

ソフトウェア バージョン TC6.1
2013 年 4 月



アドミニストレータ ガイド

Cisco TelePresence System Quick Set C20 と C20 を使用する Profile 42”

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。

この製品ドキュメンテーションは、Codec C20 を使用して Quick Set C20 および Profiles を設定する管理作業者を対象としています。

この Administrator 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 ドキュメンテーションは次の URL から入手できます。

▶ <http://www.cisco.com/go/telepresence/docs>

本ガイドの使用方法

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

目次

概要	4	信頼リストの削除 (CUCM のみ)	40
ユーザ ドキュメンテーション	5	トラブルシューティング	41
ソフトウェア	5	ログ ファイルのダウンロード	42
このバージョンの新機能	6	システム ソフトウェアのアップグレード	43
Codec C20 を使用する Profile 42" の概要	8	バックアップと復元	44
Quick Set C20 の概要	9	工場出荷時設定へのリセット	45
Web インターフェイス	10	システムの再起動	46
Web インターフェイスの開始	11	システム設定	47
システム パスワードの変更	12	システム設定の概要	48
インタラクティブ メニュー	13	オーディオ設定	51
システム情報	14	カメラの設定	52
コールの開始	15	会議設定	55
コンテンツの共有	16	FacilityService 設定	60
コールの制御および監視	17	H323 設定	61
カメラの制御	18	ネットワーク設定	64
ローカル レイアウトの制御	19	NetworkServices 設定	71
スナップショットのキャプチャ	20	電話帳の設定	76
お気に入りリストの管理	21	プロビジョニング設定	77
お気に入りリストのフォルダ	22	RTP 設定	79
システム設定	23	セキュリティ設定	80
システム設定の変更	24	SerialPort 設定	82
[管理者設定 (Administrator Settings)] メニュー パスワードの設定	25	SIP 設定	83
システムの状態	26	スタンバイの設定	86
壁紙の選択	27	SystemUnit 設定	87
呼び出し音の選択	28	Time Settings	89
ペリフェラルの概要	29	UserInterface 設定	90
ユーザ管理	30	ビデオ設定	91
サインイン バナーの追加	34	試験的設定	103
アプリケーション プログラミング インターフェイス	35	パスワードの設定	104
ビデオ システムの証明書の管理	36	システム パスワードの設定	105
信頼できる証明書のリストの管理	37	メニュー パスワードの設定	106
監査証明書の追加	38	ルート パスワードの設定	107
強力なセキュリティ モードの設定	39		

付録	108
モニタについて.....	109
Cisco TelePresence Touch 8" コントローラへの接続.....	110
最適鮮明度プロファイル.....	111
ClearPath：パケット損失の復元.....	112
Cisco TelePresence C シリーズ コーデックに接続するスピーカー システム の要件.....	113
Codec C20：物理インターフェイス.....	114
Codec C20：物理インターフェイス（続き）.....	115
ピン配列方法	116
Quick Set C20 と PrecisionHD 1080p 4x カメラとのケーブル構成	117
Quick Set C20 と PrecisionHD 1080p 12x カメラとのケーブル構成	118
Profile 42" 用の DNAM	119
工場出荷時設定へのリセット	120
タッチ 8" コントローラの工場出荷時設定へのリセット	121
技術仕様	122
サポートされている RFC	125
シスコ Web サイト内のユーザ ドキュメンテーション	126
シスコのお問い合わせ先.....	127

1 章

概要

このマニュアルは、高度なレベルで製品を管理するために必要な情報を示します。

このガイドの対象となる製品は次のとおりです。

- ・ C20 を使用する Profile 42"
- ・ Quick Set C20

ユーザ ドキュメンテーション

Cisco TelePresence Codec C シリーズのユーザ マニュアルには、さまざまなユーザ グループに適した複数のマニュアルがあります。

- ・ 『インストール 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
- ・ 『CUCM での TC エンドポイントの管理』:
製品を Cisco Unified Communications Manager (CUCM) とともに使用開始するために実行するタスク
- ・ 『管理者ガイド』(このガイド):
製品の管理に必要な情報
- ・ 『クイック リファレンス ガイド』:
製品の使用方法 (リモコンやタッチ コントローラ)
- ・ 『ユーザ ガイド』:
製品の使用方法 (リモコンやタッチ コントローラ)
- ・ 『カメラ ユーザ ガイド』:
PrecisionHD カメラのユーザ ガイド
- ・ 『API リファレンス ガイド』:
Application Programmer Interface (API) の使用方法、およびコマンドライン コマンドのリファレンス ガイド
- ・ 『TC コンソール アプリケーション ユーザ ガイド』:
無償の TC コンソール アプリケーションにより、カスタマイズ可能な高度なコーデックの機能へのグラフィカル インターフェイスが提供されます。
- ・ ナレッジ ベースの記事
- ・ 『Video conferencing room primer』:
会議室の設計とベスト プラクティスに関する一般的なガイドライン
- ・ 『Video conference room acoustics guidelines』:
認識される音声の品質を向上させるために行うべきこと
- ・ ソフトウェア リリース ノート
- ・ 法令準拠および安全上の注意ガイド
- ・ 法的情報およびライセンス情報

ユーザ ドキュメンテーションのダウンロード

ユーザ マニュアルの更新バージョンがないか、定期的にシスコの Web サイトにアクセスして確認することを推奨します。次のサイトに進みます。

▶ <http://www.cisco.com/go/telepresence/docs>

シスコの Web サイトにあるドキュメンテーションの検索ガイドラインについては、付録の ▶ 「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。

ソフトウェア

製品のソフトウェアは、シスコの Web サイトからダウンロードできます。次のサイトに進みます。

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

次のサイトから、ソフトウェア リリース ノート (TC6) を参照することを推奨します。

▶ http://www.cisco.com/en/US/products/ps11424/tsd_products_support_series_home.html

このバージョンの新機能

ここでは TC6.1 ソフトウェア バージョンで追加または変更されたシステム設定および新しい機能の概要について説明します。

ソフトウェア リリース ノート

新情報および変更のすべての概要については、ソフトウェア リリース ノート (TC6) を読むことを推奨します。

► http://www.cisco.com/en/US/products/ps11424/tsd_products_support_series_home.html を参照してください。

ソフトウェアのダウンロード

ソフトウェアのダウンロードについては、
► <http://www.cisco.com/cisco/software/navigator.html> を参照してください。

新機能および改善点

リリース キー ポリシーとソフトウェア アップグレード管理の変更点

ソフトウェア バージョン TC6.1 以降では、新しいリリース キーをインストールする必要はありません。前の TC ソフトウェア バージョンに対する有効なリリース キーがビデオ システムにあれば十分です。

TC6.1 以降、ソフトウェアは、► <http://www.cisco.com> からのみダウンロードが可能となり、CCO (シスコのオンライン接続) ID に割り当てられた有効なサービス契約を持つユーザに対してのみ提供されます。

Telnet および SSH で常にパスワードの入力を要求

Telnet または SSH を使用してビデオ システムにサインインする場合、常にパスワードの入力が求められます。これは、パスワードが空 (未設定) の場合にも適用されます。

画面上のメッセージにおける <p> および
 タグのサポート

セキュリティ上の理由から、画面上のメッセージには HTML タグ <p> および
 のみがサポートされます (Message Alert コマンドと Message Prompt コマンド)。これらのタグは、通常どおり改行になります。他のタグは解釈されません。それらは画面上にテキストとして表示されます。

診断のロギング

タッチ コントローラを使用して、ビデオ システムの診断ロギングをイネーブルにすることができます。診断ロギングはトラブルシューティングのみを目的としており、有効にするとシステム パフォーマンスが低下する場合があります。

SIP コールにおける G.729 音声コーデックのサポート

IP 電話機の相互運用性を改善するために、G.729AB オーディオ コーデックのサポートが SIP コールに追加されています。G.729 は H.323 コールではサポートされません。

ボイス メールのサポートおよびメッセージ待機インジケータ

Cisco Unified Communications Manager (CUCM) に登録されているすべてのエンドポイントにボイス メールのプロファイルを割り当てることができます。このようなエンドポイントから *Busy* または *No Answer* の信号を受信した場合、コールはボイス メールに転送されます。

タッチ コントローラがある場合は、[メッセージ (Messages)] アイコンをタップしてもボイス メールにアクセスできます。また、メッセージ待機通知も表示されます。

CUCM における共有回線のサポート

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することができます。これは、同じパーティション内の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。同じ番号を共有する各デバイスは、ライン上のもう一方のアピアランスからステータスを受け取ります。

たとえば、多くのデバイスが同じ番号を共有し、操作可能な最初のオペレータがコール (ヘルプ デスク) に応答するように、共有回線を設定できます。管理者が幹部社員へのコールを管理 (転送、介入) するアシスト コール処理は、それとは別の例です。また、ある人に属する複数のデバイスが同一のラインを共有するようにして、その人がデバイスのどれかでコールに応答したときに別のデバイスを復帰させることができます (シングル ナンバー リーチ)。

共有回線の設定方法に関する情報は、CUCM ユーザ マニュアル (『Cisco Unified Communications Manager System Guide』) から参照できます。

CUCM でのアドホック会議

Cisco Unified Communications Manager (CUCM) バージョン 8.6.2 以降で登録されたエンドポイントは、アドホック会議を呼び出すことができます。このためには、会議ブリッジが MCU として CUCM に追加されている必要があります。エンドポイントはそれが登録されている場所とは関係なく、会議に参加できます。

参加者が 2 人まで減った場合、会議はポイント ツー ポイント コールにデエスカレーションされます。

コンサルタティブ転送のサポート

コンサルタティブ転送がサポートされています。コンサルタティブ転送は、発信者が転送先に接続する前に転送者と転送先が通話するものです。

CTI または JTAPI のサポート (リモート エクスパート ソリューションのサポート)

Cisco Unified Communications Manager (CUCM) では、Java Telephony API (JTAPI) 経由でエンドポイントのコール制御を行うことができます。シスコの JTAPI では、カスタム アプリケーションによりデバイスの可用性を監視し、コールをリモートで制御することが可能です。次の機能がサポートされています。コール、応答、切断、保留、再開、ブラインド転送、コンサルタティブ転送、およびコンサルタント会議。

Cisco Unified Communications Manager (CUCM) 9.0 以降に登録されたエンドポイントは、Cisco Remote Expert Smart Solution (バージョン 1.8) をサポートします。

タッチ ユーザ インターフェイスの改良

- ・ 不在着信およびメッセージ待機インジケータ。ボイス メールに直接アクセス可能。
- ・ 新しいダイヤル パッド、ソフト キーボードおよび改良されたテキスト セレクタ
- ・ 暗号化インジケータ
- ・ コール時間インジケータ
- ・ 有効なリリース キーがない場合にリリース キーの入力が可能

システム構成の変更

新しい設定

ネットワーク DHCP RequestTFTPServerAddress

SIP プロファイル回線

SIP プロファイル メールボックス

ビデオ CamCtrlPip CallSetup モード

ビデオ CamCtrlPip CallSetup 時間

ビデオ SelfviewControl AutoResizing

変更された設定

Conference Multipoint Mode

旧: <Auto/Off/MultiWay>

新: <Auto/Off/MultiWay/CUCMMediaResourceGroup>

Video Output HDMI[x] MonitorRole

旧: <First/Second/PresentationOnly>

新: <First/Second/PresentationOnly/Recorder>

Codec C20 を使用する Profile 42” の概要

システムのインストール方法に関する説明は、Profile システムのインストールシートを参照してください。

Codec C20

- ・ フル HD ビデオ。
- ・ 高解像度でのデータ共有。
- ・ 豊富な I/O 機能。

PrecisionHD 1080p カメラ

ビジュアル コミュニケーション用に設計され、以下の機能を備えたフル HD カメラ

- ・ 12 × 光学ズーム
- ・ 高速かつ正確なパン、チルト、ズーム

モニタ

42 " フル HD LCD、16:9、1080 × 1920 の解像度。

オーディオ モジュール

以下の装備をサポートするワイド バンドのオーディオ モジュール。

- ・ 20 kHz AAC-LD。
- ・ 1 台のエコー キャンセラ。

オーディオ増幅器

非常に明瞭で自然な音声を提供する、プロファイル システム向けに最適化された DNAM

マイク

ケーブル付きマイク 2 本。

操作デバイス

- ・ タッチ 8" コントローラ。
- ・ AAA バッテリーを備えたリモート コントロール。

基本オプション

据置型の踏み板、ホイール ベース、または壁面取付型の台座



Quick Set C20 の概要

Quick Set C20 は、大規模システムの豊富なユーザ エクスペリエンスをコンパクトな会議室ベースのソリューションに組み込んだものです。Quick Set C20 は解像度のオプションとして 1080p30 または 720p60 が提供されている高解像度のビデオ コラボレーション システムであり、導入および管理が容易で直感的に使用できます。Quick Set C20 は他に例を見ない装置で、初めてビデオ ソリューションを配置する小規模な導入だけでなく、既存のビデオ会議ソリューションを組織全体で数百箇所に拡張することが可能です。

Quick Set C20

Quick Set C20 には Codec C20、PrecisionHD 1080p 4 倍ズーム カメラまたは PrecisionHD 1080p 12 倍ズーム カメラ、テーブル マイク 20 台、リモコンが含まれます。任意の HD ディスプレイに追加すれば、会議の準備は完了です。

デザインの特長

- ・ フラット パネル ディスプレイを高解像度の 1080p の会議スペースに変えます。
- ・ シンプルで直感的に接続できるため、設定は DVD プレーヤーの接続と同じくらい容易に行えます。
- ・ Quick Set C20 の解像度は、4 倍ズーム カメラの場合で最大 1080p30、12 倍ズーム カメラの場合で最大 1080p30 および 720p60 です。
- ・ 規格に準拠した 1080p ソリューション：機能を失うことなく規格ベースのビデオと互換性があります。
- ・ スマートでコンパクトなデザイン。

アプリケーションの特長

- ・ マルチメディアとプレゼンテーションをボタン 1 つで共有できます。
- ・ 基本的な API が IP (Telnet または SSH) から利用できます。
- ・ デュアル ディスプレイ オプションを利用可能。
- ・ 720p および WXGA で HD コンテンツを共有。

パフォーマンスの特長

- ・ 1080p30 までの最適な解像度。
- ・ 最大 6 Mbps の H.323/SIP。



2 章

Web インターフェイス

Web インターフェイスの開始

Web インターフェイスではビデオ会議システムにフル設定アクセスが提供されます。

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。

この章では、Web インターフェイスを使用してシステム設定とメンテナンスを行う方法について説明します。

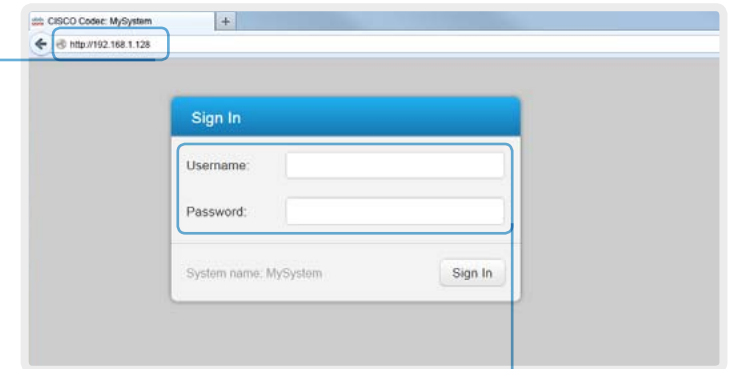
主要な Web ブラウザの最新版を使用することを推奨します。

1. 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 (IPv4 または IPv6) を特定するには、タッチ コントローラで [\[Settings \(⚙️\)\]](#) をタップするか、リモコンや画面上のメニューを使用する場合は [\[Home\] > \[Settings\] > \[System information\]](#) に進みます。



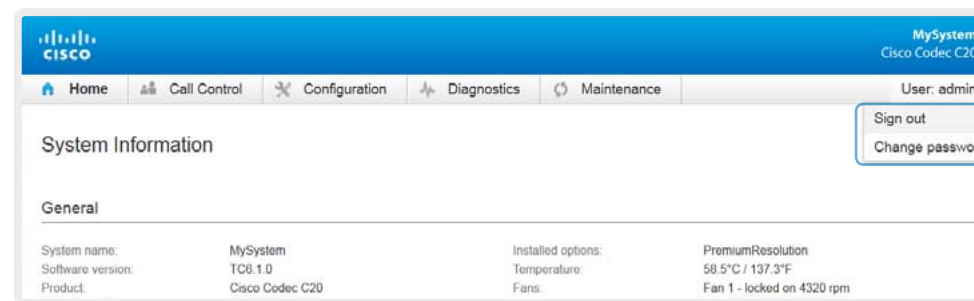
2. サインイン

ビデオ システムのユーザ名とパスワードを入力して、[\[Sign In\]](#) をクリックします。



システムでは *admin* という名前のパスワードのないデフォルト ユーザが提供されます (初めてサインインするときは [\[Password\]](#) フィールドを空白のままにします)。

admin ユーザにパスワードを設定することを強く推奨します。次のページを参照してください。



サインアウト

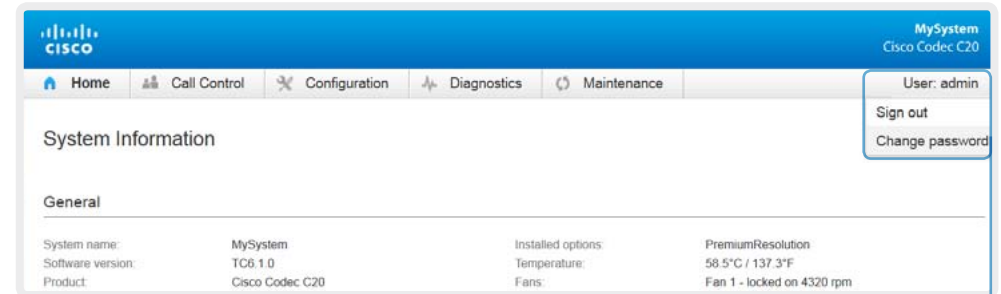
ユーザ名の上にマウスを移動して、ドロップダウン リストから [\[Sign out\]](#) を選択します。

システム パスワードの変更



システム設定へのアクセスを制限するために、デフォルトの *admin* を含む、管理者権限を持つユーザにパスワードを設定することを強く推奨します。

▶ 「パスワードの設定」 の章で、パスワード保護の詳細を確認できます。



1. [Change Password] ダイアログを開く

ユーザ名の上にマウスを移動して、ドロップダウン リストから [\[Change password\]](#) を選択します。

Change Password: admin

Current password	
New password	
Repeat new password	
Change password Cancel	

2. 新しいパスワードを設定する

現在のパスワードと新しいパスワードを要求どおりに入力し、[\[Change password\]](#) をクリックして変更を適用します。



パスワードが現在設定されていない場合は、[\[Current password\]](#) フィールドを空白のままにします。

インタラクティブ メニュー

Web インターフェイスからタスクと設定にアクセスできます。これらはサインインしたときにページの上部に表示されるメイン メニューに表示されます。

メイン メニュー項目の上にマウスを置くと、関連するサブページに移動できます。

メイン メニュー

メイン メニュー アイテムの上にマウスを置くと、関連するサブページのタイトルがドロップ ダウンします。

サブページのタイトルをクリックして開きます。ユーザにアクセス権限のあるページのみを開くことができ、その他のページは淡色表示されます。^{*}

メイン メニューの [Home] をクリックすると、[System Information] ページに戻ります。

サブページ

Call Control
Call Control
Favorites Management

Configuration
System Configuration
System Status
Personalization
Peripherals
User Administration
Sign In Banner
API
Security

Diagnostics
Troubleshooting
Log Files

Maintenance
Software Upgrade
Backup and Restore
Factory Reset
Restart

^{*} ユーザ管理、ユーザ ロール、およびアクセス権に関する詳細情報は、▶ 「ユーザ管理」 の項で確認できます。

システム情報

ビデオ システムの [Home] ページには、システムの基本設定およびステータスの概要が表示されます。

ここではシステム名や製品タイプ、システムが動作するソフトウェア バージョン、IP アドレスなどの情報が含まれます。また、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。

ホーム

System Information

General

System name:	MySystem	Installed options:	PremiumResolution
Software version:	TC6.1.0	Temperature:	58.5°C / 137.3°F
Product:	Cisco Codec C20	Fans:	Fan 1 - locked on 4320 rpm Fan 2 - locked on 4320 rpm
Serial number:	ABCD12345678		
IPv4 address:	192.168.1.128		
MAC address:	01:23:45:67:89:AB		
Valid release key:	Yes		

H323

Status:	Registered	Number:	123456
Gatekeeper:	192.168.1.1	ID:	firstname.lastname@company.com

SIP

Status:	Registered	URI:	firstname.lastname@company.com
Proxy:	192.168.1.2		

* 図に示しているシステム情報は一例です。お使いのシステムとは異なる場合があります。

コールの開始

Web インターフェイスの [Call Control] ページを使用して、コールを開始できます。

 Web インターフェイスを使用してコールを開始する場合でも、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）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。

発信

[Local phone book] または [Directory] で連絡先名を選択するか、[Search and Dial] フィールドに完全な URI または番号を入力して、相手呼び出すことができます。次に、関連する連絡先カードで [\[Call\]](#) をクリックします。

連絡先リストの検索

[Search or Dial] フィールドに 1 文字以上入力します。入力内容に応じて、[Local phone book] および [Directory] の一致するエントリがリストされます。

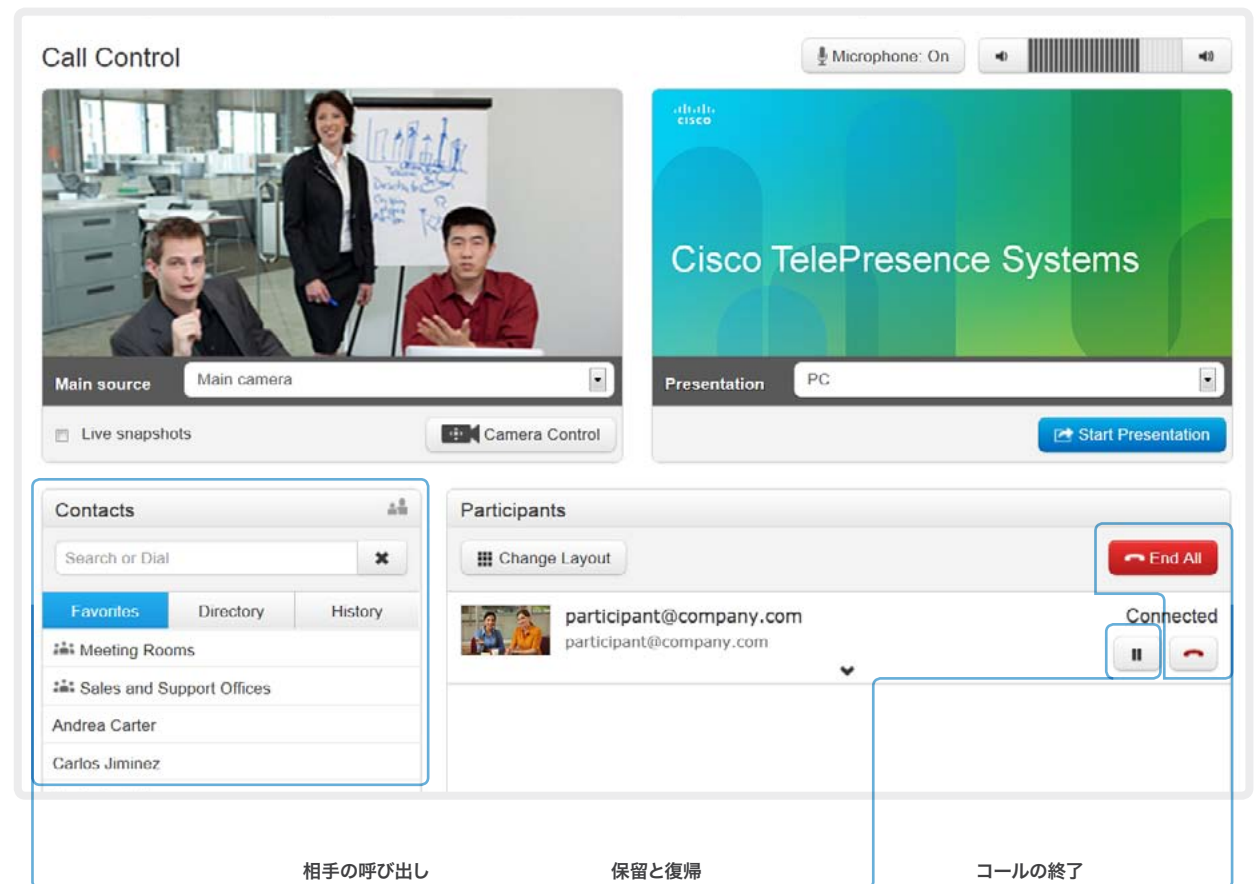
[Local phone book] または [Directory] 内のエントリを選択してから、[\[Call\]](#) をクリックします。

複数の相手に発信

ポイントツーポイントのビデオ コール（2 者間のコール）を拡張してもう 1 箇所の参加者を含めることができます。この参加者は音声のみで参加できます。

最初の参加者を呼び出したときと同じ手順で、次の会議参加者を呼び出してください。

移動先 : [Call Control] > [Call Control]



相手の呼び出し

[Local phone book] または [Directory] 内の連絡先名をクリックします。次に、連絡先カードで [\[Call\]](#) をクリックします。

または、[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 [\[Call\]](#) ボタンをクリックします。

保留と復帰

参加者の隣にある  ボタンを使用すると、その人が保留状態になります。

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

1 箇所の参加者のみコールを終了するには、その参加者の  ボタンをクリックします。

[\[End all\]](#) ボタンをクリックすると、コール全体が終了します。

コンテンツの共有

ビデオ システムの外部入力 の 1 つにプレゼンテーション ソースを接続できます。プレゼンテーション ソースとして最も多く使用されるのは PC ですが、システムの設定によってはその他のオプションを使用できる場合があります。

コールの間、遠端（もう一方の参加者）とコンテンツを共有できます。

コールを行っていない場合、コンテンツはディスプレイ上にローカルで共有されます。

移動先 : [Call Control] > [Call Control]

Call Control



Main source
Main camera

☐ Live snapshots

Microphone: On



Presentation
PC

Contacts

Search or Dial

Favorites

Directory

History

Meeting Rooms

Sales and Support Offices

Andrea Carter

Carlos Jimenez

Participants

Change Layout

participant@company.com
participant@company.com

Connected

End All

Pause

End

コンテンツの共有

- プレゼンテーション ソースをドロップダウン リストから選択します。
- [\[Start Presentation\]](#) をクリックします。

コンテンツ共有の停止 :

共有している間に表示される [\[Stop Presentation\]](#) ボタンをクリックします。

コールの制御および監視

[Call Control] ページを使用して、複数のコール機能を制御および監視できます。

移動先 : [Call Control] > [Call Control]

マイクrophon ミュート機能

このボタンをクリックすると、マイクがミュートになります。すると、テキストが *[Microphone: Off]* に変わります。

再度クリックすると、ミュートが解除されます。

The screenshot shows the Cisco TelePresence Systems interface. At the top, there are volume controls labeled '音量小' (Volume Low) and '音量大' (Volume High). Below these is a 'Microphone: On' button. The main display area shows a video feed of a participant and a presentation titled 'Cisco TelePresence Systems'. Below the video feed is a 'Camera Control' button. The 'Participants' section shows a list of participants, including 'participant@company.com' with a 'Connected' status. A 'Change Layout' button and an 'End All' button are also visible. A detailed view of the participant's call information is shown below the list, including protocol, call rates, and encryption details.

