

# Cisco TelePresence Server on Virtual Machine

## 印刷可能オンライン ヘルプ

ソフトウェア バージョン : 4.2

## はじめに

このマニュアルの内容は、Cisco TelePresence Server バージョン 4.2 の Web ユーザ インターフェイス用オンライン ヘルプです。ヘルプの内容を単一のドキュメントとして表示または印刷する際にご利用いただけます。

このマニュアルで取り上げているのは、Cisco TelePresence Server on Virtual Machine のバージョン 4.2 です。

このマニュアルの記述は、製品のユーザ インターフェイスに準じており、オンライン ヘルプ システムと同じ内容です。

章立ては、メイン インターフェイスのページごとに分かれており、各章のタイトル ページには、その中で取り上げたトピックが一覧してあります。

## 詳細情報

製品のソフトウェア ライセンスの詳細については、オンライン ヘルプを参照してください。

## Web インターフェイスへのログイン

なぜ Web インターフェイスへのログインが必要なのでしょうか。

TelePresence Server では、事前設定されたアカウントのセットを保持しておき、アカウントがないユーザのアクセスを拒否することによって、ユーザ アクセスを制限しています。各アカウントにはユーザ名とパスワードがあり、それによってそのアカウントに関連付けられた特権へのアクセスを許可するかが判定されます。

ユーザ アカウントには次の 3 つの特権レベルがあります。

- **管理者**：この特権レベルのユーザはすべての機能にアクセスできます。
- **API アクセス**：この特権レベルのユーザがアクセスできるのは API だけで、Web インターフェイスにはアクセスできません。
- **特権なし**：この特権レベルのユーザは、TelePresence Server にアクセスできません。このレベルは、アカウントを無効にするために使用します。

## タスク

Web インターフェイスへのログイン：

1. Web ブラウザのアドレス バーに、TelePresence Server のホスト名または IP アドレスを入力します。  
ログイン ページが表示されます。
2. 割り当てられた [Username] と [Password] を入力します。
3. [OK] をクリックします。

## Web インターフェイスへのログインが失敗する

[Access denied] ページが表示されますが原因は何でしょうか。

ログインできないのは、次のいずれかの理由によります。

- **ユーザ名/パスワードが無効**：入力されたユーザ名とパスワードが正しくありません。
- **空きセッションがない**：TelePresence Server で同時に許可される最大セッション数に到達しています。
- **IP アドレスと使用されたブラウザのクッキーの値が不一致**：クッキーの削除後に再度ログインを試してください。
- **このページを表示するアクセス権限がありません**：目的のページの表示に必要なアクセス権限がありません。
- **期限切れページ**：TelePresence Server にパスワード変更を要求したユーザとそのパスワード変更要求の実際の送信ユーザが異なると判断された場合、[Change password] ページが期限切れになることがあります（新しいブラウザ タブを開いて要求を送信すると、この状況が発生する場合があります）。

## システム ステータス

システム ステータスの表示 ..... 3

## システム ステータスの表示

[Status] ページには TelePresence Server のステータスの概要が表示されます。この情報にアクセスするには、[Status] に移動します。

**注：**TelePresence Server の管理には外部アプリケーションが必要です。Cisco TelePresence Conductor などの外部アプリケーションは、TelePresence Server の API を使用して会議や参加者の作成および管理を行います。詳細については『[Cisco TelePresence Server API documentation](#)』を参照してください。

表示される情報の詳細については、次の表を参照してください。

**表 1 システム ステータス**

| フィールド              | フィールドの説明  | 使用方法のヒント  |
|--------------------|---|---|
| [Model]            | TelePresence Server の具体的なモデル。   |   |
| [Serial number]    | TelePresence Server に固有のシリアル番号。   | カスタマー サポートを利用する際には、この情報を提示する必要があります。  |
| [Software version] | インストールされているソフトウェアのバージョン。  |   |
| [Build]            | インストールされているソフトウェアのビルドバージョン。   |   |
| [Uptime]           | TelePresence Server を最後に再起動してからの経過時間。   |   |
| [Host name]        | TelePresence Server に割り当てられているホスト名。   |   |
| [IP address]       | TelePresence Server に割り当てられている IP アドレス。   |   |
| [IPv6 address]     | TelePresence Server の IPv6 アドレス。  |   |
| [License mode]     | TelePresence Server が Screen Licensed モード (デフォルト) と Multiparty Licensed モードのどちらで動作しているかを示します。 | Multiparty Licensed モードを利用するには、TelePresence Server がリモート管理モードとなっており、アクティブなコールが存在せず、Multiparty Licensed モードが有効な状態で TelePresence Conductor と接続されている必要があります。 |

表 2 機能キー

| フィールド                        | フィールドの説明  | 使用方法のヒント   |
|------------------------------|---|--|
| [Virtual Machine activation] | TelePresence Server が有効化されているかどうか。  | TelePresence Server はアクティベーションされないと動作しません。   |
| [Media encryption]           | メディア暗号化が有効化されているかどうか。   | メディア暗号化機能キーによって、TelePresence Server の会議を暗号化できます。機能キーは [Configuration] > [Upgrade] ページにインストールされます。「 <a href="#">TelePresence Server のバックアップとアップグレード</a> 」を参照してください。 |
| [Screen licenses]            | TelePresence Server に割り当てられたスクリーン ライセンスの数。クラスタの場合、クラスタ全体に割り当てられたスクリーン ライセンスの数になります。<br>割り当てられるスクリーン ライセンスの数は、システムがサポートする最大数よりも少ない場合があります。 | スクリーン ライセンスを有効化するには、スクリーン ライセンス キーをインストールする必要があります。ライセンスの詳細については、「 <a href="#">TelePresence Server の会議のキャパシティについて</a> 」ページ 69 を参照してください。                           |

表 3 会議のステータス

| フィールド                   | フィールドの説明   | 使用方法のヒント                  |
|-------------------------|--|---------------------------|
| [Active conferences]    | TelePresence Server でアクティブな会議の数。                     | 会議がアクティブになるのは、参加者がいる場合です。 |
| [Active participants]   | TelePresence Server で現在会議をしている参加者（すべてのタイプ）の数。        |                           |
| [Previous participants] | これまでに会議を利用した参加者の数（最後に TelePresence Server を再起動して以降）。 |                           |

表 4 プラットフォーム ステータス

| フィールド                           | フィールドの説明                                      | 使用方法のヒント |
|---------------------------------|---|----------|
| [Processor model and frequency] | TelePresence Server のプロセッサのタイプ。               |          |
| [CPU count]                     | TelePresence Server の仮想 CPU の数。               |          |
| [AVX enabled]                   | TelePresence Server で AVX のサポートが有効化されているかどうか。 |          |

表 5 システム ログ

| フィールド | フィールドの説明  | 使用方法のヒント |
|-------|---|----------|
|       | システム ログには、シャットダウンおよびアップグレードの最新のイベントが表示されます。最後に行われたものが最初に表示されます。 |          |

表 6 診断情報

| フィールド                           | フィールドの説明  | 使用方法のヒント  |
|---------------------------------|---|---|
| <b>[Diagnostic information]</b> | 診断ファイルは、テキスト ドキュメントを含んだ <b>.zip</b> アーカイブ フォーマットで提供されます。診断ファイルをダウンロードするには、 <b>[Download file]</b> をクリックします。 | この診断情報が提供される目的は、TelePresence Server で問題が発生した場合のトラブルシューティングを支援するためです。<br>TelePresence Server で問題が発生した場合、診断テストを依頼する Cisco Technical Assistance Center (TAC) にこのファイルを提供してください。 |
| <b>[System logs]</b>            | ログ ファイルをダウンロードするには、 <b>[Download file]</b> をクリックします。  | アーカイブには有用なログ ファイルが複数含まれています。  |

## ネットワーク設定

|                               |    |
|-------------------------------|----|
| ネットワークの設定 .....               | 6  |
| DNS 定義の設定 .....               | 8  |
| IP ルートの設定 .....               | 9  |
| IP サービスの設定 .....              | 12 |
| QoS の設定 .....                 | 14 |
| SSL 証明書の設定 .....              | 17 |
| ネットワークの接続試験 .....             | 20 |
| ネットワーク統計情報の表示 (netstat) ..... | 21 |

## ネットワークの設定

TelePresence Server のネットワーク設定およびネットワーク ステータスの確認を行うには、[Network] > [Network settings] に移動します。

このページの内容

- [IP の設定](#)
- [IP ステータス](#)
- [イーサネットのステータス](#)

## IP の設定

TelePresence Server の該当するイーサネット ポートの IP 設定方法を指定します。完了したら、[Update IP configuration] をクリックします。

表 7 IPv4 設定

| フィールド                     | フィールドの説明  | 使用方法のヒント   |
|---------------------------|---|--|
| <b>[IP configuration]</b> | IP アドレスを手動で設定する必要があります。アドレスの追加または変更をした場合、TelePresence Server の再起動が必要です。 | IPv6 を使用してログインしている場合のみ TelePresence Server ポートの IPv4 を無効にできます。   |
| <b>[IP address]</b>       | ポートの IPv4 アドレスをドット区切りで指定 (192.168.4.45 など)。                             | このオプションの指定が必要となるのは、上記のように <i>手動</i> の IP 設定を選択した場合だけです。<br>ポート A の IP 設定を [Automatic by DHCP] とした場合、ここでの設定は無視されます。 |
| <b>[Subnet mask]</b>      | 使用する IP アドレスに必要なサブネット マスク (255.255.255.0 など)。                           |  |
| <b>[Default gateway]</b>  | 使用するサブネットのデフォルト ゲートウェイの IP アドレス (192.168.4.1 など)。                       |  |

表 8 IPv6 設定

| フィールド                     | フィールドの説明  | 使用方法のヒント   |
|---------------------------|---|--|
| <b>[IP configuration]</b> | [Disabled] か [Manual] を選択します。<br><br>[Manual] を選択した場合、IPv6 アドレス、プレフィックス長、およびデフォルト ゲートウェイの指定も必要です。<br><br>アドレスの追加または変更をした場合、TelePresence Server の再起動が必要です。 | ネットワークが IPv6 をサポートしていない場合は、ポートの IPv6 を無効化してください。<br><br>IPv4 を使用してログインしている場合のみ TelePresence Server ポートの IPv6 を無効にできます。 |
| <b>[IPv6 address]</b>     | [Manual] 設定を選択した場合は、IPv6 アドレスを CIDR 形式で指定します<br>( <code>fe80::202:b3ff:fe1e:8329</code> など)。  | このアドレスを入力する必要があるのは、IP 設定で [Manual] を選択した場合だけです。[Automatic via SLAAC/DHCPv6] を選択した場合、手動で入力された設定は無視されます。                 |
| <b>[Prefix length]</b>    | [Manual] を選択した場合に、プレフィックス長を指定します。   | プレフィックス長は、アドレスの固定ビット数です (10 進数)。   |
| <b>[Default gateway]</b>  | (オプション) サブネットのデフォルト ゲートウェイの IPv6 アドレスを指定します。  | グローバル、リンクローカルのどちらも指定できます。  |

## IP ステータス

IP ステータスのセクションでは、イーサネット ポートの現在の IP 設定が次のように表示されます。IP 設定は自動、手動のいずれかで設定されています。

IPv4 設定：

- [IP address]
- [Subnet mask]
- [Default gateway]

IPv6 設定：

- [IPv6 address]
- [IPv6 default gateway]
- [IPv6 link-local address]

## イーサネットのステータス

表 9 イーサネットステータス

| フィールド                     | フィールドの説明  | 使用方法のヒント  |
|---------------------------|---|---|
| <b>[Link status]</b>      | イーサネット リンクの接続状況を示します。   |   |
| <b>[Speed]</b>            | イーサネット リンクの数値。  | この値は、ポートに接続されるデバイスとのネゴシエーション、または手動設定によって決まります。              |
| <b>[Duplex]</b>           | ポートへのネットワーク接続のデュプレックスモード ([Full duplex] または [Half duplex]) 。  | この値は、ポートに接続されるデバイスとのネゴシエーション、または手動設定によって決まります。              |
| <b>[MAC address]</b>      | 当該ポートのハードウェア固定 MAC (Media Access Control) アドレス。   | この値は情報表示のみで、変更はできません。                                       |
| <b>[Packets sent]</b>     | 当該ポートから送信されたパケットの総数 (TCP および UDP の全トラフィック) 。  | この情報は、TelePresence Server からネットワークへパケットが送信されているかの確認に利用できます。 |
| <b>[Packets received]</b> | 当該ポートで受信したパケットの総数 (TCP および UDP の全トラフィック) 。  | この情報は、TelePresence Server がネットワークからパケットを受信しているかの確認に利用できます。  |
| <b>[Statistics:]</b>      | 当該ポートの詳細な統計情報。 <ul style="list-style-type: none"> <li>• [Multicast packets sent]</li> <li>• [Multicast packets received]</li> <li>• [Total bytes sent]</li> <li>• [Total bytes received]</li> <li>• [Receive queue drops]</li> <li>• [Collisions]</li> <li>• [Transmit errors]</li> <li>• [Receive errors]</li> </ul> | この情報は、リンク速度やデュプレックスのネゴシエーションなど、ネットワークに関連した問題の診断に役立ちます。      |

## DNS 定義の設定

TelePresence Server 用 DNS 設定の確認と変更をするには [Network] > [DNS] に移動します。

新しい設定を適用するには、[Update DNS configuration] をクリックします。



表 10 DNS 設定

| フィールド                      | フィールドの説明                                | 使用方法のヒント   |
|----------------------------|---|--|
| [Host name]                | TelePresence Server の名前を指定します。          | ホスト名には最大 63 文字を使用できます。<br>ネットワーク設定によっては、IP アドレスを知らなくても、このホスト名を使用して TelePresence Server と通信できる場合があります。  |
| [Name server]              | ネーム サーバの IP アドレス。                       | これは [DNS configuration] を [Manual] にした場合に必要です。   |
| [Secondary name server]    | オプションのセカンダリ ネーム サーバを指定します。              | オプションのセカンダリ ネーム サーバを設定している場合、TelePresence Server はいずれのネーム サーバにも DNS クエリを送信できます。  |
| [Domain name (DNS suffix)] | DNS ルックアップ時に、オプションのサフィックスを追加するように指定します。 | IP アドレスではなく非修飾ホスト名を使用してデバイスを参照する場合は、サフィックスを追加します。<br>たとえば、ドメイン名（サフィックス）を <i>cisco.com</i> に設定した場合、 <i>endpoint</i> というホストの IP アドレスをネーム サーバで検索するときは、実際には <i>endpoint.cisco.com</i> という検索要求を出すことになります。 |

## DNS ステータスの表示

TelePresence Server 用の現在の DNS 設定を確認するには、次の DNS ステータス フィールドが利用できます。

- [Host name]
- [Name server]
- [Secondary name server]
- [Domain name (DNS suffix)]

## IP ルートの設定

TelePresence Server に送受信される IP トラフィックを制御するには、1 つまたは複数のルートのセットアップが必要となる場合があります。

これらのルートが適切に設定されていないと、コールや Web へのアクセスができなくなる可能性があるため、この設定は重要です。

ルートを設定するには、[Network] > [Routes] に移動します。

このページの内容

- [IP ルートの設定](#)
- [現在のルート テーブル](#)

## IP ルートの設定

このセクションでは、TelePresence Server から IP パケットが送信される場合のルートを制御できます。この設定を変更するのは、TelePresence Server が接続されているネットワーク トポロジを十分理解している場合のみにする必要があります。

### 新しい IP ルートの追加

新しいルートを追加するには、次の手順を実行します。

1. 対象のネットワークの IP アドレスおよびアドレスの範囲を定義するマスク長を入力します。
2. これらのアドレス宛のトラフィックのルーティングを [Port A] のデフォルト ゲートウェイ経由とするか、[Gateway] に指定したゲートウェイ経由とするかを選択します。
3. [Add IP route] をクリックします。

新しいルートがリストに追加されます。そのルートがすでに存在する場合、または既存ルートのエイリアスとなる場合（オーバーラップ）、ルートを修正するようインターフェイスにプロンプトが表示されます。

以下の表を参照してください。

表 11 IP ルートの設定

| フィールド                             | フィールドの説明   | 使用方法のヒント  |
|-----------------------------------|--|---|
| <b>[IP address]/[mask length]</b> | <p>これらのフィールドは、当該ルートを適用する IP アドレスの範囲を指定する場合に使用します。</p> <p>IPv4 アドレッシング：対象のネットワークの IP アドレスをドット区切りの 4 つの数字列形式で入力します。可変ビットは 0 にします。</p> <p>[mask length] フィールドは、固定するビット数の指定に使用します（これによって可変のビット数が決まり、アドレスの範囲が指定されます）。</p> <p>IPv6 アドレッシング：対象のネットワークの IP アドレスを CIDR 形式で入力します。可変ビットは 0 にします。[mask length] フィールドは、固定するビット数の指定に使用します（これによって可変のビット数が決まり、アドレスの範囲が指定されます）。</p> | <p>IPv4 の例：192.168.4.128 から 192.168.4.255 の範囲にあるすべての IPv4 アドレスをルーティングするには、[IP address] を 192.168.4.128 として、[mask length] に 25 を指定します。最初の 25 ビットを固定するということは、最終 7 ビットでアドレス範囲が特定されることを意味します。</p> <p>IPv6 の例：2001:db8::0000 から 2001:db8::ffff の範囲にあるすべての IPv6 アドレスをルーティングするには、[IP address] に 2001:db8:: と入力して、[mask length] に 112 を指定します。最初の 112 ビットを固定するということは、最終 16 ビットでアドレス範囲が特定されることを意味します。</p> |
| <b>[Route]</b>                    | <p>このフィールドは、指定パターンに一致するアドレス宛の packets をどのようにルーティングするかを制御に使用します。</p>  | <p>ここでは [Port A] または [Gateway] を選択できます。</p> <p>[Gateway] を選択した場合は、パケットの宛先とするゲートウェイの IP アドレスを入力します。</p> <p>[Port A] を選択した場合、一致するパケットはポート A のデフォルトゲートウェイにルーティングされます（「<a href="#">ネットワークの設定</a>」を参照）。</p>  |

