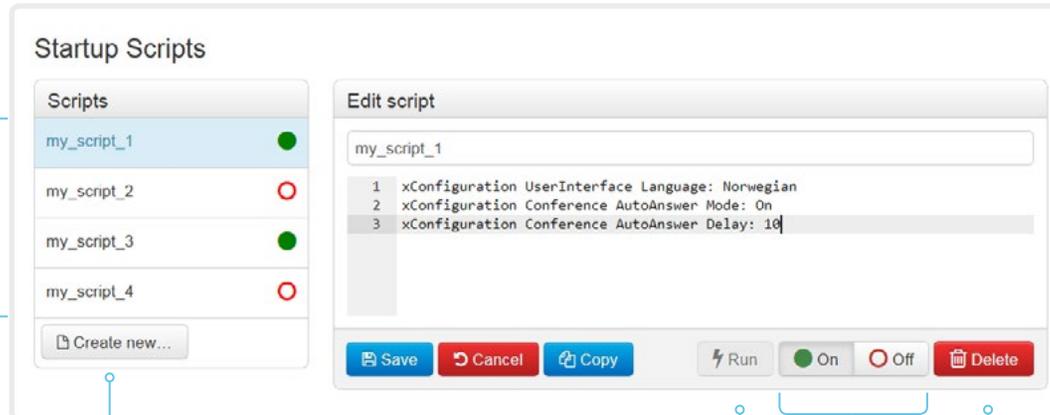
アクティブなスタートアップ スクリプトの横には緑色のドットが表示され、非アクティブなスタートアップ スクリプトの横には赤色のリングが表示されます。

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 スクリプトの作成

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. コマンド入力領域に、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)] をクリックすると、スタートアップ スクリプトがアクティブになります。

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。



図に示しているスクリプト名とコンフィギュレーションは一例です。独自のスクリプトを作成できます。

### スタートアップ スクリプトの即時実行

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 スタートアップ スクリプトと非アクティブ スタートアップ スクリプトの両方を、即時に実行できます。

### スタートアップ スクリプトのアクティブ化または非アクティブ化

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. [オン (On)] をクリックしてスクリプトをアクティブにするか、[オフ (Off)] をクリックしてスクリプトを非アクティブにします。  
アクティブ 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実行されます。

### スタートアップ スクリプトの削除

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。不正なコマンドやコンフィギュレーションが含まれる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 ファイルへのアクセス

Web 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)] に移動します。

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、Web 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、Web 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

ファイル名をクリックして、XML ファイルを開きます。

### 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。

## Web インターフェイスからの API コマンドと構成の実行

Web 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)] に移動します。

コマンド (xCommand) とコンフィギュレーション (xConfiguration) は Web 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。

**Execute API commands and configurations**

In the field below you can enter API commands (xCommand and xConfiguration) directly.

For example: xCommand Dial Number: "person@example.com" Protocol: Sip

Enter commands...

Execute

### 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。

## 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。マイクロ USB to USB ケーブルが必要です。コンピュータがシリアルポート ドライバを自動インストールしない場合には、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。