Audio	Transmit	Receive
Protocol	AACLD	AACLD

コールの詳細を表示
または非表示にします。

矢印をクリックすると、
コールの詳細情報が表
示されます。

矢印をもう一度クリック
すると、情報が非表示
になります。

コールの詳細

必要に応じて、ブラウザ
をスクロールしてコール
の詳細を表示します。

カメラの制御

[Call Control] ページを使用してカメラを制御できます。

[Camera Control] ボタンをクリックして開いたウィンドウから、カメラのパン、チルト、ズームを行い、カメラのプリセットを適用することができます。

移動先 : [Call Control] > [Call Control]

Call Control



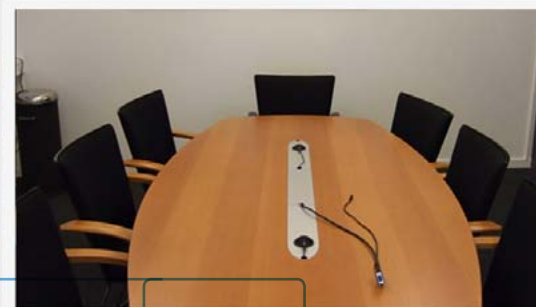
カメラ プリセット

カメラ プリセットが定義されている場合、ここに表示されます。プリセットの名前をクリックして、それを適用します。

制御するカメラを選択

矢印をクリックすると、ドロップダウンリストが開きます。次に、制御するカメラを選択します。

Camera Control for camera 1



パンとチルト

カメラのパンには左右の矢印キーを使用し、チルトには上下の矢印キーを使用します。

ズーム

ズームインとズームアウトには、+ および - を使用します。



ローカル レイアウトの制御

[Call Control] ページを使用してローカル レイアウトを選択できます。

ここでいうレイアウトとは、会議参加者のビデオとプレゼンテーションを画面に表示でき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。

移動先 : [Call Control] > [Call Control]

Microphone: On

Presentation

PC

Camera Control

Start Presentation

Participants

Change Layout

No participants connected

レイアウトの変更

1. [\[Change Layout\]](#) をクリックします。
2. 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。

コールの間にレイアウトを変更できます。

Change Layout

Auto

Equal

Prominent

Overlay

Single

スナップショットのキャプチャ

スナップショット機能はデフォルトでディセーブルになっていますが、ビデオシステムによりキャプチャされたスナップショットを [Call Control] ページに表示できます。ビデオ システムのカメラからのキャプチャに加え、プレゼンテーション チャンネルからのキャプチャも表示されます。

この機能は、たとえばカメラのビューをチェックするなど、リモート ロケーションからビデオ システムを管理する際に役立つ場合があります。

Web スナップショットを使用するには、ADMIN クレデンシャルでサイン インする必要があります。

スナップショット機能のイネーブル化

スナップショット機能は、デフォルトではディセーブルです。この機能は、リモート コントロールと画面上のメニューを使用してイネーブル化する必要があります。

- ・ [Advanced Configuration] メニューに進み、[\[Video\] > \[AllowWebSnapshots\]](#) に移動して、[On] を選択します。

コール中の遠端のスナップショット

コール中は、リモート参加者のメインカメラとプレゼンテーションチャネル（遠端）のスナップショットがキャプチャされ、図のように表示されます。スナップショットはおよそ 20 秒ごとに更新されます。



遠端のビデオ システムで Web スナップショットが無効にされていても、遠端のスナップショットがキャプチャされます。暗号化されたコールの場合にのみ、Web スナップショットが禁止されます。

移動先 : [Call Control] > [Call Control]

Call Control

Microphone: On

Main source: Main camera

Presentation: PC

Live snapshots

Camera Control

Start Presentation

Contacts

Search or Dial

Favorites Directory History

Meeting Rooms

Sales and Support Offices

Participants

Change Layout

End All

participant@company.com

Connected

遠端のスナップショット

ライブ スナップショットの取得

[Live snapshots] ボックスがチェックされているとき、スナップショットはビデオ システム (メイン カメラとプレゼンテーション) により約 2 秒ごとにキャプチャされます。

ビデオ システムからのスナップショット

お気に入りリストの管理

お気に入りリストのエントリには、タッチ コントローラ、画面上のメニュー（電話帳の [My contacts] フォルダ）、および Web インターフェイスからアクセスできます。

移動先 : [Call Control] > [Favorites Management]

Favorites Management

Favorites

Name ▾	Number
Andrea Carter	carter@company.com
Carlos Jimenez	jimenez@company.com
Maria Bartelli	bartelli@company.com
Meeting Rooms	
Sales and Support Offices	

連絡先の追加

[Add Contact] をクリックし、ポップアップするフォームに入力します。次に [Save] をクリックして連絡先をお気に入りリストに保存します。

連絡先の詳細情報の編集

連絡先の名前に続いて [Edit] をクリックします。フォーム内の詳細情報を必要に応じて変更し、[Save] をクリックします。

連絡先の削除

連絡先の名前に続いて [Edit] をクリックします。次に [Delete] をクリックしてエントリをお気に入りリストから削除します。

連絡先をフォルダに保存

ドロップダウン リストから適切なフォルダを選択します。
[No folder] は連絡先が最上位レベルに保存されることを意味します。

連絡方法の追加

連絡先ごとに、ビデオ、電話、モバイルなど複数の連絡方法を保存できます。

Name

Title

Folder

Contact method ✕
Number:
Protocol:
Call rate:
Device:

お気に入りリストのフォルダ

お気に入りリストのエントリはフォルダに整理できます。

移動先 : [Call Control] > [Favorites Management]

Favorites Management

[< Back](#)
Favorites

Name ▼	Number
Andrea Carter	carter@company.com
Carlos Jimenez	jimenez@company.com
Maria Bartelli	bartelli@company.com
Meeting Rooms	-
Sales and Support Offices	-

フォルダを開く

フォルダ名をクリックしてフォルダを開き、連絡先のリストを表示します。

フォルダの編集

- [Edit folders] をクリックします。
- 既存のフォルダの名前をクリックして、その詳細情報を表示および編集します。または [Add folder] をクリックして詳細情報を入力し、新しいフォルダを作成します。
- [Save folder] をクリックして詳細情報を保存します。または、[Delete folder] をクリックしてフォルダとすべての連絡先およびサブフォルダを削除します。

Edit folders

Select a folder to edit

Meeting Rooms
Sales and Support Offices

Folder name

Parent folder

Favorites Management

[< Back](#)
Sales and Support Offices

Name ▼	Number
Berlin Sales Office	berlin@company.com
Buenos Aires Training Center	buenosaires@company.com
Cairo Sales Office	cairo@company.com
Osaka Sales Office	osaka@company.com

システム設定

システム設定は複数のカテゴリにグループ化されます。左側のペインでカテゴリを選択すると、関連するすべての設定が右側に表示されます。

各システム設定は ▶ 「システム設定」 の章で詳しく説明します。

移動先 : [Configuration] > [System Configuration]

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強調表示されます。

System Configuration

Set Administrator Settings menu password

Search...

Conference 1

Refresh

Collapse all

Expand all

- Audio
- Cameras
- Conference**
- Experimental
- FacilityService
- H323
- Network
- NetworkServices
- Phonebook Server
- Provisioning
- RTP Ports Range
- Security
- SerialPort
- SIP
- Standby
- SystemUnit
- Time
- UserInterface
- Video

Encryption Mode	BestEffort	Save
IncomingMultisiteCall Mode	Allow	Save
MaxReceiveCallRate	6000	Save (64 to 6000)
MaxTotalReceiveCallRate	10000	Save (64 to 10000)
MaxTotalTransmitCallRate	10000	Save (64 to 10000)
MaxTransmitCallRate	6000	Save (64 to 6000)
MicUnmuteOnDisconnect Mode	On	Save
Multipoint Mode	Auto	Save
PacketLossResilience Mode	On	Save

AutoAnswer

Delay	0	Save (0 to 50)
Mode	Off	Save
Mute	Off	Save

DefaultCall

Protocol	Sip	Save
----------	-----	------

カテゴリの選択

システム設定は複数のカテゴリに構造化されます。関連する設定を表示するには、カテゴリを選択します。

リストの展開と縮小

ボタンを使用して、すべてのリストに展開するか、個々のリストに縮小します。

* 図に示している設定は一例です。お使いのシステムの設定とは異なる場合があります。

システム設定の変更

すべてのシステム設定は [System Configuration] ペインから変更できます。設定の値の領域は、ドロップダウン リストとして指定されるか、テキスト入力フィールドの後の説明テキストで指定されます。

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。

移動先 : [Configuration] > [System Configuration]

ドロップダウン リスト

矢印をクリックすると、ドロップダウンリストが開きます。優先する値を選択し、[\[Save\]](#) をクリックして変更を反映します。

System Configuration

Search...

Audio

Cameras

Conference

Experimental

FacilityService

H323

Network

NetworkServices

Phonebook Server

Conference 1

Refresh

Collapse all

Expand all

Encryption Mode

BestEffort

Save

IncomingMultisiteCall Mode

Off

On

BestEffort

Save

MaxReceiveCallRate

6000

Save

(64 to 6000)

MaxTotalReceiveCallRate

10000

Save

(64 to 10000)

MaxTotalTransmitCallRate

9000

Save

(64 to 10000)

MaxTransmitCallRate

6000

Save

(64 to 6000)

テキスト入力フィールド

テキストを入力フィールドに入力し、[\[Save\]](#) をクリックして変更を反映します。

[管理者設定 (Administrator Settings)] メニュー パスワードの設定

ビデオ会議システムの初期設定では、メニュー パスワードが設定されていないため、リモコンまたはタッチ コントローラを使用して誰でも [Administrator Settings] メニューにアクセスできます。



管理者設定はビデオ会議システムの動作に大きく影響するので、メニュー パスワードを定義することを強く推奨します。

▶ 「パスワードの設定」 の章で、パスワード保護の詳細を確認できます。

移動先 : [Configuration] > [System Configuration]

System Configuration

Conference 1

Audio

Set Administrator Settings menu password

Refresh

Collapse all

Expand all

メニュー パスワードの変更

[\[Set/Change Administrator Settings menu password\]](#) をクリックして、このダイアログを開きます。

新しいパスワードをテキスト入力フィールドに入力し、[\[Save\]](#) をクリックして保存します。

既存のパスワードをクリアするには、[\[Unlock\]](#) ボタンを使用します。

Set Administrator Settings menu password

Password

By specifying an advanced menu password, users will be prompted for a password when trying to enter the advanced settings via an end-point's user interface. Providing an empty password disables the advanced settings password check.

Unlock

Save

システムの状態

システム ステータスは複数のカテゴリにグループ化されます。左側のカラムでカテゴリを選択すると、関連するステータスが右側のウィンドウに表示されます。^{*}

移動先 : [Configuration] > [System Status]

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強調表示されます。

System Status

Search...

- Audio
- Camera
- Conference**
- Diagnostics
- Experimental
- H320 Gateway
- H323 Gatekeeper
- HttpFeedback
- MediaChannels
- Network
- NetworkServices
- Preset
- Provisioning
- Security
- SIP
- Standby
- SystemUnit
- Time

Conference

Refresh Collapse all Expand all

DoNotDisturb	Inactive
Line 1 Mode	Private
LoudestSite	
Multipoint Mode	Off

ActiveSpeaker

Mode	Auto
SiteId	0

Presentation

LastLocalSource	0
LocalSendingMode	
LocalSource	0
Mode	Off
Protocol	
SiteId	0

カテゴリの選択

システム ステータスは複数のカテゴリに構造化されます。関連するステータス情報を表示するには、カテゴリを選択します。

リストの展開と縮小

ボタンを使用して、すべてのリストに展開するか、個々のリストに縮小します。

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

壁紙の選択

定義済みの壁紙の中から、ディスプレイの背景として使用する壁紙を選択できます。

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。

タッチ コントローラを使用する場合、カスタムの壁紙はメイン ディスプレイにのみ適用され、タッチ コントローラには表示されません。

移動先 : [Configuration] > [Personalization] : [Wallpaper] タブ

Personalization

Wallpaper Ringtone

Select active wallpaper



None



Growing



Summersky



Waves



Custom

Upload custom wallpaper

Only .png files with a maximum resolution of 1920x1200 are supported.

No file selected

Browse...

Upload

カスタム壁紙ファイルのアップロード

[\[Browse...\]](#) をクリックして、カスタム壁紙イメージ ファイルを特定します。

ファイル形式は .png にする必要があり、最大イメージ サイズは、1920×1200 ピクセルです。

[\[Upload\]](#) 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。

壁紙の選択

リストから壁紙を選択します。

カスタムの壁紙をアップロードした場合は、定義済みの壁紙とともにリストに表示されます。

選択された壁紙が強調表示されます。

呼び出し音の選択

定義済みの呼び出し音から選択できます。選択された呼び出し音は、このページから再生できます。



Web インターフェイスを使用して再生を開始する場合でも、呼び出し音を再生するのはビデオ システムであり、Web インターフェイスを実行する PC ではありません。

移動先 : [Configuration] > [Personalization] : [Ringtone] タブ

呼び出し音の選択

呼び出し音をドロップダウン リストから選択して [\[Save\]](#) 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。



呼び出し音を再生する前に、保存する必要があります。

ペリフェラルの概要

このページでは、ビデオ入力およびビデオ出力の設定の概要、およびビデオシステムに接続されたカメラ、タッチ コントローラまたは ISDN リンクに関する情報を表示します。^{*}

ISDN リンクの管理

ISDN リンクがビデオ システムとペア化されていれば、このページから管理できます。

ISDN リンクの設定および使用の方法は、
▶ <http://www.cisco.com/go/isdnlink-docs> の ISDN リンクのドキュメントに説明されています。

^{*} 図に示しているペリフェラルは一例です。お使いのシステムではペリフェラルとビデオ入出力の設定が異なる場合があります。

移動先 : [Configuration] > [Peripherals]

Peripherals

Cameras

Camera 1	Cisco PrecisionHD 1080p ...
----------	-----------------------------

Video Inputs

Input 1 – HDMI	Camera
Input 2 – DVI	PC

Video Outputs

Output 1 – HDMI	1280x720, 60Hz
Output 2 – HDMI	—

ISDN Link

No ISDN Link devices are connected.

Manage ISDN Link

ユーザ管理

このページから、ビデオ会議システムのユーザ アカウントを管理できます。新規ユーザ アカウントの作成、既存ユーザの詳細情報の編集、ユーザの削除が行えます。

デフォルトのユーザ アカウント

システム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* であり、パスワードは設定されていません。



admin ユーザにパスワードを設定することを強く推奨します。

▶ 「パスワードの設定」 の章で、パスワードの詳細を確認できます。

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 ロールまたはその複数の組み合わせを保持する必要があります。

権限がオーバーラップしていない、次の 3 つのユーザ ロールが存在します。

- ・ ADMIN：このロールを持つユーザは、新規ユーザの作成および大部分の設定の変更が可能です。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電話帳の検索が可能です。このユーザはオーディオ音量の調整やメニュー言語の変更など、いくつかの設定を変更できます。
- ・ AUDIT：このロールを持つユーザは、セキュリティ監査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。



フル アクセス権がある管理者ユーザ アカウント（デフォルトの *admin* ユーザなど）は、3 つの役割をすべて所有している必要があります。

移動先：[Configuration] > [User Administration]

User Administration

User	Roles	Status
admin	Admin, Audit, User	Active
user1	User	Active

Add new user...

デフォルトのユーザ アカウント

システムにはデフォルトのユーザ アカウントとして *admin* が登録されています。このユーザにはフル アクセス権があります。

ユーザ管理（続き）

新しいユーザ アカウントの作成

次の手順に従って、新しいユーザ アカウントを作成します。

1. [\[Add New User...\]](#) をクリックします。
2. Username、Password および PIN コード * の欄に入力し、該当するユーザ ロールのチェック ボックスにチェックを入れます。
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と PIN コ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したい場合以外は、Distinguished Name (DN) Subject フィールドには入力しないでください。
3. ユーザをアクティブにするには、[Status] を **Active** に設定します。
4. [\[Create User\]](#) をクリックして変更内容を保存します。
変更を加えずに終了するには、[\[Back\]](#) ボタンを使用します。

* パスワードは Web インターフェイスとコマンドライン インターフェイスで使用されます。

PIN コードは画面上のメニューで使用されます。

移動先 : [Configuration] > [User Administration]

User Administration

User	Roles
admin	Admin, Audit, User
user1	User

Add new user...

Add new user

← Back

Username

Roles ☒ Admin ☐ Audit ☒ User

Status ☐ Active ☒ Inactive

Client Certificate DN

☒ Require password change on next user sign in
☒ Require PIN change on next user sign in

Password

Repeat Password

PIN

Repeat PIN

Used if login-required has been enabled on telepresence device menu

Create User

ユーザ管理（続き）

ユーザ権限の変更

次の手順に従って、ユーザ権限を変更します。

1. 既存のユーザ名をクリックすると、[Editing user] ウィンドウが開きます。
2. 適切なユーザ ロールのチェック ボックスにチェックを入れ、次回サインインするときにユーザがパスワードと PIN コードを変更する必要があるかを指定し、HTTPS で証明書ログインを使用する場合は Distinguished Name (DN) Subject フィールドに入力します。
3. [\[Update User\]](#) をクリックして変更内容を保存します。
変更を加えずに終了するには、[\[Back\]](#) ボタンを使用します。

パスワードまたは PIN コードの変更

次の手順に従って、パスワードまたは PIN コードを変更します。

1. 既存のユーザ名をクリックすると、[Editing user] ウィンドウが開きます。
2. 新しいパスワードまたは PIN コードを適切な入力フィールドに入力します。
3. [\[Change Password\]](#) または [\[Change PIN\]](#) をクリックして変更内容を保存します。
変更を加えずに終了するには、[\[Back\]](#) ボタンを使用します。

移動先 : [Configuration] > [User Administration]

User Administration

User	Roles
admin	Admin
user1	User

Add new user...

Editing user: user1

Back

User Privileges

Roles

☐ Admin

☐ Audit

☒ User

Status

☒ Active

☐ Inactive

Client Certificate DN

☐ Require password change on next user sign in

☐ Require PIN change on next user sign in

Update User

Change Password

Password

Repeat Password

Change Password

Change PIN

PIN

Repeat PIN

Used if login-required has been enabled on telepresence device menu

Change PIN

ユーザ管理（続き）

ユーザ アカウントの非アクティブ化

次の手順に従って、ユーザ アカウントを非アクティブにします。



少なくとも ADMIN 権限を持つ 1 ユーザを必ず**アクティブ**にしておきます。

1. 既存のユーザ名をクリックすると、[Editing user] ウィンドウが開きます。
2. [Status] を **Inactive** に設定します。
3. [\[Update User\]](#) をクリックして変更内容を保存します。
変更を加えずに終了するには、[\[Back\]](#) ボタンを使用します。

ユーザ アカウントの削除

次の手順に従って、ユーザ アカウントを削除します。



少なくとも ADMIN 権限を持つ 1 ユーザを必ず残しておきます。

1. 既存のユーザ名をクリックすると、[Editing user] ウィンドウが開きます。
2. [\[Delete user...\]](#) をクリックし、プロンプトが表示されたら確定します。

移動先 : [Configuration] > [User Administration]

User Administration

User	Roles
admin	Admin Audit User
user1	User

Add new user...

Editing user: user1

Back

User Privileges

Roles

- ☐ Admin
- ☐ Audit
- ☒ User

Status

- ☒ Active
- ☐ Inactive

Client Certificate DN

Delete user

Delete user1...

サインイン バナーの追加

サインイン バナーとは、ユーザがサインインしたときに表示されるメッセージです。

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したときに表示されます。

移動先 : [Configuration] > [Sign In Banner]

Sign In Banner

The Sign In Banner will be displayed when signing in using SSH, telnet, web and RS-232.

The information you type here will be shown to all users when they sign in.

Save

サインイン バナーの追加

ユーザがサインインしたときに表示したいメッセージを入力し、[Save] をクリックしてバナーをアクティブ化します。

```
login as: admin
The information you type here will be shown to all users when they sign in.
Using keyboard-interactive authentication.
Password: █
```

CISCO Codec: MySystem

http://192.160.1.120

The information you type here will be shown to all users when they sign in.

Sign In

Username:

Password:

System name: MySystem Sign In

アプリケーション プログラミング インターフェイス

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、シスコ製品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。製品の API ガイドに詳しい説明があります。

XML ファイル

XML ファイルはコーデックの API の一部です。それらはコーデックに関する情報を階層構造で示します。

- *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。ステータス情報は通常、API から監視されます。
- *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、およびコマンドで使用されるすべての値領域の概要が含まれます。

API コマンド

コマンド (xCommand) と構成 (xConfiguration) はこの Web ページから実行できます。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。

移動先 : [Configuration] > [API]

API

XML API

The XML files below are a part of the codec's API, and can be used by external services to inspect the state and configuration of the codec. The files are protected using Basic Authentication, thus you may be prompted for a user name and password.

File Name	Description
/configuration.xml	Configuration settings
/status.xml	Endpoint status parameters
/command.xml	Available API commands
/valuespace.xml	Value spaces of the XML files

XML ファイルを開く

XML ファイルを開くにはファイル名をクリックします。

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 コマンドの実行

コマンドまたは連続するコマンドをテキスト領域に入力し、[\[Execute\]](#) をクリックしてコマンドを発行します。

ビデオ システムの証明書の管理

証明書の検証は、Transport Layer Security (TLS) 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、ビデオ システムからサーバまたはクライアントに有効な証明書を提示する必要がある場合があります。

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) によって発行される場合があります。

証明書は右の図に示すとおりに一覧表示されます*。これらは次のサービスに使用可能です。 HTTPS、 SIP および IEEE 802.1X。

システムには複数の証明書を保存できますが、各サービスにつき 1 つの証明書だけを同時に使用できます。

認証が失敗した場合、接続は確立されません。

移動先 : [Configuration] > [Security]

Security

Certificates

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

Add certificate...

Certificate

No file selected

Browse...

Private key (optional)

No file selected

Browse...

Password (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 password.
Optionally the private key file may be supplied separately.

Add certificate...

証明書の有効化と無効化

ボタンを使用して、各種のサービスに対して証明書をオンまたはオフに切替えます。

また、証明書の表示および証明書の削除には、それぞれ対応するボタンを使用します。

証明書の追加

1. [\[Add certificate...\]](#) をクリックして証明書ダイアログを開きます。
2. [\[Browse...\]](#) をクリックしてコンピュータ上の証明書および秘密キーを探します。
3. 必要な場合には [\[Password\]](#) に入力します。
4. 青い [\[Add certificate...\]](#) ボタンをクリックして、証明書をシステムに保存します。



次のファイルを取得するには、システム管理者に連絡します。

- ・ 証明書 (ファイル形式 : .PEM)
- ・ 秘密キー。証明書と同じファイルに含まれている可能性があります (ファイル形式 : .PEM 形式)。
- ・ パスワード (秘密キーが暗号化されている場合にのみ必要)

証明書と秘密キーは、ビデオ システムの同じファイル内に保存されます。

* 図に示している証明書および証明書発行者は一例です。お使いのシステムの証明書とは異なる場合があります。

信頼できる証明書のリストの管理

証明書の検証は、Transport Layer Security (TLS) 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にビデオ 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、信頼できる認証局 (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ためには、信頼できる CA のリストがビデオ システムに存在する必要があります。CA の証明書は右の図に示すとおりに一覧表示されます*。

リストには HTTPS、SIP および IEEE 802.1X 接続の証明書を検証する CA を含める必要があります。

サーバを認証できない場合、接続は確立されません。

移動先 : [Configuration] > [Security]

Security

Certificates

Certificate Authorities

Certificate	Issuer	
CA_Certificate_1	Issuer_1	Delete... View Certificate

CA file [Browse...](#)

This system supports PEM formatted (pem) CA-files with one or more certificates within the file.

[Add certificate authority...](#)

認証局リストのアップロード



CA 証明書を含む新しいファイル内のエントリが既存のリストに追加されます。したがって、以前に保存した証明書は削除されません。

- 既存の CA 証明書をリストするには、[\[Show CAs...\]](#) をクリックします。
- [\[Add Certificate Authority...\]](#) をクリックします。
- [\[Browse...\]](#) をクリックして、お使いのコンピュータで CA 証明書のリストを含むファイル (ファイル形式 : .PEM) を探します。
- 青い [\[Add certificate authority...\]](#) ボタンをクリックして、新しい CA 証明書をシステムに保存します。



CA 証明書リスト (ファイル形式 : .PEM) を取得するには、システム管理者に連絡します。

証明書の表示と削除

証明書の表示および証明書の削除には、それぞれ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。お使いのシステムの証明書とは異なる場合があります。

監査証明書の追加

監査ログには、ビデオ システム上のすべてのサインイン アクティビティと設定の変更が記録されます。

監査ログはデフォルトではディセーブルになっていますが、画面上のメニューまたは Web インターフェイスの [\[Security\]](#) > [\[Audit\]](#) > [\[Logging\]](#) > [\[Mode\]](#) 設定を使用してイネーブルにすることができます。

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。

監査サーバの証明書の署名を検証するためには、信頼できる監査認証局 (CA) のリストがビデオ システムに存在する必要があります。

監査サーバを認証できない場合、ログは送信されません。



セキュア監査ログをイネーブルにする前に、常に監査証明書のリストをアップロードしてください。

移動先 : [\[Configuration\]](#) > [\[Security / Configuration\]](#) > [\[System Configuration\]](#)

1. 監査サーバの証明書リストのアップロード



CA 証明書を含む新しいファイル内のエントリは既存のリストに上書きされます。したがって、新しいファイルを追加すると以前に保存した監査証明書は失われます。

- [\[Add audit server certificate authority...\]](#) をクリックします。
- [\[Browse...\]](#) をクリックして、お使いのコンピュータで監査 CA 証明書のリストを含むファイル (PEM 形式) を探します。
- [\[Add audit certificate\]](#) をクリックして、証明書をシステムに保存します。



監査 CA 証明書リスト (ファイル形式 : .PEM) を取得するには、システム管理者に連絡します。

2. セキュア監査ログのイネーブル化

- [\[System Configuration\]](#) ページに移動し、[\[Security\]](#) カテゴリを選択します。
- 監査サーバの [アドレス](#) と [ポート](#) 番号を入力します。[\[Save\]](#) をクリックして変更を有効にします。
- [\[Logging Mode\]](#) ドロップダウン リストから [\[ExternalSecure\]](#) を選択します。[\[Save\]](#) をクリックして変更を有効にします。

強力なセキュリティ モードの設定

強力なセキュリティ モードは、DoD JITC への準拠が必要な場合にのみ使用する必要があります。



強力なセキュリティ モードを設定する前に、警告をよく確認してください。

強力なセキュリティ モードでは非常に厳格なパスワード要件が設定され、すべてのユーザが次のサインイン時にパスワードを変更することを要求します。

TMS からのソフトウェアのアップロード、Web スナップショット、および Web インターフェイスからの発信は、強力なセキュリティ モードでは禁止されます。

移動先 : [Configuration] > [Security]

強力なセキュリティ モードの設定

1. [\[Configure strong security mode...\]](#) をクリックして、警告をよく確認してから続行してください。
2. 強力なセキュリティ モードを使用する場合は、[\[I understand the risks of strong security mode\]](#) チェックボックスにチェックを入れ、[\[Enable strong security mode\]](#) をクリックします。
3. 警告に示されている厳格な要件を満たすようにパスワードを変更してください。システム パスワードの変更方法については、▶ [「パスワードの設定」](#) の項を参照してください。
4. コーデックを再起動して変更を有効にします。

Security

Strong security mode

WARNING

You are now about to enter strong security mode, required to adhere to DoD JITC regulations.

This will introduce the following:

- All users must change their password/PIN on the next sign in (including admin)
- New passwords 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 passwords used
 - Not more than 2 characters from the previous password can be in the same position
- Passwords must be changed at least every 30 days
- Passwords cannot be changed more than once per 24 hours
- 3 failed sign ins will lock the user account until an administrator re-activates the account
- Software upload from TMS will not be possible
- Web snapshots will not be available

☒ I understand the risks of strong security mode

[Enable strong security mode](#)

certificate au...

Strong security mode

This will disable strong security mode.

[Disable strong security mode](#)

通常モードに戻る

1. 強力なセキュリティ モードで [\[Configure strong security mode...\]](#) をクリックした後に [\[Disable strong security mode\]](#) をクリックすると、システムを通常のモードに復帰することができます。
2. コーデックを再起動して変更を有効にします。

信頼リストの削除（CUCM のみ）

[Security] ページに表示される Cisco Unified Communications Manager（CUCM）および Certification Authority Proxy Function（CAPF）の情報は、CUCM に登録されているビデオ システムの場合のみ適用されます。

Web インターフェイスを使用して、ビデオ システムに保存された既存の証明書信頼リスト（CTL）を削除できます。通常、古い CTL ファイルは削除しませんが、いくつかの場合に削除する必要があります。

CUCM、CAPF および信頼リストに関する詳細情報は、シスコの Web サイトにある『*Administering TC Endpoints on CUCM*』ガイドをお読みください。

移動先 : [Configuration] > [Security]

Security

Certificates

Cisco Unified Communications Manager (CUCM) - Certification Authority Proxy Function (CAPF) Information

CUCM status	CUCM is enabled.
CTL status	CTL is installed.
ITL status	ITL is not installed.
LSC status	Certificates are not installed.
Operation status	No pending operations...

Delete CTL/ITL

トラブルシューティング

[Troubleshooting] 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表示されます。リストは製品およびインストールによって異なる場合があります。^{*}

エラーは赤、警告は黄色で明確に示されていることに注意してください。

移動先 : [Diagnostics] > [Troubleshooting]

診断の実行

[\[Re-run diagnostics\]](#) をクリックして、リスト内の情報を最新の状態にします。

Troubleshooting

Re-run diagnostics

Diagnostics check of the most common system misconfigurations that may cause the TelePresence device to underperform or not work as expected.

CRITICAL: Valid Admin Password

No admin password set. Please secure the system with an admin password.

WARNING: Do not disturb mode

Do not disturb is turned on. Until this is **turned off**, the system cannot accept calls.