## 既存の IP ルートの表示または削除

このページには、各ルートに関する次の詳細情報が表示されます。

- IP アドレスのパターンとマスク。
- 一致したパケットのルーティング先。次の場合があります。
- Port A : Port A に設定されたデフォルトゲートウェイ。

- <IP address>：選択された特定のアドレス。
- 他の設定に基づいて自動的に設定されたルートか、手動で追加されたものか。

デフォルトのルートは IPv4 および IPv6 の[Default gateway preference] の選択に応じて自動的に設定されるものであり（「[ネットワークの設定](#)」を参照）、削除はできません。手動設定されたルートに宛先が一致しないパケットは、すべてデフォルトゲートウェイ経由でルーティングされます。

手動設定されたルートは削除できます。各ルートの横にあるチェックボックスを選択してから、[Delete selected] をクリックします。

## 現在のルート テーブル

各テーブルには、TelePresence Server の IPv4 と IPv6 のイーサネット ポート用に設定されたすべてのルート（手動および自動）が表示されます。イーサネット ポートの IP 設定を変更する場合は、[Network] > [Network settings] に移動します。

## IP サービスの設定

TelePresence Server の Web サービスへのアクセスを制御するには、[Network] > [Services] に移動します。

TelePresence Server で提供される Web サービスは、Web インターフェイスの HTTP およびコールの受発信用の SIP などです。ここで制御できるのは、これらのサービスがユニットのイーサネット インターフェイスでアクセスできるかどうか、および、これらのサービス用に TCP/UDP ポートが使用できるかどうかです。

## TCP/UDP サービスの有効化

[Network] > [Network settings] ページで有効にされている IP バージョンに応じて、IPv4/IPv6 サービスを制御するオプションがあります。

1. 有効にするサービス名の横にあるチェックボックスをオンにし、無効にするサービスのチェックボックスをオフにします。
2. 必要に応じて、サービスのポート番号を変更します  
(一般に使用されるポート番号は、デフォルトで入力されています)。
3. [Apply changes] をクリックします。

## エフェメラル ポート範囲の設定

**注：**エフェメラル ポートの最小値は、設定された TCP または UDP サービス ポートの最大値よりも大きくなければなりません。たとえば、HTTPS がポート 20000 に設定されている場合、許容されるエフェメラル ポートの最小値は 20001 です。

1. 指定するエフェメラル ポート範囲の最小ポート番号を入力します。  
デフォルト値は 49152 です。最小ポートは 10000 未満には設定できません。
2. 指定するエフェメラル ポート範囲の最大のポート番号を入力します。  
デフォルト値は最大設定の 65535 で、これは約 15000 ポートのデフォルト範囲に相当します。TelePresence Server の会議機能を妨げる可能性があるため、ポート範囲を 5000 未満に減らすことはできません。
3. [Apply changes] をクリックします。
4. 設定値をデフォルトにリセットする場合は、[Reset to default] をクリックしてから [Apply changes] をクリックします。

## デフォルト設定へのリセット

1. [Reset to default] をクリックします。  
TelePresence Server で変更されたすべての設定が、当該ページのデフォルト値に置き換えられます。変更内容はすぐには有効になりません。
2. [Apply changes] をクリックします。  
デフォルト設定が適用されます。

表 12 [Network] > [Services] のフィールドの説明

| フィールド                 | フィールドの説明  | 使用方法のヒント   |
|-----------------------|---|--|
| [HTTP]                | 該当するポートでの Web アクセスを有効または無効にできます。  | Web アクセスは、TelePresence Server の Web ページの表示や変更、およびオンライン ヘルプ ファイルの参照に必要です。   |
| [HTTPS]               | 指定したインターフェイスでのセキュア (HTTPS) Web アクセスの有効/無効の設定、および当該サービスで使用するポートの変更ができます。               | デフォルトでは、TelePresence Server は独自の SSL 証明書と秘密キーを使用します。ただし、必要に応じて新しい秘密キーと証明書をアップロードすることもできます。SSL 証明書の詳細については、「 <a href="#">SSL 証明書の設定</a> 」を参照してください。 |
| [SIP (TCP)]           | SIP (TCP) を使用した TelePresence Server への着信コールの許可/拒否の設定、および当該サービスで使用するポートの変更ができます。       |  |
| [Encrypted SIP (TLS)] | SIP (TLS) を使用した TelePresence Server への暗号化された着信コールの許可/拒否の設定、および当該サービスで使用するポートの変更ができます。 |  |

| フィールド              | フィールドの説明  | 使用方法のヒント   |
|--------------------|---|--|
| <b>[SIP (UDP)]</b> | SIP (UDP) を使用した TelePresence Server からの受発信コールの許可/拒否の設定、および当該サービスで使用するポートの変更ができます。 | このオプションを無効化すると、SIP (UDP) を使用したコールの受発信はできません。                 |
| <b>[Minimum]</b>   | エフェメラル ポート範囲の最小値。   | デフォルト値は 49152 ですが、最小 10000 から最大 60535 までの値を設定できます。           |
| <b>[Maximum]</b>   | エフェメラル ポート範囲の最大値。   | デフォルト値は 65535 ですが、最小で 15000 に設定できます。最小範囲は 5000 ポートに制限されています。 |

## QoS の設定

TelePresence Server で使用する音声およびビデオの Quality of Service (QoS) を設定するには、[Network] > [QoS] に移動します。

QoS とは、特定クラスのデータ処理をカスタマイズするネットワーク機能のことです。たとえば QoS を使用すると、音声とビデオの送信を HTTP トラフィックよりも優先させることができます。これらの設定は、発信されるすべての音声およびビデオ パケットに影響します。他のパケットはすべて QoS を 0 とした設定で送信されます。

TelePresence Server では 6 ビットの値で、タイプ オブ サービス (IPv4) またはトラフィック クラス (IPv6) の設定ができ、ネットワークではタイプ オブ サービス (ToS) または差別化サービス (DiffServ) のいずれかとして解釈されます。IPv6 QoS と IPv4 QoS は、機能的には同じであることに注意してください。

**警告：** 必要がない場合は QoS 設定を変えないでください。

QoS を設定するには 6 ビットの 2 進値を入力する必要があります。

ToS と DiffServ の値を含む QoS に関する詳細は、Internet Engineering Task Force の Web サイト [www.ietf.org](http://www.ietf.org) にある次の RFC で説明されています。

- [RFC 791](#)
- [RFC 2474](#)
- [RFC 2597](#)
- [RFC 3246](#)

このページの内容

- [QoS の設定について](#)
- [ToS 設定](#)
- [DiffServ 設定](#)
- [デフォルト設定](#)

## QoS の設定について

次の表で、[Network] > [QoS] ページの設定について説明します。

何らかの変更後は [Update QoS settings] をクリックしてください。

**表 13 IPv4 設定**

| フィールド          | フィールドの説明                                       | 使用方法のヒント                 |
|----------------|--|--------------------------|
| <b>[Audio]</b> | 音声データ パケットをネットワークで優先させるための 6 ビット バイナリ フィールド。   | 必要がない場合は、この設定を変えないでください。 |
| <b>[Video]</b> | ビデオ データ パケットをネットワークで優先させるための 6 ビット バイナリ フィールド。 | 必要がない場合は、この設定を変えないでください。 |

**表 14 IPv6 設定**

| フィールド          | フィールドの説明                                       | 使用方法のヒント                 |
|----------------|--|--------------------------|
| <b>[Audio]</b> | 音声データ パケットをネットワークで優先させるための 6 ビット バイナリ フィールド。   | 必要がない場合は、この設定を変えないでください。 |
| <b>[Video]</b> | ビデオ データ パケットをネットワークで優先させるための 6 ビット バイナリ フィールド。 | 必要がない場合は、この設定を変えないでください。 |

## ToS 設定

ToS 設定では、プレゼンダンス、遅延、スループット、信頼性をどうトレードオフするかについて抽象化したパラメータで指定します。

ToS 設定には、全 8 ビット中の 6 ビットを使用します。TelePresence Server の設定で変更できるのはビット 0 ~ 5 の値で、ビット 6 と 7 はゼロとします。

- ビット 0 ~ 2 は、IP プレシデンス（パケットの優先順位）を指定します。
- ビット 3 は遅延を指定します：0 = 通常の遅延、1 = 低遅延。
- ビット 4 はスループットを指定します：0 = 通常のスループット、1 = 高スループット。
- ビット 5 は信頼性を指定します：0 = 通常の信頼性、1 = 高信頼性。
- ビット 6 ~ 7 は将来使用するために予約されており、TelePresence Server のインターフェイスでは設定できません。

音声およびビデオ パケットに優先度を割り当てる際は、ネットワーク上の他のパケットに過度の遅延を生じさせないよう、バランスをとることが必要です。たとえば、すべての値に 1 を設定しないでください。

## DiffServ 設定

DiffServ のコードポイント設定には、全 8 ビット中の 6 ビットを使用します（可能なコードポイントは 64 あります）。TelePresence Server の設定で変更できるのはビット 0 ~ 5 の値で、ビット 6 と 7 はゼロとします。コードポイントは、DiffServ ノードによるパケット処理法の特定に利用されます。

## デフォルト設定

QoS のデフォルト設定は次のとおりです。

- [Audio] 101110 :
  - ToS の場合、IP プレシデンスが 5 に設定されたことを意味し、比較的高い優先度になります。遅延は低、スループットは高、信頼性は通常に設定されています。
  - DiffServ の場合、この指定は完全優先転送を意味します。
- [Video] 100010 :
  - ToS の場合、IP プレシデンスが 5 に設定されたことを意味し、ある程度高い優先度になります（ただし音声のプレシデンスほど高くはありません）。遅延は通常、スループットは高、信頼性は通常に設定されています。
  - DiffServ の場合、この指定は相対的優先転送を意味します（コードポイント 41）。

デフォルト設定に戻すには、[Reset to default] をクリックします。



## SSL 証明書の設定

[Network] > [Services] ページで HTTPS を有効にすると（デフォルトで有効）、TelePresence Server の Web インターフェイスに HTTPS を使用してアクセスできるようになります。

**注：** [Network] > [Services] で [Encrypted SIP (TLS)] サービスの使用を選択した場合、証明書とキーも必要です。

Cisco TelePresence Server にはローカル証明書と秘密キーがプレインストールされており、ユーザが HTTPS を使用してユニットにアクセスする際、ブラウザに対する TelePresence Server の認証に使用されます。ただし、すべての Cisco TelePresence Servers で同一のデフォルトの証明書とキーが使用されているため、セキュリティの観点から、独自の証明書と秘密キーをアップロードすることを推奨します。キーの長さは、2048 ～ 8192 ビットにすることを推奨します。

TelePresence Server は、TIP エンドポイントとの暗号化パラメータのネゴシエーションに DTLS を使用しますが、これには証明書が必要です。TelePresence Server の DTLS 実装では、カスタマーから提供された証明書を次のように処理します。

- 状況対応型の DTLS では、カスタマー提供の証明書がアップロードされている場合であっても、常にデフォルトの証明書を DTLS のネゴシエーションに使用します。
- ネゴシエーション型の DTLS では、カスタマー提供の証明書がアップロードされていれば、それを使用します（推奨される手順はこちらです）。

ネゴシエーション型の DTLS は、エンドポイントが RFC 5763 をサポートしている場合に使用され、それ以外の TIP コールでは、状況対応型の DTLS が使用されます。

独自の証明書およびキーをアップロードするには、[Network] > [SSL certificates] に移動します。

**注：** DTLS のネゴシエーションが行われるのは、TelePresence Server にメディア暗号化の機能キーがある場合だけです。

次の表を参照して必要なフィールドへの入力完了したら、[Upload certificate and key] をクリックします。証明書とキーを同時にアップロードする必要があることに注意してください。新しい証明書とキーのアップロード後は、Cisco TelePresence Server の再起動が必要です。

**注：** 証明書と秘密キーは PEM 形式にする必要があります。

証明書ストアには複数の証明書が保存される場合があります。こうした状況が生じる可能性があるのは、アップロードした単一の信頼ストア ファイルの中で、通常の BEGIN と END 証明書タグの間に複数の PEM エンコードされた証明機関の証明書が連続している場合です。

独自の証明書とキーの削除が必要な場合は、[Delete custom certificate and key] をクリックします。証明書の削除をした場合は、TelePresence Server の再起動が必要です。

次の表で、[Network] > [SSL certificates] ページにあるフィールドについて説明します。

表 15 ローカル証明書

| フィールド                | フィールドの説明   | 使用方法のヒント  |
|----------------------|--|---|
| <b>[Subject]</b>     | 証明書が発行された企業の詳細。 <ul style="list-style-type: none"> <li>• [C]：企業が登録されている国。</li> <li>• [ST]：企業がある都道府県。</li> <li>• [L]：企業がある地域または都市。</li> <li>• [O]：企業の正式名称。</li> <li>• [OU]：組織単位または部署。</li> <li>• [CN]：証明書の共通名またはドメイン名。</li> </ul> |   |
| <b>[Issuer]</b>      | 証明書の発行元の詳細。  | 自分で発行した証明書の場合、これらの詳細は [Subject] と同じです。  |
| <b>[Issued]</b>      | 証明書が発行された日付。   |   |
| <b>[Expires]</b>     | 証明書の有効期限が切れる日付。  |   |
| <b>[Private key]</b> | 秘密キーが証明書に一致するかどうか。   | ユーザの Web ブラウザは、Cisco TelePresence Server に送信するデータの暗号化に、SSL 証明書の公開キーを使用します。秘密キーは、Cisco TelePresence Server でのデータの復号化に使用されます。[Private key] フィールドに [Key matches certificate] と表示されていれば、データはどちらの方向でも正常に暗号化されています。 |

表 16 ローカル証明書の設定

| フィールド                             | フィールドの説明   | 使用方法のヒント                    |
|-----------------------------------|--|-----------------------------|
| [Certificate]                     | 組織で証明書を購入したか、独自の方法で証明書を生成した場合は、それをアップロードできます。[Choose File] をクリックし、証明書ファイルを検索して選択します。 | 証明書と秘密キーは PEM 形式にする必要があります。 |
| [Private key]                     | [Choose File] をクリックし、証明書と合わせてアップロードする秘密キーファイルを検索して選択します。                             | 証明書と秘密キーは PEM 形式にする必要があります。 |
| [Private key encryption password] | 秘密キーが暗号化形式で保存されている場合、Cisco TelePresence Server にキーをアップロードするには、パスワード入力が必要です。          |                             |

表 17 信頼ストア

| フィールド     | フィールドの説明  | 使用方法のヒント        |
|-----------|---|-----------------|
| [Subject] | 信頼ストアの証明書の詳細。通常は、ローカル証明書の確認に使用される認証局によって発行された証明書です。 |                 |
| [Issuer]  | 信頼ストアの証明書の発行者の詳細。                                   | 信頼できる証明機関の詳細です。 |
| [Issued]  | 信頼ストアの証明書が発行された日付。                                  |                 |
| [Expires] | 信頼ストアの証明書の有効期限が切れる日付。                               |                 |

表 18 信頼ストアの設定

| フィールド         | フィールドの説明   | 使用方法のヒント   |
|---------------|--|--|
| [Trust store] | <p>信頼ストアは次の 2 つの理由から必要です。</p> <ul style="list-style-type: none"> <li>SIP TLS 接続のリモート エンドの ID を確認する（着信コール、発信コール、または登録）。</li> <li>発信 HTTPS 接続のリモート エンドの ID を確認する（フィードバックの受信者または、<code>flex.participant.requestDiagnostics</code> を呼び出す API アプリケーションなど）。</li> </ul> | <p>信頼ストアの証明書ファイルを参照して選択し、[Upload trust store] をクリックします。</p> <p>証明書ストアには複数の証明書が保存される場合があります。</p> <p>検証が必要となった際（次の設定を参照）のリモート側の証明書の検証は信頼ストアに対して行われます。リモートの証明書は、信頼ストアの中にあるか、そこにあるいずれか 1 つの証明書の信頼チェーンに属している必要があります。</p> <p>削除または、更新されたファイルとの置き換えが必要な場合は、[Delete trust store] をクリックします。</p> |

| フィールド                                      | フィールドの説明                        | 使用方法のヒント   |
|--|---------------------------------|--|
| <b>[Certificate verification settings]</b> | 信頼ストアでリモート証明書の検証が必要となる状況を定義します。 | <p>次のドロップダウン オプションの 1 つを選択して、[Apply changes] をクリックします。</p> <ul style="list-style-type: none"> <li>• <b>[No verification]</b> : 信頼ストアによるリモート証明書の検証を行いません（常に信頼できるリモートエンド）。</li> <li>• <b>[Outgoing connections only]</b> : TelePresence Server は、発信する SIP TLS および HTTPS 接続のすべてに対してリモート証明書の検証を実施します。</li> <li>• <b>[Outgoing connections and incoming calls]</b> : TelePresence Server は、着信および発信する SIP TLS 接続および発信する HTTPS 接続のすべてに対してリモート証明書の検証を実施します。</li> </ul> <p><b>注</b> : 証明書の検証が有効な場合、最大 12 の subjectAltNames がサポートされます。</p> |

