Cisco Meeting アプリ

デスクトップ、モバイル アプリ、WebRTC、SIP エンドポイントのトラブルシューティング

2018 年 11 月 15 日

目次

1　Cisco ミーティング アプリケーションのインストールに関する問題

1.1　Windows アプリの msi インストーラが動作しない

Windows のデスクトップ上で msi インストーラを適切に準備できない場合は、こちらのセクションで適切な問題を探し、推奨される流れに従ってください。

1.1.1　.msi ファイルが見つからない

1. msi のダウンロード用 URL を確認します
2. SSH で MMP に接続して webbridge コマンドを入力すると、msi のダウンロード用 URL が表示されます
3. msi のダウンロード用 URL をブラウザのアドレス バーにコピー アンド ペーストし、ダウンロードを再試行します。

   ダウンロードが再び失敗する場合は、設定された URL が正しく（インストーラへのパスと一致）、msi が適切にデプロイされていることを確認してください。

1.1.2　.msi インストーラをダウンロードできるが、実行できない場合。

1. Cisco ミーティング アプリケーションがお使いのオペレーティング システムをサポートしていることを確認します。

   この情報は、[**管理者向けのアプリに関する** FAQ（App FAQs for admins）] の [**オペレーティングシステムのサポート（Operating System Support）**] セクションに記載されています。
2. Cisco の msi ファイルを実行してみます。

シスコのサポートから msi ファイルを取得し、msi ファイルを使ってアプリを正常にインストールできるかどうか確認します。その場合は msi ファイルとログ ファイルのメッセージを確認し、問題の特定を試みます。

1.2　OS X インストーラが動作しない

Mac 上で dmg インストーラを適切に準備できない場合は、こちらのセクションで適切な問題を探し、推奨される流れに従ってください。

ゲストが Mac のブラウザを使って会議に参加しようとしている場合も同じ作業を行います。そうすると、Mac は OS X アプリのダウンロードとインストールを試み、失敗しません。

1.2.1　dmg ファイルが見つからない

1. SSH で MMP に接続して **`webbridge`** コマンドを入力すると、dmg のダウンロード用 URL が表示されます
2. dmg のダウンロード用 URL をブラウザのアドレス バーにコピー アンド ペーストし、ダウンロードを再試行します。

   ダウンロードが再び失敗する場合は、設定された URL が正しく（インストーラへのパスと一致）、dmg が適切にデプロイされていることを確認してください。

1.2.2　dmg インストーラをダウンロードできるが、実行できない

1. 実行中のオペレーティング システムを Cisco ミーティング アプリケーションがサポートしていることを確認します。

   この情報は、[**管理者向けのアプリに関する** FAQ（App FAQs for admins）] の [オペレーティングシステムのサポート（Operating System Support）] セクションに記載されています。
2. Cisco の dmg ファイルを実行してみます。

シスコのウェブサイトから dmg ファイルを取得し、それを使って Cisco ミーティング アプリケーションを正常にインストールできるかどうか確認します。その場合は dmg ファイルとログ ファイルのメッセージを確認し、問題の特定を試みます。

2　Cisco ミーティング アプリケーションにログインする際の問題

ユーザが Cisco ミーティング アプリケーションにログインしようとする際に問題が生じる場合は、エラーメッセージを求めて指示に従ってください。

App2.1 がサインイン ダイアログで「no network」と報告する

www.google.com などの一般的なウェブサイトを開いてみて、ネットワーク接続を確認します。

インターネット接続が良好な場合、ファイアウォールに問題がある可能性があります。ポート 5222 が開いていることを確認します。

App2.2 がサインイン ダイアログで「unable to resolve ip address」と報告する

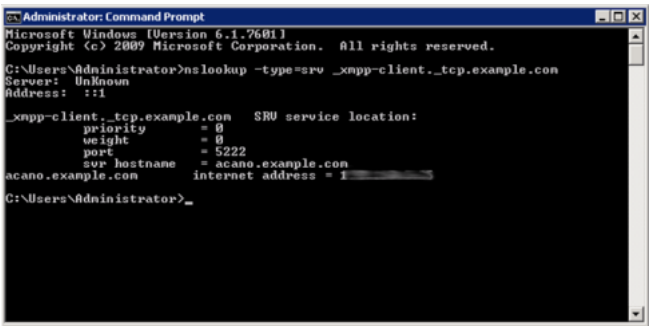
このメッセージは、アプリがドメインを IP アドレスに解決できないことを意味します。