OK: H323 Gateway Status

H323 is configured correctly and is registered to the gatekeeper.

OK: System Name

The device has a system name set.

OK: System Temperature

Not Applicable: H320 Gateway Status

Not Applicable: ISDN Link compatibility

^{*} 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

ログ ファイル^{*} は、技術サポートが必要な場合にシスコのサポート組織によって要求される可能性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。

すべての Current log ファイルは、システムを再起動するたびにタイムスタンプ付きの Historical log ファイルにアーカイブされます。Historical log ファイルの最大数に到達すると、最も古いファイルが上書きされます。

移動先 : [Diagnostics] > [Log Files]

すべてのファイルのダウンロード

[\[Download log files archive\]](#) をクリックして、手順に従います。

ログ ファイルを開く

ログ ファイルを Web ブラウザで開くには、ファイル名をクリックします。

Log Files

[Download log files archive](#)

Current logs

File Name ▼	Size	Last Modified
arm0-system.log	10 KB	2013-03-17 11:43
arm1-system.log	11 KB	2013-03-17 11:43
arm2-system.log	11 KB	2013-03-17 11:43
console	2 KB	2013-03-17 11:53
dmesg	15 KB	2013-03-17 11:41
eventlog/all.log	35 KB	2013-03-25 14:34

Historical logs

File Name ▼	Size	Last Modified
log.0.tar.gz	55 KB	2013-01-29 22:41
log.1.tar.gz	100 KB	2013-02-14 22:15
log.2.tar.gz	62 KB	2013-02-17 14:07
log.3.tar.gz	57 KB	2013-02-26 15:58
log.4.tar.gz	54 KB	2013-03-11 22:16
log.5.tar.gz	91 KB	2013-03-16 09:23
log.6.tar.gz	53 KB	2013-01-17 12:37
log.7.tar.gz	53 KB	2013-01-17 12:41
log.8.tar.gz	66 KB	2013-01-23 22:15
log.9.tar.gz	54 KB	2013-01-24 22:30
log.tar.gz	91 KB	2013-03-16 09:23

^{*} 図に示しているログ ファイルは一例です。お使いのシステムには他のファイルがある場合があります。

システム ソフトウェアのアップグレード

このビデオ会議システムは TC ソフトウェアを使用しています。このドキュメントで説明するバージョンは TC6.1 です。



ソフトウェアのバージョンに関する質問はシステム管理者に問い合わせてください。

ソフトウェア リリース ノート

新情報および変更のすべての概要については、ソフトウェア リリース ノート (TC6) を読むことを推奨します。

▶ http://www.cisco.com/en/US/products/ps11424/tsd_products_support_series_home.html を参照してください。

新しいソフトウェア

ソフトウェアのダウンロードについては、Cisco Download Software Web ページ ▶ <http://www.cisco.com/cisco/software/navigator.html> を参照してください。そして、お使いの製品に移動します。

ファイル名は「s52000tc6_1_0.pkg」のようになります (ソフトウェア バージョンごとに固有のファイル名が付けられます)。

リリース キーとオプション キー

TC ソフトウェアを使用するには有効なリリース キーが必要です。バージョン TC6.1 以降は、どの TC リリース キーにも対応しています。

それより前のリリースでは、リリース キーはメイン リリース (TC4、TC5、TC6) ごとに固有です。ソフトウェアを TC6.0 かそれ以前のバージョンにダウングレードしたい場合は、正しいキーを使用するように注意してください。

オプション キーはオプション機能をアクティブ化するのに必要です。システムには複数のオプション キーがある場合があります。

次のオプションを使用できます。

- 高品位解像度
- 高解像度
- デュアル ディスプレイ

移動先 : [Maintenance] > [Software Upgrade]

Software Upgrade

Software package No file selected

Browse...

Upload

Current software version is TC6.1.0

☐ Upgrade automatically after upload

Release key

Add

The system has valid release keys for TC5, TC6 and TC6.1+

Option key

Add

About Release and Options Keys

Any valid release key may be used to upgrade to a newer version.

Successful downgrade to TC6.0 or lower will require a valid release key for the specific version you are going to downgrade to.

Contact your Cisco representative to obtain the required release key and information about available option keys. You need to provide the serial number to get release and option keys. The serial number for this TelePresence device is ...

リリース キーとオプション キーの追加

すでに有効なリリース キーと適切なオプション キーがシステムにインストールされている場合は、この項目をスキップしてソフトウェア インストールを続行できます。

必要なキーがない場合は、シスコの営業担当者に連絡し、それらを取得してください。さらに、次の作業を行います。

- リリース キーを適切なテキスト入力フィールドに入力し、[\[Add\]](#) をクリックします。
- オプション キーを適切なテキスト入力フィールドに入力し、[\[Add\]](#) をクリックします。

オプション キーが複数ある場合は、すべてのキーについてステップ ii を繰り返します。



各システムは固有のキーを持ちます。例：

- 1TC006-1-0C22E348 (リリース キー)
- 1R000-1-AA7A4A09 (オプション キー)

新しいソフトウェアのインストール

Cisco Download Software Web ページ (左のリンク参照) から適切なソフトウェア パッケージをダウンロードして、ローカル コンピュータに格納します。これは .pkg ファイルです。

- [\[Browse...\]](#) をクリックして、新しいソフトウェアを含むダウンロードされた .pkg ファイルを探します。
- [\[Upgrade automatically after upload\]](#) チェックボックスにチェックを入れて [\[Upload\]](#) をクリックすると、インストール プロセスがすぐに開始されます。

ソフトウェアをすぐにアップロードし、後でインストールを行う場合は、チェックボックスをオフにしたままにします。

インストールの完了には最長で 30 分ほどかかる場合があります。Web ページから進捗状況を確認できます。システムはインストール後に自動的にリポートします。



リポート後に 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。

バックアップと復元

[System configuration] ページで使用可能なすべてのシステム設定は、画面上に一覧表示するか、テキスト ファイル (.tsh) として保存できます。

.tsh ファイルをシステムに再度ロードして古い設定を復元することができます。

移動先 : [Maintenance] > [Backup and Restore]

現在の設定のバックアップまたは表示

現在の設定を画面上に表示するには、[\[Preview backup\]](#) をクリックします。

設定をテキスト ファイル (.tsh) として保存するには、[\[Take backup\]](#) をクリックします。

Backup and Restore

Take backup of configuration

This will create a backup file of the configurations on the TelePresence system. The backup file can be used to restore the TelePresence system to a previous state.

[Take backup](#)
[Preview backup](#)

Restore configuration from backup

Restore the TelePresence system from a backup file. Some configurations may require a reboot to take effect.

[Browse...](#)
[Restore](#)

以前の設定の復元

[\[Browse...\]](#) をクリックし、復元したい設定を含むファイル (.tsh) を探します。

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、[\[Restore\]](#) をクリックします。

工場出荷時設定へのリセット

工場出荷時設定にリセットするとコール ログは削除され、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。リリース キーやオプション キーは維持されます。



工場出荷時設定にリセットすると元に戻すことはできません。

工場出荷時設定へのリセットに関する詳細情報は、付録の ▶ 「[工場出荷時設定へのリセット](#)」 に記述してあります。

移動先 : [Maintenance] > [Factory Reset]

Factory Reset

This will reset the TelePresence device to factory default settings, followed by an automatic reboot of the TelePresence device.

- The call logs will be deleted.
- All system parameters will be reset to default values.
- All files that have been uploaded to the TelePresence device will be deleted. This includes, but are not limited to, custom backgrounds, ring tones, certificates, and the local phonebook.
- Release keys and option keys will **not** be affected.

Backup logs and configurations

A factory reset deletes all logs and system configurations. Please consider taking a backup of logs and the system's configuration.

[Download Logs](#)
[Download Configuration Backup](#)

Warning

A factory reset cannot be undone.

[Perform a factory reset...](#)


出荷時の状態にリセットする前にシステムのログファイルおよび設定をバックアップすることをお勧めします。そうしないと、データが失われます。

[\[Download Logs\]](#) と [\[Download configuration backup\]](#) ボタンをクリックし、手順に従ってファイルをコンピュータに保存します。

工場出荷時設定へのリセット

1. [\[Perform a factory reset...\]](#) をクリックして工場出荷時設の状態にリセットする前に、提供された情報をよく確認してください。
2. [\[Reset\]](#) をクリックして選択を確定するか、[\[Cancel\]](#) をクリックして操作を取り止めます。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。

システムの再起動

システムは、Web インターフェイスを使用して、リモートでシャットダウンまたは再起動が可能です。

移動先 : [Maintenance] > [Restart]

システムの再起動

[\[Restart TelePresence device...\]](#) をクリックして、システムを再起動します。



システムが使用可能になるまでに、数分かかります。

Restart

- Restarting the TelePresence device will make it unavailable for several minutes.
- Shutting down the TelePresence device will require physical presence to turn it on again.

[Restart TelePresence device...](#)

[Shutdown TelePresence device...](#)

システムのシャットダウン

[\[Shutdown TelePresence device...\]](#) をクリックしてシステムをシャットダウンします。



システムはリモートで再びオンにすることはできません。電源ボタンを物理的に押して、電源をオンにします。

3 章

システム設定

システム設定の概要

続くページに、Web インターフェイスの [\[System Configuration\]](#) ページで設定されるシステム設定の完全なリストを示します。例では、デフォルト値または値の例のいずれかを示します。

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。



リモート コントロールまたは画面上のメニューを使用して [\[Home\]](#) > [\[Settings\]](#) > [\[System Information\]](#) に移動するか、タッチ コントローラで [\[Settings \(✕\)\]](#) > [\[System Information\]](#) をタップして、システムの IP アドレス (IPv4 または IPv6) を探します。

オーディオ設定	51	Conference [1..1] Multipoint Mode	58
Audio Microphones Mute Enabled	51	Conference [1..1] PacketLossResilience Mode	58
Audio SoundsAndAlerts KeyTones Mode	51	Conference [1..1] Presentation OnPlacedOnHold	58
Audio SoundsAndAlerts RingTone	51	Conference [1..1] Presentation Policy	58
Audio SoundsAndAlerts RingVolume	51	Conference [1..1] Presentation RelayQuality	58
Audio Volume	51	Conference [1..1] VideoBandwidth MainChannel Weight	57
		Conference [1..1] VideoBandwidth Mode	57
		Conference [1..1] VideoBandwidth PresentationChannel Weight	58
カメラの設定	52	FacilityService 設定	60
Cameras Camera [1..1] Backlight	52	FacilityService Service [1..5] CallType	60
Cameras Camera [1..1] Brightness Level	52	FacilityService Service [1..5] Name	60
Cameras Camera [1..1] Brightness Mode	52	FacilityService Service [1..5] Number	60
Cameras Camera [1..1] DHCP	54	FacilityService Service [1..5] Type	60
Cameras Camera [1..1] Flip	52		
Cameras Camera [1..1] Focus Mode	52	H323 設定	61
Cameras Camera [1..1] Gamma Level	53	H323 NAT Address	61
Cameras Camera [1..1] Gamma Mode	53	H323 NAT Mode	61
Cameras Camera [1..1] IrSensor	53	H323 Profile [1..1] Authentication LoginName	61
Cameras Camera [1..1] Mirror	53	H323 Profile [1..1] Authentication Mode	61
Cameras Camera [1..1] Whitebalance Level	53	H323 Profile [1..1] Authentication Password	62
Cameras Camera [1..1] Whitebalance Mode	53	H323 Profile [1..1] CallSetup Mode	62
Cameras PowerLine Frequency	52	H323 Profile [1..1] Gatekeeper Address	62
		H323 Profile [1..1] Gatekeeper Discovery	62
会議設定	55	H323 Profile [1..1] H323Alias E164	62
Conference [1..1] AutoAnswer Delay	55	H323 Profile [1..1] H323Alias ID	62
Conference [1..1] AutoAnswer Mode	55	H323 Profile [1..1] PortAllocation	63
Conference [1..1] AutoAnswer Mute	55		
Conference [1..1] DefaultCall Protocol	56	ネットワーク設定	64
Conference [1..1] DefaultCall Rate	56	Network [1..1] Assignment	64
Conference [1..1] DoNotDisturb DefaultTimeout	56	Network [1..1] DHCP RequestTFTPServerAddress	65
Conference [1..1] DoNotDisturb Mode	55	Network [1..1] DNS Domain Name	66
Conference [1..1] Encryption Mode	56	Network [1..1] DNS Server [1..3] Address	66
Conference [1..1] FarEndControl Mode	56	Network [1..1] IEEE8021X AnonymousIdentity	68
Conference [1..1] FarEndControl SignalCapability	56	Network [1..1] IEEE8021X Eap Md5	68
Conference [1..1] IncomingMultisiteCall Mode	59	Network [1..1] IEEE8021X Eap Peap	69
Conference [1..1] MaxReceiveCallRate	57	Network [1..1] IEEE8021X Eap Tls	69
Conference [1..1] MaxTotalReceiveCallRate	57	Network [1..1] IEEE8021X Eap Ttls	69
Conference [1..1] MaxTransmitCallRate	57	Network [1..1] IEEE8021X Identity	68
Conference [1..1] MicUnmuteOnDisconnect Mode	55	Network [1..1] IEEE8021X Mode	68

Network [1..1] IEEE8021X Password.....	68	NetworkServices SIP Mode.....	73	SerialPort 設定	82
Network [1..1] IEEE8021X TlsVerify.....	68	NetworkServices SNMP CommunityName.....	73	SerialPort BaudRate.....	82
Network [1..1] IEEE8021X UseClientCertificate.....	68	NetworkServices SNMP Host [1..3] Address.....	73	SerialPort LoginRequired.....	82
Network [1..1] IPStack.....	64	NetworkServices SNMP Mode.....	73	SerialPort Mode.....	82
Network [1..1] IPv4 Address.....	64	NetworkServices SNMP SystemContact.....	74	SIP 設定	83
Network [1..1] IPv4 Gateway.....	64	NetworkServices SNMP SystemLocation.....	74	SIP ListenPort.....	85
Network [1..1] IPv4 SubnetMask.....	64	NetworkServices SSH AllowPublicKey.....	74	SIP Profile [1..1] Authentication [1..1] LoginName.....	83
Network [1..1] IPv6 Address.....	65	NetworkServices SSH Mode.....	74	SIP Profile [1..1] Authentication [1..1] Password.....	83
Network [1..1] IPv6 Assignment.....	65	NetworkServices Telnet Mode.....	74	SIP Profile [1..1] DefaultTransport.....	83
Network [1..1] IPv6 DHCPOptions.....	65	NetworkServices XMLAPI Mode.....	71	SIP Profile [1..1] DisplayName.....	83
Network [1..1] IPv6 Gateway.....	65	電話帳の設定	76	SIP Profile [1..1] Line.....	85
Network [1..1] MTU.....	69	Phonebook Server [1..1] ID.....	76	SIP Profile [1..1] Mailbox.....	84
Network [1..1] QoS Diffserv Audio.....	66	Phonebook Server [1..1] Type.....	76	SIP Profile [1..1] Outbound.....	84
Network [1..1] QoS Diffserv Data.....	67	Phonebook Server [1..1] URL.....	76	SIP Profile [1..1] Proxy [1..4] Address.....	84
Network [1..1] QoS Diffserv ICMPv6.....	67	プロビジョニング設定	77	SIP Profile [1..1] Proxy [1..4] Discovery.....	84
Network [1..1] QoS Diffserv NTP.....	67	Provisioning Connectivity.....	77	SIP Profile [1..1] TlsVerify.....	83
Network [1..1] QoS Diffserv Signalling.....	67	Provisioning ExternalManager Address.....	78	SIP Profile [1..1] Type.....	84
Network [1..1] QoS Diffserv Video.....	66	Provisioning ExternalManager Domain.....	78	SIP Profile [1..1] URI.....	83
Network [1..1] QoS Mode.....	66	Provisioning ExternalManager Path.....	78	スタンバイの設定	86
Network [1..1] RemoteAccess Allow.....	70	Provisioning ExternalManager Protocol.....	78	Standby BootAction.....	86
Network [1..1] Speed.....	69	Provisioning HttpMethod.....	77	Standby Control.....	86
Network [1..1] TrafficControl Mode.....	69	Provisioning LoginName.....	77	Standby Delay.....	86
Network [1..1] VLAN Voice Mode.....	70	Provisioning Password.....	77	Standby StandbyAction.....	86
Network [1..1] VLAN Voice VlanId.....	70	プロビジョニング モード (Provisioning Mode).....	77	Standby WakeupAction.....	86
NetworkServices 設定	71	RTP 設定	79	SystemUnit 設定	87
NetworkServices CTMS Encryption.....	75	RTP Ports Range Start.....	79	SystemUnit CallLogging Mode.....	87
NetworkServices CTMS Mode.....	74	RTP Ports Range Stop.....	79	SystemUnit ContactInfo Type.....	87
NetworkServices H323 Mode.....	71	セキュリティ設定	80	SystemUnit IrSensor.....	88
NetworkServices HTTP Mode.....	71	Security Audit Logging Mode.....	80	SystemUnit MenuLanguage.....	87
NetworkServices HTTPS Mode.....	72	Security Audit OnError Action.....	80	SystemUnit Name.....	87
NetworkServices HTTPS OCSP Mode.....	72	Security Audit Server Address.....	80	Time Settings	89
NetworkServices HTTPS OCSP URL.....	72	Security Audit Server Port.....	80	Time DateFormat.....	89
NetworkServices HTTPS VerifyClientCertificate.....	72	Security Session InactivityTimeout.....	81	Time TimeFormat.....	89
NetworkServices HTTPS VerifyServerCertificate.....	72	Security Session ShowLastLogon.....	81	タイムゾーン (Time Zone).....	89
NetworkServices MultiWay Address.....	71	UserInterface 設定	90	UserInterface TouchPanel DefaultPanel.....	90
NetworkServices MultiWay Protocol.....	71				
NetworkServices NTP Address.....	73				
NetworkServices NTP Mode.....	73				

ビデオ設定	91				
Video AllowWebSnapshots.....	101	Video Layout RemoteLayoutFamily	98	Video Output HDMI [1,2] MonitorRole.....	101
Video CamCtrlPip CallSetup Duration.....	96	Video Layout ScaleToFrame	94	Video Output HDMI [1,2] OverscanLevel	102
Video CamCtrlPip CallSetup Mode.....	96	Video Layout ScaleToFrameThreshold	94	Video Output HDMI [1,2] Resolution	102
Video DefaultPresentationSource.....	93	Video Layout Scaling	94	Video Output HDMI [1,2] RGBQuantizationRange	101
Video Input DVI [2] RGBQuantizationRange	94	Video MainVideoSource	93	Video PIP ActiveSpeaker DefaultValue Position	97
Video Input DVI [2] Type	94	Video Monitors	98	Video PIP Presentation DefaultValue Position.....	97
Video Input HDMI [1..1] RGBQuantizationRange	93	Video OSD AutoSelectPresentationSource	99	Video Selfview.....	95
Video Input Source [1..2] CameraControl Camerald.....	92	Video OSD EncryptionIndicator.....	99	Video SelfviewController AutoResizing.....	95
Video Input Source [1..2] CameraControl Mode.....	92	Video OSD InputMethod Cyrillic	100	Video SelfviewDefault FullscreenMode.....	96
Video Input Source [1..2] Name	91	Video OSD InputMethod InputLanguage	100	Video SelfviewDefault Mode.....	95
Video Input Source [1..2] OptimalDefinition Profile.....	92	Video OSD LoginRequired	100	Video SelfviewDefault OnMonitorRole	96
Video Input Source [1..2] OptimalDefinition Threshold60fps	93	Video OSD MenuStartupMode	98	Video SelfviewDefault PIPPosition	96
Video Input Source [1..2] PresentationSelection	91	Video OSD MissedCallsNotification	99	Video SelfviewPosition	95
Video Input Source [1..2] Quality	93	Video OSD Mode.....	98	Video Wallpaper	102
Video Input Source [1..2] Type.....	91	Video OSD MyContactsExpanded	100		
Video Input Source [1] Connector	91	Video OSD Output.....	100	試験の設定	103
Video Input Source [2] Connector	91	Video OSD TodaysBookings	99		
Video Layout LocalLayoutFamily.....	97	Video OSD VirtualKeyboard	99		
		Video Output HDMI [1,2] CEC Mode	101		

オーディオ設定

Audio Microphones Mute Enabled

音声ミュートが許可されるかどうかを決定します。デフォルトの値は True です。

必要なユーザ ロール：ADMIN

値スペース：<True/InCallOnly>

True：音声ミュートが使用可能になります。

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

例：Audio Microphones Mute Enabled: True

Audio SoundsAndAlerts KeyTones Mode

リモコンのキーを押したとき、またはタッチ コントローラでテキストや番号を入力したときにキーボード タッチ音（キー トーン）を出すようにシステムを設定できます。

必要なユーザ ロール：USER

値スペース：<Off/On>

Off：入力時にキー トーンが再生されません。

On：キーを押すかテキストを入力したときにキー トーンが聞こえます。

例：Audio SoundsAndAlerts KeyTones Mode: Off

Audio SoundsAndAlerts RingTone

着信コールの呼び出し音を選択します。

必要なユーザ ロール：USER

値スペース：<Marbles/IceCrystals/Polaris/Alert/Discreet/Fantasy/Jazz/Nordic/Echo/Rhythmic>

範囲：呼出音のトーンをリストから選択します。

例：Audio SoundsAndAlerts RingTone: Jazz

Audio SoundsAndAlerts RingVolume

着信コールの呼出音の音量を設定します。

必要なユーザ ロール：USER

値スペース：<0..100>

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

例：Audio SoundsAndAlerts RingVolume: 50

Audio Volume

スピーカーの音量を調整します。

必要なユーザ ロール：USER

値スペース：<0..100>

範囲：値は 0 ～ 100 である必要があります。1 ～ 100 の値は -34.5 dB ～ 15 dB (0.5 dB 刻み) の範囲に対応します。値 0 は、音声が入っていないことを意味します。

例：Audio Volume: 70

カメラの設定

Cameras PowerLine Frequency

電線周波数ちつき防止をサポートするカメラ、つまり PrecisionHD 1080p のカメラに適用されます。

必要なユーザ ロール：ADMIN

値スペース：<50Hz/60Hz>

50Hz：50 Hz に設定。

60Hz：60 Hz に設定。

例：Cameras PowerLine Frequency: 50Hz

Cameras Camera [1..1] Backlight

この設定は、逆光補正をオンまたはオフにします。逆光補正は、部屋の中で人物の背後に強い光がある場合に役立ちます。逆光補正がないと、こちらの画像が相手に非常に暗い状態で見えてしまいます。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：カメラの逆光補正をオフにします。

On：カメラの逆光補正をオンにします。

例：Cameras Camera 1 Backlight: Off

Cameras Camera [1..1] Brightness Mode

カメラの明るさモードを設定します。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Manual>

Auto：カメラの明るさはシステムによって自動的に設定されます。

Manual：カメラの明るさの手動設定をイネーブルにします。明るさのレベルは Cameras Camera Brightness Level 設定を使用して設定されます。

例：Cameras Camera 1 Brightness Mode: Auto

Cameras Camera [1..1] Brightness Level

明るさレベルを設定します。注：カメラの明るさモードを Manual に設定する必要があります。

必要なユーザ ロール：ADMIN

値スペース：<1..31>

範囲：1 ～ 31 の値を選択します。

例：Cameras Camera 1 Brightness Level: 1

Cameras Camera [1..1] Flip

フリップ モード（垂直フリップ）を使用すると、画像を上下反転できます。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Off/On>

Auto：カメラの上下が逆に置かれると、画像は自動的に上下反転します。この設定は、マウント方向を自動的に検出するカメラだけに有効です。

Off：ビデオを通常の方法で画面に表示します。

On：イネーブルにすると画面のビデオが反転します。この設定は、カメラが上下逆にマウントされたが、マウント方向を自動的に検出できない場合に使用されます。

例：Cameras Camera 1 Flip: Off

Cameras Camera [1..1] Focus Mode

カメラの焦点モードを設定します。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Manual>

Auto：コールが接続されると、カメラはオートフォーカスになります。カメラの移動（パン、チルト、ズーム）後も同様です。システムは、オートフォーカスを数秒間だけ使用して正しい焦点に設定します。その後、オートフォーカスはカメラが焦点調整し続けることを防ぐためオフになります。

Manual：オートフォーカスをオフにし、カメラの焦点を手動で調整します。

例：Cameras Camera 1 Focus Mode: Auto

Cameras Camera [1..1] Gamma Mode

ガンマ モードをサポートするカメラに適用されます。ガンマ モード設定により、ガンマ修正がイネーブルになります。ガンマは、画像ピクセルとモニタの明るさとの間の関係を表します。Cisco TelePresence の PrecisionHD 720p カメラはガンマ モードをサポートします。PrecisionHD 1080p カメラではガンマ モードはサポートされません。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Manual>

Auto：自動がデフォルトであり、推奨設定です。

Manual：厳しい光条件では、モードをマニュアルにスイッチして、ガンマ レベルの設定によって使用するガンマ テーブルを明示的に指定する場合があります。

例：Cameras Camera 1 Gamma Mode: Auto

Cameras Camera [1..1] Gamma Level

ガンマ レベルを設定して、使用するガンマ修正テーブルを選択できます。この設定は、明るさの設定を変更しても十分な結果が得られない困難な光条件に役立つことがあります。注：カメラのガンマ モードを Manual に設定する必要があります。

必要なユーザ ロール：ADMIN

値スペース：<0..7>

範囲：0 ～ 7 の値を選択します。

例：Cameras Camera 1 Gamma Level: 0

Cameras Camera [1..1] IrSensor

IR センサー LED はカメラの前面にあり、IR センサーがリモート コントローラからアクティブ化されたとき明滅します。コーデック C シリーズと PrecisionHD カメラの両方が IR センサーを持っており、そのうち同時に 1 つだけをイネーブルにする必要があります。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：カメラの IR センサーをディセーブルにします。

On：カメラの IR センサーをイネーブルにします。

例：Cameras Camera 1 IrSensor: On

Cameras Camera [1..1] Mirror

ミラー モード（水平反転）を使用して画面の画像を反転できます。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Off/On>

Auto：カメラの上下が逆に置かれると、画像は自動的に左右反転します。カメラを上下逆に取り付けることができ、上下逆に取り付けられたことを自動検出できるカメラにこの設定を使用します。

Off：セルフビューを通常モードで表示します。つまり、セルフビューは他の人から自分を見るような感覚になります。

On：セルフビューをミラー モードで表示します。つまり、セルフビューは反転され、セルフビューは鏡の中の自分を見るような感覚になります。

例：Cameras Camera 1 Mirror: Off

Cameras Camera [1..1] Whitebalance Mode

カメラのホワイトバランス モードを設定します。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Manual>

Auto：カメラはカメラのビューによって常にホワイトバランスを調整します。

Manual：カメラのホワイトバランスの手動設定をイネーブルにします。ホワイト バランスのレベルは Cameras Camera Whitebalance Level 設定を使用して設定します。

例：Cameras Camera 1 Whitebalance Mode: Auto

Cameras Camera [1..1] Whitebalance Level

ホワイトバランス レベルを設定します。注：カメラのホワイトバランス モードを Manual に設定する必要があります。

必要なユーザ ロール：ADMIN

値スペース：<1..16>

範囲：1 ～ 16 の値を選択します。

例：Cameras Camera 1 Whitebalance Level: 1

Cameras Camera [1..1] DHCP

DHCP をサポートするカメラ（例：Cisco TelePresence PrecisionHD 1080p 12X カメラ）に適用されます。カメラが LAN に接続されている必要があります。設定されている場合、このコマンドはデジタイズ チェーン接続されたカメラの SW アップグレードのサポートをイネーブルにします。これはカメラの DHCP 機能をイネーブルにし、MAC および IP アドレス検索を強制起動します。カメラを LAN 接続しなくなった場合、DHCP をリセットするようにしてください。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：カメラの DHCP をディセーブルにします。注：この設定は、カメラが LAN に接続されていないときに適用する必要があります。

On：カメラで DHCP をイネーブルにします。カメラは自動的に再起動されます。再起動後に DHCP が開始し、IP アドレスが取得されます。結果を知るにはコマンド「xStatus Camera」を実行します。

例：Cameras Camera 1 DHCP: Off

会議設定

Conference [1..1] AutoAnswer Mode

自動応答モードを設定します。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：着信コールは、リモート コントロールで OK キーまたはグリーンの Call キーを押すか、タッチ コントローラで Accept キーをタップすることによって手動応答する必要があります。

On：自動応答をイネーブルにして、システムを着信コールすべてに自動応答させます。

例：Conference 1 AutoAnswer Mode: Off

Conference [1..1] AutoAnswer Mute

着信コールが自動的に応答する場合にマイクロフォンをミュートするかどうか決定します。注：AutoAnswer モード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