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

### ビデオ システムの設定値

シリアル通信はデフォルトで有効になっています。動作を変更するには、次の設定を使用します。

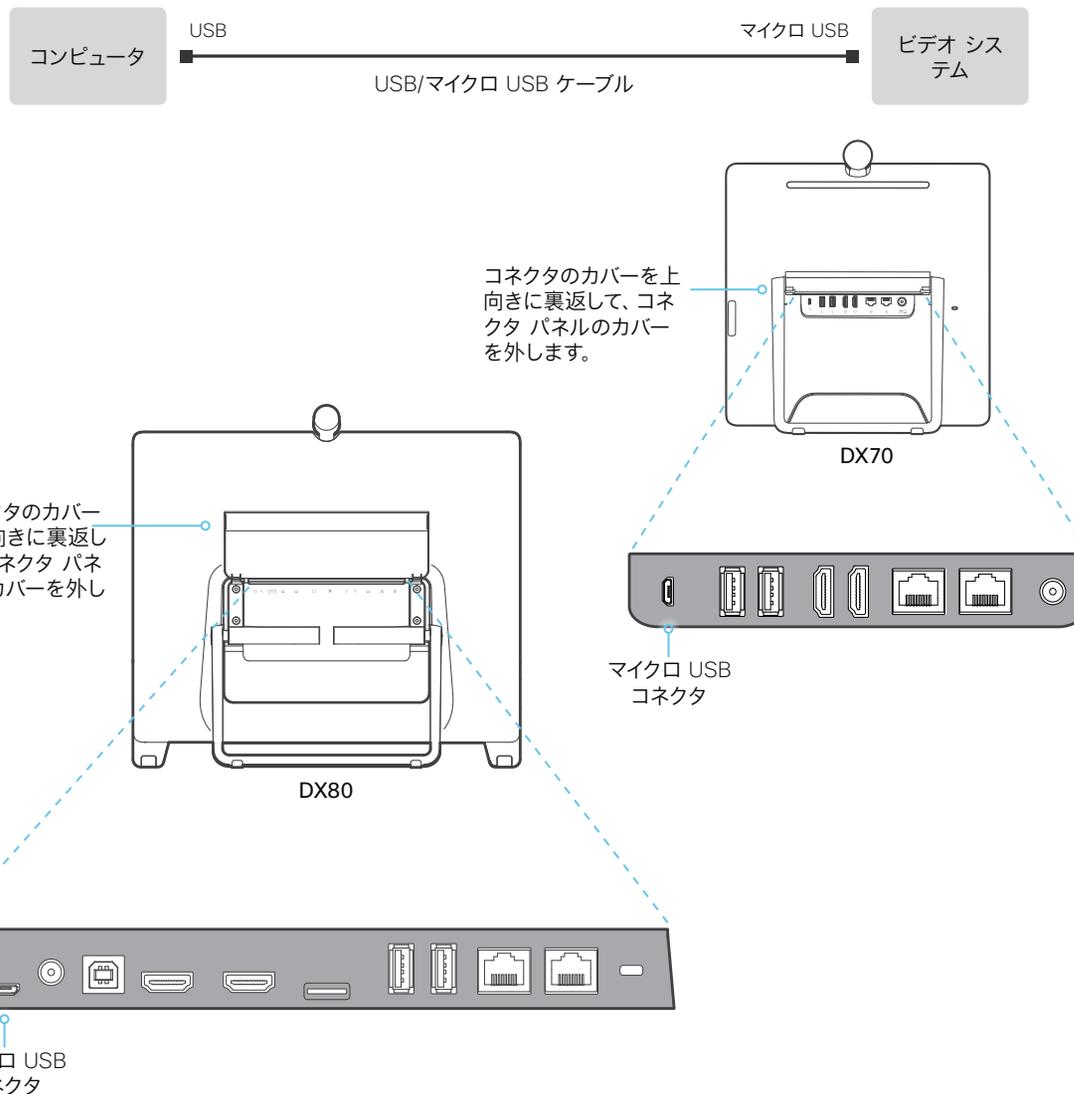
`[シリアルポート (SerialPort)] > [モード (Mode)]`

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)]`

シリアル ポートの設定を変更した後、ビデオ システムを再起動します。

ビデオ システムが CUCM からプロビジョニングされている場合、シリアル ポートの設定を CUCM から設定する必要があります。



## 技術仕様

### ソフトウェアの互換性

- ・ コラボレーション エンドポイント ソフトウェア パーシジョン 8.2 以降

### 製品の同梱物:

- ・ 内蔵の HD カメラとマイクを備えた DX80 システムまたは DX70 システム
- ・ ネットワーク ケーブル
- ・ HDMI/USB ケーブル (DX80 のみ)
- ・ 電源アダプタおよび使用地域向けの電源コード

### 統合型の HD カメラ

- ・ ディスプレイから -5° ~ 70°
- ・ 水平視野角 63°
- ・ 垂直視野角 38°
- ・ 解像度: 1080p30
- ・ F 2.2
- ・ 顔認識に基づくインスタント フォーカス
- ・ ブライバシー シャッター

### ユーザ インターフェイス

- ・ 画面上のグラフィカル ユーザ インターフェイス

### 言語のサポート

- ・ 英語、アラビア語、カタロニア語、チェコ語、デンマーク語、オランダ語、フィンランド語、フランス語、ドイツ語、ヘブライ語、ハンガリー語、イタリア語、日本語、韓国語、ノルウェー語、ポーランド語、ポルトガル語 (ブラジル)、中国語 (簡体字)、スペイン語、ロシア語、スウェーデン語、中国語 (繁体字)、トルコ語、ロシア語 (ソフトウェア バージョンによって異なります)