## ネットワークの接続試験

**[Network connectivity]** ページは、TelePresence Server とリモートのビデオ会議デバイス（ホスト）間のネットワークで問題が発生した場合のトラブルシューティングに使用できます。

このページでは、TelePresence Server の Web インターフェイスから別のデバイスへの ping を実行して、そのデバイスへのルートをトレースできます。この結果から、TelePresence Server とリモート ホスト間でネットワークが接続されているかがわかります。

リモート デバイスとの接続をテストするには、**[Network] > [Connectivity]** に移動します。接続をテストするデバイスの IP アドレスまたはホスト名をテキスト ボックスに入力して、**[Test connectivity]** をクリックします。

クエリの発信インターフェイスおよびリモート ホストの IP アドレスが表示されます。

ping の結果として、ラウンドトリップ時間（ミリ秒）、およびエコー応答の TTL（パケット存続時間）値が示されます。

TelePresence Server とリモート ホスト間にある各中継ホスト（通常はルータ）について、ホストの IP アドレスと応答所要時間が示されます。

TelePresence Server からのメッセージには、すべてのデバイスが応答するとは限りません。応答しなかったデバイスのルーティング エントリは <unknown> と表示されます。一部のデバイスは、無効な ICMP 応答パケットを送信することが知られています（たとえば、無効な ICMP チェックサム）。無効な ICMP 応答も TelePresence Server に認識されないため、これらの応答も <unknown> と表示されます。

**注：** ping のメッセージは、TelePresence Server からリモート ホストの IP アドレスに送信されます。つまり、特定のホストへの IP ルートを TelePresence Server が持っていれば ping は成功します。この機能は TelePresence Server の IP ルーティング設定をテストするものであり、セキュリティに関する意味はありません。

**注：** リモート ホストへ ping できない場合はネットワーク設定の確認が必要ですが、特に注意すべきなのは NAT を使用しているファイアウォールです。

## ネットワーク統計情報の表示 (netstat)

[Network] > [Netstat] に移動し、TelePresence Server に接続するすべての TCP および UDP について、現在のステータスを表示します。

netstat のデータが更新されるのは、UI ページのロードまたは更新、[Refresh] のクリック、または [Resolve names] チェックボックスのオン/オフをしたタイミングです。

表 19 Netstat フィールドの説明

| フィールド             | 説明   |
|-------------------|--|
| [Resolve names]   | このチェックボックスをオンにすると、アドレスの DNS ルックアップが実行され、可能な場合はホスト名が表示されます。チェックボックスをオフにすると IP アドレスが表示されます。データはチェックボックスのオン/オフ切り替え時に更新されます。   |
| [Protocol]        | [tcp4]、[tcp6]、[udp4]、[udp6] のいずれか。接続に使用されているインターネットのプロトコルとアドレッシング方式が示されます。   |
| [Recv-Q]          | 当該接続において、TelePresence Server でまだ処理されていないためキューに残っているバイト数。   |
| [Send-Q]          | 当該接続において、リモート側でまだ確認されていないためキューに残っているバイト数。  |
| [Local Address]   | 当該接続における TelePresence Server のアドレス。[Resolve names] がオンになっていない場合、このフィールドではローカル ソケットがアドレス:ポートの形式で表示されます。[Resolve names] がオンの場合、ソケットはホスト名:サービス名の形式で表示されます（可能な場合）。<br>例：ts.example.com:http または 127.0.0.1:80 |
| [Foreign Address] | 当該接続のリモート側アドレス。[Resolve names] がオンになっていない場合、このフィールドでは外部ソケットがアドレス:ポートの形式で表示されます。[Resolve names] がオンの場合、ソケットはホスト名:サービス名の形式で表示されます（可能な場合）。<br>例：browser.example.com:http または 192.168.3.1:80                 |

| フィールド            | 説明  |
|------------------|---|
| <b>[State]</b>   | 接続の状態。詳細については、 <a href="http://tools.ietf.org/html/rfc793#section-3.2">http://tools.ietf.org/html/rfc793#section-3.2</a> を参照してください。 |
| <b>[Service]</b> | TelePresence Server が当該接続で提供するサービスの名前。サービス名は [Network] > [Services] ページへのハイパーリンクとなっており、必要に応じてサービス設定を変更できます。                         |

## 設定

|   |    |
|---|----|
| システム設定 .....                              | 22 |
| SIP の設定 .....                             | 23 |
| システム時刻の表示 .....                           | 26 |
| TelePresence Server のバックアップとアップグレード ..... | 27 |
| TelePresence Server のシャットダウンと再起動 .....    | 30 |
| 管理者パスワードの変更 .....                         | 31 |

## システム設定

システム設定を変更するには、[Configuration] > [System settings] に移動し、フィールドを編集後（詳細は表を参照）、[Apply changes] をクリックします。

ほとんどの会議のデフォルト設定は TelePresence Conductor などの管理システムを使用して行われます。

**表 20** すべての設定された会議の設定

| フィールド                                 | フィールドの説明  | 使用方法のヒント              |
|---------------------------------------|---|-----------------------|
| <b>[Display video preview images]</b> | これをオンにすると、会議参加者のビデオ ストリームが、サムネイル形式のプレビュー画像として TelePresence Server のユーザ インターフェイスに表示されます。 | デフォルトでは有効（オン）になっています。 |

| フィールド  | フィールドの説明   | 使用方法のヒント   |
|--|--|--|
| <b>[Show event log messages on console]</b>                      | <p>このチェックボックスをオンにすると、シリアル コンソールへのイベント ログ出力が有効になり、オフにすると無効になります。</p> <p>この設定は、TelePresence Server を再起動した後も保持されます。</p> <p>このチェックボックスをオフにしても、電源投入時からメディア リソースが利用可能になるまでの間は、TelePresence Server のイベント ログ メッセージはシリアル コンソールに出力されます。メディア リソースが利用可能になれば、TelePresence Server からコンソールへのイベント ログ メッセージ送信は停止されます。</p> | <p>デフォルトでこのチェックボックスはオフにされているので、イベント ログのシリアル出力は無効になっています。このデフォルト設定は TelePresence Server のパフォーマンスを向上させるためのものなので、シリアル出力設定を有効にするとパフォーマンスに影響する可能性があります。</p> <p>イベント ログ メッセージの取得には、syslog サーバの使用を推奨します。「<a href="#">Syslog を使用したログイン</a>」ページ 51 を参照してください。</p> |
| <b>[Disable serial console input during startup]</b>             | このチェックボックスをオンにすると、TelePresence Server の起動中にコンソールから入力されても受け付けられません。   | コンソール ユーザの操作による通常のブート シーケンスの中断を防止する観点から、このチェックボックスはオンにしておくことを推奨します。  |
| <b>[Require administrator login for serial console commands]</b> | このチェックボックスをオンにすると、TelePresence Server は、特定できないユーザのコンソール コマンドを受け付けません。  | <p>不正なユーザが物理アクセスを取得した場合にシリアル コンソールを保護する観点から、このチェックボックスはオンにしておくことを推奨します。</p> <p><b>注：</b> TelePresence Server のコンソールは Unicode 文字を受け付けません。コンソール アクセスに使用するアカウントのユーザ名とパスワードは、ASCII 文字のみに制限されています。</p>  |
| <b>[Idle serial console session timeout]</b>                     | アイドル状態になってから TelePresence Server がコンソール セッションを開いたまま維持する時間 (分)。   | 無人のコンソール セッションを不正ユーザに開放したままにしないように、短い値を指定することを推奨します。   |

## SIP の設定

[SIP setting] ページでは、TelePresence Server の SIP 設定を管理できます。

この情報にアクセスするには、[Configuration] > [SIP settings] に移動します。

デフォルトの更新または設定を随時変更するには、次の表を参照してフィールドを編集し、[Apply changes] をクリックします。

表 21 SIP

| フィールド                         | フィールドの説明  | 使用方法のヒント  |
|-------------------------------|---|---|
| [Outbound call configuration] |   | <p>[Use trunk] :</p> <ul style="list-style-type: none"> <li>指定した SIP サーバアドレスに、トランク経由で発信 SIP コールを転送します。</li> <li>Cisco Video Communication Server (VCS) や Cisco Unified Call Manager (CUCM) などの SIP サーバは、TelePresence Server からの発信 SIP コールをオンワード ルーティングします。</li> </ul> <p>[Call direct] :</p> <ul style="list-style-type: none"> <li>可能な場合、TelePresence Server は SIP コールを直接接続します。[Outbound address] および [Outbound domain] パラメータは使用されません。</li> <li>TelePresence Server はトランクを使用しません。</li> </ul> |
| [Outbound address]            | SIP レジストラまたはトランク接続先のホスト名または IP アドレス。  | [Outbound call configuration] が [Call direct] に設定されている場合、TelePresence Server はこのフィールドを無視します。  |
| [Outbound domain]             | トランクの接続先ドメイン。   | <p>[Outbound call configuration] が [Call direct] に設定されている場合、TelePresence Server はこのフィールドを無視します。</p> <p>指定されたアドレスに @ 記号が含まれていない場合、TelePresence Server はすべての発信 SIP コールでこの値を使用します。</p> <p>発信ドメインを指定しない場合、TelePresence Server は代わりに発信アドレスを使用します。</p>  |
| [Username]                    | SIP デバイス（トランクの接続先またはエンドポイント）が認証を必要とする場合、そのデバイスの認証に TelePresence Server はこのユーザ名を使用します。 |   |



| フィールド                              | フィールドの説明   | 使用方法のヒント  |
|------------------------------------|--|---|
| <b>[Password]</b>                  | SIP デバイス（トランクの接続先またはエンドポイント）が認証を必要とする場合、そのデバイスの認証に TelePresence Server はこのパスワードを使用します。   | SIP の接続先が認証を必要としない場合もありますが、必要とする場合は、ここでのユーザ名とパスワードの組み合わせによるログインを受け入れるように設定する必要があります。  |
| <b>[Outbound transport]</b>        | TelePresence Server が発信コールに使用するプロトコルを選択します。<br>指定できるのは、[TCP]、[UDP]、[TLS] のいずれかです。  | TelePresence Server は、トランクの接続先との通信にこのプロトコルを使用します。<br>暗号化の機能キーがインストールされており、シグナリングを暗号化する場合は、[TLS] を選択します。<br>TelePresence Server は、着信接続で使用されているすべてのプロトコル（TCP、UDP、または TLS）を受け入れ、それらの応答には同じプロトコルを使用するので、ここでの [Outbound transport] 設定は関係しません。これらのサービスは、[Network] > [Services] ページで有効化しておく必要があります。  |
| <b>[Advertise Dual IPv4/IPv6]</b>  | IPv4 と IPv6 が混合しているネットワークで TelePresence Server が SIP コールをサポートする場合、[Use ANAT] を選択します。   | デフォルトは [Disabled] です。ANAT（代替ネットワーク アドレス タイプ）を使用するように設定した場合、デバイスはセッション記述で ANAT 構文をサポートします。詳細については、 <a href="http://tools.ietf.org/html/rfc4091">http://tools.ietf.org/html/rfc4091</a> を参照してください。  |
| <b>[Negotiate SRTP using SDES]</b> | TelePresence Server が SDES を使用して SRTP のネゴシエーションをする際、次のいずれかのオプションで行うかを選択します。 <ul style="list-style-type: none"> <li>• [For secure transports (TLS) only]</li> <li>• [For all transports]</li> </ul> （注：このパラメータが表示されるのはメディア暗号化の機能キーがある場合だけです）。 | TelePresence Server は、SIP での暗号化の使用をサポートしています。<br>SIP で暗号化を使用する場合、音声およびビデオ メディアは Secure Real-time Transport Protocol (SRTP) を使用して暗号化されます。SRTP 使用時におけるキー交換のデフォルトのメカニズムは、Session Description Protocol Security Description (SDES) です。SDES のキー交換はクリア テキストで行われるので、コール制御メッセージ用のセキュアな転送と併用して SRTP を使用することを推奨します。TelePresence Server の設定では、SIP コール制御メッセージに使用可能なセキュアな転送メカニズムとして Transport Layer Security (TLS) も使用できます。<br>デフォルト設定は [For secure transports (TLS) only] です。 |

## システム時刻の表示

TelePresence Server は、時刻の同期に Network Time Protocol (NTP) を使用します。

時刻を設定するには、[Configuration] > [Time] に移動します。

## システム時間

表示される現在時刻は、TelePresence Server に基づいたものです。

## NTP

TelePresence Server は NTP プロトコルをサポートしています。TelePresence Server を自動で NTP サーバと同期させる場合は、NTP 設定を入力し、[Update NTP settings] をクリックします。

変更を有効にするためにシステムを再起動するようプロンプトが表示されます。

TelePresence Server は、1 時間ごとに NTP サーバと同期します。

NTP サーバが TelePresence Server で有効なイーサネット インターフェイスのいずれかにローカルで接続されている場合、TelePresence Server は自動的にそのポートを使用して NTP サーバと通信します。

NTP サーバがローカル接続でなく、NTP サーバのネットワーク/IP アドレスへの特定の IP ルートが指定されていない場合、TelePresence Server はデフォルト ゲートウェイに設定されたポートを使用して NTP サーバと通信します ([Network] > [Routes] を参照)。

TelePresence Server と NTP サーバ間にファイアウォールがある場合は、UDP ポート 123 への NTP トラフィックを許可するようにファイアウォールを設定します。

表 22 デバイス時刻の設定

| フィールド        | フィールドの説明   | 使用方法のヒント  |
|--------------|--|---|
| [Enable NTP] | このチェックボックスをオンにすると、TelePresence Server で NTP プロトコルが有効になります。 |   |
| [UTC offset] | ユーザのタイムゾーンと UTC のオフセット。                                    | 英国夏時間やその他の地域でのサマータイムなど、地域固有のタイムゾーンに対応する場合は、このオフセットの手動更新が必要です。 |

| フィールド      | フィールドの説明                                     | 使用方法のヒント |
|------------|--|----------|
| [NTP host] | ネットワークのタイム キーパーとして機能しているサーバの IP アドレスまたはホスト名。 |          |

## NAT（ネットワーク アドレス変換）越えでの NTP の使用

NAT が TelePresence Server のネットワークにローカルな設定である場合、追加の設定は不要です。

NAT が NTP サーバのローカル ネットワークで行われている場合は、TelePresence Server からの NTP データが NTP サーバの UDP ポート 123 へ転送されるように、NAT 転送テーブルを設定する必要があります。

## TelePresence Server のバックアップとアップグレード

このページの内容

- [TelePresence Server メイン ソフトウェア イメージのアップグレード](#)
- [設定のバックアップと復元](#)
- [TelePresence Server 機能の有効化](#)

## TelePresence Server メイン ソフトウェア イメージのアップグレード

TelePresence Server メイン ソフトウェア イメージは、アップグレードする必要がある唯一のファームウェア コンポーネントです。

**TelePresence Server メイン ソフトウェア イメージをアップグレードするには、次の手順を実行します。**

1. [Configuration] > [Upgrade] に移動します。
2. 現在インストールされているバージョンを、メイン ソフトウェア イメージの [Current version] で確認します。
3. より新しいイメージが使用可能でないかを、[サポート ページ](#)にログオンして確認します。
4. 使用可能な最新のイメージをダウンロードして、ローカル ハード ドライブに保存します。
5. イメージ ファイルを解凍します。
6. TelePresence Server の Web ブラウザ インターフェイスにログオンします。
7. [Configuration] > [Upgrade] に移動します。

- ハード ドライブ上の解凍したファイルを検索します。  
ここでのボタンの表示は [Browse...] や [Choose File] など、使用するブラウザに応じて異なる場合があります。
- [Upload software image] をクリックします。ブラウザが TelePresence Server へのファイルのアップロードを開始し、新しいブラウザ ウィンドウが開いてアップロードの進捗状況が表示されます。完了すると、ブラウザのウィンドウが更新され、"Main image upgrade completed." と表示されます。
- アップグレードのステータスが [TelePresence Server software upgrade status] フィールドに表示されます。
- [TelePresence Server](#) をシャットダウンして再起動します。

## 設定のバックアップと復元

[Configuration] > [Upgrade] ページのバックアップと復元のセクションでは、TelePresence Server 設定のバックアップと復元を Web インターフェイスを使用して実行できます。これを利用すると、以前の設定へ復帰したり、設定を別のユニットにコピーして効率的に複製を作成したりすることができます。

設定をバックアップするには、[Save backup file] をクリックし、生成された configuration.xml ファイルを安全な場所に保存します。

後で設定を復元するには、次の手順を実行します。

- [Configuration] > [Upgrade] に移動します。
- 以前保存した configuration.xml ファイルを検索して選択します。  
ここでのボタンの表示は [Browse...] や [Choose File] など、使用するブラウザに応じて異なる場合があります。
- 保存された設定で上書きする対象を、現在の [Network settings] のみ、[User settings] のみ、またはその両方にするかを選択します。  
上書き指定はデフォルトでオフにされていますが、これは既存のネットワーク設定およびユーザ アカウントの維持をユーザが望むであろうと想定しているからです。
- [Restore backup file] をクリックします。

新しいコンフィギュレーション ファイルを TelePresence Server に復元する場合、設定を上書きする部分を指定できます。

- [Network settings] をオンにすると、ネットワーク設定は指定したファイルの内容で上書きされます。  
通常このチェックボックスをオンにするのは、同じ TelePresence Server でバック アップしておいたファイルから復元する場合か、稼働していない TelePresence Server を置き換える場合だけです。