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。

例：Conference 1 AutoAnswer Mute: Off

Conference [1..1] AutoAnswer Delay

システムによって自動的に応答される前に着信コールがどれくらい待つ必要があるかを定義します（秒単位）。注：AutoAnswer モード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

値スペース：<0..50>

範囲：0 ～ 50 秒の値を選択します。

例：Conference 1 AutoAnswer Delay: 0

Conference [1..1] MicUnmuteOnDisconnect Mode

すべてのコールが切断されたとき、マイクロフォンが自動的にミュート解除されるかどうかを決定します。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

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。

例：Conference 1 MicUnmuteOnDisconnect Mode: On

Conference [1..1] DoNotDisturb Mode

着信コールのアラートの必要があるかどうか決定します。

必要なユーザ ロール：USER

値スペース：<Off/On/Timed>

Off：着信コールは通常どおり機能します。

On：すべての着信コールは拒否され、不在履歴として登録されます。発信者はビジー信号を受信します。割り込み不可がオンになっていることを示すメッセージがタッチ コントローラまたはメイン ディスプレイに表示されます。サイレント モード中に受信されたコールは、不在履歴として表示されます。

Timed：API を使用してサイレント モードのオンとオフを切り替える場合にのみ、このオプションを選択します（xCommand Conference DoNotDisturb Activate と xCommand Conference DoNotDisturb Deactivate）。

例：Conference 1 DoNotDisturb Mode: Off

Conference [1..1] DoNotDisturb DefaultTimeout

この設定はサイレント セッションのデフォルト期間、つまり着信コールが拒否され、不在履歴として登録される時間を決定します。ユーザ インターフェイス（リモコンまたはタッチ コントローラ）または Conference DoNotDisturb Mode 設定を使用して、より早くセッションを終了することができます。デフォルト値は 60 分です。

必要なユーザ ロール：ADMIN

値スペース：<0..1440>

*範囲：*サイレント セッションが自動的にタイムアウトするまでの分数を 0 ~ 1440（24 時間）の間で選択します。

例：Conference 1 DoNotDisturb DefaultTimeout: 60

Conference [1..1] FarEndControl Mode

リモート側（遠端）にこちら側のビデオ ソースの選択とローカル カメラの制御（パン、チルト、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

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、チルト、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、チルト、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、こちら側では通常どおり可能です。

例：Conference 1 FarEndControl Mode: On

Conference [1..1] FarEndControl SignalCapability

遠端制御（H.224）信号機能モードを設定します。

必要なユーザ ロール：ADMIN

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。

例：Conference 1 FarEndControl SignalCapability: On

Conference [1..1] Encryption Mode

会議の暗号化モードを設定します。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。

必要なユーザ ロール：ADMIN

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。

例：Conference 1 Encryption Mode: BestEffort

Conference [1..1] DefaultCall Protocol

システムからコールを発信するときに使用されるデフォルトのコール プロトコルを設定します。

必要なユーザ ロール：ADMIN

値スペース：<H323/Sip/H320>

H.323：[H.323] を選択するとコールは H.323 コールとして設定されます。

Sip：[SIP] を選択するとコールは SIP コールとして設定されます。

H320：[H320] を選択するとコールは H.320 コールとして設定されます（Cisco TelePresence ISDN リンクゲートウェイに接続されている場合のみ）。

例：Conference 1 DefaultCall Protocol: H323

Conference [1..1] DefaultCall Rate

システムからコールを発信するときに使用されるデフォルトのコール レートを設定します。

必要なユーザ ロール：ADMIN

値スペース：<64..6000>

*範囲：*64 ~ 6000 kbps の値を選択します。

例：Conference 1 DefaultCall Rate: 768

Conference [1..1] MaxTransmitCallRate

コールを発信または受信するときに使用される最大送信ビット レートを指定します。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

値スペース：<64..6000>

*範囲：*64 ～ 6000 kbps の値を選択します。

例：Conference 1 MaxTransmitCallRate: 6000

Conference [1..1] MaxReceiveCallRate

コールを発信または受信するときに使用される最大受信ビット レートを指定します。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

値スペース：<64..6000>

*範囲：*64 ～ 6000 kbps の値を選択します。

例：Conference 1 MaxReceiveCallRate: 6000

Conference [1..1] MaxTotalTransmitCallRate

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

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

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

必要なユーザ ロール：ADMIN

値スペース：<64..10000>

*範囲：*64 ～ 10000 の値を選択します。

例：Conference 1 MaxTotalTransmitCallRate: 9000

Conference [1..1] MaxTotalReceiveCallRate

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

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

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

必要なユーザ ロール：ADMIN

値スペース：<64..10000>

*範囲：*64 ～ 10000 の値を選択します。

例：Conference 1 MaxTotalReceiveCallRate: 9000

Conference [1..1] VideoBandwidth Mode

会議のビデオ帯域幅モードを設定します。

必要なユーザ ロール：ADMIN

値スペース：<Dynamic/Static>

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

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

例：Conference 1 VideoBandwidth Mode: Dynamic

Conference [1..1] VideoBandwidth MainChannel Weight

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 チャネルおよびプレゼンテーション チャネルに配信されます。メイン チャネルの重みが 2 で、プレゼンテーション チャネルの重みが 1 の場合、メイン チャネルはプレゼンテーション チャネルの 2 倍の帯域幅を使用します。

必要なユーザ ロール：ADMIN

値スペース：<1..10>

*範囲：*1 ～ 10。

例：Conference 1 VideoBandwidth MainChannel Weight: 5

Conference [1..1] VideoBandwidth PresentationChannel Weight

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

値スペース：<1..10>

*範囲：*1 ～ 10。

例：Conference 1 VideoBandwidth PresentationChannel Weight: 5

Conference [1..1] PacketLossResilience Mode

パケットロス復元モードを設定します。この設定は、設定された後に開始されたコールにのみ適用されます。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

*Off：*パケットロス復元をディセーブルにします。

*On：*パケットロス復元をイネーブルにします。

例：Conference 1 PacketLossResilience Mode: On

Conference [1..1] Presentation Policy

プレゼンテーション サービスの実行方法を制御します。

必要なユーザ ロール：ADMIN

値スペース：<LocalRemote/LocalOnly>

*LocalRemote：*プレゼンテーションはローカルで表示され、リモート側に送信されます。

*LocalOnly：*プレゼンテーションはローカルにだけ表示されます。

例：Conference 1 Presentation Policy: LocalRemote

Conference [1..1] Presentation RelayQuality

このバージョンでは適用されません。

Conference [1..1] Presentation OnPlacedOnHold

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

必要なユーザ ロール：ADMIN

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。

例：Conference 1 Presentation OnPlacedOnHold: NoAction

Conference [1..1] Multipoint Mode

ビデオ システムがマルチパーティ ビデオ会議を処理する方法を定義します。

Cisco TelePresence Video Communication Server (VCS) に登録すると、ビデオ システムは MultiWay ネットワーク ソリューションを使用できます。MultiWay では、マルチポイント コントロール ユニット (MCU) がビデオ ネットワークに含まれていることが必要です。Cisco Unified Communications Manager (CUCM) に登録すると、ビデオ システムは CUCM 会議ブリッジを使用できます。Multiway および CUCM 会議ブリッジを使用すれば、多くの参加者との会議を設定できます。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Off/MultiWay/CUCMMediaResourceGroupList>

*Auto：*MultiWay サービスを使用できる場合、マルチ パーティ会議に MultiWay が使用されます。サービスが使用できない場合、マルチポイント モードは自動的に Off に設定されます。

*Off：*マルチパーティ会議は許可されません。

*MultiWay：*MultiWay を使用してマルチパーティ会議が設定されます。マルチポイント モードは、MultiWay サービスが使用できない場合、たとえばサーバ アドレスが NetworkServices MultiWay Address 設定に指定されていない場合、自動的に Off に設定されます。

*CUCMMediaResourceGroupList：*マルチパーティ会議 (アドホック会議) は CUCM で設定された会議ブリッジによってホストされます。この設定は、CUCM 環境で CUCM によりプロビジョニングされるものであり、ユーザが手動で設定すべきではありません。

例：Conference 1 Multipoint Mode: Auto

Conference [1..1] IncomingMultisiteCall Mode

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

必要なユーザ ロール：ADMIN

値スペース：<Allow/Deny>

Allow：すでに通話している間に、誰かが電話をかけてきた場合、通知されます。着信コールを受け入れるかどうかは任意です。進行中のコールは、着信コールに応答するときに保留になる場合があります。またはコールをマージすることができます（MultiSite または MultiWay のサポートが必要です）。

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

例：Conference 1 IncomingMultisiteCall Mode: Allow

FacilityService 設定

FacilityService Service [1..5] Type

最大 5 種類のファシリティ サービスを同時にサポートできます。この設定で、どのようなサービスかを選択できます。ファシリティ サービスは、FacilityService サービス名と FacilityService サービス番号の両方の設定が正しく設定されていないと使用できません。

タッチ コントローラでは、タイプが Helpdesk の FacilityService Service 1 だけを使用できます。ファシリティ サービスは、リモート コントロールと画面上のメニューを使用する場合には使用できません。

必要なユーザ ロール：ADMIN

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

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

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

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

Emergency：緊急サービスには、このオプションを選択します。

Security：セキュリティ サービスには、このオプションを選択します。

Catering：ケータリング サービスには、このオプションを選択します。

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

例：FacilityService Service 1 Type: Helpdesk

FacilityService Service [1..5] Name

各ファシリティ サービスの名前を設定します。最大 5 種類のファシリティ サービスがサポートされます。

ファシリティ サービスは、FacilityService サービス名と FacilityService サービス番号の両方の設定が正しく設定されていないと使用できません。

タッチ コントローラでは FacilityService Service 1 だけを使用でき、その名前がファシリティ サービス コール ボタンに使用されます。ファシリティ サービスは、リモート コントロールと画面上のメニューを使用する場合には使用できません。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 255>

フォーマット：最大 255 文字の文字列。

例：FacilityService Service 1 Name: ""

FacilityService Service [1..5] Number

各ファシリティ サービスの番号を設定します。最大 5 種類のファシリティ サービスがサポートされます。

ファシリティ サービスは、FacilityService サービス名と FacilityService サービス番号の両方の設定が正しく設定されていないと使用できません。

タッチ コントローラでは、FacilityService Service 1 だけを使用できます。ファシリティ サービスは、リモート コントロールと画面上のメニューを使用する場合には使用できません。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 255>

フォーマット：最大 255 文字の文字列。

例：FacilityService Service 1 Number: ""

FacilityService Service [1..5] CallType

各ファシリティ サービスにコール タイプを設定します。最大 5 種類のファシリティ サービスがサポートされます。

ファシリティ サービスは、FacilityService サービス名と FacilityService サービス番号の両方の設定が正しく設定されていないと使用できません。

タッチ コントローラでは、FacilityService Service 1 だけを使用できます。ファシリティ サービスは、リモート コントロールと画面上のメニューを使用する場合には使用できません。

必要なユーザ ロール：ADMIN

値スペース：<Video/Audio>

Video：ビデオ コールには、このオプションを選択します。

Audio：オーディオ コールには、このオプションを選択します。

例：FacilityService Service 1 CallType: Video

H323 設定

H323 NAT Mode

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

必要なユーザ ロール : ADMIN

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 メニューで「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。

例 : H323 NAT Mode: Off

H323 NAT Address

NAT サポートのルータに外部 / グローバル IP アドレスを入力します。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

* Port 5555-6555

* Port 2326-2487

必要なユーザ ロール : ADMIN

値スペース : <S: 0, 64>

フォーマット : 有効な IPv4 アドレスまたは IPv6 アドレス。

例 : H323 NAT Address: ""

H323 Profile [1..1] Authentication Mode

H.323 プロファイルの認証モードを設定します。

必要なユーザ ロール : ADMIN

値スペース : <Off/On>

Off : H.323 Gatekeeper Authentication Mode が Off に設定されている場合、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 : H.323 Gatekeeper Authentication Mode が On に設定され、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。注 : コーデックとゲートキーパーの両方で認証ログイン名と認証パスワードが定義されることが必要です。

例 : H323 Profile 1 Authentication Mode: Off

H323 Profile [1..1] Authentication LoginName

システムは、H.323 ゲートキーパーに認証ログイン名と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。注 : H.323 Gatekeeper Authentication Mode がイネーブルになっている必要があります。

必要なユーザ ロール : ADMIN

値スペース : <S: 0, 50>

フォーマット : 最大 50 文字の文字列。

例 : H323 Profile 1 Authentication LoginName: ""

H323 Profile [1..1] Authentication Password

システムは、H.323 ゲートキーパーに認証ログイン名と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。注：H.323 Gatekeeper Authentication Mode がイネーブルになっている必要があります。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 50>

フォーマット：最大 50 文字の文字列。

例：H323 Profile 1 Authentication Password: ""

H323 Profile [1..1] CallSetup Mode

H.323 コール コンフィギュレーション モードは、H.323 を確立するときにゲートキーパーまたはダイレクト コールを使用するかどうかを定義します。

注：ダイレクト H.323 コールは、H.323 コール コンフィギュレーション モードがゲートキーパーに設定されていても行うことができます。

必要なユーザ ロール：ADMIN

値スペース：<Direct/Gatekeeper>

Direct：H.323 コール発信のためダイヤリングするときに IP アドレスを使用する必要があります。

Gatekeeper：システムは、H.323 コールを発信するためにゲートキーパーを使用します。このオプションを選択する場合は H323 Profile Gatekeeper Address および H323 Profile Gatekeeper Discovery 設定も行う必要があります。

例：H323 Profile 1 CallSetup Mode: Gatekeeper

H323 Profile [1..1] Gatekeeper Discovery

システムが H.323 ゲートキーパーに登録する方法を決定します。

必要なユーザ ロール：ADMIN

値スペース：<Manual/Auto>

Manual：システムは、ゲートキーパーの IP アドレスで指定された特定のゲートキーパーを使用します。

Auto：システムは自動的に使用可能なゲートキーパーに登録しようとします。あるゲートキーパーが 30 秒以内にコーデックから送信された要求に応答すると、この特定のゲートキーパーが使用されます。これには、ゲートキーパーが自動検出モードにあることも必要です。ゲートキーパーが応答しなかった場合は、H.323 コールにゲートキーパーを使用しないため、IP アドレスを手動で指定する必要があります。

例：H323 Profile 1 Gatekeeper Discovery: Manual

H323 Profile [1..1] Gatekeeper Address

ゲートキーパーの IP アドレスを入力します。注：H.323 Call Setup Mode を Gatekeeper に設定し、Gatekeeper Discovery を Manual に設定する必要があります。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 255>

フォーマット：有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

例：H323 Profile 1 Gatekeeper Address: "192.0.2.0"

H323 Profile [1..1] H323Alias E164

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

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 30>

フォーマット：最大 30 文字のコンパクト文字列。使用できる文字は、0 ～ 9、*、# です。

例：H323 Profile 1 H323Alias E164: "90550092"

H323 Profile [1..1] H323Alias ID

H.323 ゲートキーパー 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 を指定します。例："firstname.lastname@company.com", "My H.323 Alias ID"

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 49>

フォーマット：最大 49 文字の文字列。

例：H323 Profile 1 H323Alias ID: "firstname.lastname@company.com"

H323 Profile [1..1] PortAllocation

H.323 ポート割り当ての設定は、H.323 コール シグナリングに使用する 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

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。RTP および RTCP メディア データの場合、システムは範囲 2326 ～ 2487 の UDP ポートを使用しています。各メディア チャネルは 2 つの隣接ポートを使用しています。つまり RTP と RTCP がそれぞれ 2330 と 2331 を使用しています。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。

例：H323 Profile 1 PortAllocation: Dynamic

ネットワーク設定

Network [1..1] IPStack

システムがサポートするインターネット プロトコルを選択します。

注：この設定の変更後、システムを再起動してください。

必要なユーザ ロール：ADMIN

値スペース：<IPv4/IPv6>

IPv4：SIP コールおよび H323 コールに IP バージョン 4 が使用されます。

IPv6：SIP コールおよび H323 コールに IP バージョン 6 が使用されます。

例：Network 1 IPStack: IPv4

Network [1..1] Assignment

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

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（スタティック 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。

例：Network 1 Assignment: DHCP

Network [1..1] IPv4 Address

システムのスタティック IPv4 ネットワーク アドレスを入力します。この設定は、Network 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

値スペース：<S: 0, 64>

フォーマット：有効な IPv4 アドレス。

例：Network 1 IPv4 Address: "192.0.2.0"

Network [1..1] IPv4 Gateway

IPv4 ネットワーク ゲートウェイを定義します。この設定は、Network 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

値スペース：<S: 0, 64>

フォーマット：有効な IPv4 アドレス。

例：Network 1 IPv4 Gateway: "192.0.2.0"

Network [1..1] IPv4 SubnetMask

IPv4 ネットワークのサブネット マスクを定義します。この設定は、Network 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

値スペース：<S: 0, 64>

形式：有効な IPv4 アドレス形式。

例：Network 1 IPv4 SubnetMask: "255.255.255.0"

Network [1..1] IPv6 Assignment

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

値スペース：<Static/DHCPv6/Autoconf>

Static：コードブ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。

例：Network 1 IPv6 Assignment: Autoconf

Network [1..1] IPv6 Address

システムのスタティック IPv6 ネットワーク アドレスを入力します。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

値スペース：<S: 0, 64>

フォーマット：有効な IPv6 アドレス。

例：Network 1 IPv6 Address: "ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff"

Network [1..1] IPv6 Gateway

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

値スペース：<S: 0, 64>

フォーマット：有効な IPv6 アドレス。

例：Network 1 IPv6 Gateway: "ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff"

Network [1..1] IPv6 DHCPOptions

一連の DHCP オプション（NTP アドレスや DNS サーバなど）を DHCPv6 サーバから取得します。

必要なユーザ ロール：ADMIN

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ディセーブルにします。

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。

例：Network 1 IPv6 DHCPOptions: On

Network [1..1] DHCP RequestTFTPServerAddress

この設定は、Cisco Unified Communications Manager (CUCM) に登録されたビデオ システムにのみ使用されます。

この設定は、TFTP サーバ（プロビジョニング サーバ）のアドレスを自動的に検出できるように、エンドポイントが DHCP サーバに DHCP オプション 150 を要求するかを決定します。

この設定が Off になっている場合、または DHCP サーバがオプション 150 をサポートしていない場合は、Provisioning ExternalManager Address 設定を使用して TFTP サーバ アドレスを手動で設定する必要があります。

注：Network VLAN Voice Mode 設定が Auto であり、Cisco Discovery Protocol (CDP) により ID が音声 VLAN に割り当てられている場合、オプション 150 のリクエストは必ず送信されます。つまり、Network DHCP RequestTFTPServerAddress の設定は無視されます。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：ビデオ システムは DHCP オプション 150 のリクエストを送信しません。TFTP サーバのアドレスを手動で設定する必要があります。この規則の例外については、上記の注を参照してください。

On：ビデオ システムは自動的に TFTP サーバのアドレスを検出できるように、オプション 150 のリクエストを DHCP に送信します。

例：Network 1 DHCP RequestTFTPServerAddress: Off

Network [1..1] DNS Domain Name

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

値スペース: <S: 0, 64>

フォーマット: 最大 64 文字の文字列。

例: Network 1 DNS Domain Name: ""

Network [1..1] DNS Server [1..3] Address

DNS サーバのネットワーク アドレスを定義します。最大で 3 つ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

値スペース: <S: 0, 64>

フォーマット: 有効な IPv4 アドレスまたは IPv6 アドレス。

例: Network 1 DNS Server 1 Address: ""

Network [1..1] QoS Mode

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

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。

例: Network 1 QoS Mode: Diffserv

Network [1..1] QoS Diffserv Audio

注: この設定は、Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内で音声パケットに持たせる優先順位を定義します。

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

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

必要なユーザ ロール: ADMIN

値スペース: <0..63>

範囲: 0 ～ 63 の値を選択します。数字が大きいほど、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。

例: Network 1 QoS Diffserv Audio: 0

Network [1..1] QoS Diffserv Video

注: この設定は、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 チャンネル (共有コンテンツ) 上のパケットも、ビデオ パケットのカテゴリに属します。

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

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

必要なユーザ ロール: ADMIN

値スペース: <0..63>

範囲: 0 ～ 63 の値を選択します。数字が大きいほど、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。

例: Network 1 QoS Diffserv Video: 0

Network [1..1] QoS Diffserv Data

注：この設定は、Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内でデータ パケットに持たせる優先順位を定義します。

パケットのプライオリティは、0 ～ 63 です。数字が大きいほど、優先順位が高くなります。Data 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

値スペース：<0..63>

範囲：0 ～ 63 の値を選択します。数字が大きいほど、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。

例：Network 1 QoS Diffserv Data: 0

Network [1..1] QoS Diffserv Signalling

注：この設定は、Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

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

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

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

必要なユーザ ロール：ADMIN

値スペース：<0..63>

範囲：0 ～ 63 の値を選択します。数字が大きいほど、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。

例：Network 1 QoS Diffserv Signalling: 0

Network [1..1] QoS Diffserv ICMPv6

注：この設定は、Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

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

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

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

必要なユーザ ロール：ADMIN

値スペース：<0..63>

範囲：0 ～ 63 の値を選択します。数字が大きいほど、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。

例：Network 1 QoS Diffserv ICMPv6: 0

Network [1..1] QoS Diffserv NTP

注：この設定は、Network QoS Mode が Diffserv に設定されている場合にのみ有効になります。

IP ネットワーク内で NTP パケットに持たせる優先順位を定義します。

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

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

必要なユーザ ロール：ADMIN

値スペース：<0..63>

範囲：0 ～ 63 の値を選択します。数字が大きいほど、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。

例：Network 1 QoS Diffserv NTP: 0

Network [1..1] IEEE8021X Mode

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

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。

例：Network 1 IEEE8021X Mode: Off

Network [1..1] IEEE8021X TlsVerify

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。

この設定は、Network [1..1] IEEE8021X Eap Tls がイネーブル（On）の場合にだけ有効です。

必要なユーザ ロール：ADMIN

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。

例：xConfiguration Network 1 IEEE8021X TlsVerify: Off

Network [1..1] IEEE8021X UseClientCertificate

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。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

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

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

例：Network 1 IEEE8021X UseClientCertificate: Off

Network [1..1] IEEE8021X Identity

802.1X ID は 802.1X 認証に必要なユーザ名です。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 64>

フォーマット：最大 64 文字の文字列。

例：Network 1 IEEE8021X Identity: ""

Network [1..1] IEEE8021X Password

802.1X パスワードは 802.1X 認証に必要なパスワードです。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 32>

フォーマット：最大 32 文字の文字列。

例：Network 1 IEEE8021X Password: ""

Network [1..1] IEEE8021X AnonymousIdentity

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

値スペース：<S: 0, 64>

フォーマット：最大 64 文字の文字列。

例：Network 1 IEEE8021X AnonymousIdentity: ""

Network [1..1] IEEE8021X Eap Md5

MD5（メッセージ ダイジェスト アルゴリズム 5）モードを設定します。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

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）。

例：Network 1 IEEE8021X Eap Md5: On

Network [1..1] IEEE8021X Eap Ttls

TTLS（トンネリングされたトランスポート層セキュリティ）モードを設定します。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

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）。

例：Network 1 IEEE8021X Eap Ttls: On

Network [1..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。RFC5216 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

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）。

例：Network 1 IEEE8021X Eap Tls: On

Network [1..1] IEEE8021X Eap Peap

Peap（保護拡張認証プロトコル）モードを設定します。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

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）。

例：Network 1 IEEE8021X Eap Peap: On

Network [1..1] MTU

イーサネット MTU（最大伝送単位）を設定します。

必要なユーザ ロール：ADMIN

値スペース：<576..1500>

範囲：576 ～ 1500 バイトの値を選択します。

例：Network 1 MTU: 1500

Network [1..1] Speed

イーサネット リンクの速度を設定します。

注：TC6.0 より古いソフトウェア バージョンを実行している場合、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

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

Auto：リンク速度を自動ネゴシエートします。

10half：10 Mbps 半二重に強制リンクします。

10full：10 Mbps 全二重に強制リンクします。

100half：100 Mbps 半二重に強制リンクします。

100full：100 Mbps 全二重に強制リンクします。

1000full：1 Gbps 全二重に強制リンクします。

例：Network 1 Speed: Auto

Network [1..1] TrafficControl Mode

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決定します。

必要なユーザ ロール：ADMIN

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。

例：Network 1 TrafficControl: On

Network [1..1] RemoteAccess Allow

ssh/telnet/HTTP/HTTPS へのアクセスの IP アドレスをフィルタします。

必要なユーザ ロール : ADMIN

値スペース : <S: 0, 255>

フォーマット : 最大 255 文字の文字列、カンマ区切りの IP アドレスまたは IP 範囲。

例 : Network 1 RemoteAccess Allow: "192.168.1.231, 192.168.1.182"

Network [1..1] VLAN Voice Mode

VLAN 音声モードを設定します。タッチ コントローラの Provisioning Wizard によって、プロビジョニング インフラストラクチャとして Cisco UCM (Cisco Unified Communications Manager) を選択した場合、VLAN 音声モードは自動的に Auto に設定されます。

必要なユーザ ロール : ADMIN

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。

例 : Network 1 VLAN Voice Mode: Off

Network [1..1] VLAN Voice VlanId

VLAN 音声 ID を設定します。この設定は、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

値スペース : <1..4094>

範囲 : 1 ~ 4094 の値を選択します。

例 : Network 1 VLAN Voice VlanId: 1

NetworkServices 設定

NetworkServices XMLAPI Mode

ビデオ システムの XML API をイネーブルまたはディセーブルにします。セキュリティ上の理由からこれをディセーブルにできません。XML API をディセーブルにすると、TMS などとのリモート管理機能が制限され、ビデオ システムに接続できなくなります。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：XML API はディセーブルになります。

On：XML API はイネーブルになります（デフォルト）。

例：NetworkServices XMLAPI Mode: On

NetworkServices MultiWay Address

MultiWay アドレスは Video Communication Server に設定された Conference Factory Alias と等しい必要があります。Multiway™ 会議により、ビデオ エンドポイントのユーザは既存のコールにサード パーティを追加できます。Multiway™ は次の場合に使用できます。

- 1) 既存のコールに他のユーザを追加する必要がある場合。
- 2) コール中にサード パーティからのコールがあり、既存のコールにその人を含める必要がある場合。

要件：Codec C20 は、ソフトウェア バージョン TC3.0（以降）、Video Communication Server (VCS) バージョン X5（以降）および Codian MCU バージョン 3.1（以降）を実行する必要があります。Multiway™ 会議に参加するよう招待されるビデオ システムは、H.323 コールの場合 H.323 routeToMC ファシリティ メッセージ、SIP コールの場合 SIP REFER メッセージをサポートする必要があります。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 255>

フォーマット：最大 255 文字の文字列（有効なダイヤル URI）。

例：NetworkServices MultiWay Address: "h323:multiway@company.com"

NetworkServices MultiWay Protocol

MultiWay コールに使用するプロトコルを決定します。

必要なユーザ ロール：ADMIN

値スペース：<Auto/H323/Sip>

Auto：システムが MultiWay コールのプロトコルを選択します。

H323：H323 プロトコルが MultiWay コールに使用されます。

Sip：SIP プロトコルが MultiWay コールに使用されます。

例：NetworkServices MultiWay Protocol: Auto

NetworkServices H323 Mode

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

必要なユーザ ロール：ADMIN

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）。

例：NetworkServices H323 Mode: On

NetworkServices HTTP Mode

Web ブラウザを使用したシステムへのアクセスを有効または無効にする HTTP モードを設定します。Web インターフェイスは、システム管理、コール転送などの、コール管理、診断およびソフトウェアのアップロードに使用されます。

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

値スペース：<Off/On>

Off：HTTP プロトコルはディセーブルになります。

On：HTTP プロトコルはイネーブルになります。

例：NetworkServices HTTP Mode: On

NetworkServices HTTPS Mode

HTTPS は、ユーザのページ要求と Web サーバから返されるページの暗号化と復号化を実行する Web プロトコルです。

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

値スペース：<Off/On>

Off：HTTPS プロトコルはディセーブルになります。

On：HTTPS プロトコルはイネーブルになります（デフォルト）。

例：NetworkServices HTTPS Mode: On

NetworkServices HTTPS VerifyServerCertificate

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

必要なユーザ ロール：ADMIN

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。

例：NetworkServices HTTPS VerifyServerCertificate: Off

NetworkServices HTTPS VerifyClientCertificate

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、クライアントは自分自身を識別するためにビデオ システムに証明書を提示するように要求されることがあります。

必要なユーザ ロール：ADMIN

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。

例：NetworkServices HTTPS VerifyClientCertificate: Off

NetworkServices HTTPS OCSP Mode

OCSP（Online Certificate Status Protocol）レスポンス 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 をイネーブルにして、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 レスポンス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