### システム管理

- ・ 組み込みの SNMP, Telnet, SSH, XML、および SOAP による総合的管理
- ・ Web サーバ、HTTP、および HTTPS を使用したりリモート ソフトウェア アップロード
- ・ 画面上のメニュー システム

### ディレクトリ サービス

- ・ ローカル ディレクトリ (お気に入り) のサポート
- ・ 社内ディレクトリ (Cisco Unified Communications Manager リリースおよび Cisco TelePresence Management Suite 利用)
- ・ LDAP および H.350 をサポートするサーバ ディレクトリ (Cisco TelePresence Management Suite が 必要)
- ・ 日時を含む着信、発信、および不在着信のコール履歴

### 電源

- ・ 定格: 最大 60 W
- ・ 省電力スタンバイ モード

### 動作温度および湿度

- ・ 周囲温度: 0 ~ 40 °C (32 ~ 95°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° (-4 ~ 140°F) (結露しないこと)

### DX80 システムの寸法

- ・ 幅: 56.5 cm (22.2 インチ)
- ・ 高さ: 51.2 cm (20.2 インチ)
- ・ 奥行: 8.9 cm (3.5 インチ)
- ・ 重量: 7.1 kg (15.65 ポンド)

### DX70 システムの寸法

- ・ 幅: 35.31 cm (13.91 インチ)
- ・ 高さ: 37.71 cm (14.84 インチ)
- ・ 奥行: 6.23 cm (2.45 インチ)
- ・ 重量: 3.4 kg (7.5 ポンド)

### 認定および適合規格

#### EU/EEC

- ・ 指令 2006/95/EC (低電圧指令)
  - 規格 IEC/EN 60950-1
- ・ 指令 2004/108/EC (EMC 指令)
  - 規格 EN 55022、クラス B
  - 規格 EN 55024
  - 規格 EN 61000-3-2/-3-3
- ・ 指令 2011/65/EU (RoHS)

#### 米国/カナダ

- ・ UL 60950-1 認証取得
- ・ CAN/CSA C22.2 No. 60950-1-07 認証取得
- ・ FCC CFR 47 Part15、クラス B に準拠
- ・ CFR 47 Part 15.247 に準拠
- ・ CFR 47 Part 15.407 に準拠
- ・ CFR 47 Part 2.1093 FCC 対象 KDB に準拠

### 帯域幅

- ・ 最大 3 Mbps

### 解像度とフレーム レートの最小帯域幅

- ・ 768 kbps から 720p30
- ・ 1472 kbps から 1080p30

### ファイアウォール トラバース

- ・ Cisco TelePresence Expressway テクノロジー

### ビデオ標準

- ・ H.263
- ・ H.263+
- ・ H.264
- ・ AVC (H.264/MPEG-4 Part 10 Advanced Video Coding)

### ビデオ入力

HDMI ビデオ入力 X 1。最大 1920 X 1080@60 fps (HD1080p60) までのフォーマット (以下を含む) をサポートします。

- ・ 640 X 480
- ・ 720 X 480
- ・ 800 X 600
- ・ 1024 X 768
- ・ 1280 X 720
- ・ 1366 X 768
- ・ 1920 X 1080

Extended Display Identification Data (EDID)

### ビデオ出力

HDMI 出力 (1 個) \* (将来の使用に備えて予約済み) 以下のフォーマットをサポートします。

- ・ 1920 X 1080@60 fps (1080p60)

VESA モニタ電源管理

Extended Display Identification Data (EDID)

\* HDMI バージョン 1.3

## 技術仕様 (2/2 ページ)

### ライブ ビデオ解像度 (エンコード/デコード)

最大 1920 X 1080@30 fps (HD1080p30) までのエンコードまたはデコード ビデオ フォーマット (以下を含む) をサポートします。

- ・ 176 X 144 @ 30 fps (QCIF) (デコードのみ)
- ・ 352 X 288 @ 30 fps (CIF)
- ・ 512 X 288 @ 30 fps (w288p)
- ・ 576 X 448 @ 30 fps (448p)
- ・ 640 X 480 @ 30 fps (VGA)
- ・ 704 X 576 @ 30 fps (4CIF)
- ・ 768 X 448 @ 30 fps (w448p)
- ・ 800 X 600 @ 30 fps (SVGA)
- ・ 1024 X 576 @ 30 fps (w576p)
- ・ 1024 X 768 @ 30 fps (XGA)
- ・ 1280 X 720 @ 30 fps (HD720p)
- ・ 1280 X 768 @ 30 fps (WXGA)
- ・ 1280 X 1024 @ 30 fps (SXGA)
- ・ 1440 X 900 @ 30 fps (WXGA+)
- ・ 1680 X 1050 @ 30 fps (WSXGA+)
- ・ 1920 X 1080 @ 30 fps (HD1080p)