他のアクティブな TelePresence Server からネットワーク設定をコピーして競合が発生した場合（たとえば、両方で同一の固定 IP アドレスを使用する設定になったなど）、どちらか一方、あるいは両方のデバイスに IP 経由で到達できなくなる場合があります。[Network settings] をオンにしなければ、QoS 設定を除いた既存のネットワーク設定は、復元操作で上書きされません。QoS 設定は、[Network settings] チェックボックスの指定とは無関係に上書きされます。

- [User settings] をオンにすると、現在のユーザ アカウントとパスワードは、指定したファイルの内容で上書きされます。
- ユーザ設定を上書きする際に、現在使用しているログインに対応するユーザ アカウントが復元用のファイル内に存在しない場合は、ファイルのアップロード後に再ログインする必要があります。

## TelePresence Server 機能の有効化

TelePresence Server の機能の多くは、使用する前にアクティベーションする必要があります（TelePresence Server がアクティベーションされていない状態では、Web インターフェイス上部のバナーに警告が目立つように表示されますが、それ以外のすべての Web インターフェイスは通常どおりに表示および機能します）。

新しい TelePresence Server であればすでにアクティベーションされているはずですが、新しいファームウェア バージョンへのアップグレード後や、新たな機能を有効にする場合はアクティベーションが必要です。適切なアクティベーション キーの取得について販売店へお問い合わせください。

各キーは TelePresence Server ごとに固有のものです。有効なキーの取得には、キーの要求時にデバイスのシリアル番号が必要です。

キーを適用する手順は、TelePresence Server のアクティベーションや拡張機能を有効にする場合と同じです。

キーを TelePresence Server に適用するには、次の手順を実行します。

1. 機能がすでにアクティブであるかを、[Feature management] リストを参照して確認します。  
製品アクティベーション キーも、このリストに表示されます。
2. 受け取ったキーを [Add key] フィールドに入力しますが、その際にはダッシュ記号も含めて受け取ったものとまったく同じように入力する必要があります。
3. [Add Key] をクリックします。

ブラウザ ウィンドウが更新され、新しく追加された機能と入力したキーがリストに反映されます。

有効なキーでなかった場合は、再入力するように求められます。

キーが期限切れになっている場合もあります。その場合は、失効日が表示されるか、または、機能がすでに有効期限切れになっていることの警告が表示されます。期限切れのキーは、対応する機能を無効にしてもリストに残ります。

4. 後日再入力する必要があるかもしれないので、キーを記録しておきます。

TelePresence Server および機能のアクティベーションは、成功すれば即座に有効化され、TelePresence Server の再起動後も有効なまま維持されます。

一部のタイプの機能は削除できます。機能を削除するには、キーの横の [remove] をクリックします。

## スクリーン ライセンスの適用

スクリーン ライセンスのアクティベーション キーは、TelePresence Server のシリアル番号にリンクされています。スクリーン ライセンスのアクティベーション キーは、機能のアクティベーションと同様の方法で TelePresence Server に直接入力できます（手順は前述）。

## TelePresence Server のシャットダウンと再起動

アップグレードの一部として TelePresence Server を再起動する際、または電源を切る際に、シャットダウンが必要となる場合があります。

**警告：** TelePresence Server をシャットダウンすると、すべてのアクティブ コールが切断されます。

**TelePresence Server をシャットダウンするには、次の手順を実行します。**

1. [Configuration] > [Shutdown] に移動します。
2. [Shut down TelePresence Server] をクリックします。

ボタンの表示が [Confirm TelePresence Server shutdown] に変わります。

3. 再度ボタンをクリックして確認します。

TelePresence Server のシャットダウンが開始されます。ページ上部のバナーが、シャットダウンの開始を示す表示に変わります。

シャットダウンが完了すると、ボタンの表示が [Restart TelePresence Server] に変わります。

4. 最後にこのボタンをクリックすると TelePresence Server の再起動が開始されます。

## 管理者パスワードの変更

このページでは、TelePresence Server にログインする管理者パスワードを変更できます。これは「管理者」権限を必要とする現在のユーザに適用されます。このページにアクセスするには、[Configuration] > [Change password] に移動します。

管理者パスワードは、定期的に変更することを推奨します。パスワードは何かにかき写して、安全な場所に保管するようにしてください。

パスワードを変更するには、新しいパスワードを 2 回入力し、[Change password] をクリックします。

## 会議

|                                     |    |
|-------------------------------------|----|
| 会議リストの表示.....                       | 31 |
| 会議ステータスの表示.....                     | 33 |
| エンドポイントおよびグループ ステータスの表示.....        | 38 |
| エンドポイントまたはエンドポイント グループの統計情報の表示..... | 41 |

## 会議リストの表示

[Conferences] ページには、会議の状態（例：アクティブ/非アクティブ）に関係なく、TelePresence Server に設定されている会議がすべて表示されます。

このリストにアクセスするには、[Conferences] に移動します。

デフォルトで会議は、名前のアルファベット順でソートされています。リストのソート順を切り替えるか、ステータスや URI でソートするには、該当する列ヘッダーをクリックします。

このページでは、次の操作ができます。

- 会議を削除する。
- 会議名をクリックしてステータスを表示する。

リストには、各会議に関する次の情報が表示されます。

表 23 会議リストの詳細

| フィールド           | フィールドの説明  | 使用方法のヒント   |
|-----------------|---|--|
| <b>[Name]</b>   | 事前に設定された会議の名前。  | 会議の名前をクリックすると、会議のステータスと参加者が表示されます。   |
| <b>[URIs]</b>   | 会議に割り当てられた URI。   | <p>リモート管理モードの場合、TelePresence Server はゲートキーパーに個々の会議の URI を登録しません。</p> <p>会議には、参加者がダイヤルできる最大 2 つの多目的 URI を指定できます。URI が PIN で保護されている場合、そのステータスが表示されます。</p> <p>1 つの URI は複数の PIN をサポートできるので、ゲスト/主催者の PIN をそれぞれ設定できます。</p> <p>個々の参加者は、ダイヤル可能な自分の URI を指定できますが、このリストには表示されません。</p>   |
| <b>[Status]</b> | <p>会議のステータスとして次のものが表示されます。</p> <ul style="list-style-type: none"> <li>• <i>[Scheduled]</i></li> <li>• <i>[Active]</i></li> <li>• <i>[Inactive]</i></li> <li>• <i>[Ending]</i></li> </ul> <p>このフィールドには、会議の設定に関する警告が表示される場合があります。</p> | <p>会議には次のものがあります。</p> <ul style="list-style-type: none"> <li>• ステータスが <i>[Scheduled]</i> の会議では、会議開始までの時間が示されます。</li> <li>• ステータスが <i>[Active]</i> の会議では <i>[(&lt;X&gt; endpoints, &lt;N&gt; screens)]</i> と表示されます。またはすべてのエンドポイントが音声のみであれば <i>[Active (&lt;X&gt; endpoints)]</i> と表示されます。</li> <li>• ステータスが <i>[Inactive]</i> の会議の表示は、参加者がいない点を除けば <i>[Active]</i> な場合と基本的には同じです。ただし、URI および開始までの時間と期間の表示もできます。</li> <li>• <i>[Ending]</i> は会議が破棄処理中であることを示します。この処理中、残りの参加者には退出口ビーが表示されます。</li> </ul> <p>ステータスには、会議の期間やロックの有無に関する追加情報が表示される場合があります。たとえば、<i>[Inactive - Ends in 5 hours and 27 minutes [Locked]]</i> などの表示です。</p> <p>会議の設定に関する警告が表示される場合があります。たとえば、<i>[[No participants allowed - limited to 0 participants]]</i> などの表示です。</p> |



## 会議ステータスの表示

会議の [Status] ページには、会議実施中のステータスが表示されます。[Conferences] に移動して会議の名前をクリックすると、[Status] ページが表示されます。

このページでは、会議について次の情報を確認できます。

- 会議がアクティブであるか、および会議に参加しているエンドポイント数
- ロックされているか
- コンテンツ チャンネルが含まれているか
- 参加者の有無、いる場合は個々のステータス
- 参加していたユーザの有無、いた場合はその名前
- 会議に割り当てられた URI の有無

## [Conference] > [Conference Name] > [Status] ページで可能な操作

- 参加者を選択し、[Disconnect selected] で切断する
- [Disconnect all] ですべての参加者を切断し、実質的に会議を終了させる
- [1つのエンドポイント、またはすべてのエンドポイントにメッセージを送信する](#)
- [More...] をクリックして、参加している特定のエンドポイントに関する追加のステータス情報を表示する、あるいは [Expand all] をクリックして、すべてのアクティブなエンドポイントについて表示する（詳細は次の表を参照）

## 会議ステータスの参照

表 24 ステータス

| フィールド                           | フィールドの説明  | 使用方法のヒント   |
|---------------------------------|---|--|
| <b>[Status]</b>                 | <p>会議のステータスとして次のものが表示されます。</p> <ul style="list-style-type: none"> <li>• <i>[Scheduled]</i></li> <li>• <i>[Active]</i></li> <li>• <i>[Inactive]</i></li> <li>• <i>[Ending]</i></li> </ul> <p>このフィールドには、会議の設定に関する警告が表示される場合があります。</p> | <p>会議には次のものがあります。</p> <ul style="list-style-type: none"> <li>• ステータスが <i>[Scheduled]</i> の会議では、会議開始までの時間が示されます。</li> <li>• ステータスが <i>[Active]</i> の会議では <i>[(&lt;X&gt; endpoints, &lt;N&gt; screens)]</i> と表示されます。またはすべてのエンドポイントが音声のみであれば <i>[Active (&lt;X&gt; endpoints)]</i> と表示されます。</li> <li>• ステータスが <i>[Inactive]</i> の会議の表示は、参加者がいない点を除けば <i>[Active]</i> な場合と基本的には同じです。ただし、URI および開始までの時間と期間の表示もできます。</li> <li>• <i>[Ending]</i> は会議が破棄処理中であることを示します。この処理中、残りの参加者には退出口ビーが表示されます。</li> </ul> <p>ステータスには、会議の期間やロックの有無に関する追加情報が表示される場合があります。たとえば、<i>[Inactive - Ends in 5 hours and 27 minutes [Locked]]</i> などの表示です。</p> <p>会議の設定に関する警告が表示される場合があります。たとえば、<i>[[No participants allowed - limited to 0 participants]]</i> などの表示です。</p> |
| <b>[URIs]</b>                   | <p>会議に割り当てられた URI。</p>  | <p>会議には、参加者がダイヤルできる最大 2 つの多目的 URI を指定できます。URI が PIN で保護されている場合、そのステータスが表示されます。</p> <p>1 つの URI は複数の PIN をサポートできるので、ゲスト/主催者の PIN をそれぞれ設定できます。</p> <p>個々の参加者は、ダイヤル可能な自分の URI を指定できますが、このリストには表示されません。</p>  |
| <b>[Conference lock status]</b> | <p>会議がロックされているかを示します。</p>   |  |

| フィールド            | フィールドの説明                    | 使用方法のヒント   |
|------------------|-----------------------------|--|
| <b>[Content]</b> | コンテンツ チャンネルが現在使用中かどうかを示します。 | <p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• <b>[No current presentation]</b> : コンテンツ共有が会議で有効化されていますが、コンテンツのアクティブなコントリビュータがいません。</li> <li>• <b>[Presentation from &lt;endpoint display name&gt;]</b> : コンテンツのアクティブなコントリビュータがいます。</li> </ul> <p>詳細については「<a href="#">コンテンツ チャンネルのサポート</a>」を参照してください。</p> |

表 25 すべての参加者

| フィールド              | フィールドの説明  | 使用方法のヒント  |
|--------------------|---|---|
| <b>[Endpoint]</b>  | 現在アクティブな会議に参加しているエンドポイントの名前。                                    | <p>会議がアクティブでない場合、このセクションには <b>[No endpoints]</b> と表示されます。</p> <p>特定の参加者を会議から削除するには、該当するチェックボックスをオンにして、<b>[Disconnect selected]</b> を選択します。</p> <p>エンドポイントの名前をクリックすると、<b>[Status]</b> ページに移動します。</p> |
| <b>[Type]</b>      | エンドポイントのタイプ。  |   |
| <b>[Authority]</b> | 会議の参加者のロール（および付随する権限）を <b>[Chair]</b> または <b>[Guest]</b> で示します。 | 管理システムで <b>chair/guest</b> の制御レベルが明示的に適用されている会議を除き、すべての参加者はデフォルトで <b>[Chair]</b> とされます。   |







| フィールド            | フィールドの説明  | 使用方法のヒント  |
|------------------|---|---|
| <b>[Status]</b>  | エンドポイントのステータス。  | <p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>[Joining conference]：この会議に参加設定しているエンドポイントです。</li> <li>[In conference]：この会議に現在参加中のエンドポイントです。</li> <li>[Attempting to re-establish call]：エンドポイントがビジーで、再試行が行われています。</li> </ul> <p>追加ステータス情報は、[xx failed to join]（グループ化されたエンドポイント）、[packet loss detected]、[video to muted]、[video from muted]、[video muted]（音声も同様）、[important]、[audio-only]などの形式で表示されます。</p> <p>事前に設定されたエンドポイントが会議開始時にビジーであった場合、TelePresence Server は会議中に最大 5 回の再試行を行い、ビジーでなくなった場合はその段階で接続します。再試行の間隔は、5、15、30、60、120 秒です。</p>  |
| <b>[More...]</b> | <p>[More...] をクリックすると、送受信されるストリームのプレビューが表示されます。会議に対するエンドポイントの動作も制御できます。</p> <p>リスト内のすべてのエンドポイントのステータス情報を詳細表示させるには、[Expand / Collapse All] をクリックします。</p> | <p>次の作業を実行できます。</p> <p>音声のミュート  およびミュート解除 </p> <p>ビデオのミュート  およびミュート解除 </p> <p>参加者を重要（ストリーム送信のみ）  または非重要に指定 </p> <p>ビデオ ストリームがトランスコードされていない場合、送受信されるビデオ ストリームのプレビューは使用できません。そうした場合は [No preview] メッセージが表示されます。</p> <p>また [All Participants] ペインの下部には、プレビュー ペインが表示できない理由として [* Preview Panes are not available for non-transcoded (SVC) video streams] と表示されます。</p> |

表 26 以前の参加者

| フィールド             | フィールドの説明                   | 使用方法のヒント  |
|-------------------|----------------------------|---|
| <b>[Endpoint]</b> | この会議に以前参加していたエンドポイントの名前です。 | <p>参加者を会議に再接続するには、該当するチェックボックスをオンにして、[Retry connection] を選択します。</p> <p>エンドポイントの名前をクリックすると、[Status] ページに移動します。</p> |

| フィールド                             | フィールドの説明              | 使用方法のヒント   |
|-----------------------------------|-----------------------|--|
| <b>[Type]</b>                     | エンドポイントのタイプ。          |  |
| <b>[Reason for disconnection]</b> | エンドポイントが会議に参加していない理由。 | <p>TelePresence Server は次の例のいずれかの理由でエンドポイントを接続解除した可能性があります。</p> <ul style="list-style-type: none"> <li>• [requested by administrator]：エンドポイントは管理者により切断されました。</li> <li>• [call rejected]：相手側がコールを拒否しました。</li> <li>• [left conference]：エンドポイントは会議の終了時に切断されました。</li> <li>• [requested via API]：エンドポイントは API 経由で切断されました。</li> <li>• [no answer]：エンドポイントがコールに応答しませんでした。</li> <li>• [busy]：エンドポイントがビジーで接続に失敗しました（SIP コールの場合はエンドポイントがコールを拒否した可能性もあります）。</li> <li>• [destination unreachable]：エンドポイントに到達できませんでした。</li> <li>• [Encryption not supported by far end]：暗号化が必要なコールにもかかわらず相手側で暗号化がサポートされていない、あるいは暗号化が禁止されているコールにもかかわらず相手側が暗号化を要求しています。</li> <li>• [timeout]：接続がタイムアウトしました。</li> <li>• [insufficient free ports]：空きポート不足のためエンドポイントが切断されました。</li> <li>• [conference port limit reached]：会議のポートの制限に達したためエンドポイントが切断されました。</li> <li>• [Conference locked]：会議がロックされているためコールは接続できませんでした。</li> <li>• [Product not activated]：TelePresence Server にアクティベーション キーがインストールされていないため、コールの発信/受信ができませんでした。</li> <li>• [Protocol error]：プロトコル エラーによりエンドポイントが切断されました。</li> <li>• [Network error]：ネットワーク エラーによりエンドポイントが切断されました。</li> </ul> |

| フィールド | フィールドの説明 | 使用方法のヒント   |
|-------|----------|--|
|       |          | <ul style="list-style-type: none"> <li>• [Unavailable]：使用できないエンドポイントです。</li> <li>• [Capability negotiation error]：エンドポイントと TelePresence Server 間で相互互換性のあるコール セットアップのネゴシエーションができません。</li> <li>• [Insufficient token allocation]：トークンの仕様または割り当てが TIP/MUX コールに不適切です。</li> <li>• [TIP/MUX negotiation failure]：TIP/MUX ネゴシエーションが正常に完了しなかったためエンドポイントが切断されました。</li> <li>• [No media received]：メディアの送信が予期せず停止してから 30 秒以上経過したため、TelePresence Server がエンドポイントを切断しました。</li> <li>• [unspecified error]：エンドポイントが切断されましたが、TelePresence Server は原因を把握できていません。</li> </ul> |