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。

例：NetworkServices HTTPS OCSP Mode: Off

NetworkServices HTTPS OCSP URL

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

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 255>

フォーマット：最大 255 文字の文字列。

例：NetworkServices HTTPS OCSP URL: "http://ocspserver.company.com:81"

NetworkServices NTP Mode

ネットワーク タイム プロトコル (NTP) は、リファレンス タイム サーバにシステムの時刻を同期するために使用されます。タイム サーバは時間の更新のために、以後 24 時間ごとに照会されます。時間は、画面上部に表示されます。システムは、H.235 認証を必要とするゲートキーパーまたはボーダー コントローラに送信されるメッセージのタイムスタンプに時間を使用します。システムは、H.235 認証を必要とするゲートキーパーまたはボーダー コントローラに送信されるメッセージのタイムスタンプに時間を使用します。また、発信履歴、不在着信、および受信コールのタイムスタンプにも使用されます。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Off/Manual>

Auto：システムは、ネットワーク上の DHCP サーバから指定されたアドレスによって NTP サーバを使用します。DHCP サーバが使用されない場合、または DHCP サーバが NTP サーバ アドレスをシステムに指定しない場合、システムはユーザが指定した、スタティックに定義された NTP サーバ アドレスを使用します。

Off：システムは NTP サーバを使用しません。

Manual：システムは、ユーザが指定したによってスタティックに定義された NTP サーバ アドレスを常に使用します。

例：NetworkServices NTP Mode: Manual

NetworkServices NTP Address

ネットワーク タイム プロトコル サーバのアドレスを定義するために、NTP のアドレスを入力します。このアドレスは、NTP Mode が Manual に設定された場合、または 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ます。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 64>

フォーマット：有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

例：NetworkServices NTP Address: "1.ntp.tandberg.com"

NetworkServices SIP Mode

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

必要なユーザ ロール：ADMIN

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)。

例：NetworkServices SIP Mode: On

NetworkServices SNMP Mode

ネットワーク管理システムでは、管理上の対応を補償する条件についてネットワーク接続デバイス (ルータ、サーバ、スイッチ、プロジェクトなど) 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。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

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。

例：NetworkServices SNMP Mode: ReadWrite

NetworkServices SNMP Host [1..3] Address

最大 3 個の SNMP マネージャのアドレスを入力します。

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ません。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 64>

フォーマット：有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

例：NetworkServices SNMP Host 1 Address: ""

NetworkServices SNMP CommunityName

ネットワーク サービス SNMP コミュニティ名を入力します。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

値スペース：<S: 0, 50>

フォーマット：最大 50 文字の文字列。

例：NetworkServices SNMP CommunityName: "public"

NetworkServices SNMP SystemContact

ネットワーク サービス SNMP システム接点の名前を入力します。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 50>

フォーマット：最大 50 文字の文字列。

例：NetworkServices SNMP SystemContact: ""

NetworkServices SNMP SystemLocation

ネットワーク サービス SNMP システム ロケーションの名前を入力します。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 50>

フォーマット：最大 50 文字の文字列。

例：NetworkServices SNMP SystemLocation: ""

NetworkServices SSH Mode

SSH (または Secure Shell) プロトコルは、コーデックとローカル コンピュータ間でのセキュアな暗号化通信を提供できます。

必要なユーザ ロール：ADMIN

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)。

例：NetworkServices SSH Mode: On

NetworkServices SSH AllowPublicKey

Secure Shell (SSH) 公開キー認証をコーデックへのアクセスに使用できます。

必要なユーザ ロール：ADMIN

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。

例：NetworkServices SSH AllowPublicKey: On

NetworkServices Telnet Mode

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) 接続で使用するネットワーク プロトコルです。

必要なユーザ ロール：ADMIN

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。

例：NetworkServices Telnet Mode: Off

NetworkServices CTMS Mode

この設定は Cisco TelePresence Multipoint Switch (CTMS) によって制御されるマルチパーティ会議を許可するかどうかを決定します。

TC5.0 以降のソフトウェアを実行するビデオ システムは、CTMS バージョン 1.8 以降で制御される暗号化されていないマルチパーティ会議を開始するか、それに参加できます。暗号化された会議は、ソフトウェア バージョン TC6.0 および CTMS 1.9.1 以降でサポートされます。暗号化は NetworkServices CTMS Encryption 設定により指定されます。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：CTMS によるマルチパーティ会議は禁止されます。

On：CTMS によるマルチパーティ会議が許可されます。

例：NetworkServices CTMS Mode: On

NetworkServices CTMS Encryption

この設定は Cisco TelePresence Multipoint Switch (CTMS) によって制御されるマルチパーティ会議に参加する場合に、ビデオ システムが暗号化をサポートするかどうかを示します。

CTMS は会議に 3 種類のセキュリティ設定を割り当てます。非セキュア（暗号化しない）、ベスト エフォート（すべての参加者が暗号化をサポートしている場合は暗号化し、それ以外の場合は暗号化しない）セキュア（常に暗号化）。

必要なユーザ ロール：ADMIN

値スペース：<Off/BestEffort>

Off: ビデオ システムは暗号化を許可しないため、セキュアな CTMS 会議（暗号化）に参加できません。ベスト エフォートの CTMS 会議に参加する場合、その会議は非セキュアにダウングレードされます（暗号化しない）。

BestEffort: ビデオ システムは、CTMS と暗号化パラメータをネゴシエートし、セキュアな CTMS 会議（暗号化）に参加できます。CTMS のバージョンが 1.9.1 より古い場合には、この値を使用しないでください。

例：NetworkServices CTMS Encryption: Off

電話帳の設定

Phonebook Server [1..1] ID

外部の電話帳の名前を入力します。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 64>

フォーマット：最大 64 文字の文字列。

例：Phonebook Server 1 ID: ""

Phonebook Server [1..1] Type

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

値スペース：<VCS/TMS/Callway/CUCM>

VCS：電話帳が Cisco TelePresence ビデオ コミュニケーション サーバにある場合は、VCS を選択します。

TMS：電話帳が Cisco TelePresence 管理スイート サーバにある場合は、TMS を選択します。

Callway：電話帳が WebEx TelePresence サブスクリプション サービス（旧称：CallWay）によって提供される場合は、Callway を選択します。詳細については WebEx Telepresence のプロバイダーにお問い合わせください。

CUCM：電話帳が Cisco Unified Communications Manager にある場合は、CUCM を選択します。

例：Phonebook Server 1 Type: TMS

Phonebook Server [1..1] URL

外部電話帳のサーバ アドレス（URL）を入力します。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 255>

フォーマット：最大 255 文字の文字列。

例：Phonebook Server 1 URL: "http://tms.company.com/tms/public/external/phonebook/phonebookservice.asmx"

プロビジョニング設定

Provisioning Connectivity

この設定は、プロビジョニング サーバからの内部または外部のコンフィギュレーションを要求するかどうかを、デバイスがどのように検出するか制御します。

必要なユーザ ロール：ADMIN

値スペース：<Internal/External/Auto>

Internal：内部コンフィギュレーションを要求します。

External：外部コンフィギュレーションを要求します。

Auto：内部または外部のコンフィギュレーションを要求するかどうかを自動的に NAPTR クエリーを使用して検出します。NAPTR の応答に「e」フラグがある場合、外部コンフィギュレーションが要求されます。それ以外の場合、内部コンフィギュレーションが要求されます。

例：Provisioning Connectivity: Auto

プロビジョニング モード (Provisioning Mode)

プロビジョニング システム (外部マネージャ) を使用してビデオ システムを設定できます。これにより、ビデオ会議のネットワーク管理者は複数のビデオ システムを同時に管理することができます。

この設定により、使用するプロビジョニング システムの種類を選択します。プロビジョニングは、オフに切り替えることも可能です。詳細については、プロビジョニング システムのプロバイダー / 担当者にお問い合わせください。

必要なユーザ ロール：ADMIN

値スペース：<Off/TMS/VCS/CallWay/CUCM/Auto>

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。

TMS：ビデオ システムは TMS (Cisco TelePresence 管理システム) を使用して設定されます。

VCS：このバージョンでは適用されません。

Callway：ビデオ システムは WebEx TelePresence サブスクリプション サービス (旧称: CallWay) を使用して設定します。

CUCM：ビデオ システムは CUCM (Cisco Unified Communications Manager) を使用して設定されます。

Auto：プロビジョニング サーバはビデオ システムによって自動的に選択されます。

例：Provisioning Mode: TMS

Provisioning LoginName

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。Provisioning Mode が Callway (WebEx TelePresence) の場合、ビデオ番号を入力します。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 80>

フォーマット：最大 80 文字の文字列。

例：Provisioning LoginName: ""

Provisioning Password

これは、指定サーバとのビデオ システムの認証に使用されるクレデンシャルのパスワード部分です。この設定は、プロビジョニング サーバが要求する場合、使用する必要があります。Provisioning Mode が Callway (WebEx TelePresence) の場合、アクティベーション コードを入力します。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 64>

フォーマット：最大 64 文字の文字列。

例：Provisioning Password: ""

Provisioning HttpMethod

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

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。

例：Provisioning HttpMethod: POST

Provisioning ExternalManager Address

外部マネージャやプロビジョニング システムの IP アドレスまたは DNS 名を入力します。

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

値スペース：<S: 0, 64>

フォーマット：有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

例：Provisioning ExternalManager Address: ""

Provisioning ExternalManager Protocol

セキュア管理を使用するかどうかを指定します。

必要なユーザ ロール：ADMIN

値スペース：<HTTP/HTTPS>

HTTP: HTTP に設定してセキュアな管理をディセーブルにします。HTTP は NetworkServices HTTP Mode の設定でイネーブルにする必要があります。

HTTPS: HTTPS に設定してセキュアな管理をイネーブルにします。HTTPS は NetworkServices HTTPS Mode の設定でイネーブルにする必要があります。

例：Provisioning ExternalManager Protocol: HTTP

Provisioning ExternalManager Path

外部マネージャ / プロビジョニング システムへのパスを設定します。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

値スペース：<S: 0, 255>

フォーマット：最大 255 文字の文字列。

例：Provisioning ExternalManager Path: "tms/public/external/management/SystemManagementService.asmx"

Provisioning ExternalManager Domain

VCS プロビジョニング サーバの SIP ドメインを入力します。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 64>

フォーマット：最大 64 文字の文字列。

例：Provisioning ExternalManager Domain: "any.domain.com"

RTP 設定

RTP Ports Range Start

RTP ポート範囲の最初のポートを指定します。「H323 Profile [1..1] PortAllocation」設定も参照してください。

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

値スペース：<1024..65502>

*範囲：*1024 ～ 65502 の値を選択します。

例：RTP Ports Range Start: 2326

RTP Ports Range Stop

RTP ポート範囲の最後のポートを指定します。「H323 Profile [1..1] PortAllocation」設定も参照してください。

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

値スペース：<1056..65535>

*範囲：*1056 ～ 65535 の値を選択します。

例：RTP Ports Range Stop: 2486

セキュリティ設定

Security Audit Logging Mode

監査ログを記録または送信する場所を設定します。External モードまたは ExternalSecure モードを使用する場合は、Security Audit Server Address 設定と Security Audit Server Port 設定で監査サーバのアドレスとポート番号を入力する必要があります。

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：AUDIT

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サーバ（syslog サーバ）に監査ログを送信します。監査サーバは TCP をサポートする必要があります。

ExternalSecure：システムは監査 CA の証明書によって検証された外部監査サーバ（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 リスト内の証明書の common_name パラメータが監査サーバの IP アドレスと一致する必要があります。

例：Security Audit Logging Mode: Off

Security Audit Server Address

監査サーバの IP アドレスを入力します。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。

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：AUDIT

値スペース：<S: 0, 64>

フォーマット：有効な IPv4 アドレスまたは IPv6 アドレス。

例：Security Audit Server Address: ""

Security Audit Server Port

システムが監査ログを送信する監査サーバのポートを入力します。デフォルト ポートは 514 です。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。

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：AUDIT

値スペース：<0..65535>

範囲：0 ～ 65535 の値を選択します。

例：Security Audit Server Port: 514

Security Audit OnError Action

監査サーバへの接続が失われた場合にどのように動作するかを記述します。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。

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：AUDIT

値スペース：<Halt/Ignore>

Halt：停止状態が検出された場合、システムはリブートし、停止状態が過ぎ去るまではオーディタだけが装置の操作を許可されます。停止状態が過ぎ去ると、監査ログは監査サーバに再スプールされます。次のような停止状態があります。ネットワークの違反（物理リンクなし）、動作中の監査サーバが存在しない（または間違った監査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。

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監査サーバに再度監査ログを送信します。

例：Security Audit OnError Action: Ignore

Security Session ShowLastLogon

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

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。

例：Security Session ShowLastLogon: Off

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ほどの時間を受け入れるか決定します。

必要なユーザ ロール：ADMIN

値スペース：<0..10000>

範囲：1 ～ 10000 秒の値を選択します。または、非アクティブ状態により自動ログアウトを強制しない場合は、0 を選択します。

例：Security Session InactivityTimeout: 0

SerialPort 設定

SerialPort Mode

シリアル ポート（Y 字型ケーブルによるカメラ ポート経由で接続）をイネーブルまたはディセーブルにします。

必要なユーザ ロール：ADMIN

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。

例：SerialPort Mode: On

SerialPort BaudRate

シリアル ポートに、ボー レート（データ送信レート、ビット / 秒）を指定します。デフォルト値は 38400 です。

シリアル ポートの他の接続パラメータは次のとおりです。データ ビット:8。パリティ:なし。ストップ ビット:1。フロー制御:なし。

必要なユーザ ロール：ADMIN

値スペース：<9600/19200/38400/57600/115200>

範囲：リストされているボー レート（bps）からボー レートを選択します。

例：SerialPort BaudRate: 38400

SerialPort LoginRequired

シリアル ポートに接続するときにログインが必要かどうかを決定します。

必要なユーザ ロール：ADMIN

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。

例：SerialPort LoginRequired: On

SIP 設定

SIP Profile [1..1] URI

SIP の URI または番号は、システムをアドレス指定するために使用されます。これは、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る URI です。Uniform Resource Identifier (URI) は、リソースを識別または指定するときに使用されるコンパクト文字列です。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 255>

フォーマット：最大 255 文字のコンパクト文字列。

例：SIP Profile 1 URI: "sip:firstname.lastname@company.com"

SIP Profile [1..1] DisplayName

設定されたとき、着信コールは SIP URI ではなく、DisplayName を報告します。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 255>

フォーマット：最大 255 文字の文字列。

例：SIP Profile 1 DisplayName: ""

SIP Profile [1..1] Authentication [1..1] LoginName

これは、SIP プロキシへの認証に使用されるクレデンシャルのユーザ名部分です。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 128>

フォーマット：最大 128 文字の文字列。

例：SIP Profile 1 Authentication 1 LoginName: ""

SIP Profile [1..1] Authentication [1..1] Password

これは、SIP プロキシへの認証に使用されるクレデンシャルのパスワード部分です。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 128>

フォーマット：最大 128 文字の文字列。

例：SIP Profile 1 Authentication 1 Password: ""

SIP Profile [1..1] DefaultTransport

LAN で使用するトランスポート プロトコルを選択します。

必要なユーザ ロール：ADMIN

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。

例：SIP Profile 1 DefaultTransport: Auto

SIP Profile [1..1] TlsVerify

TLS 接続の場合、SIP CA リストをビデオシステムにアップロードできます。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：検証せずに TLS 接続を許可するには、Off に設定します。TLS 接続は、サーバから受信した x.509 証明書をローカル CA リストと確認せずにセットアップできます。これは通常、コーデックに SIP CA リストがアップロードされていない場合、選択する必要があります。

On：TLS 接続を確認するには、On に設定します。x.509 証明書が CA リストで検証された、サーバへの TLS 接続だけが許可されます。

例：SIP Profile 1 TlsVerify: Off

SIP Profile [1..1] Outbound

ファイアウォール トラバース、接続の再利用および冗長性のための、クライアント開始接続メカニズムをオンまたはオフにします。現在のバージョンは RFC 5626 をサポートします。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：プロキシ アドレス リストに最初に設定されている単一プロキシに接続します。

On：プロキシ アドレス リストのサーバへの複数のアウトバウンド接続をセットアップします。

例：SIP Profile 1 Outbound: Off

SIP Profile [1..1] Proxy [1..4] Address

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。SIP プロファイル発信がイネーブルの場合、複数のプロキシをアドレス指定できます。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 255>

フォーマット：有効な IPv4 アドレス、IPv6 アドレス、または DNS 名。

例：SIP Profile 1 Proxy 1 Address: ""

SIP Profile [1..1] Proxy [1..4] Discovery

SIP プロキシ アドレスを手動とダイナミック ホスト コンフィギュレーション プロトコル (DHCP) のどちらを使用して取得するかを選択します。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Manual>

Auto：Auto が選択されると、ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) を使用して SIP プロキシ アドレスを取得します。

Manual：Manual が選択されると、手動で設定された SIP プロキシ アドレスが使用されます。

例：SIP Profile 1 Proxy 1 Discovery: Manual

SIP Profile [1..1] Type

ベンダーまたはプロバイダーに SIP 拡張および特別な動作をイネーブルにします。

必要なユーザ ロール：ADMIN

値スペース：<Standard/Alcatel/Avaya/Cisco/Microsoft/Nortel>

Standard：標準 SIP プロキシ (Cisco TelePresence VCS および Broadsoft でテスト済み) に登録するときに使用されます。

Alcatel：Alcatel-Lucent OmniPCX Enterprise に登録するときに使用されます。注：このモードはフル サポートされていません。

Avaya：Avaya Communication Manager に登録するときに使用されます。注：このモードはフル サポートされていません。

Cisco：Cisco Unified Communication Manager に登録するときに使用されます。

Microsoft：Microsoft LCS または OCS に登録するときに使用されます。注：このモードはフル サポートされていません。

Nortel：Nortel MCS 5100 または MCS 5200 PBX に登録するときに使用されます。注：このモードはフル サポートされていません。

例：SIP Profile 1 Type: Standard

SIP Profile [1..1] Mailbox

Cisco Unified Communications Manager (CUCM) に登録すると、個人用ボイス メールボックスを所有するオプションが与えられます。メール ボックスの番号 (アドレス) をこの設定に入力するか、またはボイス メール ボックスがない場合は文字列を空のままにしてください。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 255>

フォーマット：最大 255 文字の文字列。

例：SIP Profile 1 Mailbox: "12345678"

SIP Profile [1..1] Line

Cisco Unified Communications Manager (CUCM) に登録すると、エンドポイントを共有回線の一部にすることができます。これは、複数のデバイスが同じディレクトリ番号を共有することを意味します。RFC 4235 で規定されているように、同じ番号を共有する各デバイスは、ライン上のもう一方のアピアランスからステータスを受け取ります。

共有回線はエンドポイントではなく CUCM によって設定されることに注意してください。そのため、手動でこの設定を変更しないでください。CUCM は必要に応じてこの情報をエンドポイントにプッシュします。

必要なユーザ ロール：ADMIN

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）。

例：SIP Profile 1 Line: Private

SIP ListenPort

SIP TCP/UDP ポートでの着信接続のリッスンをオンまたはオフにします。オフにした場合、エンドポイントは SIP レジストラ(CUCM または VCS)を介してのみ到達可能になります。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

値スペース：<On/Off>

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。

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。

例：SIP ListenPort: On

スタンバイの設定

Standby Control

システムがスタンバイ モードに移動するかどうかを決定します。

必要なユーザ ロール：ADMIN

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ったときにスタンバイ モードを開始します。注：スタンバイ遅延を適切な値に設定する必要があります。

例：Standby Control: On

Standby Delay

スタンバイ モードに入る前に、システムがアイドル モードのまま経過する時間の長さ（分単位）を定義します。注：Standby Control をイネーブルにする必要があります。

必要なユーザ ロール：ADMIN

値スペース：<1..480>

範囲：1 ～ 480 分の値を選択します。

例：Standby Delay: 10

Standby BootAction

コーデックの再起動後のカメラの位置を定義します。

必要なユーザ ロール：ADMIN

値スペース：<None/Preset1/Preset2/Preset3/Preset4/Preset5/Preset6/Preset7/Preset8/Preset9/Preset10/Preset11/Preset12/Preset13/Preset14/Preset15/RestoreCameraPosition/DefaultCameraPosition>

None：アクションはありません。

Preset1 ～ Preset15：再起動後、カメラ位置は選択したプリセットによって定義された位置にセットされます。

RestoreCameraPosition：再起動後、カメラ位置は前回のブート前の位置にセットされます。

DefaultCameraPosition：再起動後、カメラ位置は工場出荷時のデフォルトの位置にセットされます。

例：Standby BootAction: DefaultCameraPosition

Standby StandbyAction

スタンバイ モードに入るときのカメラ位置を定義します。

必要なユーザ ロール：ADMIN

値スペース：<None/PrivacyPosition>

None：アクションはありません。

PrivacyPosition：プライバシーのためカメラを横向き位置に向けます。

例：Standby StandbyAction: PrivacyPosition

Standby WakeupAction

スタンバイ モードを抜けるときのカメラ位置を定義します。

必要なユーザ ロール：ADMIN

値スペース：<None/Preset1/Preset2/Preset3/Preset4/Preset5/Preset6/Preset7/Preset8/Preset9/Preset10/Preset11/Preset12/Preset13/Preset14/Preset15/RestoreCameraPosition/DefaultCameraPosition>

None：アクションはありません。

Preset1 ～ Preset15：スタンバイを抜けるとき、カメラ位置は選択したプリセットによって定義された位置にセットされます。

RestoreCameraPosition：スタンバイを抜けるとき、カメラ位置はスタンバイに入る前の位置にセットされます。

DefaultCameraPosition：スタンバイを抜けるとき、カメラ位置は工場出荷時のデフォルトの位置にセットされます。

例：Standby WakeupAction: RestoreCameraPosition

SystemUnit 設定

SystemUnit Name

システム装置の名前を定義するためにシステム名を入力します。H.323 エイリアス ID がシステムに設定されている場合、この ID がシステム名の代わりに使用されます。次の場合にシステム名が表示されます。

- 1) コーデックが SNMP エージェントとして機能している場合。
- 2) DHCP サーバ向け。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 50>

フォーマット：最大 50 文字の文字列。

例：SystemUnit Name: "Meeting Room"

SystemUnit MenuLanguage

スクリーンまたはタッチ コントローラのメニューで使用する言語を選択します。

必要なユーザ ロール：USER

値スペース：<English/ChineseSimplified/ChineseTraditional/Czech/Danish/Dutch/Finnish/French/German/Hungarian/Italian/Japanese/Korean/Norwegian/Polish/PortugueseBrazilian/Russian/Spanish/SpanishLatin/Swedish/Turkish>

例：SystemUnit MenuLanguage: English

SystemUnit ContactInfo Type

メイン ディスプレイまたはタッチ コントローラの左上隅にあるステータス フィールドに表示する、連絡先情報の種類を選択します。情報は、xStatus SystemUnit ContactInfo コマンドでも読み込むことができます。

必要なユーザ ロール：ADMIN

値スペース：<Auto/None/IPv4/IPv6/H323Id/E164Alias/H320Number/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。アドレスはデフォルトのコール プロトコルおよびシステム登録によって異なります。

None：ステータス フィールドに連絡先情報を表示しません。

IPv4：連絡先情報として IPv4 アドレスを表示します。

IPv6：連絡先情報として IPv6 アドレスを表示します。

H323Id：連絡先情報として H.323 ID を表示します (H323 Profile [1..1] H323Alias ID 設定を参照)。

E164Alias：連絡先情報として H.323 E164 エイリアスを表示します (H323 Profile [1..1] H323Alias E164 設定を参照)。

H320Number：連絡先情報として H.320 番号を表示します (Cisco TelePresence ISDN リンク ゲートウェイに接続されている場合のみ)。

SipUri：連絡先情報として SIP URI を表示します (SIP Profile [1..1] URI 設定を参照)。

SystemName：連絡先情報としてシステム名を表示します (SystemUnit Name 設定を参照)。

DisplayName：連絡先情報として表示名を表示します (SIP Profile [1..1] DisplayName 設定を参照)。

例：SystemUnit ContactInfo Type: Auto

SystemUnit CallLogging Mode

システムが受信または送信するコールのコール ログニング モードを設定します。コール ログは、Web インターフェイスまたは xHistory コマンドを使用して表示できます。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：ログニングをディセーブルにします。

On：ログニングをイネーブルにします。

例：SystemUnit CallLogging Mode: On

SystemUnit IrSensor

コーデック C シリーズと PrecisionHD カメラの両方が IR センサーを持っており、そのうち同時に 1 つだけをイネーブルにする必要があります。IR センサー LED はコーデックの前面とカメラにあり、リモコンから IR 信号を受信すると明滅します。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Off/On>

Auto：カメラの IR センサーがイネーブルの場合、システムはコーデックの IR センサーを自動的にディセーブルにします。そうでない場合、コーデックの IR センサーはイネーブルになります。

Off：コーデックの IR センサーをディセーブルにします。

On：コーデックの IR センサーをイネーブルにします。

例：SystemUnit IrSensor: Auto

Time Settings

タイムゾーン (Time Zone)

Windows の時間帯の表記形式を使用してシステム所在地のタイム ゾーンを設定します。

必要なユーザ ロール : USER

値スペース : <GMT-12:00 (International Date Line West)/GMT-11:00 (Midway Island, Samoa)/GMT-10:00 (Hawaii)/GMT-09:00 (Alaska)/GMT-08:00 (Pacific Time (US & Canada); Tijuana)/GMT-07:00 (Arizona)/GMT-07:00 (Mountain Time (US & Canada))/GMT-07:00 (Chihuahua, La Paz, Mazatlan)/GMT-06:00 (Central America)/GMT-06:00 (Saskatchewan)/GMT-06:00 (Guadalajara, Mexico City, Monterrey)/GMT-06:00 (Central Time (US & Canada))/GMT-05:00 (Indiana (East))/GMT-05:00 (Bogota, Lima, Quito)/GMT-05:00 (Eastern Time (US & Canada))/GMT-04:30 (Caracas)/GMT-04:00 (La Paz)/GMT-04:00 (Santiago)/GMT-04:00 (Atlantic Time (Canada))/GMT-03:30 (Newfoundland)/GMT-03:00 (Buenos Aires, Georgetown)/GMT-03:00 (Greenland)/GMT-03:00 (Brasilia)/GMT-02:00 (Mid-Atlantic)/GMT-01:00 (Cape Verde Is.)/GMT-01:00 (Azores)/GMT (Casablanca, Monrovia)/GMT (Coordinated Universal Time)/GMT (Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London)/GMT+01:00 (West Central Africa)/GMT+01:00 (Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna)/GMT+01:00 (Brussels, Copenhagen, Madrid, Paris)/GMT+01:00 (Sarajevo, Skopje, Warsaw, Zagreb)/GMT+01:00 (Belgrade, Bratislava, Budapest, Ljubljana, Prague)/GMT+02:00 (Harare, Pretoria)/GMT+02:00 (Jerusalem)/GMT+02:00 (Athens, Istanbul, Minsk)/GMT+02:00 (Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius)/GMT+02:00 (Cairo)/GMT+02:00 (Bucharest)/GMT+03:00 (Nairobi)/GMT+03:00 (Kuwait, Riyadh)/GMT+03:00 (Moscow, St. Petersburg, Volgograd)/GMT+03:00 (Baghdad)/GMT+03:30 (Tehran)/GMT+04:00 (Abu Dhabi, Muscat)/GMT+04:00 (Baku, Tbilisi, Yerevan)/GMT+04:30 (Kabul)/GMT+05:00 (Islamabad, Karachi, Tashkent)/GMT+05:00 (Ekaterinburg)/GMT+05:30 (Chennai, Kolkata, Mumbai, New Delhi)/GMT+05:45 (Kathmandu)/GMT+06:00 (Sri Jayawardenepura)/GMT+06:00 (Astana, Dhaka)/GMT+06:00 (Almaty, Novosibirsk)/GMT+06:30 (Rangoon)/GMT+07:00 (Bangkok, Hanoi, Jakarta)/GMT+07:00 (Krasnoyarsk)/GMT+08:00 (Perth)/GMT+08:00 (Taipei)/GMT+08:00 (Kuala Lumpur, Singapore)/GMT+08:00 (Beijing, Chongqing, Hong Kong, Urumqi)/GMT+08:00 (Irkutsk, Ulaan Bataar)/GMT+09:00 (Osaka, Sapporo, Tokyo)/GMT+09:00 (Seoul)/GMT+09:00 (Yakutsk)/GMT+09:30 (Darwin)/GMT+09:30 (Adelaide)/GMT+10:00 (Guam, Port Moresby)/GMT+10:00 (Brisbane)/GMT+10:00 (Vladivostok)/GMT+10:00 (Hobart)/GMT+10:00 (Canberra, Melbourne, Sydney)/GMT+11:00 (Magadan, Solomon Is., New Caledonia)/GMT+12:00 (Fiji, Kamchatka, Marshall Is.)/GMT+12:00 (Auckland, Wellington)/GMT+13:00 (Nuku alofa)>