### 音声標準

- ・ 64 kbps AAC-LD
- ・ OPUS
- ・ G.722
- ・ G.722.1
- ・ G.711mu
- ・ G.711a
- ・ G.729AB

### 音声機能

- ・ 最大 48 kHz のサンプリング レート
- ・ ハイクオリティ 20 kHz オーディオ
- ・ 音響エコー キャンセラ
- ・ オートゲイン コントロール
- ・ 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

- ・ 内蔵マイク アレイ
- ・ HDMI 音声 1

### 音声出力

- ・ ライン出力 1 個、ミニジャック (DX70)
- ・ 1 HDMI (デジタル メイン音声)

### デュアル ストリーム

- ・ H.239 (H.323) デュアル ストリーム
- ・ BFCP (SIP) デュアル ストリーム
- ・ 最大 1080p (1920 X 1080) の解像度をサポート

### マルチポイント サポート

- ・ Cisco Ad-Hoc Conferencing (Cisco Unified Communications Manager, Cisco TelePresence Server および Cisco TelePresence Conductor が必要)

### プロトコル

- ・ SIP

### 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.235v3 および Advanced Encryption Standard (AES)
- ・ キーの自動生成と交換
- ・ デュアル ストリームでサポート

### 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 で H.245 デュアルトーン多重周波数 (DTMF) トーン
- ・ NTP による日時のサポート
- ・ パケット損失時のダウンスピード機能
- ・ URI ダイアル
- ・ TCP/IP
- ・ DHCP
- ・ IEEE 802.1x ネットワーク認証
- ・ IEEE 802.1Q 仮想 LAN
- ・ IEEE 802.1p QoS およびサービス クラス
- ・ Cisco ClearPath

### IPv6 ネットワークのサポート

- ・ H.323 および SIP に対するデュアル スタックの IPv4 および IPv6
- ・ DHCP, SSH, HTTP, HTTPS, DNS, 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 IP アドレスの割り当て、ステートレス自動設定および DHCPv6 をサポート

### サポートされるインフラストラクチャ

- ・ Cisco Unified Communications Manager 8.6.2 以降
- ・ Cisco TelePresence Video Communication Server (Cisco VCS)

### セキュリティ機能

- ・ Web インターフェイス (HTTPS/HTTP) および SSH を使用した管理
- ・ パスワードで保護された IP 管理
- ・ パスワードで保護された管理メニュー
- ・ IP サービスのディセーブル
- ・ ネットワーク設定の保護

### ネットワーク インターフェイス

- ・ 内部 2 ポートの Cisco イーサネット スイッチ (RJ-45) 10/100/1000BASE-T (自動ネゴシエーションのみ)

### その他のインターフェイス

- ・ USB ポート 3 個
- ・ MicroSD カード スロット 1 個 (将来の使用に備えて)
- ・ メンテナンス目的の Micro-USB ポート 1 個

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。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