## エンドポイントおよびグループ ステータスの表示

エンドポイントのステータスが利用できるのは、リモート管理モードのアクティブな会議に属するエンドポイントだけです。ここである程度エンドポイントを制御できます。

1. [Conference] に移動し、[Status] ページを選択します。
2. エンドポイントまたはグループ名をクリックします。
3. 次の表を参照して、エンドポイントの確認または制御をします。
4. 最新のステータス表示にするには、ブラウザのページを更新します。

表 27 エンドポイントから得られる情報

| フィールド                    | フィールドの説明  | 使用方法のヒント   |
|--------------------------|---|--|
| [Country code/extension] | これらのフィールドは、エンドポイントから返された情報を表示しています。製造元によっては得られる情報の詳細が異なる可能性があります。 | この情報は、エンドポイントの最初の接続完了後に表示されます（現在接続しているかどうかは関係ありません）。 |
| [Manufacturer code]      |   |  |
| [Product]                |   |  |
| [Version]                |   |  |

表 28 ステータス

| フィールド                                     | フィールドの説明  | 使用方法のヒント   |
|---|---|--|
| <b>[Connected to conference]</b>          | エンドポイントが現在会議に参加しているかどうか、参加している場合はその会議名。   | 会議名をクリックすると、その会議のステータス ページに移動します。  |
| <b>[Call status]</b>                      | コールが接続されているかどうか。接続している場合は、コールが着信であるか発信であるか。   |  |
| <b>[Protocol]</b>                         | コールで使用されているプロトコル (SIP など)。  |  |
| <b>[Endpoint advertised capabilities]</b> | コールのネゴシエーション時にエンドポイントがアドバタイズした機能。   | 例：音声、ビデオ、ビデオ コンテンツ、暗号化トラフィック、非暗号化トラフィックなど。   |
| <b>[Audio channels]</b>                   | Cisco TelePresence Server と相手側との間で、受信および送信の音声チャンネルが開かれているかどうか。  |  |
| <b>[Video channels]</b>                   | Cisco TelePresence Server と相手側との間で、受信および送信のビデオ チャンネルが開かれているかどうか。<br><br>[Single-stream] または [Multi-stream] は、ビデオ チャンネルの現在の動作モードを示します。 | エンドポイントは最初にシングル ストリーム エンドポイントとして会議に参加し、その状態はマルチストリームのネゴシエーションが完了するまで継続されます。また、コールに最初に参加したエンドポイントが他のエンドポイントの参加を待つ間も [single-stream] と表示されます。  |
| <b>[Extended video channels]</b>          | Cisco TelePresence Server と相手側との間で、受信および送信の拡張ビデオ チャンネルが開かれているかどうか。  |  |
| <b>[Received audio gain mode]</b>         | エンドポイントで、TelePresence Server から受信する音声に設定されている音声ゲイン モード。この表示は [<use default>]、[Automatic]、[Fixed]、[Disabled] のいずれかになります。               | [<use default>]：このエンドポイントは会議のオート ゲイン コントロール設定を継承しています。<br><br>[Automatic]：TelePresence Server は、このエンドポイントが受信する音声のゲインを動的に調整し、他の参加者の受信レベルに合わせます。<br><br>[Disabled]：このエンドポイントが受信する音声のゲイン コントロールは無効化されています。<br><br>[Fixed]：TelePresence Server は、エンドポイントが受信する音声を、固定比率で調整します。この設定は、エンドポイントの設定ページにある [Received audio gain] フィールドで行います。 |

| フィールド  | フィールドの説明  | 使用方法のヒント   |
|--|---|--|
| <b>[Bandwidth]</b>                           | このコールのメディアで使用される、各方向のネットワーク帯域幅。   | エンドポイント グループの場合、合計の帯域幅ではなく、各コールの帯域幅を示します。  |
| <b>[Preview]</b>                             | ビデオ ストリームのサンプルとなる静止画像。  | プレビューの静止画像は、受信と送信の両方のストリーム画面から得たもので、各方向の帯域幅使用量の下に表示されます。プレビューはクリックすると更新されます。<br>ビデオ ストリームがトランスコードされていない場合、送受信されるビデオ ストリームのプレビューは使用できません。そうした場合は [No preview] メッセージが表示されます。 |
| <b>[Endpoint X]</b>                          | (エンドポイント グループのみ) エンドポイント グループ内の各エンドポイントの接続ステータス。  |  |
| <b>[Duration]</b>                            | エンドポイント/エンドポイント グループがこの会議に参加していた時間。   |  |
| <b>[Disconnect]</b>                          | このコントロールを使用すると、エンドポイント/エンドポイント グループを会議から切断できます。   |  |
| <b>[Mute audio from / Unmute audio from]</b> | このコントロールを使用すると、当該エンドポイントから受け取る音声のミュート、ミュート解除が行えます。これは、このエンドポイントからの音声を他の会議参加者が聞けるかどうかの切り替えになります。     |  |
| <b>[Mute audio to / Unmute audio to]</b>     | このコントロールを使用すると、当該エンドポイントに送る音声のミュート、ミュート解除が行えます。エンドポイントに送る音声をミュートにすると、そのエンドポイントでは何も聞こえなくなります。        |  |
| <b>[Mute video from / Unmute video from]</b> | このコントロールを使用すると、当該エンドポイントから受け取るビデオのミュート、ミュート解除が行えます。これは、このエンドポイントからのビデオを他の会議参加者が表示できるかどうかの切り替えになります。 |  |



| フィールド                                    | フィールドの説明   | 使用方法のヒント  |
|--|--|---|
| <b>[Mute video to / Unmute video to]</b> | このコントロールを使用すると、当該エンドポイントに送るビデオのミュート、ミュート解除が行えます。エンドポイントに送るビデオをミュートにすると、そのエンドポイントではビデオを表示できなくなります。  |   |
| <b>[Tidy view]</b>                       | このコントロールを使用すると、エンドポイント/エンドポイントグループに送信される表示レイアウトを整理できます。<br>マルチストリーム エンドポイントの場合、このボタンは無効化されます。  | TelePresence Server は、他の参加者のビデオ ストリームを表示する PiP (Pictures in Picture) を自動的に中央に配置します。また、スクリーン間に配置することで PiP を少し大きくできる場合は移動します。この配置は、参加者が会議に参加したり、会議から退出したりする状況にあわせて動的に行われます。<br>必要に応じてこの表示整理オプションを利用すれば、エンドポイントに送信されるレイアウトで参加者の PiP 配置を手動でリセットして中央に移動できます。 |
| <b>[Send message]</b>                    | これをクリックすると、エンドポイントにメッセージが送信されます。<br><br>[Send message] ページは次のように操作します。<br><br>1. メッセージを入力後、ターゲット エンドポイントでの位置を選択し、メッセージの表示時間 (秒) を指定します。<br><br>2. [Send message] をクリックします。 | このボタンが有効化されるのは、マルチストリームのエンドポイントで次の条件が満たされている場合だけです。<br><ul style="list-style-type: none"><li>• エンドポイントで ActiveControl が利用できる。</li><li>• エンドポイントがメッセージをサブスクライブしている。</li><li>• 会議でメッセージ機能が有効化されている。</li></ul>   |

## エンドポイントまたはエンドポイント グループの統計情報の表示

1. [Conference] に移動し、[Status] ページを選択します。
2. エンドポイントまたはグループ名をクリックします。エンドポイントの [Status] ページが表示されます。
3. [Statistics] をクリックして、[Endpoint Statistics] ページを表示します。

この情報は、次の最大 4 つのセクションに表示されます：[Audio]、[Auxiliary audio]、[Video]、[Content channel]

各チャンネルの統計情報は、[Receive stream] 統計情報および [Transmit stream] 統計情報の 2 つのリストにグループ化されます。

- データは 3 秒ごとに自動更新されます。また手動でのデータ更新も可能で、ブラウザ ページを更新するか [Refresh] をクリックすることで、最新の統計情報を取得できます。

マルチスクリーンのエンドポイントの場合、[Multiscreen Stream Selection] ページが表示されます。目的のストリームを選択すると [Endpoint Statistics] ページに移動し、そのチャンネルに関連したすべてのストリームのデータを参照できます。

マルチストリーム エンドポイントのビデオ ストリームの最大数は、受信が 4 で送信が 16 です。マルチストリーム エンドポイントのビデオ、音声、コンテンツ ストリームは、それぞれ次のように表示されます：[Rx Audio]、[Tx Audio]、[Rx Video]、[Tx Video]、[Content][Multistream Stream Selection] ページでストリームを選択すると、指定したストリームだけの [Endpoint Statistics] ページを表示できます。

**注：**特定のマルチスクリーン チャンネルを選択すると、そのチャンネルに関連付けられたすべてのストリームのデータが表示されます。これに対してマルチストリーム エンドポイントでは、ストリームがそれぞれ独立しているため、ストリームを個別に選択する必要があります。個別に選択すると [Endpoint Statistics] ページにそのストリームのデータだけが表示されます。

**表 29 受信ストリームの統計情報**

| フィールド              | フィールドの説明  |
|--------------------|---|
| [Receive stream]   | 受信ストリームに使用されるコーデック。ビデオおよびコンテンツ チャンネルでは、ビデオ ストリームのサイズも表示されます。  |
| [Encryption]       | ストリームが暗号化されているかどうか。   |
| [Channel bit rate] | ネゴシエーションされて使用可能になった、音声/ビデオ/コンテンツを Cisco TelePresence Server に送信するエンドポイント用帯域幅。   |
| [Receive bit rate] | このフィールドが適用されるのは、ビデオおよびコンテンツ チャンネルの受信ストリームだけです。これは Cisco TelePresence Server がエンドポイントに送信を要求したビット レート (ビット/秒) です。最後に測定されたビット レートはカッコ内に表示されます。 |
| [Received jitter]  | これは、当該チャンネルで Cisco TelePresence Server にパケットが到達したタイミングのパケット間での変動を表します。この数値が小さいほど、パケットが想定どおりに到達していることを示します。                                  |
| [Receive energy]   | このフィールドが適用されるのは音声の受信ストリームだけで、音声信号の強度を示します。単位はミリデシベルで、-34000 のような大きな負の値になるほど無音状態に近づき、ゼロに近い負の値になるほど大きな音になります。                                 |

| フィールド                       | フィールドの説明   |
|-----------------------------|--|
| [Packets received / errors] | Cisco TelePresence Server で受信された音声/ビデオ/コンテンツ パケットの数。2 番目の数値は、シーケンスの中断や不正な RTP などによる、音声/ビデオ/コンテンツのパケット レベルのエラー数です。これは、ビデオ（実際のビデオ データ）に何らかのエラーが生じたパケット数とは異なります。  |
| [Packets total / missing]   | 当該エンドポイントから Cisco TelePresence Server を宛先とした音声パケットの数。2 番目の数値は、受信したが破損していたパケットの数を示します。  |
| [Frames received / errors]  | エンドポイントに現在送信中の音声/ビデオ/コンテンツ ストリームのフレーム レート、および受信した音声/ビデオ/コンテンツ フレームの総数とエラーとなったフレーム数。  |
| [Frame rate]                | このフィールドが適用されるのは、ビデオおよびコンテンツの受信ストリームです。これは、エンドポイントと TelePresence Server 間で 1 秒間に送信/受信されたフレームの数です。   |
| [Fast update requests sent] | 当該チャンネルで TelePresence Server から送信されたクイック更新要求（FUR）の数。たとえば、パケットが失われた場合は TelePresence Server がエンドポイントに FUR を送信します。  |
| [ClearPath FEC]             | <p>当該ストリームで使用される前方誤り訂正（FEC）の統計情報。エンドポイントが FEC をストリームに適用できないか、ActiveControl のネゴシエーションを TelePresence Server とできない場合、この値は [Not supported] となります。</p> <p>それ以外の場合は、オーバーヘッド率、および復元されたパケット数の 2 つの統計情報が示されます。</p> <p>オーバーヘッド率は、元のストリームに対して挿入された FEC パケット数を計測したものです。エンドポイントがストリーム内の各パケットにコピーを 1 つずつ挿入した場合、オーバーヘッドは 100 % になります。エンドポイントがコピーを挿入するパケットが 2 つに 1 つであればオーバーヘッドは 50 % になり、4 つに 1 つであれば 25 % になります。RTCP レポートのタイミングや計測する間隔によっては、実際の統計情報が常にこれらのレベルと完全に一致するとは限りません。</p> <p>復元されたパケット数は、元のパケットが失われたため TelePresence Server がエンドポイントの FEC パケットから復元したパケットの数を単純にカウントしたものです。</p> |
| [ClearPath LTRF]            | LTRF（長時間参照フレーム）が有効な場合に、[N repair frames received] という形式でレポートされます。これは LTRF がストリームで使用された回数を示します。   |

表 30 送信ストリームの統計情報

| フィールド             | フィールドの説明   |
|-------------------|--|
| [Transmit stream] | 送信ストリームに使用されるコーデック。ビデオおよびコンテンツ チャンネルでは、ビデオ ストリームのサイズも表示されます。 |
| [Encryption]      | ストリームが暗号化されているかどうか。  |

| フィールド                                  | フィールドの説明  |
|--|---|
| <b>[Channel bit rate]</b>              | ネゴシエーションされて使用可能になった、音声/ビデオ/コンテンツをエンドポイントに送信する Cisco TelePresence Server 用帯域幅。   |
| <b>[Transmit bit rate]</b>             | このフィールドが適用されるのはビデオおよびコンテンツ送信ストリームだけで、現時点で Cisco TelePresence Server が送信を試みているビット レートを示します。実際のビット レートは Cisco TelePresence Server から出力されるビデオ データのレートを単純に計測したもので、カッコ内に表示されます。  |
| <b>[Packets sent / reported lost]</b>  | エンドポイント宛の音声/ビデオ/コンテンツ パケットの数。2 番目の数値は、エンドポイントで受信されなかったパケットとしてエンドポイントから報告された数です。   |
| <b>[Frame rate]</b>                    | このフィールドが適用されるのは、ビデオおよびコンテンツのストリームです。これは、エンドポイントと TelePresence Server 間で 1 秒間に送信/受信されたフレームの数です。  |
| <b>[Fast update requests received]</b> | 当該チャンネルでエンドポイントから送信され TelePresence Server で受信したクイック更新要求 (FUR) の数。   |
| <b>[ClearPath FEC]</b>                 | 当該ストリームで使用される前方誤り訂正の統計情報。<br>オーバーヘッド率、および復元をレポートされたパケット数の 2 つの統計情報があります。<br>オーバーヘッド率は、元のストリームに対して挿入された FEC パケット数を計測したものです。<br>TelePresence Server がストリーム内の各パケットにコピーを 1 つずつ挿入した場合、オーバーヘッドは 100 % になります。TelePresence Server がコピーを挿入するパケットが 2 つに 1 つであればオーバーヘッドは 50 % になり、4 つに 1 つであれば 25 % になります。TelePresence Server がストリームに FEC を現在適用していない場合、オーバーヘッドは 0 % になります。<br>この数字は、元のパケットが失われたため TelePresence Server の FEC パケットから復元したことをエンドポイントがレポートしたパケットの数です。 |
| <b>[ClearPath LTRF]</b>                | 長時間参照フレームが当該ストリームで使用されているかどうか。エンドポイントが ActiveControl のネゴシエーションを TelePresence Server とできない場合、この値は [Not supported] となります。それ以外の場合、この値は [Enabled] となり、これは LTRF がエンドポイントに送信され、必要に応じて使用できることを意味します。   |

## ユーザ

|                  |    |
|------------------|----|
| ユーザ リストの表示 ..... | 45 |
| ユーザの追加と更新 .....  | 45 |

## ユーザ リストの表示

[Users] ページには、TelePresence Server にあるすべてのユーザ アカウントの概要が示されます。

**表 31 ユーザ リストの詳細**

| フィールド                  | フィールドの説明  |
|------------------------|---|
| <b>[User ID]</b>       | TelePresence Server の Web インターフェイスにアクセスする際に必要なユーザ名。このテキストは任意の文字セットで入力できますが、一部のクライアントは Unicode 文字をサポートしていないので注意してください。   |
| <b>[Name]</b>          | ユーザの名前（オプション。表示されない場合があります）。  |
| <b>[Access rights]</b> | <p>当該ユーザに許可されたロールおよび関連する権限。権限には、[Administrator]、[API access]、[None] の 3 つのレベルがあります。</p> <p>[None]：このユーザは TelePresence Server からロックアウトされます。</p> <p>[API access]：このユーザは、当該 TelePresence Server の XML-RPC インターフェイスで API コマンドを実行できます。</p> <p>[Administrator]：Web インターフェイスへの API アクセスおよび管理アクセス権限を持っています。</p> |

## ユーザの削除

ユーザを選択して、[Delete selected users] をクリックします。[admin] ユーザは削除できません。

## ユーザの追加と更新

TelePresence Server のユーザ アカウントの追加、編集、削除は、ユーザ リストにアクセスすることで行えます ([Users] に移動)。

ユーザ アカウントの追加と編集に関する情報はほとんど同じです。相違点は次の表で説明されています。

## ユーザの追加

1. [Users] に移動します。
2. [Add new user] をクリックします。
3. 必要に応じて次の表を参照し、ユーザ アカウントの詳細を入力します。
4. [Add user] をクリックします。

## ユーザの更新

1. [Users] に移動します。
2. ユーザ ID をクリックします。
3. 必要に応じて次の表を参照し、ユーザ アカウントの詳細を変更します。
4. [Modify user] をクリックします。
5. パスワードを変更する場合は、[Change password] をクリックします。