範囲 : リストのタイム ゾーンからタイム ゾーンを選択します。コマンドライン インターフェイスを使用している場合、タイプ ミスに注意します。

例 : Time Zone: "GMT (Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London)"

Time TimeFormat

時間のフォーマットを設定します。

必要なユーザ ロール : USER

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。

例 : Time TimeFormat: 24H

Time DateFormat

日付のフォーマットを設定します。

必要なユーザ ロール : USER

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。

例 : Time DateFormat: DD_MM_YY

UserInterface 設定

UserInterface TouchPanel DefaultPanel

デフォルトとして連絡先リスト、スケジュールされた会議のリスト、ダイヤル パッドのうちどれをタッチ コントローラに表示するか選択します。

必要なユーザ ロール：USER

値スペース：<ContactList/MeetingList/Dialpad>

ContactList：連絡先リスト（お気に入り、ディレクトリおよび履歴）がタッチ コントローラのデフォルトとして表示されます。

MeetingList：スケジュールされた会議のリストがタッチ コントローラのデフォルトとして表示されます。

Dialpad：ダイヤル パッドがタッチ コントローラのデフォルトとして表示されます。

例：UserInterface TouchPanel DefaultPanel: ContactList

ビデオ設定

Video Input Source [1..2] Name

ビデオ入力ソースの名前を入力します。

必要なユーザ ロール：ADMIN

値スペース：<S: 0, 50>

フォーマット：最大 50 文字の文字列。

例：Video Input Source 1 Name: ""

Video Input Source [1] Connector

ビデオ入力ソース 1 でアクティブにするビデオ入力コネクタを選択します。

必要なユーザ ロール：ADMIN

値スペース：<HDMI>

HDMI：入力ソース 1 として HDMI を使用する場合は、HDMI を選択します。

例：Video Input Source 1 Connector: HDMI

Video Input Source [2] Connector

ビデオ入力ソース 2 でアクティブにするビデオ入力コネクタを選択します。

必要なユーザ ロール：ADMIN

値スペース：<DVI>

DVI：入力ソース 2 として DVI-I 2 を使用する場合は、DVI-I を選択します。

例：Video Input Source 2 Connector: DVI

Video Input Source [1..2] Type

ビデオ入力に接続された入力ソースのタイプを設定します。

必要なユーザ ロール：ADMIN

値スペース：<other/camera/PC/DVD/document_camera>

Other：他のタイプの装置を指定ビデオ入力に接続する場合、Other を選択します。

Camera：指定されたビデオ入力に接続されているカメラがある場合は、Camera を選択します。

PC：指定されたビデオ入力に接続されている PC がある場合は、PC を選択します。

DVD：指定されたビデオ入力に接続されている DVD プレーヤーがある場合は、DVD を選択します。

Document_Camera：指定されたビデオ入力に接続されているドキュメント カメラがある場合は、Document_Camera を選択します。

例：Video Input Source 1 Type: PC

Video Input Source [1..2] PresentationSelection

一般に、どの入力ソースでもプレゼンテーション ソースとして使用できます。通常、メイン カメラ（セルフ ビュー）はプレゼンテーション ソースとしては使用されません。

この設定を使用して、プレゼンテーション ソースをローカル ビデオ システムのディスプレイに自動的に表示するかどうかを定義します。プレゼンテーションを遠端と共有する場合、常に追加のアクション（タッチ コントローラで [Start Presenting] をタップするかリモコンのプレゼンテーション キーを押す）が必要です。

すべての入力ソースのデフォルト値は Manual です。

必要なユーザ ロール：ADMIN

値スペース：<Manual/Automatic/Hidden>

Manual：入力ソースの内容は、ローカル ビデオ システムのディスプレイで選択するまで表示されません。リモコンまたはタッチ コントローラを使用して、どの入力ソースを表示するかを選択します。

Automatic：入力ソースの内容は、ローカル ビデオ システムのディスプレイに自動的に表示されます。複数の入力ソースにアクティブ コンテンツ（Automatic に設定）がある場合、最新のものが使用されます。

Hidden：入力ソースは、プレゼンテーションのソースとして使用されることはありません。

例：Video Input Source 1 PresentationSelection: Manual

Video Input Source [1..2] CameraControl Mode

ビデオ入力がアクティブなときに指定ビデオ入力ソースのカメラ制御をイネーブルにするかどうかを選択します。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：カメラ制御をディセーブルにします。

On：カメラ制御をイネーブルにします。

例：Video Input Source 1 CameraControl Mode: On

Video Input Source [1..2] CameraControl Camerald

カメラの ID を表示します。この値は、この製品に固定されます。

値スペース：<1>

範囲：カメラの ID を表示します。

Video Input Source [1..2] OptimalDefinition Profile

最適鮮明度設定を有効にするために、Video Input Source Quality を Motion に設定する必要があります。

最適鮮明度プロファイルは、会議室の光の状態とビデオ入力（カメラ）の品質に合わせる必要があります。光の状態とビデオ入力が優れていれば、プロファイルも向上します。このとき、良い光の条件で、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、Normal または Medium プロファイルを使用することを推奨します。ただし、光の条件が良い場合、特定のコール レートの解像度を大きくするために、High プロファイルを設定できます。

異なる最適鮮明度プロファイルに使用する一般的な解像度、コール レートおよび送信フレーム レートの一部を次の表に示します。デュアル ビデオを使用しないことを前提としています。解像度は、発信側と着信側の両方のシステムでサポートされている必要があります。

60 fps のフレーム レートを使用する場合、決定に Video Input Source OptimalDefinition Threshold60fps 設定を使用します。

さまざまな最適鮮明度プロファイル、コール レート、フレーム レートで使用する一般的な解像度								
フレーム レート	最適 鮮明度 プロファイル	コール レート						
		256 kbps	768 kbps	1152 kbps	1472 kbps	2560 kbps	4 Mbps	6 Mbps
30 fps	Normal	512×288	1024×576	1280×720	1280×720	1920×1080	1920×1080	1920×1080
	Medium	640×360	1280×720	1280×720	1280×720	1920×1080	1920×1080	1920×1080
	High	768×448	1280×720	1280×720	1920×1080	1920×1080	1920×1080	1920×1080
60 fps	Normal	256×144	512×288	768×448	1024×576	1280×720	1280×720	1280×720
	Medium	256×144	768×448	1024×576	1024×576	1280×720	1280×720	1280×720
	High	512×288	1024×576	1280×720	1280×720	1280×720	1280×720	1280×720

必要なユーザ ロール：ADMIN

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。

例：Video Input Source 1 OptimalDefinition Profile: Normal

Video Input Source [1..2] OptimalDefinition Threshold60fps

各ビデオ入力について、この設定は 60 fps で送信する最低解像度をシステムに通知します。これより低い解像度すべてについて、最大送信フレーム レートは 30 fps となります。使用可能な帯域幅が適切であれば、これより高い解像度で 60 fps も可能です。

必要なユーザ ロール：ADMIN

値スペース：<512_288/768_448/1024_576/1280_720/1920_1080/Never>

512_288：512x288 にしきい値を設定します。

768_448：768x448 にしきい値を設定します。

1024_576：1024x576 にしきい値を設定します。

1280_720：1280x720 にしきい値を設定します。

1920_1080：1920x1080 にしきい値を設定します。

Never：60 fps を送信するしきい値を設定しません。

例：Video Input Source 1 OptimalDefinition Threshold60fps: 1280_720

Video Input Source [1..2] Quality

ビデオのエンコードと送信のときには、高解像度と高フレーム レートとの間にトレード オフが存在します。一部のビデオ ソースでは、高フレーム レートが高解像度より重要であり、逆の場合もあります。この品質設定は、指定のソースに対して、高フレーム レートと高解像度のどちらにプライオリティを設定するかを指定します。

必要なユーザ ロール：ADMIN

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。

例：Video Input Source 1 Quality: Motion

Video MainVideoSource

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。ビデオ入力ソースは「Video Input Source [1..n] Connector」で設定されます。

必要なユーザ ロール：USER

値スペース：<1/2>

範囲：メイン ビデオ ソースとして使用されるソースを選択します。

例：Video MainVideoSource: 1

Video DefaultPresentationSource

デフォルトのプレゼンテーションのソースとして使用する入力ソースを定義します（リモート コントロールの Presentation キーを押したとき）。タッチ コントローラを使用する場合、この設定の影響はありません。Video Input Source n Connector 設定は、入力ソース n に使用する入力コネクタを定義します。

必要なユーザ ロール：USER

値スペース：<1/2>

範囲：プレゼンテーション ソースとして使用されるビデオ ソースを選択します。

例：Video DefaultPresentationSource: 2

Video Input HDMI [1..1] RGBQuantizationRange

HDMI 入力を持つすべてのデバイスは、CEA-861 で規定されている RGB のビデオ量子化範囲のルール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ないため、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することができます。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Full/Limited>

Auto：RGB の量子化の範囲は、AVI インフォフレームの RGB 量子化範囲ビット（Q0、Q1）に基づいて自動的に選択されます。AVI インフォフレームが使用できない場合、RGB 量子化範囲は CEA-861-E に従ったビデオ形式に基づいて選択されます。

Full：完全な量子化の範囲。R、G、B の量子化範囲にはすべてのコード値（0 ～ 255）が含まれます。これは CEA-861-E で規定されています。

Limited：限定された量子化の範囲。極端なコード値を除いた R、G、B の量子化範囲（16 ～ 235）。これは CEA-861-E で規定されています。

例：Video Input 1 HDMI 1 RGBQuantizationRange: Auto

Video Input DVI [2] RGBQuantizationRange

DVI 入力を持つすべてのデバイスは、CEA-861 で規定されている RGB のビデオ量子化範囲のルール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ないため、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することができます。ほとんどの DVI ソースは完全な量子化範囲を想定するため、デフォルト値は Full に設定されます。

必要なユーザ ロール：ADMIN

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。

例：Video Input 1 DVI 2 RGBQuantizationRange: Full

Video Input DVI [2] Type

公式 DVI 規格は、デジタル信号とアナログ信号の両方をサポートします。ほとんどの場合、デフォルトの AutoDetect 設定で信号がアナログ RGB かデジタルかを検出できます。ただし DVI-I ケーブルを使用した場合（これらのケーブルはアナログとデジタル両方の信号を伝送できます）、まれに自動検出に失敗することがあります。この設定により、AutoDetect を上書きし、正しい DVI ビデオ入力を選択できます。

必要なユーザ ロール：ADMIN

値スペース：<AutoDetect/Digital/AnalogRGB>

AutoDetect：信号がアナログ RGB かデジタルかを自動的に検出するには、AutoDetect に設定します。

Digital：アナログとデジタルの両方のピンを持つ DVI-I ケーブルを使用し、AutoDetect が失敗する場合、Digital に設定すると DVI ビデオ入力を強制的に Digital にします。

AnalogRGB：アナログとデジタルの両方のピンを持つ DVI-I ケーブルを使用し、AutoDetect が失敗する場合、AnalogRGB に設定すると DVI ビデオ入力を強制的に AnalogRGB にします。

例：Video Input DVI 2 Type: AutoDetect

Video Layout Scaling

イメージとそれを配置するフレームとの間に違いがある場合、システムがイメージまたはフレームのアスペクト比をどのように調整するかを定義します。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：アスペクト比の調整はありません。

On：システムがアスペクト比を自動的に調整できるようにします。

例：Video Layout Scaling: On

Video Layout ScaleToFrame

ビデオ入力ソースのアスペクト比がコンポジション内の対応するイメージ フレーム アスペクト比と一致しない場合の対処方法を定義します。たとえば、4:3 入力（XGA など）を 16:9 出力（HD720 など）に表示する場合です。

必要なユーザ ロール：ADMIN

値スペース：<Manual/MaintainAspectRatio/StretchToFit>

Manual：ビデオ入力ソースとターゲット イメージ フレーム間のアスペクト比の違いが Video Layout ScaleToFrameThreshold 設定（パーセンテージ）よりも小さい場合、イメージはフィットするよう拡大されます。そうでない場合は、元のアスペクト比が維持されます。

MaintainAspectRatio：入力ソースのアスペクト比を維持し、フレームの残りの部分（文字のボクシングや柱のボクシング）は黒で埋めます。

StretchToFit：イメージのフレームにフィットするよう入力ソースを（水平または垂直に）拡張します。注：一般的な制限として、1 方向を拡大しながら別の方向を縮小することはできません。このような状況で、コーデックは letterboxing を適用します。

例：Video Layout ScaleToFrame: MaintainAspectRatio

Video Layout ScaleToFrameThreshold

Video Layout ScaleToFrame が Manual に設定されている場合に限り適用できます。ビデオ入力ソースとターゲット イメージ フレーム間のアスペクト比の違いが ScaleToFrameThreshold 設定（パーセンテージ）よりも小さい場合、イメージはフィットするよう拡大されます。そうでない場合は、元のアスペクト比が維持されます。

必要なユーザ ロール：ADMIN

値スペース：<0..100>

範囲：0 ～ 100 % の値を選択します。

例：Video Layout ScaleToFrameThreshold: 5

Video Selfview

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指定します。
この設定は TC6.0 以降、Video SelfviewDefault Mode 設定に変わりました。

必要なユーザ ロール：USER

値スペース：<Off/On>

- Off*：画面にセルフビューを表示しません。
- On*：画面にセルフビューを表示します。

例：Video Selfview: On

Video SelfviewPosition

画面上で小さいセルフビューの PiP（Picture in Picture）を表示する位置を選択します。
この設定は TC6.0 以降、Video SelfviewDefault PIPPosition 設定に変わりました。

必要なユーザ ロール：ADMIN

値スペース：<UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight>

- 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。

例：Video SelfviewPosition: LowerRight

Video SelfviewController AutoResizing

セルフ ビューのフレーム サイズを次のルールに従って自動的に変更するように設定できます。セルフ ビュー フレームと重なるフレームが変化すると、サイズは全画面から PiP（Picture in Picture）に減少します。モニタに他に何も表示されていない場合、サイズは PiP から全画面に増大します。MonitorRole が First である場合、最後のルールはモニタに適用されません。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

- Off*：セルフ ビューは自動的にサイズ変更されません。
- On*：セルフ ビューは前述したとおり自動的にサイズ変更されます。

例：Video SelfviewController AutoResizing: On

Video SelfviewDefault Mode

メイン ビデオ ソース（セルフビュー）をコールの後に画面に表示するかどうかを指定します。セルフ ビュー ウィンドウの位置とサイズはそれぞれ、Video SelfviewDefault PIPPosition 設定および Video Selfview FullscreenMode 設定によって決定されます。

この設定は TC6.0 以降、Video Selfview 設定に変わりました。

必要なユーザ ロール：ADMIN

値スペース：<Off/Current/On>

- Off*：セルフ ビューはコール退出時にオフにされます。
- Current*：セルフ ビューはそのままの状態が残ります。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。
- On*：セルフ ビューはコール退出時にオンにされます。

例：Video SelfviewDefault Mode: Current

Video SelfviewDefault FullscreenMode

コール終了後にメイン ビデオ ソース（セルフ ビュー）を全画面表示するか、小さいピクチャ イン ピクチャ（PiP）画面で表示するかを設定します。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 SelfviewDefault Mode 設定を参照）。

必要なユーザ ロール：ADMIN

値スペース：<Off/Current/On>

Off：セルフ ビューは PiP として表示されます。

Current：セルフ ビューの画像のサイズはコール終了時に未変更の状態に保たれます。つまりコール中に PiP であった場合はコール終了後にも PiP のままであり、コール中に全画面であった場合はコール終了後にも全画面のままです。

On：セルフ ビューの画像は全画面表示されます。

例：Video SelfviewDefault FullscreenMode: Current

Video SelfviewDefault PIPPosition

コール終了後のセルフ ビューの小さいピクチャ イン ピクチャ（PiP）画面の位置を設定します。この設定はセルフ ビューがオンであり（Video SelfviewDefault 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 SelfviewDefault FullscreenMode 設定を参照）にのみ有効です。

この設定は TC6.0 以降、Video SelfviewPosition 設定に変わりました。

必要なユーザ ロール：ADMIN

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。

例：Video SelfviewDefault PIPPosition: Current

Video SelfviewDefault OnMonitorRole

コール終了後にメイン ビデオ ソース（セルフビュー）に表示するモニタ / 出力を設定します。この値には、Video Output HDMI MonitorRole 設定で異なる出力に対して設定されたモニタ ロールが反映されます。

この設定は、セルフビューが全画面表示されていてもピクチャ イン ピクチャ（PiP）で表示されていても適用されますが、Video Monitors 設定が Dual に設定されている場合に限られます。

必要なユーザ ロール：ADMIN

値スペース：<First/Second/Current>

First：セルフ ビューの画像は、Video Output HDMI MonitorRole が First に設定されている場合に出力に表示されます。

Second：セルフ ビューの画像は、Video Output HDMI MonitorRole が Second に設定されている場合に出力に表示されます。

Current：コール終了時、セルフビューの画像はコール中のものと同じ出力に保たれます。

例：Video SelfviewDefault OnMonitorRole: Current

Video CamCtrlPip CallSetup Mode

コールをセットアップする短い間、この設定を使用してセルフ ビューがオンにされます Video CamCtrlPip CallSetup Duration 設定は、それが維持される時間の長さを指定します。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

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。

例：Video CamCtrlPip CallSetup Mode: Off

Video CamCtrlPip CallSetup Duration

この設定は Video CamCtrlPip CallSetup Mode 設定がオンである場合のみ有効です。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

値スペース：<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。

例：Video CamCtrlPip CallSetup Duration: 10

Video PIP ActiveSpeaker DefaultValue Position

通話中のスピーカーのピクチャ イン ピクチャ (PiP) 画面の位置を設定します。この設定は通話中のスピーカーが PiP に表示されるビデオ レイアウトを使用する場合、つまりオーバーレイ レイアウト、またはカスタム レイアウト (Video Layout LocalLayoutFamily 設定を参照) 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

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。

例：Video PIP ActiveSpeaker DefaultValue Position: Current

Video PIP Presentation DefaultValue Position

プレゼンテーションのピクチャ イン ピクチャ (PiP) 画面の位置を設定します。この設定は、リモコンやタッチ コントローラを使用するなどしてプレゼンテーションが明示的に PiP に最小化されている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

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。

例：Video PIP Presentation DefaultValue Position: Current

Video Layout LocalLayoutFamily

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

値スペース：<Auto/FullScreen/Equal/PresentationSmallSpeaker/PresentationLargeSpeaker/Prominent/Overlay/Single>

Auto：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、ローカル レイアウトとして使用されます。レイアウト データベースの詳細については、xCommand Video Layout LoadDb コマンドを参照してください。

FullScreen：FullScreen 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プレゼンテーションはフルスクリーンで表示されます。この値の使用は TC6.0 以降では推奨されません。

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。

PresentationSmallSpeaker：PresentationSmallSpeaker 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。この値の使用は TC6.0 以降では推奨されません。

PresentationLargeSpeaker：PresentationLargeSpeaker 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。この値の使用は TC6.0 以降では推奨されません。

Prominent：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、音声切り替えられます。

Overlay：Overlay レイアウト ファミリがローカル レイアウトとして使用されます。通話中のスピーカー、または (存在する場合) プレゼンテーションは全画面表示となり、他の参加者は小さいピクチャ イン ピクチャ (PiP) となります。通話中のスピーカーが遷移するとき、音声切り替えられます。

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。

例：Video Layout LocalLayoutFamily: Auto

Video Layout RemoteLayoutFamily

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

値スペース : <Auto/FullScreen/Equal/PresentationSmallSpeaker/PresentationLargeSpeaker/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。レイアウト データベースの詳細については、xCommand Video Layout LoadDb コマンドを参照してください。

FullScreen : FullScreen 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プレゼンテーションはフルスクリーンで表示されます。この値の使用は TC6.0 以降では推奨されません。

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。

PresentationSmallSpeaker : PresentationSmallSpeaker 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。この値の使用は TC6.0 以降では推奨されません。

PresentationLargeSpeaker : PresentationLargeSpeaker 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。この値の使用は TC6.0 以降では推奨されません。

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 : Overlay レイアウト ファミリがリモート レイアウトとして使用されます。通話中のスピーカー、または（存在する場合）プレゼンテーションは全画面表示となり、他の参加者は小さいピクチャ イン ピクチャ (PiP) となります。通話中のスピーカーが遷移するとき、音声切り替えられます。

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。

例 : Video Layout RemoteLayoutFamily: Auto

Video Monitors

モニター レイアウト モードを設定します。

必要なユーザ ロール : ADMIN

値スペース : <Single/Dual/DualPresentationOnly>

Single : 同じレイアウトがすべてのモニターに表示されます。

Dual : 最初のモニターにはコールのすべての関係者が、2 番目のモニターにはプレゼンテーション（存在する場合）が表示されます。セルフ ビューは、Video SelfviewDefault OnMonitorRole の設定に応じて、2 番目のモニターに表示できます。

DualPresentationOnly : 最初のモニターにはコールのすべての関係者が、2 番目のモニターにはプレゼンテーション（存在する場合）が表示されます。

例 : Video Monitors: Single

Video OSD Mode

ビデオ OSD（On Screen Display）モードでは、情報およびアイコンを画面に表示するかどうかを定義できます。

必要なユーザ ロール : ADMIN

値スペース : <Off/On/Disabled>

Off : オン スクリーン メニュー、アイコンおよびインジケータを非表示にします。

On : オン スクリーン メニュー、アイコンおよびインジケータを表示します。

Disabled : Disabled に設定すると、プレゼンテーション共有と同時に 1080p30 を行うため通常 GUI によって使用される追加リソースを C20 が使用できます。GUI が無効にされるため、C20 は Cisco TelePresence Touch または外部制御パネルによって制御される必要があります。

例 : Video OSD Mode: On

Video OSD MenuStartupMode

ビデオ システムまたはコーデックをブートした後の OSD（オン スクリーン ディスプレイ）メニューの状態を設定します。この設定は、ビデオ システムがリモコンと画面上のメニューによって操作される場合にのみ適用されます。

必要なユーザ ロール : ADMIN

値スペース : <Closed/Home>

Closed : OSD メニューは自動的に展開されません。この設定は、OSD に表示される内容を完全に制御する必要があるサードパーティ統合には推奨されます。

Home : OSD メニューでは Home メニューを展開して表示します。

例 : Video OSD MenuStartupMode: Home

Video OSD VirtualKeyboard

テキストが入力フィールドに入力されるときに仮想キーボードを画面上に自動的に表示するかどうかを設定します。この設定は、ビデオ システムがリモコンと画面上のメニューによって操作される場合にのみ適用されます。

必要なユーザ ロール：ADMIN

値スペース：<UserSelectable/AlwaysOn>

UserSelectable：仮想キーボードを開くときと閉じるときにユーザがソフトボタンを押す必要があります。

AlwaysOn：テキストを入力フィールドに入力できる限り、仮想キーボードは画面上に自動的に表示されます。

例：Video OSD VirtualKeyboard: UserSelectable

Video OSD EncryptionIndicator

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。この設定は、暗号化されたコールと暗号化されていないコール、つまりセキュアな会議と非セキュアな会議の両方に適用されます。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

値スペース：<Auto/AlwaysOn/AlwaysOff>

Auto：Conference Encryption Mode 設定が BestEffort に設定され、コールが暗号化されている場合、暗号化インジケータがコールの最初の数秒間に表示されます。Conference Encryption Mode 設定が BestEffort に設定され、コールが暗号化されていない場合、バツ印の付いた暗号化インジケータがコール全体にわたり表示されます。Conference Encryption Mode 設定が BestEffort に設定されていない場合、暗号化インジケータはまったく表示されません。

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。これは、すべての Conference Encryption Mode 設定で暗号化されたコールと暗号化されていないコールの両方に適用されます。

AlwaysOff：暗号化インジケータは画面上に表示されません。これは、すべての Conference Encryption Mode 設定で暗号化されたコールと暗号化されていないコールの両方に適用されます。

例：Video OSD EncryptionIndicator: Auto

Video OSD MissedCallsNotification

まだ応答されていない着信コールがある場合に、OSD（オン スクリーン ディスプレイ）に不在着信通知ダイアログ ボックスを表示するかどうかを設定します。この設定は、ビデオ システムがリモコンと画面上のメニューによって操作される場合にのみ適用されます。タッチ コントローラを使用する場合は、通知ダイアログ ボックスは OSD ではなくタッチ ディスプレイに表示されます。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：OSD には不在着信を示すインジケータが表示されません。この設定は、OSD に表示される内容を完全に制御する必要があるサードパーティ統合には推奨されます。

On：OSD に不在着信の通知が表示されます。

例：Video OSD MissedCallsNotifications: On

Video OSD AutoSelectPresentationSource

プレゼンテーションのソースを自動的に選択するかどうかを決定します。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：プレゼンテーション ソースの自動選択をディセーブルにします。

On：プレゼンテーション ソースの自動選択をイネーブルにします。

例：Video OSD AutoSelectPresentationSource: Off

Video OSD TodaysBookings

この設定は、メイン OSD メニューに今日のシステムの予約を表示するために使用できます。これには、Cisco TelePresence Management Suite (TMS) などの外部予約システムからシステムを予約可能であることが必要です。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：今日の予約を表示しません。

On：このシステムの予約に関する情報を画面に表示します。

例：Video OSD TodaysBookings: Off

Video OSD MyContactsExpanded

ローカルの連絡先を OSD（On Screen Display）の電話帳ダイアログに表示する方法を設定します。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：ローカルの連絡先は、電話帳ダイアログで MyContacts という別のフォルダに配置されます。

On：電話帳内のローカルの連絡先が電話帳ダイアログの最上位に表示されます。

例：Video OSD MyContactsExpanded: Off

Video OSD Output

ビデオ OSD（オン スクリーン ディスプレイ）出力では、スクリーン メニュー、情報およびアイコンを表示するモニタを定義できます。デフォルトでは、OSD は Video OSD Output 1 に接続されたモニタに送られます。画面に OSD が表示されない場合、OSD 出力を再設定する必要があります。リモート コントロールからキー シーケンスを入力するか、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よってこれを実行できます。

リモコン使用：Disconnect キーを押し、* # * # 0 x # と続けます（x はアウトプット 1 ～ 2）。

Web インターフェイス使用：Web ブラウザを開き、コーデックの IP アドレスを入力します。[Advanced Configuration] メニューを開き、[Video OSD Output] に移動して、ビデオ出力を選択します。

コマンドライン インターフェイス使用：コマンドライン インターフェイスを開いて、コーデックに接続します（この方法がよくわからない場合、コーデックの API ガイドを参照してください）。次のコマンドを入力します。xConfiguration Video OSD Output [1..2]（OSD 出力を選択します）

必要なユーザ ロール：ADMIN

値スペース：<1/2>

範囲：HDMI の出力として [1] を選択するか、または DVI-I の出力として [2] を選択します。

例：Video OSD Output: 1

Video OSD InputMethod InputLanguage

コーデックで、画面のメニューでのキリル文字入力をイネーブルにできます。注：xConfiguration Video OSD inputMethod Cyrillic が On に設定されていることが必要です。

必要なユーザ ロール：ADMIN

値スペース：<Latin/Cyrillic>

Latin：リモコンを使用してラテン文字を入力できます（デフォルト）。

Cyrillic：リモコンを使用してキリル文字を入力できます。注：キリル文字の字体を持つ Cisco TelePresence リモート コントロールが必要です。

例：Video OSD InputMethod InputLanguage: Latin

Video OSD InputMethod Cyrillic

画面のメニューでメニュー入力言語をキリル モードに設定します。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：画面のメニューでキリル モードをメニュー入力言語として使用できません。

On：画面のメニューでキリル モードをメニュー入力言語として使用できます。これにより、Video OSD InputMethod InputLanguage の設定が可能になります。

例：Video OSD InputMethod Cyrillic: Off

Video OSD LoginRequired

オン スクリーン ディスプレイ（OSD）へのアクセス前に、システムがユーザのログインを要求するかを決定します。有効にすると、ユーザは自分のユーザ名と自分の PIN を入力する必要があります。ユーザのログイン後、ユーザは自分のロールで許可されているコンフィギュレーション変更とコマンドだけを実行できます。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：OSD へのログインは不要です。

On：ユーザはオン スクリーン ディスプレイ（OSD）にアクセスするためにログインする必要があります。

例：Video OSD LoginRequired: Off

Video AllowWebSnapshots

ローカル入力ソース、リモート サイトおよびプレゼンテーション チャネルで取得されるスナップショットを許可または拒否します。許可された場合、Web インターフェイスの [Call Control] ページは、アイドル中のときもコール中のときもスナップショットを表示します。

注：この機能はデフォルトでディセーブルであり、オン スクリーン ディスプレイ (OSD) から、直接接続されたタッチコントローラから、またはコーデックのシリアル ポートでイネーブルにする必要があります (カメラ ポートと Y 字型ケーブル)。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：Web スナップショットは取得できません。