2016 年 6 月

## 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。

- RFC 2190 『RTP Payload Format for H.263 Video Streams』
- RFC 2460 『Internet protocol, version 6 (IPv6) specification』
- RFC 2617 『Digest Authentication』
- RFC 2782 『DNS RR for specifying the location of services (DNS SRV)』
- RFC 2976 『The SIP INFO Method』
- RFC 3016 『RTP Payload Format for MPEG-4 Audio/ Visual Streams』
- RFC 3261 SIP 『Session Initiation Protocol』
- RFC 3262 『Reliability of Provisional Responses in SIP』
- RFC 3263 『Locating SIP Servers』
- RFC 3264 『An Offer/Answer Model with SDP』
- RFC 3311 『UPDATE method』
- RFC 3361 『DHCP Option for SIP Servers』
- RFC 3388 『Grouping of Media Lines in the Session Description Protocol (SDP)』
- RFC 3420 『Internet Media Type message/sipfrag』
- RFC 3515 『Refer method』
- RFC 3550 RTP 『RTP: A Transport Protocol for Real-Time Applications』
- RFC 3551 『RTP Profile for Audio and Video Conferences with Minimal Control』
- RFC 3581 『Symmetric Response Routing』
- RFC 3605 『RTCP attribute in SDP』
- RFC 3711 『The Secure Real-time Transport Protocol (SRTP)』
- RFC 3840 『Indicating User Agent Capabilities in SIP』
- RFC 3890 『A Transport Independent Bandwidth Modifier for SDP』
- RFC 3891 『The SIP “Replaces” Header』
- RFC 3892 『Referred-By Mechanism』
- RFC 3960 『Early Media』
- RFC 3986 『Uniform Resource Identifier (URI): Generic Syntax』
- RFC 4028 『Session Timers in SIP』
- 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 4145 『TCP-Based Media Transport in the SDP』
- RFC 4235 『An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)』
- RFC 4566 『SDP: Session Description Protocol』
- RFC 4568 『SDP: Security Descriptions for Media Streams』
- RFC 4574 『The Session Description Protocol (SDP) Label Attribute』
- 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 4583 『Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams』  
draft-ietf-bfcpbis-rfc4583bis-00 『Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams』
- RFC 4585 『Extended RTP Profile for RTCP-Based Feedback』
- RFC 4629 『RTP Payload Format for ITU-T Rec.H.263 Video』
- RFC 4733 『RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals』
- RFC 4796 『The SDP Content Attribute』
- RFC 4862 『IPv6 stateless address autoconfiguration』
- RFC 5104 『Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)』
- RFC 5168 『XML Schema for Media Control』
- RFC 5245 『Interactive Connectivity Establishment (ICE)』: オファーまたはアンサー プロトコル用のネットワーク アドレス変換 (NAT) 通過のためのプロトコル
- RFC 5389 『Session Traversal Utilities for NAT (STUN)』
- RFC 5577 『RTP Payload Format for ITU-T Recommendation G.722.1』
- RFC 5589 『SIP Call Control Transfer』
- RFC 5626 『Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)』
- RFC 5766 『Traversal Using Relays around NAT (TURN)』: Session Traversal Utilities for NAT (STUN) のためのリレー拡張
- RFC 5768 『Indicating Support for Interactive Connectivity Establishment (ICE) in the Session Initiation Protocol (SIP)』
- RFC 5905 『Network Time Protocol Version 4: Protocol and Algorithms Specification』
- RFC 6156 『Traversal Using Relays around NAT (TURN) Extension for IPv6』
- RFC 6184 『RTP Payload Format for H.264 Video』

## シスコ Web サイト内のユーザ ドキュメンテーション

Cisco TelePresence 製品のユーザ マニュアルは、▶ <http://www.cisco.com/go/telepresence/docs> で入手できます。

正しい製品が見つかるまで、右ペイン内の製品カテゴリを選択します。以下の順にパスをたどってください。

[コラボレーション デスク エンドポイント (Collaboration Desk Endpoints)] >

[DX シリーズ (DX Series)] >

[DX シリーズ (DX Series)]

または、次のショートリンクを使用してドキュメンテーションを検索します。▶ <http://www.cisco.com/go/dx-docs> [英語]

ドキュメントは、次のカテゴリに編成されます。

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

- ・ 管理者ガイド: 製品の管理に必要な情報
- ・ CUCM での TelePresence エンドポイントの導入ガイド: Cisco Unified Communications Manager (CUCM) でビデオ システムの使用を開始するために実行するタスク

[保守と運用 (Maintain and Operate)] > [エンドユーザ ガイド (End-User Guides)]

- ・ ユーザ ガイド: 製品の使用方法

[リファレンス ガイド (Reference Guides)] > [コマンド リファレンス (Command references)]

- ・ API リファレンス ガイド: アプリケーション プログラミング インターフェイス (API) のリファレンス ガイド

[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)] > [ライセンス情報 (Licensing Information)]

- ・ オープン ソースのドキュメント: この製品で使用されているオープン 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 > リリース ノート

- ・ ソフトウェア リリース ノート

## シスコのお問い合わせ先

シスコの Web サイトでは、シスコの世界各地のお問い合わせ先を確認できます。

参照先: ▶ <http://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は、代理店にご連絡ください。

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. シスコの商標一覧は [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks) をご覧ください。Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

### シスコ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。シスコ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。By using this product you agree to comply with applicable laws and regulations. 米国および現地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。