## ユーザ詳細の参照情報

表 32 ユーザ詳細

| フィールド               | フィールドの説明  | 詳細情報  |
|---------------------|---|---|
| [User ID]           | ユーザのログイン名または ID 番号を指定します。<br>この値は、TelePresence Server へのアクセスに必要なユーザ名です。 | このテキストは任意の文字セットで入力できますが、一部のクライアントは Unicode 文字をサポートしていないので注意してください。<br><b>注：</b> TelePresence Server のコンソールは Unicode 文字を受け付けません。コンソールアクセスに使用するアカウントのユーザ名とパスワードは、ASCII 文字のみに制限されています。 |
| [Name]              | ユーザの名前。   | オプション。  |
| [Password]          | このユーザのパスワードを入力します。  | このテキストは任意の文字セットで入力できますが、一部のクライアントは Unicode 文字をサポートしていないので注意してください。  |
| [Re-enter password] | パスワードを再入力します。   | パスワードの入力フィールドがデフォルトでアクティブになるのは、新規にユーザを追加したときだけです。既存のユーザを更新する場合は、[Change password] をクリックすることで、これらのフィールドが編集可能になります。   |

| フィールド                  | フィールドの説明   | 詳細情報 |
|------------------------|--|------|
| <b>[Access rights]</b> | <p>ユーザのロールをドロップダウンで選択します。ロールに許可される権限には、次のものがあります。</p> <p><b>[None]</b>：このユーザは TelePresence Server からロックアウトされます。</p> <p><b>[API access]</b>：このユーザは、当該 TelePresence Server の XML-RPC インターフェイスで API コマンドを実行できます。</p> <p><b>[Administrator]</b>：Web インターフェイスへの API アクセスおよび管理アクセス権限を持っています。</p> |      |

## ログ

|                        |    |
|------------------------|----|
| イベント ログの使用 .....       | 48 |
| イベント キャプチャ フィルタ .....  | 48 |
| イベント表示フィルタ .....       | 49 |
| プロトコル メッセージのロギング ..... | 50 |
| Syslog を使用したロギング ..... | 51 |
| コール詳細レコードの使用 .....     | 54 |
| API クライアント .....       | 56 |
| フィードバック受信者 .....       | 57 |
| Call Home の使用 .....    | 57 |

## イベント ログの使用

高度なトラブルシューティングを必要とする複雑な問題が発生した場合は、TelePresence Server ログから情報を収集することが必要な場合があります。通常、こうしたログの取得は、カスタマー サポートの支援を受けて実行します。

## イベント ログ

TelePresence Server は、サブシステムで生成されたメッセージのうち、最後にキャプチャされたものから 2000 件保存しています。これらは [Event log] ページに表示されます ([Logs > Event log])。これらのメッセージは一般に情報の提供を意図したのですが、状況によっては [Warning] または [Error] がイベント ログに表示される場合もあります。

カスタマー サポートは、TelePresence Server の動作やパフォーマンスに特定の問題が発生した場合、ログに記録されたメッセージを解釈して、その重要度を判定します。

次の作業を実行できます。

- 列ヘッダーをクリックしてイベントをソートします。
- ページ番号をクリックすると、ログの表示を 100 イベント単位で移動できます。
- すべてのシステム ログを 1 つの zip ファイルとしてダウンロードするには、[Download system logs] をクリックします。
- イベント ログをテキストとしてダウンロードするには、[Logs] > [Event log] に移動して、[Download event log] をクリックします。
- 表示パラメータを変更すると、関心のある情報だけに絞り込めます ([Logs] > [Event display filter])。
- トレースで収集する詳細レベルを変更するには、[Logs] > [Event capture filter] のページを編集します。

**注：** イベント キャプチャ フィルタの変更は、カスタマー サポートから指示された場合だけにしてください。これらの設定を変更すると、TelePresence Server のパフォーマンスを低下させる可能性があります。

- 保管や分析用に、ネットワークにある複数の Syslog サーバにイベント ログを送信することができます。送信するサーバは [Logs] > [Syslog] のページで指定します。
- ログを消去するには、[Clear event log] をクリックします。

## イベント キャプチャ フィルタ

イベント キャプチャ フィルタは、TelePresence Server でどのイベントをログに保持するかを指定します。デフォルトでこのフィルタは、すべての TelePresence Server のサブシステムから、エラー、警告、および情報イベントを取得するように設定されています。



**注：** イベント キャプチャ フィルタの変更は、カスタマー サポートから指示された場合だけにしてください。

たとえば TelePresence Server に生じた問題のトラブルシューティングをする際には、サポート担当者から、次のようにしてビデオ サブシステムの詳細なトレースをキャプチャするように指示されることがあります。

1. [Logs] > [Event capture filter] に移動します。
2. [Detailed trace] を [VIDEO] ドロップダウン リストから選択します。  
パフォーマンスが影響を受ける可能性があることを、TelePresence Server が警告します。
3. [OK] をクリックします（これは一時的に詳細レベルを上げるだけで、問題の解決後に戻すことができます）。
4. [Update settings] をクリックします。

TelePresence Server は、他のすべてのサブシステムのデフォルト情報にあわせて、ビデオ サブシステムから詳細なトレース情報を収集するようになります。

## イベント表示フィルタ

イベント表示フィルタを使用すると、イベント ログのサブセットの表示や、特定エントリの強調表示ができます。このフィルタが機能する対象は保存されたエントリであり、どのイベントが取得されるかには影響しません。

イベント表示フィルタを変更するには、[Logs] > [Event display filter] に移動します。

## メッセージのテキストによるフィルタリング

1. [Filter string] に入力すると、保存されたイベントのうち、指定した文字列を含むものだけ表示されます。
2. [Highlight string] に入力すると、フィルタリングされた結果の中で指定した文字列が強調表示され簡単に見つけることができます。
3. [Update display] をクリックします。

TelePresence Server は、イベント ログをフィルタリングおよび強調表示された状態で表示します。

## 現在の表示レベル

TelePresence Server には、すべてのイベントをログに記録する多数のサブシステムがあります。サブシステムごと、またはすべてのサブシステムに対して、表示する詳細レベルを変更できます。

たとえば、SIP エラーのみを確認する場合には、次の手順を実行します。

1. ページの下部までスクロールして、[Set all to:] ボタンとその横のドロップダウンを表示させます。
2. ドロップダウンで [None] を選択します。
3. [Set all to:] をクリックします。  
すべてのサブシステムの表示レベルが [None] に変更されます。
4. SIP サブシステムの横のドロップダウン リストで [Errors only] を選択します。
5. [Update settings] をクリックします。  
TelePresence Server は SIP エラーだけを表示します。

## プロトコル メッセージのロギング

[Protocols log] ページでは、TelePresence Server が送受信する各種プロトコルのメッセージが記録されます。

メッセージの量がパフォーマンスに影響するため、プロトコル ロギングはデフォルトでは無効化されていますが、トラブルシューティングのサポートのためにカスタマー サポートから有効化するように求められる場合があります。

プロトコル メッセージのロギングを開始するには、次の手順を実行します。

1. ログに記録するプロトコルを選択します。
2. [Enable protocols logging] をクリックすると、指定したプロトコル メッセージの記録が開始されます。
3. 解決したい問題の発生状況を再現するのに必要なテストを実行します。
4. [Download as XML] をクリックして、サポートに送信可能な XML ファイルとしてログを取得します。

問題が解決したら、今後のユニットのパフォーマンスに影響が出ないように [Disable protocols logging] および [Clear log] をクリックします。

| フィールド             | 説明   |
|-------------------|--|
| [Current status]  | [Enabled] または [Disabled]。デフォルトは [Disabled] です。 |
| [Messages logged] | ログに記録されたメッセージ数。                                |

| フィールド                     | 説明  |
|---------------------------|---|
| <b>[Protocol filters]</b> | <ul style="list-style-type: none"> <li>• [BFCP]</li> <li>• [SIP]</li> <li>• [XCCP]</li> </ul> <p>キャプチャするプロトコル メッセージのチェックボックスをオンにします。これらはキャプチャ フィルタであり、表示フィルタではないので、特定のプロトコルのチェックを外してプロトコル ログイングを有効にすると、TelePresence Server はチェックが外されたプロトコルのメッセージを一切キャプチャしなくなります。</p> <p>ログイングが有効になっている間は、どのプロトコルをログに記録するかは変更できません。キャプチャ フィルタを変更するには、ログイングを無効にし、チェックボックスの変更をしてから、再度ログイングを有効にします。</p> |

## プロトコル メッセージのリモート ログイング

プロトコル ログは HTTP または HTTPS で使用できるので、ログの記録先をリモート デバイスにすることができます。プロトコル ログイングを有効または無効に設定しても、リモート デバイスへのログ送信は無効になりません。最大 2 つの同時ログ ストリームを随時利用できます。

リモート デバイスへのプロトコル メッセージのログイングを開始させるには、次の手順を実行します。

1. リモート デバイスから `http[s]://<ip address>/protocols_log_stream` への HTTP POST 要求を送信します。この POST 要求には、有効なユーザとパスワード パラメータを `authenticationUser=username&authenticationPassword=password` の形式で指定しておく必要があります。

次の記述は `wget` での使用例です (Linux システム用)。

```
wget https://<IP address>/protocols_log_stream --post-data=authenticationUser=username&authenticationPassword=password
```

(API 権限のみのユーザが有効と想定)。

2. これ以降、プロトコル ログの全コンテンツは、この TCP 接続を介してリモート デバイスに戻されます。ログ ストリームは、リモート デバイスで TCP 接続が中断されるまで継続されます。

## Syslog を使用したログイング

保管や分析用に、ネットワークにある複数の Syslog サーバに [イベント ログ](#) を送信することができます。

syslog ファシリティを設定するには、[Logs] > [Syslog] に移動します。

## Syslog の設定

syslog の設定時は、次の表を参照してください。

**表 33 Syslog 設定**

| フィールド                 | フィールドの説明   | 使用方法のヒント  |
|-----------------------|--|---|
| [Host address 1 to 4] | 4 つまでの syslog レシーバ ホストの IP アドレスを入力します。   | 設定した各ホストに送信されたパケット数は、IP アドレスの横に表示されます。  |
| [Facility value]      | <p>Cisco TelePresence Server からのイベントを Syslog ホストで識別するための設定可能な値。次のオプションから選択します。</p> <ul style="list-style-type: none"> <li>• [0] : カーネル メッセージ</li> <li>• [1] : ユーザレベル メッセージ</li> <li>• [2] : メール システム</li> <li>• [3] : システム デーモン</li> <li>• [4] : セキュリティ/認証メッセージ (注 1 を参照)</li> <li>• [5] : syslogd 内部生成メッセージ</li> <li>• [6] : ライン プリンタ サブシステム</li> <li>• [7] : ネットワーク ニュース サブシステム</li> <li>• [8] : UUCP サブシステム</li> <li>• [9] : クロック デーモン (注 2 を参照)</li> <li>• [10] : セキュリティ/認証メッセージ (注 1 を参照)</li> <li>• [11] : FTP デーモン</li> <li>• [12] : NTP サブシステム</li> <li>• [13] : ログ監査 (注 1 を参照)</li> </ul> | <p>Cisco TelePresence Server として記憶できる値を選択します。</p> <p><b>注 1 :</b> 各種オペレーティング システムのデーモンとプロセスでは、ファシリティ値の 4、10、13、14 を、セキュリティ/認証、監査、およびアラート メッセージ用に使用しているので、これらは識別しにくい状況になっています。</p> <p><b>注 2 :</b> 各種オペレーティング システムでは、ファシリティ値の 9 と 15 の両方がクロック (cron/at) メッセージに使用されています。</p> <p>明示的にファシリティ値が割り当てられていないプロセスおよびデーモンは、「ローカル使用」ファシリティ値 (16 ~ 21) のいずれかを使用する場合もあれば、「ユーザレベル」ファシリティ値 (1) を使用する場合もあるので、これらの値の 1 つを選択することを推奨します。</p> |

| フィールド | フィールドの説明   | 使用方法のヒント |
|-------|--|----------|
|       | <ul style="list-style-type: none"> <li>• [14] : ログアラート (注1を参照)</li> <li>• [15] : クロックデーモン (注2を参照)</li> <li>• [16] : ローカル使用0 (local0)</li> <li>• [17] : ローカル使用1 (local1)</li> <li>• [18] : ローカル使用2 (local2)</li> <li>• [19] : ローカル使用3 (local3)</li> <li>• [20] : ローカル使用4 (local4)</li> <li>• [21] : ローカル使用5 (local5)</li> <li>• [22] : ローカル使用6 (local6)</li> <li>• [23] : ローカル使用7 (local7)</li> </ul> |          |

## Syslog の使用

syslog レシーバホストに転送されるイベントは、イベントログのキャプチャフィルタによって制御されています。

syslog サーバを定義するには、IP アドレスを入力し、[Update syslog settings] をクリックします。設定された各ホストに送信されたパケット数は、IP アドレスの横に表示されます。

**注：**次のインジケータでイベントの重大度が示されます。

- [0] 緊急：システムが使用不能 (Cisco TelePresence Server では不使用)
- [1] アラート：すぐにアクションを実行する必要あり (Cisco TelePresence Server では不使用)
- [2] 重要：クリティカルな状態 (Cisco TelePresence Server では不使用)
- [3] エラー：エラー状態 (Cisco TelePresence Server の *error* イベントで使用)
- [4] 警告：警告状態 (Cisco TelePresence Server の *warning* イベントで使用)
- [5] 注意：正常だが重要な状態 (Cisco TelePresence Server の *info* イベントで使用)
- [6] 情報：情報メッセージ (Cisco TelePresence Server の *trace* イベントで使用)
- [7] デバッグ：デバッグレベルメッセージ (Cisco TelePresence Server の *detailed trace* イベントで使用)

## コール詳細レコードの使用

TelePresence Server は、最大 2000 件のコール詳細レコードを表示できます。ただし TelePresence Server では、コール詳細レコードを長期間保持するようには考慮されていません。CDR ログを保持したい場合は、ダウンロードして別の場所に保存する必要があります。

CDR ログがいっぱいになると、最も古いログが上書きされます。

CDR ログの表示と制御をするには、[Logs] > [CDR log] にアクセスします。使用可能なオプションの詳細および表示される情報については、次の表を参照してください。

- [コール詳細レコードのログ制御](#)
- [コール詳細レコードのログ](#)

## コール詳細レコードのログ制御

CDR のログには、多くの情報が記録されます。ここで行える制御は、有効な情報の選択表示に役立ちます。必要な変更の設定後 [Update display] をクリックすると、変更が適用されます。オプションの説明については、次の表を参照してください。

表 34 ステータスおよび表示

| フィールド             | フィールドの説明  | 使用方法のヒント   |
|-------------------|---|--|
| [Messages logged] | 現在ログにある CDR の数。   |  |
| [Filter records]  | TelePresence Server がログに記録する CDR レコードタイプの一覧。                            | すべてのレコードを表示させるには、すべてのボックスを空白のままにします。特定のレコードタイプだけが必要であれば、該当するレコードのボックスをオンにします。    |
| [Filter string]   | このフィールドは、表示されるコール詳細レコードの範囲の制限に使用します。フィルタ文字列では、大文字と小文字が区別されません。          | フィルタ文字列の適用先は、ログ表示の [Message] フィールドです。特定レコードが展開して詳細表示されている場合、それらにもフィルタ文字列は適用されます。 |
| [Expand details]  | デフォルトの CDR ログの表示は、各イベントの簡単な説明を示すだけです。利用可能な場合は、リストのオプションを選択すると詳細が表示されます。 | [All] を選択すると、その他のオプションの選択状況にかかわらず、すべてのメッセージが最も詳細に表示されます。                         |

## コール詳細レコードのログ

コール詳細レコードのログは、最大 2000 行まで含む長い表で表示され、複数のページにまたがる場合もあります。ログの表示は、上記のフィルタリングに加えて、次の操作が可能です。

- どの列もヘッダーをクリックして、昇順または降順での並べ替えができます。
- 特定の会議または参加者の GUID に関連するすべてのレコードを表示するようにログをフィルタリングするには GUID をクリックします（フィルタリングを元に戻すには、[Show all] をクリックします）。
- 表示されているレコードリストの特定ページに移動するには、ページ番号をクリックします。

ログをテキスト エディタで処理したり、将来の参照用にアーカイブしたりする場合は、[Download as XML] をクリックします。このボタンは現在保存されているすべてのレコードをダウンロードするので、Web ページで設定した表示フィルタは無視されます。