On：Web スナップショットをキャプチャし、Web インターフェイスに表示できます。

例：Video AllowWebSnapshots: Off

Video Output HDMI [1,2] RGBQuantizationRange

HDMI 出力を使用するデバイスは CEA-861 で定義されている RGB のビデオ量子化範囲のルール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ないため、ディスプレイの完全なイメージを取得するためにこの設定を使用して設定を上書きすることができます。ほとんどの HDMI ディスプレイは完全な量子化範囲を予期するため、デフォルト値は Full に設定されます。

必要なユーザ ロール：ADMIN

値スペース：<Auto/Full/Limited>

Auto：RGB の量子化の範囲は、AVI インフォフレームの RGB 量子化範囲ビット (Q0、Q1) に基づいて自動的に選択されます。AVI インフォフレームが使用できない場合、RGB 量子化範囲は CEA-861-E に従ったビデオ形式に基づいて選択されます。

Full：完全な量子化の範囲。R、G、B の量子化範囲にはすべてのコード値 (0 ～ 255) が含まれます。これは CEA-861-E で規定されています。

Limited：限定された量子化の範囲。極端なコード値を除いた R、G、B の量子化範囲 (16 ～ 235)。これは CEA-861-E で規定されています。

例：Video Output HDMI 1 RGBQuantizationRange: Full

Video Output HDMI [1,2] CEC Mode

HDMI 出力は、Consumer Electronics Control (CEC) をサポートしています。オンに設定し (デフォルトはオフ)、HDMI 出力に接続されたモニタが CEC 互換であって、CEC が設定されている場合、システムがスタンバイに入るときシステムは CEC を使用してモニタをスタンバイに設定します。同様に、システムがスタンバイから復帰するとき、システムはモニタを起動します。CEC については、製造業者によって異なるマーケティング名称が使用されていることに注意してください。例：Anynet+ (Samsung)、Aquos Link (シャープ)、BRAVIA Sync (Sony)、HDMI-CEC (日立)、Kuro Link (パイオニア)、CE-Link および Regza Link (東芝)、RIHD (オンキヨー)、HDAVI Control、EZ-Sync、VIERA Link (Panasonic)、EasyLink (Philips)、NetCommand for HDMI (三菱)。

必要なユーザ ロール：ADMIN

値スペース：<Off/On>

Off：CEC 制御をディセーブルにします。

On：CEC 制御をイネーブルにします。

例：Video Output HDMI 1 CEC Mode: Off

Video Output HDMI [1,2] MonitorRole

HDMI モニタ ロールは、ビデオ出力 HDMI コネクタに接続されたモニタにどのビデオ ストリームを表示するかを示します。

必要なユーザ ロール：ADMIN

値スペース：<First/Second/PresentationOnly/Recorder>

First/Second：マルチ モニタ設定でのモニタの役割を定義します。シングル モニタ設定では、First と Second との違いはありません。

PresentationOnly：アクティブな場合プレゼンテーション ビデオ ストリームを表示し、他のものは表示しません。

Recorder：ローカル メイン ビデオを含むすべての参加者を表示します。アクティブであれば、プレゼンテーション も表示されます。

例：Video Output HDMI 1 MonitorRole: First

Video Output HDMI [1,2] OverscanLevel

一部の TV やその他のモニタは、システムのビデオ出力で送信されるイメージ全体を表示せず、イメージの外側部分をカットする場合があります。この場合、システムがビデオ解像度の外側部分を使用しないようにするためにこの設定を使用できます。この場合、ビデオと OSD メニューの両方が拡大縮小されます。

必要なユーザ ロール：ADMIN

値スペース：<Medium/High/None>

Medium：システムは出力解像度の外側 3 % を使用しません。

High：システムは出力解像度の外側 6 % を使用しません。

None：システムは出力解像度すべてを使用します。

例：Video Output HDMI 1 OverscanLevel: None

Video Output HDMI [1,2] Resolution

ビデオ出力 HDMI コネクタに接続されたモニタの優先解像度を選択します。これはモニタに解像度を強制します。

必要なユーザ ロール：ADMIN

値スペース：<Auto/640_480_60/800_600_60/1024_768_60/1280_1024_60/1280_720_50/1280_720_60/1920_1080_50/1920_1080_60/1280_768_60/1360_768_60/1366_768_60/1600_1200_60/1680_1050_60/1920_1200_60>

Auto：システムは接続されたモニタのネゴシエーションに基づいて自動的に最適な解像度の設定を試行します。

範囲：640x480@60p、800x600@60p、1024x768@60p、1280x1024@60p、1280x720@50p、1280x720@60p、1920x1080@50p、1920x1080@60p、1280x768@60p、1360x768@60p、1366x768@60p、1600x1200@60p、1680x1050@60p、1920x1200@60p

例：Video Output HDMI 1 Resolution: Auto

Video Wallpaper

アイドル状態のときのビデオ画面の背景画像（壁紙）を選択します。

必要なユーザ ロール：USER

値スペース：<None/Custom/Growing/Summersky/Waves>

None：画面に背景画像がありません。背景は黒です。

Custom：システムに保存されているカスタムの壁紙を、画面の背景画像として使用します。デフォルトでは、保存されたカスタムの壁紙はなく、背景は黒です。Web インターフェイスを使用してシステムにカスタムの壁紙をアップロードできます。サポートされる最大解像度は 1920x1200 です。

Summersky、*Growing*、*Waves*：選択した背景画像が画面に表示されます。

例：Video Wallpaper: Summersky

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。

4 章

パスワードの設定

システム パスワードの設定

システムの Web インターフェイスやコマンドライン インターフェイスにサインインするには、ユーザ名とパスワードが必要です。

ビデオ システムは完全なクレデンシャルを持つデフォルトのユーザ アカウントとともに提供されます。ユーザ名は *admin* であり、初期状態ではデフォルト ユーザにパスワードは設定されていません。



admin ユーザおよび同様のクレデンシャルを持つその他のユーザに対してパスワードを設定し、システム設定へのアクセスを制限することを強く推奨します。

パスワードのコピーを安全な場所に保管してください。パスワードを忘れた場合は、ユニットを工場出荷時設定にリセットする必要があります。

他のユーザ アカウント

ビデオ システムに任意の数のユーザ アカウントを作成できます。

ユーザ アカウントの作成と管理の方法に関する詳細情報は、▶ [「ユーザ管理」](#) の項で確認できます。

自分のシステム パスワードの変更

システム パスワードを変更するには、次の手順に従います。

パスワードが現在設定されていない場合は、[\[現在のパスワード \(Current password\)\]](#) を空白の状態で使用します。パスワードを削除するには、[\[新しいパスワード \(New password\)\]](#) フィールドを空白のままにします。

1. ユーザ名と現在のパスワードを使用して Web インターフェイスにサインインします。
2. 右上隅のユーザ名をクリックして、ドロップ ダウン メニューの [\[Change password\]](#) を選択します。
3. [\[現在のパスワード \(Current password\)\]](#) と [\[新しいパスワード \(New password\)\]](#) の入力フィールドにそれぞれパスワードを入力後、新しいパスワードを再入力します。

パスワードの形式は、0 ～ 64 文字の文字列です。

4. [\[パスワード変更 \(Change Password\)\]](#) をクリックします。

他のユーザのシステム パスワードの変更

管理者権限を持っている場合は、次の手順を実行して、すべてのユーザのパスワードを変更することができます。

1. ユーザ名とパスワードを使用して Web インターフェイスにサインインします。
2. [\[Maintenance\]](#) タブに移動し、[\[User administration\]](#) を選択します。
3. 対象のユーザをリストから選択します。
4. 新しいパスワードと PIN コードを入力します。
5. [\[保存 \(Save\)\]](#) をクリックします。

メニュー パスワードの設定

ビデオ会議システムの初期設定では、メニュー パスワードが設定されていないため、リモコンまたはタッチ コントローラを使用して誰でも [管理者設定 (Administrator Settings)] メニューにアクセスできます。



管理者設定はシステムの動作に大きく影響するので、メニュー パスワードを設定することを強く推奨します。

メニュー パスワードの設定には Web インターフェイスまたはリモコンを使用する必要があります。タッチ コントローラは使用できません。

Web インターフェイスからのメニュー パスワードの設定

1. ユーザ名と現在のパスワードを使用して Web インターフェイスにサイン インします。
2. [\[Configuration\]](#) > [\[System Configuration\]](#) に移動します。
3. [\[Set/Change Administrator Settings menu password\]](#) をクリックして、メニュー パスワード ダイアログを開きます。
4. 入力フィールドにパスワードを入力します。
5. [\[Save\]](#) をクリックしてパスワードを設定 / 変更します。



システムの IP アドレスを特定するには、タッチ コントローラで [\[設定 \(Settings\) \(X\)\]](#) > [\[システム情報 \(System information\)\]](#) をタップするか、リモコンや画面上のメニューを使用して [\[ホーム \(Home\)\]](#) > [\[設定 \(Settings\)\]](#) > [\[システム情報 \(System information\)\]](#) に進みます。

リモコンを使用したメニュー パスワードの設定

1. 画面上のメニューから、[\[ホーム \(Home\)\]](#) > [\[設定 \(Settings\)\]](#) > [\[管理者設定 \(Administrator settings\)\]](#) > [\[メニュー パスワードの設定 \(Set menu password\)\]](#) の順に移動します。

パスワードの形式は、0 ~ 255 文字の文字列です。

パスワードを非アクティブ化するには、パスワード入力フィールドを空白にします。

2. 入力フィールドにメニューのパスワードを入力します。入力したパスワードは表示されずに、各文字はアスタリスク (*) に置き換えられます。

リモート コントロールの # キーを押すと、小文字、大文字、数字 (abc/ABC/123) を切り替えます。

3. 変更内容を保存するには [\[保存 \(Save\)\]](#) を選択し、保存しない場合は [\[キャンセル \(Cancel\)\]](#) を選択します。
4. [\[ホーム \(Home\)\]](#) () を押して終了します。

ルート パスワードの設定

ルート ユーザのパスワードを設定して、ビデオ システムのファイル システムを保護することができます。

ルート ユーザは、デフォルトではディセーブルになっています。ルート ユーザをイネーブルにして、ルートのパスワードを設定するには、コマンドライン インターフェイスを使用する必要があります。

root ユーザのアクティブ化とパスワードの設定

ルート ユーザをアクティブにして、パスワードを設定するには、次の手順を実行します。

1. ネットワークまたはシステムのシリアル データ ポート（使用可能な場合）経由でシステムに接続し、コマンドライン インタフェース（SSH または Telnet）を開きます。
2. ユーザ名とパスワードを使用してシステムにサインインします。このユーザには管理者権限が必要です。
3. 次のコマンドを入力します。

```
systemtools rootsettings on <password>
```



ルートのパスワードをシステム（admin）のパスワードと同じにすることはできません。

付録

モニタについて

メイン モニタへの接続

メイン モニタは、ビデオ出力 HDMI 1（メイン モニタのデフォルト コネクタ）または HDMI 2* に接続できます。

コーデックはモニタのネイティブ解像度を識別し、可能であればこれを出力します。通常はこれにより、接続されたモニタの最適な画像が提供されます。自動処理に失敗した場合、[\[ビデオ\(Video\)\] > \[出力\(Output\)\] > \[HDMI n\] > \[解像度 \(Resolution\)\]](#) 設定を使用して解像度を手動で選択しなければなりません。

HDMI 1 への接続

メイン モニタを HDMI 1 に接続すると、画面上(OSD - オン スクリーン ディスプレイ) のメニュー、アイコン、その他の情報は自動的にモニタに表示されます。これは、HDMI 1 がコーデックのデフォルトのビデオ出力であるためです。

HDMI 2 への接続

メイン モニタを HDMI 2* 出力に接続すると、メニュー、アイコン、その他の情報は自動的に画面上に表示されません。OSD を選択された出力に移す必要があります。



HDMI 2 には音声がありません。

Codec C20 のビデオ出力



HDMI 1（メイン モニタのデフォルト コネクタ）

HDMI 2*

OSD の移動

リモコンまたは Web インターフェイスを使用して OSD 出力を移すことができます。

リモート コントロール

メイン モニタに接続されているコネクタを特定し、リモコンで次のキー シーケンスを実行します。

- [Disconnect * # * # 0 x #](#) x=1 (HDMI 1) x=2 (HDMI 2)

例：HDMI 2 を OSD の出力として設定。

- * - # - * - # - 0 - 2 - #

Web インターフェイス

[System Configuration] ページを開きます。[\[Video\] > \[OSD\] > \[Output\]](#) に進み、メイン モニタのビデオ出力コネクタを選択します。

デュアル モニタ



Dual Display オプションが必要です。

デュアル モニタの設定を実行したい場合、メイン モニタをビデオ出力 HDMI 1 に接続し、第 2 モニタをコーデックのビデオ出力 HDMI 2 に接続します。

デュアル モニタの設定

レイアウトを 2 台のモニタに分散するには、[詳細設定 (Advanced configuration)] (画面上のメニュー) に進みます。または [System Configuration] ページ (Web インタフェース) を開きます。[\[ビデオ\(Video\)\] > \[モニタ \(Monitors\)\]](#) に移動し、[デュアル (Dual)] を選択します。

* HDMI 2 の使用には Dual Display オプションが必要です。

Cisco TelePresence Touch 8" コントローラへの接続

Cisco TelePresence Touch 8" コントローラはリモコンと画面メニューに代わる装置です。

タッチ コントローラがコーデックに接続されている場合、リモコンは使用できません。リモコンを使用するには、タッチ コントローラの接続を解除（ペア解除）しなければなりません。

Touch 8" は、ソフトウェア バージョン TC4.1 以降を実行する C シリーズのコーデックで使用できます。

LAN ソケット（イーサネット）へ

電源ソケットへ

コーデックのアドレス

タッチ コントローラの接続

タッチ コントローラは LAN を介してコーデックに接続する必要があります。接続は、上の図のように、同梱の電源アダプタで行います。

接続できるように、コーデックの [\[NetworkServices\]](#) > [\[SSH\]](#) > [\[Mode\]](#) 設定が [On] になっていることを確認してください。

タッチ コントローラをコーデックに関連付ける処理をペア化と呼びます。コーデックは、スイッチをオンにしてから 30 分間のみペア化が可能であることをシグナリングしていることに注意してください。

タッチ コントローラとビデオ システムを同じサブネット上に保つことを推奨します。

タッチ コントローラの設定

タッチ コントローラが電源に接続されると、設定手順が始まります。画面に表示される指示に従います。

コーデックがタッチ コントローラに表示される使用可能なコーデックのリストにない場合、その IP アドレスを入力してコーデックを手動で選択できます。

タッチ コントローラにソフトウェアのアップグレードが必要な場合は、設定手順の一部で新しいソフトウェアがコーデックからダウンロードされ、自動的にユニットにインストールされます。タッチ コントローラはアップグレード後に再起動します。

コーデック アドレスが上部バナーに表示されているかチェックすれば、タッチ コントローラがコーデックに正常にペア化されていることを確認できます。

タッチ インストールの詳細情報は、シスコの Web サイトにある『[Cisco TelePresence Touch 8 inch Installation Guide](#)』を参照してください。

* この設定は、画面上のメニュー（リモコン）の [詳細設定（Advanced Configuration）] または Web インターフェイスの [System Configuration] ページにあります。

最適鮮明度プロファイル

理想的な光の条件下で、帯域幅（コール レート）の要件を大幅に減らすことができます。

最適鮮明度プロファイルは、会議室の光の状態とビデオ入力（カメラ）の品質に合わせる必要があります。光の状態とビデオ入力が優れていれば、プロファイルも向上します。このとき、良い光の条件で、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。

一般に、最適鮮明度プロファイルを Normal に設定することが推奨されます。ただし、光の条件が良い場合は、プロファイルを決定する前にさまざまな Optimal Definition Profile 設定でエンドポイントをテストすることを推奨します。

Web インターフェイスの [System Configuration] に進み、[\[Video\] > \[Input\] > \[Source \[1..n\]\] > \[OptimalDefinition\] > \[Profile\]](#) 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。

解像度のしきい値を設定して、60 fps でのビデオ送信を可能にするタイミングを指定できます。このしきい値より低いすべての解像度では、最大送信フレーム レートは 30 fps とします。それより高い解像度では、使用可能な帯域幅が十分であれば 60 fps にすることが可能です。

Web インターフェイスの [System Configuration] に進み、[\[Video\] > \[Input\] > \[Source \[1..n\]\] > \[OptimalDefinition\] > \[Threshold60fps\]](#) に移動して、しきい値を設定します。

最適鮮明度設定を有効にするには、ビデオ入力の品質設定を Motion に設定する必要があります。ビデオ入力の品質を 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 インターフェイスの [System Configuration] に進み、[\[Video\] > \[Input\] > \[Source \[1..n\]\] > \[Quality\]](#) に移動して、ビデオ品質パラメータを Motion に設定します。

▶ 「システム設定」の章で、ビデオ設定の詳細情報を確認できます。



High

通常、専用のビデオ会議室で使用されます。優れた全体的なエクスペリエンスを実現するには、非常に良い光の条件と高品質のビデオ入力が必要です。

理想的な条件下では、帯域幅要件が Normal と比べて最大 50% 削減できます。



Medium

通常は、安定した良い光の条件と高品質のビデオ入力を備えた会場で使用されます。

帯域幅要件は Normal と比べて最大 25% 削減できます。



Normal

この設定は、室内の光が中程度か不十分であるオフィス環境でよく使用されます。

さまざまな最適鮮明度プロファイル、コール レート、フレーム レートで使用される一般的な解像度

フレーム レート	最適 鮮明度 プロファイル	コール レート						
		256 kbps	768 kbps	1152 kbps	1472 kbps	2560 kbps	4 Mbps	6 Mbps
30 fps	Normal	512×288	1024×576	1280×720	1280×720	1920×1080	1920×1080	1920×1080
	Medium	640×360	1280×720	1280×720	1280×720	1920×1080	1920×1080	1920×1080
	High	768×448	1280×720	1280×720	1920×1080	1920×1080	1920×1080	1920×1080
60 fps	Normal	256×144	512×288	768×448	1024×576	1280×720	1280×720	1280×720
	Medium	256×144	768×448	1024×576	1024×576	1280×720	1280×720	1280×720
	High	512×288	1024×576	1280×720	1280×720	1280×720	1280×720	1280×720

ClearPath : パケット損失の復元

ClearPath により、エラーを起こしやすい環境でビデオ システムを使用する場合の経験品質を向上させる、高度なパケット損失復元メカニズムが導入されます。

お使いのビデオ システムで ClearPath をイネーブルにしておくことを推奨します。

[詳細設定 (Advanced configuration)] (画面上のメニュー) に進むか、[System Configuration] ページ (Web インターフェイス) を開きます。

- ・ [\[Conference 1\]](#) > [\[PacketLossResilience\]](#) > [\[Mode\]](#) に移動します。

ClearPath をディセーブルにするには [Off] を選択し、ClearPath をイネーブルにするには [On] を選択します。

Cisco TelePresence C シリーズ コーデックに接続するスピーカー システムの要件

シスコは、TelePresence エンドポイントでのカメラからスクリーンへの遅延を最小限にするために、多くの作業を行っています。

新しいコンシューマ TV には通常、「モーション フロー」または同様のテクノロジーが装備されており、標準フレームの間に新しいビデオ フレームを挿入して、よりスムーズなイメージが作成されるようにしています。この処理には時間がかかるため、リップ同期を維持するために、TV は音声を遅らせて音声とビデオが同時に受信されるようにします。

シスコのエンドポイントのエコー キャンセラは、このような遅延を最大 30 ミリ秒にまで処理できます。多くの顧客の TV は、リアル タイムのビデオ通信用に作られていないため、遅延が 30 ミリ秒よりも長くなる場合があります。

C シリーズのコーデックとともにこのような TV を使用する場合、さらなる遅延を生じさせる「モーション フロー」、「ナチュラル モーション」またはその他のビデオ処理を無効にすることをお勧めします。

また、一部のコンシューマ TV は、TV エクスペリエンスを向上させる「仮想サラウンド」効果や「ダイナミック コンプレッション」などの高度な音声処理をサポートしています。このような処理はアコースティック エコー キャンセラの不具合を引き起こすため、無効にする必要があります。

一部のモニタには「ゲーム モード」と呼ばれる設定が装備されています。このモードは、応答時間を短縮するために設計されており、通常は遅延を軽減できます。

Codec C20 : 物理インターフェイス

前面パネル LED

コーデックの前面の LED はコーデックの状態を示します。

- LED が **off** であれば、コーデックはオフになっています。
- LED はコーデックのブート中およびシャット ダウン中に**緑色**に点滅します。
- LED は赤外線 (IR) ポートがアクティブ化されると**緑色**に点滅します。これは、リモコンを使用している場合に動作します。
- LED はコーデックがオンになっている場合と、スタンバイ モードまたはプレゼンテーション モードの場合に**緑色**に点灯します。
- LED が**赤色**の場合、エラーが発生したことを示します。



Codec C20 : 物理インターフェイス (続き)

背面パネル

基本設定で使用されるコネクタは**太字**で強調表示されます。



マイク 1-2

ミニ ジャック 3.5mm 4 極コネクタ。メイン コネクタである Mic 1 に接続します。

オーディオ入力

RCA ソケット、モノラル混合。PC および VCR や DVD プレーヤーなどの外部再生デバイスに接続するときに使用。

オーディオ出力

RCA ソケット、モノラル。ローカル スピーカー システムへ接続するときに使用。

ネットワーク コネクタ

イーサネット インターフェイス、1 x 10Mb/100Mb/1 ギガビット イーサネット LAN (RJ-45 ジャック) インターフェイス。

USB

現在は使用していません。

カメラ制御ポート

VISCA ™ * プロトコルを使用した、電源およびカメラ制御 (パン、チルト、ズーム) のためのカメラ制御 (RS-232) ポート。ピン 4 はカメラ制御ポートのメイン カメラに 12 V DC/1 A を提供します。

PC 用 DVI-I 入力

DVI-I ソケット、PC のプレゼンテーション用デジタル / アナログ ビデオ入力。

カメラ用 HDMI 入力

HDMI ソケット、カメラ用デジタル ビデオ入力。

メイン モニタ用 HDMI 出力

メイン モニタ用 HDMI ソケット、デジタル ビデオおよび音声出力。

第 2 モニタ用 HDMI 出力

HDMI ソケット、第 2 モニタ用デジタル ビデオ出力。

電源ソケット

電源ソケットは外部アダプタから +12V/5A (最大) を受け入れます。

外部アダプタは 100/240V 50/60Hz を受け入れ、最大負荷は 75W です。

電源スイッチ

電源スイッチ (ボタン) は背面にあります。

- ・ ボタンを押すとコーデックが起動します。
- ・ ボタンを 1 秒間押し続けると、コーデックがシャット ダウンされます。
- ・ ボタンを 7 秒間押し続けると、コーデックが強制的にシャット ダウンされます。

ケンジントン ロック

ケンジントン ロックを使用して、コーデックの移動を防止したり、盗難を防止することができます。

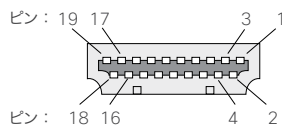
*VISCA ™ は Sony Corporation の商標です。

ピン配列方法

このページでは C20 のピン配列方法の概要を示します。

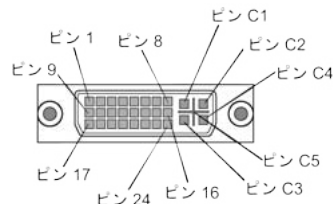
HDMI のピン配列

ソケットの外観図

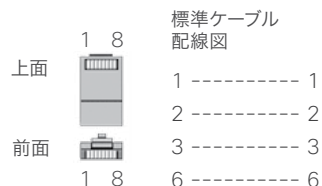


DVI-I のピン配列

ソケットの外観図

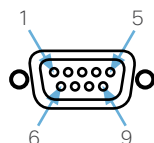


RJ-45 コネクタのピン配列

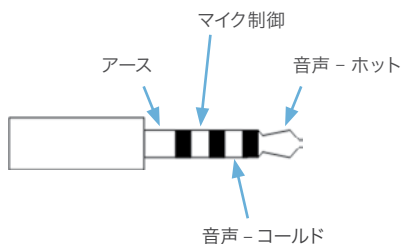


RS232 9 ピン D-SUB ピン配列

ソケットの外観図



マイク、3.5 mm ミニ ジャック、4 極



RCA のピン配列

ソケットの外観図



ピン配列：カメラのケーブル

信号名	RJ-45 ピン		D-SUB ピン
+12V DC	1	ツイスト ペア	4
GND	2		5
RX	3	ツイスト ペア	2
TX	6		3
NC	4	ツイスト ペア	1
NC	5		6
GND	7	ツイスト ペア	5
+12V DC	8		4

HDMI のピン配列

ピン	割り当て	ピン	割り当て
1	T.M.D.S. データ 2+	11	T.M.D.S. クロック シールド
2	T.M.D.S. データ 2 シールド	12	T.M.D.S. クロック
3	T.M.D.S. データ 2-	13	CEC
4	T.M.D.S. データ 1	14	予約済み (N.C. オン デバイス)
5	T.M.D.S. データ 1 シールド	15	SCL
6	T.M.D.S. データ 1-	16	SDA
7	T.M.D.S. データ 0	17	DDC/CEC アース
8	T.M.D.S. データ 0 シールド	18	+5 V の電力 (最大 50 mA)
9	T.M.D.S. データ 0-	19	ホット プラグ検出
10	T.M.D.S. クロック +		

ピン配列：VISCA™カメラ制御

RJ11、8 ピン シールド付きモジュラ ジャック

ピン	信号名
8	+12V (ディジタイゼーション接続した場合、プレゼンス 2.8mA の電流源)
7	GND
6	TXD (出)
5	NC (接続なし)
4	NC (接続なし)
3	RXD (入)
2	GND
1	+12V

Codec C20 のオーディオ コネクタ

	マイクの入力ジャック	RCA ライン入力	RCA ライン出力
コネクタのピン配列	Tip = ホット Ring 1 = コールド Ring 2 = マイク control シールド = GND	ピン = シグナル シールド = GND	ピン = シグナル シールド = GND
信号タイプ	Balanced	Unbalanced	Unbalanced
コネクタ (コーデック)	ミニ ジャック 3.5mm	メス RCA/phono	メス RCA/phono
入力インピーダンス	1.5kOhm/leg	18k Ω	
出力インピーダンス			100 Ω
最大入力レベル	-18.3dBu +/-2 dB	9.0dBu +/-2 dB	
最大出力レベル			8.2dBu +/-2 dB
ファントム電源	12V +/-1V		
ファントム電源抵抗のピン「tip」	1.7kOhm		
ファントム電源抵抗のピン「ring 1」	1.7kOhm		
周波数応答	20Hz-20kHz +/-1 dB	20Hz-20kHz +/-1 dB	20Hz-20kHz +/-1 dB
信号対雑音比	-85 dB	-95 dB	-95 dB

Quick Set C20 と PrecisionHD 1080p 4x カメラとの ケーブル構成

図は、モニター、PC、PrecisionHD 1080p 4x カメラ、マイク、スピーカー（該当する場合）、LAN、線間電圧を Codec C20 に接続する場合の基本設定を示します。

Quick Set C20 の以前の出荷バージョンでは、PrecisionHD 1080p 4x カメラ（PrecisionHD 1080p 4x* カメラ）の暫定バージョンが同梱されていました。



ビデオ コールでシステムを使用するには、オレンジ色のソケットをすべて接続する必要があります。



他の機器を接続または接続解除するときは必ず、コーデックのスイッチをオフにして線間電圧から切断する必要があります。



Quick Set C20 と PrecisionHD 1080p 12x カメラとの ケーブル構成

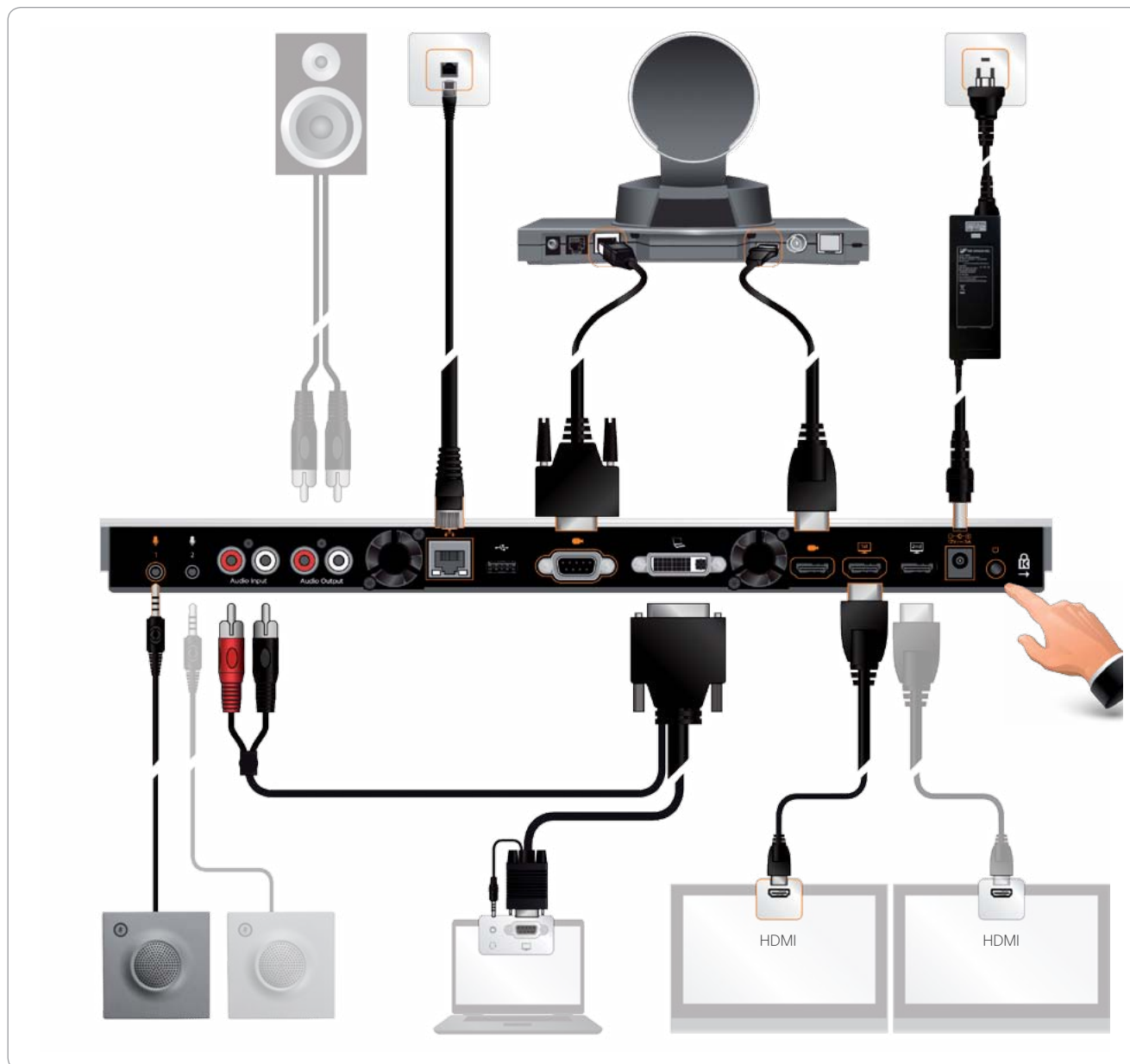
図は、モニタ、PC、PrecisionHD 1080p 12x カメラ、マイク、スピーカー（該当する場合）、LAN、線間電圧を Codec C20 に接続する場合の基本設定を示します。



ビデオ コールでシステムを使用するには、オレンジ色のソケットをすべて接続する必要があります。



他の機器を接続または接続解除するときは必ず、コーデックのスイッチをオフにして線間電圧から切断する必要があります。



Profile 42" 用の DNAM

DNAM (Digital Natural Audio Module) は、特別に設計された 2 つの異なるモジュールで構築されます。それらは増幅器とスピーカー キャビネットです。

DNAM スピーカー

3 ウェイの中央スピーカー システム

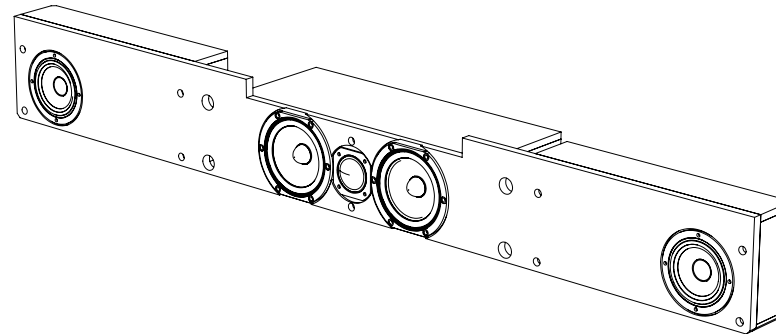
- ・ 周波数範囲 50 Hz - 20 kHz
- ・ 2 × 100 mm 低中音域スピーカー、公称 8 Ω、優良品質 (SEAS Prestige シリーズ)
- ・ 1 × 25 mm ドーム ツィーター、公称 6 Ω、優良品質
- ・ DNAM の増幅器から受信した音声信号をデジタルフィルタリング
- ・ すべてのスピーカーで最大電力 70 ワットを長時間持続
- ・ 密閉型 MDF スピーカー キャビネット

統合ステレオ スピーカ

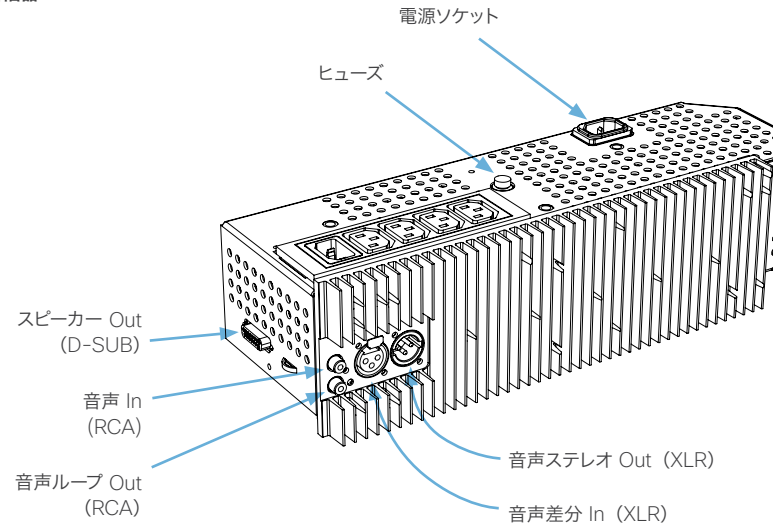
両方の側が

- ・ 1 × 90 mm の全音域スピーカー、公称 8 Ω、優良品質
- ・ 周波数範囲 70 Hz - 20 kHz
- ・ 密閉型 MDF スピーカー キャビネット

DNAM スピーカー



DNAM 増幅器



DNAM 増幅器

- ・ 5 × 50 ワットの連続的な平均出力電力
- ・ 音声 (20 Hz - 20 kHz) の完全な周波数範囲
- ・ 音声細部の明瞭さを最適にするための、すべてのチャネルのデジタル シグナル処理とフィルタリング
- ・ 中央チャネルのデジタル クロスオーバー フィルタリング
- ・ In/Out

音声 In : SPDIF (ステレオ) または同じコネクタを使用してアナログ (モノラル)

音声ループ Out : 入力から直接ライン出力。SPDIF In であっても常にアナログ

音声差分 In : メス XLR、ピン割り当て : 1 - GND、2 - 信号 (+), 3 - 信号 (-)

音声ステレオ Out : オス XLR、共通 GND 設定

スピーカー Out : メス D-SUB 15 ピン

- ・ ヒューズ 2A 250V 低速、5 × 20 mm、リトルヒューズ タイプ 215002。



常にこのタイプのヒューズを使用してください。異なるタイプを使用すると、重大なハードウェア障害が発生する可能性があります。

スペアのヒューズ

Profile システムには 2 つのスペア DNAM ヒューズが支柱に装着されています。

ヒューズを交換する場合は、ヒューズやヒューズ ホルダーを破損しないよう注意してください。

- ・ ヒューズ ホルダーを少し内側に押し、反時計回りに回してヒューズを取り外します。
- ・ ヒューズやヒューズ ホルダーを再度挿入する場合は、少し内側に押し、ホルダーをロックされるまで注意深く時計回りに回します。

工場出荷時設定へのリセット

工場出荷時のデフォルト設定にビデオ システムをリセットしなければならない場合は、タッチ コントローラまたは Web インターフェイスを使用することを推奨します。これらの方法のいずれも使用できない場合は、ビデオ システムの電源ボタンを使用できます。

リモコンと画面上のメニューでは出荷時の状態へのリセットを行えません。

ビデオ システムを出荷時の状態にリセットすると、以下のことが行われます。

- ・ コール ログが削除されます。
- ・ パスワードがデフォルト値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、カスタマイズされた背景、証明書、お気に入りリスト（個人アドレス帳）および非アクティブのソフトウェア イメージが含まれますが、それらだけに限定されません。
- ・ リリース キーとオプション キーは影響を受けません。
- ・ システムはリセット後に自動的に再起動されます。



工場出荷時設定にリセットすると元に戻すことはできません。



工場出荷時設定にリセットする前に現在の設定をバックアップした場合は、Web ブラウザを開き、次の手順で操作します。

- ・ ビデオ システムの IP アドレスをアドレス バーに入力し、サインインします。
- ・ [\[Maintenance\]](#) > [\[Backup and Restore\]](#) に移動します。
- ・ [\[Take backup\]](#) をクリックし、指示に従ってファイルをコンピュータに保存します。

タッチ

1. スリープ モードになっている場合は、タッチ スクリーンを静かにタップします。
2. [\[設定 \(Settings\) \(⚙️\)\]](#) > [\[管理者設定 \(Administrator Settings\)\]](#) > [\[リセット \(Reset\)\]](#) に移動します。
3. [\[初期設定へのリセット \(Factory Reset\)\]](#) ボタンを押します。

システムが工場出荷時設定へと戻され、自動的に再起動されます。これには数分かかることがあります。

システムは再起動後、メイン画面に通知を表示して、工場出荷時設定にリセットされたことを確認します。通知は約 10 秒後に非表示になります。

Web



タッチ コントローラの [\[設定 \(Settings\) \(⚙️\)\]](#) > [\[システム情報 \(System Information\)\]](#) をタップして、システムの IP アドレス (IPv4 または IPv6) を特定します。

1. 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。
2. [\[Maintenance\]](#) > [\[Factory Reset\]](#) に移動します。
3. 表示された情報をよく確認してから、[\[Perform a factory reset\]](#) をクリックします。
4. 工場出荷時設定へのリセットを実行することを確認して、赤い [\[Reset\]](#) ボタンをクリックします。

システムが工場出荷時設定へと戻され、自動的に再起動されます。これには数分かかることがあります。

システムは再起動後、メイン画面に通知を表示して、工場出荷時設定にリセットされたことを確認します。通知は約 10 秒後に非表示になります。

電源ボタン

1. システムがシャット ダウンし、電源 LED がオフになるまで電源ボタンを押し続け、システムの電源を切ります。
2. LED がゆっくり点滅しはじめるまで電源ボタンを押し続けます（約 10 秒間）。その後、ボタンを放します。
3. LED が点滅しはじめてから 4 秒以内に、電源ボタンを 2 回押します。ここで LED がより速く点滅します。システムが工場出荷時設定へと戻され、自動的に再起動されます。これには数分かかることがあります。

システムは再起動後、メイン画面に通知を表示して、工場出荷時設定にリセットされたことを確認します。通知は約 10 秒後に非表示になります。



- 4 秒以内に電源ボタンを 2 回押すのに失敗すると、システムは工場出荷時設定に戻されず、確認メッセージは表示されません。この場合、手順 1 に戻り、再試行してください。



正面図



背面図

電源ボタン

タッチ 8" コントローラの工場出荷時設定へのリセット

タッチ 8" コントローラを工場出荷時設定にリセットするには、新しいメッセージ インジケータやミュート ボタンを使用する必要があります。

タッチ コントローラを工場出荷時設定にリセットすると、ログが削除され、設定とペア化情報が失われます。

タッチ コントローラはリセット後に再起動され、ビデオ システムに改めてペア化する必要があります。ペア化に成功すると、ビデオ システムから新しい設定を受け取ります。



工場出荷時設定にリセットすると元に戻すことはできません。

タッチ

1. 新しいメッセージ インジケータやミュート ボタンの位置を確認します。
新しいメッセージ インジケータは少し見分けにくいですが、感嘆符の付いたボタンです。



2. 新しいメッセージ インジケータを押し、点灯するまで押し続けます（約 10 秒）。
3. ミュート ボタンを 2 回押します。
タッチ コントローラが工場出荷時設定へと自動的に戻され、再起動されます。

技術仕様

Quick Set C20

セットの同梱物：

- Codec C20、PrecisionHD 1080p 4x または 12x カメラ、
- テーブル マイクروفोन 20 基、リモコン、ケーブルおよび電源

BANDWIDTH

- H.323/SIP、最大 6 Mbps ポイントツーポイント

ファイアウォール トラバーサル

- Cisco TelePresence Expressway テクノロジー
- H.460.18、H.460.19 ファイアウォール トラバーサル

VIDEO の標準

- H.261、H.263、H.263+、H.264

VIDEO の機能

- ネイティブ 16:9 ワイド画面
- 高度な画面レイアウト
- インテリジェント ビデオ管理
- ローカル自動レイアウト

ビデオ入力 (2 系統)

1 つの HDMI 入力。サポートされる形式：

- 1920 × 1080@60 fps (1080p60)
- 1920 × 1080@50 fps (1080p50)
- 1920 × 1080@30 fps Hz (1080p30)
- 1920 × 1080@25 fps (1080p25)
- 1280 × 720@60 fps (720p60)
- 1280 × 720@50 fps (720p50)
- 640 × 480@60 fps (480p60)
- 800 × 600@60 fps (SVGA)
- 1024 × 768@60, 70, 75, 85 fps (XGA)
- 1280 × 1024@60, 75 fps (SXGA)

1 つの DVI-I 入力。サポートされる形式：

アナログ (VGA)

- 1920 × 1080@60 Hz (1080p60)
- 1280 × 720@60 Hz (720p60)
- 1600 × 1200@60 Hz (UXGA)
- 1280 × 1024@60, 75 Hz (SXGA)
- 1280 × 960@60 Hz
- 1024 × 768@60, 70, 75, 85 Hz (XGA)
- 1920 × 1200@50 Hz (WUXGA)
- 1680 × 1050@60 Hz (WSXGA+)

- 1440 × 900@60 Hz (WXGA+)
- 1280 × 800@60 Hz (WXGA)
- 1280 × 768@60 Hz (WXGA)

デジタル (DVI-D)：

- HDMI と同様。above.

- Extended Display Identification Data (EDID)

ビデオ出力 (2 系統)

2 つの HDMI 出力。サポートされる形式：

- 1920 × 1080@60 fps (1080p60)
- 1280 × 720@60 fps (720p60)
- 1366 × 768@60 fps (WXGA)
- 1280 × 768@60 fps (WXGA)
- 1280 × 1024@60 fps (SXGA)
- 1024 × 768@60 fps (XGA)
- 800 × 600@60 fps (SVGA)
- 640 × 480@60 fps (VGA)

- VESA モニタ電源管理
- Extended Display Identification Data (EDID)

ライブ ビデオ解像度 (ENCODE/DECODE)

- 176 × 144@30, 60 fps (QCIF)
- 352 × 288@30, 60 fps (CIF)
- 512 × 288@30, 60 fps (w288p)
- 576 × 448@30, 60 fps (448p)
- 768 × 448@30, 60 fps (w448p)
- 704 × 576@30, 60 fps (4CIF)
- 1024 × 576@30, 60 fps (w576p)
- 640 × 480@30, 60 fps (VGA)
- 800 × 600@30, 60 fps (SVGA)
- 1024 × 768@30 fps (XGA)
- 1280 × 768@30 fps (WXGA)
- 1280 × 720@30 fps (720p30)
- 1280 × 720@60 fps (720p60)*
- 1920 × 1080@30 fps (1080p30)*

- 768 kbps から 720p30
- 1152 kbps* から 720p60
- 1472 kbps* から 1080p30

AUDIO の標準

- G.711、G.722、G.722.1、G.729AB (SIP コール専用)、
- 64 kbps AAC-LD

AUDIO の機能

- 高品質 20 kHz
- 1 台のアコースティック エコー キャンセラ
- オートゲイン コントロール (AGC)
- オートノイズ リダクション
- アクティブ リップ シンク

音声入力 (4 系統)

- マイク 2 本、4 ピン ミニ ジャック
- 2 RCA/ フォノ (モノラル混合)

音声出力 (3 系統)

- 2 RCA/ フォノ (デュアル モノラル)
- 1 HDMI (デジタル メイン音声)

DUAL 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
- WXGA (1280 × 768) までの解像度をサポート
- デュアル ストリームがアクティブの場合、最大のメイン ビデオ ストリームは 30fps で 720p

マルチポイントのサポート

- Cisco TelePresence Multiway のサポート (Cisco TelePresence Video Communication Server [Cisco VCS] および Cisco TelePresence MCU が必要)
- Cisco Telepresence Multipoint Switch (CTMS) でホストされたマルチポイント会議にネイティブで参加する機能

プロトコル

- H.323
- SIP
- ISDN (Cisco TelePresence ISDN リンクが必要)

EMBEDDED 暗号化

- H.323/SIP ポイントツーポイント
- 規格準拠：H.235v3 および 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 NETWORK の機能

- 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 での H.245 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
- 802.1x ネットワーク認証
- 802.1Q 仮想 LAN
- 802.1p QoS およびサービス クラス
- ClearPath
- メディアネット：Mediatrace とメタデータ

IPv6 NETWORK のサポート

- H323 および SIP に対する単一コール スタックのサポート
- DHCP、SSH、HTTP、HTTPS、DNS、DiffServ に対するデュアル スタックの IPv4 および IPv6
- スタティックおよび自動設定 (ステートレス アドレス自動設定) の両方をサポート

CISCO UNIFIED COMMUNICATIONS MANAGER

(Cisco UCM バージョン 8.6 以上が必要)

- Cisco Unified Communications Manager のネイティブ登録
- Cisco Unified Communications Manager の基本的なプロビジョニング
- Cisco Unified Communications Manager からのファームウェア アップグレード
- Cisco Discovery Protocol および DHCP オプション 150 のサポート
- 保留、保留解除、転送、および社内ディレクトリ検索などの基本的なテレフォニー機能

**セキュリティ機能**

- HTTPS および SSH による管理
- IP 管理パスワード
- メニュー管理パスワード
- 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

- 1 LAN/ イーサネット (RJ-45) 10/100/1000 Mbit

その他のインターフェイス

- 将来の使用に備えた USB デバイス

PRECISIONHD 1080P 12X カメラ

- 1/3" CMOS
- 12 倍ズーム
- +15°/-25° チルト、+/- 90° パン
- 垂直視角度 43.5°
- 水平視角度 72°
- フォーカス距離 0.3m-無限
- 1920 × 1080 ピクセル プログレッシブ @ 60fps
- サポートされるその他のフォーマット (ディップ スイッチにて設定可能):
 - 1920 × 1080@60 Hz (HDMI 専用)
 - 1920 × 1080@50 Hz (HDMI 専用)
 - 1920 × 1080@30 Hz
 - 1920 × 1080@25 Hz
 - 1280 × 720@60 Hz
 - 1280 × 720@50 Hz
 - 1280 × 720@30 Hz
 - 1280 × 720@25 Hz
- 自動または手動によるフォーカス、輝度調整、ホワイト バランス
- 遠端カメラ制御
- デュアル HDMI および HD-SDI 出力
- 画像の上下逆置きと自動裏返し

PRECISIONHD 1080P 4X カメラ

- 1/3" CMOS
- 4 倍ズーム
- +15°/-25° チルト、+/- 90° パン
- 垂直視角度 43.5°
- 水平視角度 72°
- フォーカス距離 0.3m-無限
- 1920 × 1080 ピクセル プログレッシブ @ 30fps / 1280 × 720 ピクセル プログレッシブ @ 60fps
- 自動または手動によるフォーカス、輝度調整、ホワイト バランス
- 遠端カメラ制御
- 画像の上下逆置きと手動による裏返し

注: Quick Set C20 の以前の出荷バージョンでは、PrecisionHD 1080p 4x カメラの暫定バージョンが同梱されていました。

システム管理

- Cisco TelePresence Management Suite (Cisco TMS) のサポート
- 組み込みの SNMP、Telnet、SSH、XML、SOAP により包括的に管理
- Web サーバ、SCP、HTTP、HTTPS を介したリモート ソフトウェアのアップロード
- リモコンと画面メニューのシステム

ディレクトリ サービス

- ローカル ディレクトリ (個人アドレス帳) のサポート
- 社内ディレクトリ
- LDAP および H.323 をサポートするサーバ ディレクトリ使用時、エントリ数無制限 (Cisco TMS が必要)
- 社内ディレクトリ数無制限 (Cisco TMS 経由)
- 受信コールの日付と時刻
- 発信コールの日付と時刻
- 不在着信の日付と時刻

電源

- 自動検知の電源
- 100-120/200-240 VAC、60/50 Hz
- コーデックおよびメイン カメラ用に最大 75 W

動作温度および湿度

- 周囲温度 0° C から 35° C (32° F から 95° F)
- 相対湿度 (RH) 10% ~ 90%

保管および輸送の温度

- RH 10-90% において -20° C から 60° C (-4° F から 140° F) (非凝縮)

寸法**Codec C20 :**

- 長さ: 13.8 インチ /35.0cm
- 高さ: 1.2 インチ /3.0cm
- 奥行: 5 インチ /12.7cm
- 重量: 4 ポンド / 1.8 kg

MTBF 製品 RELIABILITY/MTBF

信頼性の予測値は、電源投入時間に基づいて想定される規則性のない電子部品の平均故障間隔 (MTBF) で表されます。

電源投入時間 (POH) > 69000 時間

耐用年数 > 6 年

ISO 9001 証明書をご希望の場合はお問い合わせください。

承認**EU/EEC**

- ディレクティブ 2006/95/EC (低電圧ディレクティブ)
 - 規格 EN 60950-1
- ディレクティブ 2004/108/EC (EMC ディレクティブ)
 - 規格 EN 55022、クラス A
 - 規格 EN 55024
 - 規格 EN 61000-3-2/-3-3

- ディレクティブ 2011/65/EU (RoHS)

本製品はクラス A 製品です。国内環境で本製品を使用すると、電波障害を引き起こす可能性があります。その場合には、ユーザが十分な対策を講じるように求められることがあります。

USA

- UL 60950-1 に従って認証
- FCC15B クラス A に準拠

注: この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に準拠していることが確認済みです。これらの制限は、商業環境で装置を使用しときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でのこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

カナダ

- CAN/CSA C22.2 No. 60950-1 に応じて認証★セグメント分割★ ★セグメント分割★
- このクラス A デジタル装置は、カナダの ICES-003 に準拠しています
- Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada

* オプションが必要

すべての仕様は予告なく変更されることがあり、システムの仕様書と異なる場合があります。

これらのドキュメント内のすべての画像は、表現目的でのみ使用されており、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. 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.

2013 年 3 月



C20 を使用する Profile 42”

装置の全付属品：

- フル HD LCD ディスプレイ、Codec C20、Touch 8” ユーザー インターフェイス デバイス、リモコン、PrecisionHD カメラ (1080p)、テーブル マイク 20 基および任意の設置品：台座スタンド、ホイール ベースまたは壁面取り付け台座。

モニタ

- フル HD LCD、16:9、1080x1920 解像度

ベース

- 床置き用の脚
- ホイール ベース
- 壁面取り付け台座

BANDWIDTH

QuickSet C20 と同様

ファイアウォール トラバース

QuickSet C20 と同様

VIDEO の標準

QuickSet C20 と同様

VIDEO の機能

QuickSet C20 と同様

ビデオ入力 (2 系統)

QuickSet C20 と同様

ビデオ出力 (2 系統)

QuickSet C20 と同様

ライブ ビデオ解像度 (ENCODE/DECODE)

QuickSet C20 と同様

AUDIO の標準

QuickSet C20 と同様

AUDIO の機能

QuickSet C20 と同様

音声入力 (4 系統)

QuickSet C20 と同様

音声出力 (3 系統)

QuickSet C20 と同様

DUAL ストリーム

QuickSet C20 と同様

マルチポイントのサポート

QuickSet C20 と同様

プロトコル

QuickSet C20 と同様

EMBEDDED 暗号化

QuickSet C20 と同様

IP NETWORK の機能

QuickSet C20 と同様

IPv6 NETWORK のサポート

QuickSet C20 と同様

CISCO UNIFIED COMMUNICATIONS MANAGER

QuickSet C20 と同様

セキュリティ機能

QuickSet C20 と同様

ネットワーク インターフェイス

QuickSet C20 と同様

その他のインターフェイス

QuickSet C20 と同様

PRECISIONHD 1080P 12x カメラ

QuickSet C20 と同様

システム管理

- QuickSet C20 と同様、
- Cisco TelePresence Touch 8” ユーザー インターフェイス デバイス

ディレクトリ サービス

QuickSet C20 と同様

電源

- 自動検知の電源
- 100-120/200-240 VAC、60/50 Hz、最大 6 A
- コーデックおよびメイン カメラ用に最大 75 W
- 最大定格電力 (システム全体) 265 W

動作温度および湿度

- 周囲温度 0° C から 35° C (32° F から 95° F)
- 相対湿度 (RH) 10% ~ 90%

保管および輸送の温度

- RH 10-90% において -20° C から 60° C (-4° F から 140° F) (非凝縮)

寸法

- 高さ：63.78 インチ / 162 cm
- 幅：38.58 インチ / 98 cm
- 奥行き：6.7 インチ / 17 cm
- 重量：202.8 ポンド / 92 kg

MTBF 製品 RELIABILITY/MTBF

信頼性の予測値は、電源投入時間に基づいて想定される規則性のない電子部品の平均故障間隔 (MTBF) で表されます。

電源投入時間 (POH) > 69000 時間

耐用年数 > 6 年

ISO 9001 証明書をご希望の場合はお問い合わせください。

承認

EU/EEC

- ディレクティブ 2006/95/EC (低電圧ディレクティブ)
 - 規格 EN 60950-1
- ディレクティブ 2004/108/EC (EMC ディレクティブ)
 - 規格 EN 55022、クラス A
 - 規格 EN 55024
 - 規格 EN 61000-3-2/-3-3
- ディレクティブ 2011/65/EU (RoHS)

本製品はクラス A 製品です。国内環境で本製品を使用すると、電波障害を引き起こす可能性があります。その場合には、ユーザが十分な対策を講じるように求められることがあります。

USA

- UL 60950-1 に従って認証
- FCC15B クラス A に準拠

注 この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に準拠していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起ることがあります。住宅地でのこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

カナダ

- CAN/CSA C22.2 No. 60950-1 に応じて認証★セグメント分割★ ★セグメント分割★
- このクラス A デジタル装置は、カナダの ICES-003 に準拠しています
- Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada

すべての仕様は予告なく変更されることがあり、システムの仕様書と異なる場合があります。

これらのドキュメント内のすべての画像は、表現目的でのみ使用されており、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. 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.

2013 年 3 月

サポートされている RFC

RFC（コメント要求）群には、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的および組織内のドキュメントが含まれます。

サポートされる最新の RFC および草案

- RFC 1889 『RTP: A Transport Protocol for Real-time Applications』
- 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 3420 『Internet Media Type message/sipfrag』
- RFC 3515 『Refer method』
- RFC 3550 『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 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 4587 『RTP Payload Format for H.261 Video Streams』
- 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 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 5905 『Network Time Protocol Version 4: Protocol and Algorithms Specification』
- 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

一般に、Cisco TelePresence 製品のユーザ マニュアルはこのサイトから入手できます。

▶ <http://www.cisco.com/go/telepresence/docs>

右ペインの製品カテゴリを選択してから製品を探す必要があります。以下の順にパスをたどってください。

TelePresence >

TelePresence Solutions Platform >

TelePresence Quick Set >

Cisco TelePresence Quick Set Series

また、マニュアルを検索するために次の短いリンクを使用できます。

▶ <http://www.cisco.com/go/quickset-docs>

ドキュメントは、次のカテゴリに編成されています。

インストール ガイド：

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

スタートアップ ガイド：

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

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：

保守と運用 > メンテナンスとオペレーション ガイド

ユーザ ガイドとクイック リファレンス ガイド：

保守と運用 > エンドユーザ ガイド

API リファレンス ガイド：

リファレンス ガイド > コマンド リファレンス

ナレッジ ベースの記事とよく寄せられる質問 (FAQ)：

Troubleshoot and Alerts > Troubleshooting Guides

CAD 図面：

Reference Guides > Technical References

ビデオ会議室ガイドライン：

設計 > 設計ガイド

ソフトウェア ライセンス情報：

Software Downloads, Release and General Information > Licensing Information

法令準拠および安全上の注意：

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

ソフトウェア リリース ノート：

Software Downloads, Release and General Information > Release Notes

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します。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

TANDBERG はシスコの一部です。TANDBERG® is a registered trademark belonging to Tandberg ASA.

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。

移動先: ► <http://www.cisco.com/web/siteassets/contacts>

©2008 Cisco Systems, Inc. All rights reserved.

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

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

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

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

お問い合わせ先: シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間: 平日 10:00~12:00、13:00~17:00

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