**注：**ユニットの負荷が大きい状況では CDR ログをダウンロードしないでください。パフォーマンスが低下する場合があります。

ログのメモリを空にするには [Clear all records] をクリックします。

**警告：**[Clear all records] は、TelePresence Server にあるレコードをすべて完全にクリアします。一度クリアされたレコードは再取得できません。

## CDR ログの参照情報

次の表では、CDR ログのフィールドについて説明します。

**表 35 CDR ログの詳細**

| フィールド               | フィールドの説明               | 使用方法のヒント   |
|---------------------|------------------------|--|
| <b>[#]</b> (レコード番号) | コール詳細レコードの一意のインデックス番号。 |  |
| <b>[Time]</b>       | コール詳細レコードが作成された時刻。     | レコードはさまざまな会議イベントの発生に応じて作成されます。レコードの作成時刻は、イベントが発生した時刻です。<br><br>受信した CDR ログ イベントは、ローカルのタイム スタンプで保存されます (UTC ではありません)。<br><br>時刻が変更された場合 (システム時刻の変更や NTP 経由での更新)、CDR ログに変更後の新しい時刻を示すイベントが記録されます。既存のレコードについては、タイム スタンプの変更は行われません。 |
| <b>[Conference]</b> | レコードに適用される会議の GUID。    | 新規の会議が作成される際に、グローバル一意識別子 (GUID) が付与されます。特定の会議に関係するすべてのレコードにはこの識別子が表示されるので、これを利用すると会議イベントの監査をしやすくなります。<br><br>GUID をクリックすると、該当する会議の関連レコードだけが表示されます。   |

| フィールド                | フィールドの説明                        | 使用方法のヒント  |
|----------------------|---------------------------------|---|
| <b>[Participant]</b> | レコードに適用される参加者の GUID。            | 個々の参加者はグローバル意識別子（GUID）で示されるので、これを利用すると、レコード管理がシンプルになります。<br>GUID をクリックすると、該当する参加者の関連レコードだけが表示されます。  |
| <b>[Message]</b>     | コール詳細レコードのタイプおよび簡単な説明（使用可能な場合）。 | [>>] をクリックすると、当該タイプの全メッセージの詳細を展開できます。<br>この操作は、[All] を選択して [Update display] をクリックすると、すべてのメッセージに対して実行できるので、[Filter string] と併用すると、特定の単語を含んだメッセージを持つレコードの検索に便利です。 |

## API クライアント

TelePresence Server は、ユニットへの要求を行った最新 10 個の API クライアントをログに記録します。このリストを表示させるには、[Logs] > [API clients] をクリックします。

5 分より長い間 API 要求を行っていないクライアントはグレーで表示されます。

API クライアントのリストを更新するには、[Refresh] をクリックします。すべてのデータをクリアするには、[Reset statistics] をクリックします。これでクリアされるのは、API クライアントの現在のリストです。クライアントが新しいコマンドを送信すれば、このリストに追加されます。

このページはデフォルトで、[Time since last request] 列でソートされています。

**表 36 API クライアントの詳細**

| フィールド                            | フィールドの説明                       | 使用方法のヒント  |
|----------------------------------|--------------------------------|---|
| <b>[Client IP]</b>               | 要求を送信するクライアントの IP アドレス。        |   |
| <b>[Time since last request]</b> | クライアントが最後に要求を送信してからの時間。        |   |
| <b>[Last request method]</b>     | API クライアントが最後に送信した API 要求メソッド。 |   |
| <b>[Last request user]</b>       | クライアントが API 要求で使用したユーザ名。       | 最後に送信した API 要求が認証に失敗したクライアントは、ここで <b>[(authentication failed)]</b> のフラグが付けられます。 |



| フィールド                                       | フィールドの説明              | 使用方法のヒント  |
|---|-----------------------|---|
| <b>[Requests received since last reset]</b> | 最後にリセットされてから受信した要求の数。 | 1 秒以内に複数の要求が受信された場合、カッコ内に秒あたりの平均数が表示されます。<br><br>現在のしきい値は、秒あたり 1.8 要求です。<br><br>「過剰要求」クライアントは、TelePresence Server と現在通信している場合にだけフラグが付けられます。<br><br>最後のリセットからの経過時間が、テーブル下側のボタンの横に表示されます。 |

## フィードバック受信者

TelePresence Server はフィードバック イベントをパブリッシュすることで、何らかの変更が生じた際にイベントをリッスンしている受信者がアクションをとれるようにしています。フィードバック受信者のリストを表示するには、[Logs] > [Feedback receivers] をクリックします。

設定されたすべてのフィードバック受信者を削除するには、[Delete all] をクリックします。この操作は取り消すことができません。

リスト中の各受信者は、次の詳細情報を保持しています。

表 37 フィードバック受信者の詳細

| フィールド                 | フィールドの説明      | 使用方法のヒント  |
|-----------------------|---------------|---|
| <b>[Index]</b>        | 受信者のリスト内での位置。 |   |
| <b>[Receiver URI]</b> | 受信者の完全修飾 URI。 | 受信者は Cisco TelePresence Management Suite などのソフトウェア アプリケーションである可能性があり、適切な API コールを使用してフィードバック イベントに応答し、フィードバックの送信元から変更リストを取得することができます。 |

## Call Home の使用

**注：** TelePresence Server は現在匿名でのレポートしかサポートしていません。

TelePresence Server は、サーバのステータスや発生した障害のレポートを Cisco Call Home サービスに送信できます。TelePresence Server から Call Home へのレポート送信には常にセキュアな接続 (HTTPS) が使用されます。

Call Home が無効な場合は（デフォルト設定）、[Call Home mode] が選択されるまで、デバイスからはどのタイプのレポートも送信されません。Call Home を有効にすると、手動でのレポート送信、または、自動送信機能の設定が可能です。

[Anonymous Call Home] を使用する場合、匿名で送信されたレポートは表示できません。これを利用できるのはシスコのエンジニアだけで、潜在的な問題の診断目的でのみ使用されます。

**注：** Call Home レポートについて質問がある場合は、Cisco TAC にお問い合わせください。

[Call Home mode] で [anonymous] を選択した場合、[Automatic Call Home enabled] をオンにして、TelePresence Server が自動的にレポートを送信するように設定できます。この変更が適用されると、デバイスは保留中のレポートを即座に送信します。それ以降は、想定外のデバイスの再起動やメディア リソースの再起動についての診断レポートは自動的に送信され、手動での操作は必要ありません。

Call Home を自動で実行したくない場合は、[Call Home now] をクリックすれば、いつでも手動でレポートを送信できます。

[Device inventory] レポートは常に使用可能なもので、これが存在していても特殊な状況やエラーが発生しているわけではありません。Call Home の自動処理が有効な場合、TelePresence Server は起動時に毎回これらのレポートを送信します。

**Call Home を設定するには、次の手順を実行します。**

1. [Logs] > [Call Home] に移動します。  
[Status] セクションには、この機能が有効であるかどうか、および、現在使用できるレポートが表示されます。
2. [Call Home mode] で、[Anonymous Call Home] を選択します。
3. （オプション）手動操作なしで TelePresence Server にレポートを送信させる場合は、[Automatic Call Home enabled] をオンにします。
4. [Apply changes] をクリックします。  
"Are you sure you want to apply configuration changes?" という確認ダイアログが表示されます。
5. 次に進むには [OK] を、設定変更を破棄するには [Cancel] をクリックします。  
[Automatic Call Home] が有効な場合、TelePresence Server は保留中の全レポートをすぐに送信します。
6. （オプション）[Current reports] にある現在のレポートを手動で送信するには、[Call Home now] をクリックします。

表 38 ステータス フィールド

| フィールド                                    | 説明  |
|--|---|
| <b>[Call Home status]</b>                | <p>[Call Home status] を次のいずれか 1 つで示します。</p> <ul style="list-style-type: none"> <li>• [Automatic – Anonymous Call Home] : [Call Home mode] が有効になっていて [Automatic Call Home enabled] がオンになっている。</li> <li>• [Enabled – Anonymous Call Home] : [Call Home mode] が有効になっていて [Automatic Call Home enabled] がオフになっている。</li> <li>• [Disabled] (デフォルト)</li> </ul> <p>[Call Home mode] が無効になっている場合、起動時に TelePresence Server はこれをイベント ログに記録します。[Call Home mode] が有効 ([Anonymous Call Home]) になっているのにレポートの自動送信が設定されていない場合も、TelePresence Server はメッセージをログに記録します。</p> |
| <b>[Current reports]</b>                 | 使用可能なレポートのリスト。  |
| <b>[Submission status]</b>               | <p>日付と時刻など、最新のレポートの送信ステータスを示します。</p> <p>レポート送信がされていない場合、ステータスは [Not sent] となります。</p>  |
| <b>[Last submitted report reference]</b> | このフィールドが表示されるのは [Unexpected media resource restart diagnostics] または [Unexpected device restart diagnostics] レポートが送信された場合だけです。レポートの分析用に、この参照番号を Cisco TAC に提供する場合があります。  |
| <b>[Call Home now]</b>                   | <p>[Current reports] にある現在のレポートを手動で送信します。</p> <p>手動でのレポート送信時または、自動レポート送信の有効化時には、データがシスコに送信されることを確認するポップアップが表示されます。</p> <p>レポートの送信は 3 回まで再試行されます。3 回目の試行に失敗すると、Web インターフェイスにバナーが表示されます。</p>  |

表 39 設定フィールド

| フィールド                                | 説明  |
|--------------------------------------|---|
| <b>[Call Home mode]</b>              | [Anonymous Call Home] を有効にします (デフォルトは、レポートを送信できない [Disabled] です)。         |
| <b>[Automatic Call Home enabled]</b> | TelePresence Server から、必要に応じて診断レポートを送信したり、起動時にインベントリ レポートを送信したりできるようにします。 |

## 参照先

|  |    |
|--|----|
| コンテンツ チャンネルのサポート .....                   | 60 |
| レイアウト表示での参加者の表示法について .....               | 61 |
| レイアウト エクスペリエンスの改善 .....                  | 66 |
| エンドポイントのタイプ .....                        | 67 |
| エンドポイントの相互運用性 .....                      | 68 |
| TelePresence Server の会議のキャパシティについて ..... | 69 |
| マニュアルの入手方法およびテクニカル サポート .....            | 72 |
| シスコの法的情報 .....                           | 72 |
| シスコの商標または登録商標 .....                      | 73 |

## コンテンツ チャンネルのサポート

ほとんどの TelePresence エンドポイントでは、コンテンツ チャンネルと呼ばれる 2 番目のビデオ チャンネルを使用できます。通常、これはライブ ビデオと並行して実行されるプレゼンテーションに使用されます。

- SIP システムでは、コンテンツに BFCP というプロトコルを使用します。
- Cisco CTS システムおよび他の TIP システムでは、コンテンツ共有の制御に TIP を使用します。

2 番目のビデオ チャンネルをサポートしていないエンドポイントも考慮して、TelePresence Server ではメイン ビデオでのコンテンツ使用が可能です。この機能が有効化されている場合、そうしたエンドポイントに対して TelePresence Server は、メイン ビデオ チャンネルでコンテンツ送信を行います。コンテンツ チャンネルがアクティブにされている間、コンテンツ チャンネルは通常のビデオで構成されます（コンテンツは最大ペインに表示され、他の参加者のビデオ ストリームはディスプレイ下部中央に並べて配置されたペインに表示されます）。

## レイアウト表示での参加者の表示法について

**注：**TelePresence Server がリモート管理モードで動作している場合、TelePresence Server のユーザ インターフェイスからはこれらのオプションを設定できません。

このページの内容

- [会議のレイアウト](#)
  - [1 スクリーン システムに送信されるレイアウト](#)
  - [2 スクリーン システムに送信されるレイアウト](#)
  - [3 スクリーン システムに送信されるレイアウト](#)
  - [4 スクリーン システムに送信されるレイアウト](#)
- [1 テーブル モード](#)
- [表示レイアウトに影響する設定オプション](#)
  - [セルフ ビューの設定](#)
  - [会議設定での全画面表示](#)
  - [メイン ビデオ内コンテンツの許可](#)
  - [エンドポイントの囲み枠の表示設定](#)
- [参加者への「重要」マーク付け](#)
- [ミュートになった参加者](#)

## 会議のレイアウト

TelePresence Server では、システムのスクリーン数および他の会議参加者の特性に応じて、異なるレイアウトが選択されます。エンドポイントでは、相手先カメラ制御機能や DTMF キー 2 および 8 を使用してレイアウトを選択することもできます。また、後述する選択肢の 1 つを事前設定することもできます。TelePresence Server では、1 ～ 4 スクリーンの標準エンドポイントおよびイマーシブ エンドポイントが利用可能で、会議に参加しているシステムを任意に組み合わせて、タイプの異なるシステム上に表示させることができます。

TelePresence Server の基本的な動作として、「最大音量」の参加者が最も目立つレイアウトのペインに表示されます。使用可能なペイン数をコントリビュータの数が超過した場合、「最小音量」の参加者は表示から除外されます。

## 1 スクリーン システムに送信されるレイアウト

デフォルトのレイアウトは、画面全体または参加者ごとのレイアウトに設定できます。このデフォルト設定は参加者がオーバーライドすることができ、レイアウト選択の変更には相手先カメラ制御機能または DTMF キー 2 および 8 を使用します。

ActivePresence レイアウトの場合、最大音量の参加者は全画面で表示され、他の追加参加者は画面下部に位置する最大 6 つの均等サイズのオーバーレイ ペインに表示されます。追加の参加者にはすべて [Participant Overflow] アイコンが付けられます。

TelePresence Server における 1 スクリーン エンドポイントのレイアウトは、[Default layout type for single-screen endpoints] の設定に従って構成されます。

**表 40 1 スクリーン エンドポイントに送信されるレイアウト**

|  |   |
|--|---|
|  | [Single] : エンドポイントは、単一の全画面ペインに表示されます。   |
|  | [ActivePresence] : エンドポイントは 1 つの全画面ペインに表示され、追加の参加者は、画面下部に配置された最大 6 つの均等サイズのオーバーレイ ペインに表示されます。追加の参加者には [Participant Overflow] アイコンが付けられ、非表示の参加者数とともに画面右下に表示されます。 |
|  | [Prominent] : エンドポイントは 1 つの大型ペインに表示され、他の追加参加者は、画面下部に配置された最大 6 つの均等サイズのペインに表示されます。追加の参加者には [Participant Overflow] アイコンが付けられ、非表示の参加者数とともに画面右下に表示されます。             |
|  | [Equal] : エンドポイントは、最大 4 X 4 個の均等サイズ ペインにグリッド パターンで表示されます。   |
|  | ペインの各行には、リモート マルチスクリーン システムの各画面を表示するか、少ない画面数のリモート システムを組み合わせるかのいずれかが可能です。   |




## 2 スクリーン システムに送信されるレイアウト

**表 41 2 スクリーン システムに送信されるレイアウト**

|  |   |
|--|---|
|  | TelePresence Server が会議室切り替え表示モードになっていて、1 つの会議に 3 または 4 スクリーンの TelePresence システムが参加している場合、このレイアウトが TelePresence Server からその会議に参加している 2 スクリーン システムに送信されます。 |
|  | 4 つのペインの各行には、リモートの 4 スクリーン システムの 4 画面を表示するか、少ない画面数のシステムを組み合わせるかのいずれかが可能です。  |
|  | TelePresence Server がこのレイアウトを適用するのは、会議で 1 または 2 スクリーン システムしか使われていない場合です (すべてのビデオ ストリームが使用可能なペインに収まる場合)。可能な場合、オーバーレイ ペイン (最大 6) は自動的に中央に配置されます。            |

### 3 スクリーン システムに送信されるレイアウト

**表 42 3 スクリーン システムに送信されるレイアウト**

|  |   |
|--|---|
|   | <p>PIP なしのレイアウトが利用可能で、強制的に PIP が非使用にされます。DTMF 2 および 8/FECC を使用して選択できます。</p>   |
|   | <p>TelePresence Server が会議室切り替え表示モードになっていて、1 つの会議に 3 または 4 スクリーンの TelePresence システムが参加している場合、このレイアウトが TelePresence Server からその会議に参加している 3 スクリーン システムに送信されます。</p> <p>4 つの大型ペインの中央行には、リモートの 4 スクリーン システムの 4 画面を表示するか、1 ~ 3 画面の会議参加者を組み合わせて表示するかのいずれかが可能です。この行を中央に正しく配置するため、TelePresence Server は 3 スクリーンの中央部分にペインを表示して、左側スクリーンの左端または右側スクリーンの右端を使用しないようにします。</p> |
|  | <p>TelePresence Server がこのレイアウトを 3 スクリーン システムに適用するのは、会議に 4 スクリーンの TelePresence システムが使われていない場合です。</p>  |

### 4 スクリーン システムに送信されるレイアウト

TelePresence Server がこのレイアウトを会議の 4 スクリーン システムに送信するのは、次の場合です。



4 つのペインの各行（4 つの全画面ペインの行または、6 つの小型オーバーレイ ペインの行）には、4 スクリーン システムを表示するか、少ない画面数のリモート システムを組み合わせて表示するかのいずれかが可能です。可能な場合、オーバーレイ ペインは自動的に中央に配置されます。

## 表示レイアウトに影響するエンドポイント設定オプション

### セルフ ビューの設定

エンドポイントの [Self view] 設定で指定されるのは、TelePresence Server にエンドポイントで自分のビデオ ストリームを表示させるようにするかどうか、つまり、参加者が自分自身の様子を見られるようにするかどうかです。この設定がオフの場合、エンドポイントは自分のビデオ ストリームを表示しません。

エンドポイントに自分のビデオを表示させる場合、使用可能な表示ペインに参加者を配置する際に TelePresence Server はセルフビューを常に最後に配置します。これは仮にそのコール内で最大音量の参加者の 1 人であったとしても（つまり他の会議参加者に対しては目立つ形式で表示されている）同じです。

## 1 スクリーン エンドポイントの全画面表示

TelePresence Server が参加者をレイアウト ペインに配置する際、「最大音量」の参加者を優先して最も目立つペインに表示し、「最小音量」の参加者はより小さなペインに表示します。ただし、TelePresence システム（通常使用するのは大型で高解像度のディスプレイ）と、より低品質のビデオしか利用できないシステム（動画対応の携帯電話など）が混在する会議の場合は、低解像度の参加者が全画面ペインに表示されるのは必ずしも望ましくないことがあります。

1 スクリーン システムの場合は [Show full screen view of single-screen endpoints] 設定により、エンドポイントを大型の全画面ペインに表示するのを許可するかどうかと、許可する場合はその方法を指定します。設定できるのは、[Always]、[Dynamic]、[Disabled] です。

- [Always] : 1 スクリーン エンドポイントがマルチスクリーン エンドポイントのメイン ペインに表示されることを常に許可します。
- [Dynamic] : 1 スクリーン エンドポイントがマルチスクリーン エンドポイントのメイン ペインに表示されるのは、会議に他のマルチスクリーン エンドポイントが参加していない場合です。マルチスクリーン エンドポイントが会議に参加すると、1 スクリーン エンドポイントは PiP ストリップに下がります。
- [Disabled] : 1 スクリーン エンドポイントがマルチスクリーン エンドポイントのメイン ペインに表示されることはありません。

マルチスクリーンのエンドポイントおよびエンドポイント グループでは、この設定は表示されません。

## メイン ビデオ内コンテンツの許可

追加チャンネルをサポートしていないエンドポイントはそのままではコンテンツが見られないため、この機能によって、エンドポイントのメイン ビデオ チャンネルで TelePresence Server から会議コンテンツを送信できるようにしています。



コンテンツ チャンネルのストリームには構成されたレイアウト内の最大ペインが割り当てられ、メイン ビデオ チャンネルに表示されます。コンテンツ ストリームのレイアウト下部には、他の参加者を最大 6 名まで表示するペインが並べて配置されます。連続ペインは中央に配置されます。



## エンドポイントの囲み枠の表示設定

[Show borders around endpoints] が有効になっていると、TelePresence Server は小型ペインに表示されている参加者に囲み枠を付けます。この囲み枠は、全画面ペインで表示中の参加者には付けられません。

TelePresence Server が描画する囲み枠の色は、発言中のスピーカーがブルーで、その他はグレーです。たとえば、全員がミュートにしている場合や、誰も発言していない場合など、強調表示される発言中のスピーカーがない状況も存在します。

この設定を特定のエンドポイントで有効にしても、そのエンドポイントに送信されるビデオ レイアウトに囲み枠が表示されるだけで、他の参加者に表示される際にその発言者が同じように枠で囲まれるわけではありません。他の参加者の表示にはそれぞれの [Show borders around endpoints setting] 設定が反映されます。

## 参加者への「重要」マーク付け

個々の会議では、1人のアクティブな参加者を「重要」と設定できます。これは、どのコントリビュータをどのレイアウトペインに表示するかを TelePresence Server が決定する際に、発言の音量の大きさに基づいて配置するのではなく、この設定をした参加者を最優先にするとということです。「[会議ステータスの表示](#)」にあるエンドポイントの管理設定を参照してください。

## ミュートになった参加者

### 音声ミュート

Web インターフェイスで自分の音声をミュートにした参加者の音声は、会議に出力されません。また TelePresence Server は表示レイアウト ペインに参加者を配置する際に、ミュートにしている参加者よりもミュートにしていない参加者を優先します。

他の参加者に対して、ミュートにしている参加者についての特別な表示はされないので注意してください。単純に、その参加者の話す声が聞こえなくなるだけです。

### ビデオ ミュート

Web インターフェイスで自分のビデオをミュートにした参加者のビデオは、会議に出力されません。音声のミュートを別途設定しない限り、音声の出力は続きます。

## レイアウト エクスペリエンスの改善

TelePresence Server はデフォルトでマルチストリーム ビデオをサポートしています。

これは、マルチストリームに対応したエンドポイントでは、複数のビデオ ストリームをローカルで 1 つの会議レイアウトに構成することができ、ユーザ エクスペリエンスが向上することを意味します。ただし、すべてのエンドポイントが可能な限り最適なエクスペリエンスになるよう引き続きサポートされます。

そのため TelePresence Server は、マルチストリームの送信機能をアドバタイズし、マルチストリーム対応のエンドポイントが必要なストリームをサブスクライブできるようにします。

TelePresence Server はマルチストリームに対応したエンドポイントから最大 4 つのメイン ビデオ ストリームを受信できます。また、同一のビデオ ソースを異なる解像度とフレーム レートで受信できるので、たとえばエンドポイントからは 1080p30 と 720p60、あるいは 720p30 と 480p30 を両方送信することが可能です。

TelePresence Server からエンドポイントへも、異なる解像度とフレーム レートで最大 16 のビデオ ストリームを送信できます。これによりマルチストリーム対応エンドポイントは、1 つの会議レイアウトに複数のビデオ ストリームをローカルで構成できます。

この機能については、いくつかの重要事項があります。

- この機能がサポートされるのは、リモート管理モードにある Cisco TelePresence Server on Virtual Machine と Cisco Multiparty Media 310/320 だけです。
- TelePresence Server ではマルチストリームおよびシングル ストリームの両方のエンドポイントが参加する会議をサポートしています。
- スイッチド メディア ストリームの暗号化が提供されています。
- 前方誤り訂正およびレート コントロールを使用したマルチストリーム コールの復元機能が提供されています。
- マルチストリームのサポートは SIP 経由のものだけです (H.323 と TIP は不可)。
- デフォルトではイネーブルです。ただし、API の `multistreamMode` パラメータを使用して無効にできます。
- TelePresence Server では、マルチストリーム対応エンドポイントとの間で H.264 SVC チャネルを使用して送受信されるビデオ ストリームをサポートしています。
- カスケード リンクでのマルチストリームはサポートされません。
- マルチストリームはすべてのトークン レベルでサポートされています。ただし、メイン ビデオのビット レートは 500 kbps 以上でなければなりません。

## 注：

- TIP エンドポイントは、マルチストリーム対応エンドポイントでは、発言中のスピーカーのセグメントだけの表示になります。
- グループ化されたエンドポイントが会議に加わると、すべてのエンドポイントがトランスコード モードに切り替えられます。

## エンドポイントのタイプ

表 43 エンドポイントのタイプ

| エンドポイントのタイプ<br>(UI に表示) | ハードウェアの名前とモデル番号  |
|-------------------------|--|
| [Standard]              | <p>標準のビデオ エンドポイント。以下は例。</p> <ul style="list-style-type: none"> <li>• EX60/EX90</li> <li>• 任意の C シリーズ コーデック (C20、C40、C60、C90)</li> <li>• Cisco Jabber</li> <li>• Microsoft Lync</li> <li>• その他の非 TIP サードパーティ エンドポイント</li> </ul> <p>また、TelePresence Server に不明なエンドポイント タイプであるかも表示されます。</p>   |
| [Cascade]               | 別の TelePresence Server (Media 310/320、MSE 8710、または Cisco TelePresence Server on Virtual Machine) へのカスケード コール。  |
| [Group of N endpoints]  | エンドポイントのグループ。このリストに個々のグループ メンバーは含まれません。  |
| [Legacy TIP endpoint]   | <ul style="list-style-type: none"> <li>• タイプ不明の Cisco CTS システム、レガシー ソフトウェア (CTS 1.6/1.7 から 1.7.3 まで) を実行しているエンドポイント。</li> <li>• Cisco CTS 1 スクリーン システム、レガシー ソフトウェア (CTS 1.6/1.7 から 1.7.3 まで) を実行しているエンドポイント。以下は例。 <ul style="list-style-type: none"> <li>• CTS 500</li> <li>• CTS 1000</li> <li>• CTS 1100</li> </ul> </li> <li>• Cisco CTS 3 スクリーン システム、レガシー ソフトウェア (CTS 1.6/1.7 から 1.7.3 まで) を実行しているエンドポイント。以下は例。 <ul style="list-style-type: none"> <li>• Cisco TelePresence System 3000 シリーズ (CTS 30x0)</li> <li>• Cisco TelePresence System 3200 シリーズ (CTS 32x0)</li> </ul> </li> </ul> |

|                                  |   |
|----------------------------------|---|
| エンドポイントのタイプ<br>(UI に表示)          | ハードウェアの名前とモデル番号   |
| [SIP telepresence]               | タイプ不明の Cisco CTS または他の TIP 対応システムで CTS 1.7.4 以降を実行中のもの。   |
| [SIP single screen telepresence] | Cisco CTS または他の TIP 対応 1 スクリーン システムで CTS 1.7.4 以降を実行中のもの。<br>以下は例。 <ul style="list-style-type: none"> <li>• CTS 500</li> <li>• CTS 1000</li> <li>• CTS 1100</li> </ul>  |
| [SIP three screen telepresence]  | Cisco CTS または他の TIP 対応 3 スクリーン システムで CTS 1.7.4 以降を実行中のもの。<br>以下は例。 <ul style="list-style-type: none"> <li>• Cisco TelePresence System 3000 シリーズ (CTS 30x0)</li> <li>• Cisco TelePresence System 3200 シリーズ (CTS 32x0)</li> <li>• Cisco TelePresence TX9000</li> <li>• Cisco TelePresence TX9200</li> </ul> |
| [Multistream]                    | シスコがサポートするマルチストリーム対応エンドポイント。  |

## エンドポイントの相互運用性

**表 44 エンドポイントでサポートされている機能**

| 機能                                    | サポートしているエンドポイント                        | 注意   |
|---------------------------------------|--|--|
| パネルの切り替え<br>レイアウトで最大<br>音量の参加者を<br>表示 | T3、CTS 3200、CTS 3000、<br>TX9000、TX9200 | CTS 1300 およびエンドポイント グループは最大音量の参加者を表示できません。<br><br><b>注：</b> 一部の T3 システムは位置反映音声機能を提供していません (T3 Custom)。 |

| 機能      | サポートしているエンドポイント   | 注意   |
|---------|---|--|
| 会議終了の通知 | <ul style="list-style-type: none"> <li>• CTS 500</li> <li>• CTS 1000</li> <li>• CTS 1100</li> <li>• CTS 1300</li> <li>• CTS 3000</li> <li>• CTS 3010</li> <li>• CTS 3200</li> <li>• CTS 3210</li> <li>• TX9000</li> <li>• TX9200</li> </ul> | これらのエンドポイントは、TelePresence Server から通知を受け取ると、独自の会議終了の警告を生成します。他のタイプのエンドポイントで使用されるオーバーレイ メッセージの代わりに、アイコンが表示されます。 |

## TelePresence Server の会議のキャパシティについて

ここでは、Cisco TelePresence Server のすべてのタイプの情報を記載しています。特定モデルに関連する情報を検索してください。

### ライセンス キーおよびスクリーン ライセンス

TelePresence Server のライセンス モデルは「スクリーン ライセンス」に基づいており、ライセンス アクティベーション キーを購入する形式で提供されています。スクリーン ライセンスによって TelePresence Server の会議キャパシティがアクティブになります。TelePresence Server のフル キャパシティは最大ライセンス数を適用することでアクティブになりますが、最大数は次のようにハードウェア プラットフォームごとに異なります。

| ハードウェア プラットフォーム  | スクリーン ライセンスの最大数   |
|--|-------------------|
| TelePresence Server MSE 8710                           | 12                |
| 2、3、または 4 つの TelePresence Server MSE 8710s によるクラスター    | それぞれ、24、36、または 48 |
| TelePresence Server 7010                               | 12                |
| TelePresence Server on Media 310                       | 6                 |
| 2 つの TelePresence Servers on Media 310 のクラスター          | 12                |
| TelePresence Server on Media 320                       | 12                |
| TelePresence Servers on Media 310 と Media 320 の混在クラスター | 18                |
| 2 つの TelePresence Servers on Media 320 のクラスター          | 24                |
| TelePresence Server on Virtual Machine (8 コア)          | 4                 |
| TelePresence Server on Virtual Machine (8 コア、HD)       | 5                 |

| ハードウェア プラットフォーム   | スクリーン ライセンスの最大数 |
|---|-----------------|
| TelePresence Server on Virtual Machine (30 vCPU、高密度 VM) | 10              |
| TelePresence Server on Media 400v                       | 18              |
| TelePresence Server on Media 410v                       | 27              |

TelePresence Server MSE 8710s のライセンス適用では、スーパーバイザの Web インターフェイスを介してシャーシにライセンス キーを適用してから、これらのブレードが格納されたスロットにスクリーン ライセンスを割り当てます。

その他のプラットフォームのライセンス適用では、TelePresence Server の Web インターフェイスを使用して、[Configuration] > [Upgrade] ページでライセンス キーを適用します。

## クラスタのライセンス適用

TelePresence Server MSE 8710 ブレードのクラスタにライセンスを適用する場合は、各ブレードのスロットにライセンスを割り当てることを推奨します。実際には、アクティベートされたスクリーン ライセンスは有効な状態でプールされ、使用可能なスクリーン ライセンスと、クラスタ内のブレードに割り当てられたスクリーン ライセンスの合計が一致するように、マスター ブレードに割り当てられます。

TelePresence Servers on Media 310/320 プラットフォームのクラスタのライセンス適用では、各ユニットにライセンス キーを適用することを推奨します。実際には、スレーブがダウンした場合でもマスターがすべてのライセンスを管理しますが、将来的にユニットを分割したい場合や、ユニットの 1 つで深刻な障害が発生した場合でも、クラスタの分割後に当該ユニットをカバーするだけのライセンスが適用されていることとなります。

## 動作モード

TelePresence Server 7010 および MSE 8710 の動作モードには、リモートで管理するモードとローカルで管理するモードの 2 つがあります。動作モードは、スクリーン ライセンスが、同時発生コールをホストするキャパシティに換算される方法に影響があります。

**注：** TelePresence Server on Media 310/320 および Cisco TelePresence Server on Virtual Machine ではローカル管理モードをサポートしていません。これらのプラットフォームの場合、TelePresence Server を Cisco TelePresence Conductor や Cisco TelePresence Exchange System などのシステムで管理する必要があります。

リモート管理モードに関する情報は、Media 310/320 および Virtual Machine プラットフォームに関係します。仮にそこで使われるソフトウェアにローカル/リモート管理モードという概念がない場合でも同様です。

## ローカル管理モード (7010 および MSE 8710 のみ)

各スクリーン ライセンスは、TelePresence Server とエンドポイント間のコール数の固定値に換算されます。1 スクリーン ライセンスは、次のように HD モードに基づいて 1 または 2 コールに換算されます。

- 「フル HD」モードのライセンスでは、最大 1080p30 または 720p60 のビデオ（および付随する音声とコンテンツ チャネル）での 1 コールが可能。
- 「HD」モードのライセンスでは、最大 720p30 または w448p60 のビデオ（および付随する音声とコンテンツ チャネル）での 2 コールが可能。

たとえば、ローカル管理モードの TelePresence Server 7010 の場合、6 つのスクリーン ライセンスでホストできるのは、1080p30 までの場合、最大 6 コール、720p30 までの場合、最大 12 コールです。

個々の TelePresence Server ユニットには、ビデオ ポート、音声専用ポート、コンテンツ ポートの数に制限があります。各ビデオ ポートには、コンテンツ使用の有無にかかわらず、該当するコンテンツ ポートが割り当てられます。

ローカル管理モードの TelePresence Servers で利用可能な 2 つの HD モードでのポート割り当て方法の詳細については、同時発生コールの制限をまとめた次の表を参照してください。

## リモート管理モード (すべてのモデル)

リモート管理モードの場合、スクリーン ライセンスのコール割り当ては、よりきめ細かい方法で行われます。1 スクリーン ライセンスで、フル HD の 1 コール分のキャパシティをロック解除できます（ローカル管理モードと同様）。あまりリソースを必要としないコールであればより多くのコール分を解除できます。

たとえば、1 つのスクリーン ライセンスで、1080 であれば 1 コール分、720 であれば 2 コール、448 であれば 4 コール、360 であれば 8 コール分のキャパシティに対応します。

## コール制限

次の表で、前述した各動作モードでの TelePresence Server のコール キャパシティを説明しています。

### ローカル管理モードでの同時発生コールの制限 (7010 および MSE 8710 のみ)

**表 45 HD モードでのハードウェア タイプごとのポート割り当て**

| ハードウェア構成         | ビデオ ポート | コンテンツ ポート | 音声専用ポート |
|------------------|---------|-----------|---------|
| 7010             | 24      | 24        | 10      |
| 8710             | 24      | 24        | 10      |
| 2 つの 8710s のクラスタ | 48      | 48        | 20      |

| ハードウェア構成          | ビデオ ポート | コンテンツ ポート | 音声専用ポート |
|-------------------|---------|-----------|---------|
| 3 つの 8710s のクラスター | 72      | 72        | 30      |
| 4 つの 8710s のクラスター | 96      | 96        | 40      |

表 46 フル HD モードでのハードウェア タイプごとのポート割り当て

| ハードウェア構成          | ビデオ ポート | コンテンツ ポート | 音声専用ポート |
|-------------------|---------|-----------|---------|
| 7010              | 12      | 12        | 10      |
| 8710              | 12      | 12        | 10      |
| 2 つの 8710s のクラスター | 24      | 24        | 20      |
| 3 つの 8710s のクラスター | 36      | 36        | 30      |
| 4 つの 8710s のクラスター | 48      | 48        | 40      |

リモート管理モードでの同時発生コールの制限

## マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool (BST) の使用、サービス要求の送信、追加情報の収集に関する詳細については、『What's New in Cisco Product Documentation』 ([www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html](http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html)) を参照してください。

『What's New in Cisco Product Documentation』に配信登録すると、新しい（または改訂された）シスコ技術情報のリストが RSS フィードとして提供され、リーダー アプリケーションを使ってコンテンツがデスクトップに直接配信されるようにすることができます。RSS フィードは無料のサービスです。

## シスコの法的情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティングシステムの UCB (University of California, Berkeley) のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.



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

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

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

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

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

© 2015 Cisco Systems, Inc. All rights reserved.

## シスコの商標または登録商標

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)