1. **Dnslookup** を使用してドメインを検索するよう、ユーザに求めてください。

   たとえば、コマンド プロンプトで次と同様の内容を入力します。

   ```
   nslookup -type=srv _xmpp-client._tcp.example.com
   ```

   そして、適切な IP アドレスとポートが表示されるか確認します。例：



複数のレコードがある場合は、最も優先度が低くウェイトが大きいものが最初に選択されます。

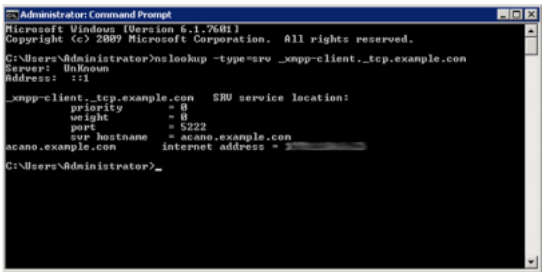
App2.3 がサインイン ダイアログで「unable to connect – check your username and try again」と報告する

1. xmpp-client SRV レコードと DNS A レコードを確認します。

   設定が誤っているか、設定が行われていません。たとえば、コマンド プロンプトで次と同様の内容を入力します。

   nslookup -type=srv _xmpp-client._tcp.example.com

   適切な IP アドレスとポートが表示されるかどうか確認します。

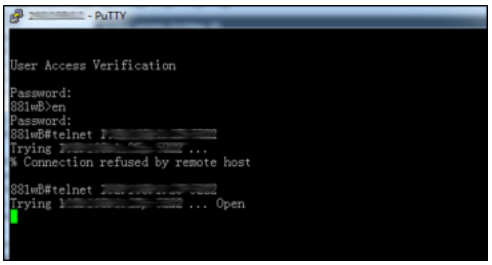


App2.4 がサインイン ダイアログで「unable to connect –try again later」と報告する

このメッセージは、ドメインが IP アドレスに解決されているものの、XMPP サーバが応答しないことを意味します。

1. 解決済みの IP アドレスに到達可能であるかどうか確認してください（つまり、ブロックされた XMPP サーバへのポート 5222）。

   コマンド プロンプトで puTTy を使ってポート 5222 に Telnet で接続してみます。こちらは、Cisco ルータ上のポート 5222 経由で Cisco Meeting Server に Telnet で接続を試みる例です。接続が拒否される場合は、ネットワークによってポートがブロックされているか、サーバが起動していないことを意味します。

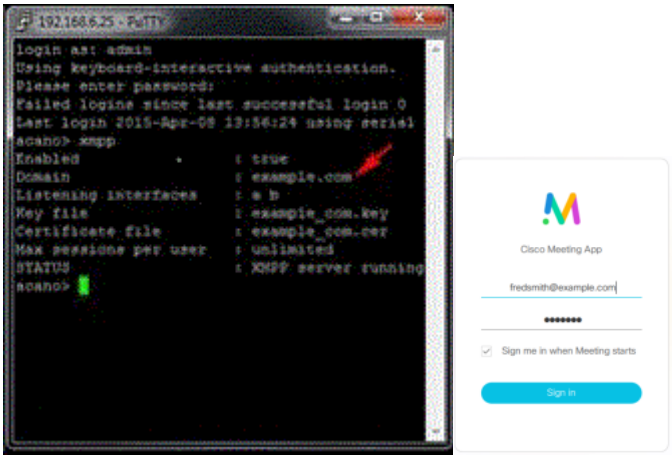


2. サインイン用のユーザ名のドメイン部分が XMPP ドメインと同じであることを確認します。例：

   ログイン用ユーザ名：fredsmith@example.com

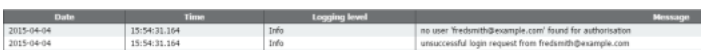
   xmpp ドメイン：**example.com**

   確認を行うには、MMP に SSH で接続して **xmpp** コマンドを入力し、XMPP ドメインをチェックします。XMPP ドメインとログイン用のユーザ名のドメイン部分が異なる場合は、ログイン用ユーザ名のドメイン部分が XMPP ドメインと一致するように変更します。



App2.5 がサインイン ダイアログで「username or password is incorrect」と報告する

1. コア サーバ ログを開き、「LDAP lookup; has the LDAP accountbeen suspended or is it wrong」を検索します。



2. ウェブ管理画面の [**ステータス**（Status）] > [**ユーザー**（Users）] ページのリストにユーザが載っていることを確認します。
3. ユーザがこれらの認証情報を使用して別のアプリケーションにサインインできるかどうか確認し、LDAP 管理チームと確認を行います。

App2.6 が証明書の警告を報告する

警告「Certificate failure. The connecting server is not presenting a valid certificate」が表示される場合：

1. 当社の証明書ガイドで XMPP 証明書の要件、特に次の項目を指定する必要性があることを確認します。
    - 証明書の CN フィールド中の XMPP サーバの DNS レコード
    - subjectAltName フィールド中の XMPP サーバの XMPP ドメイン名および DNS レコード。

問題が解決されない場合は次のものをシスコサポートに送信してください。

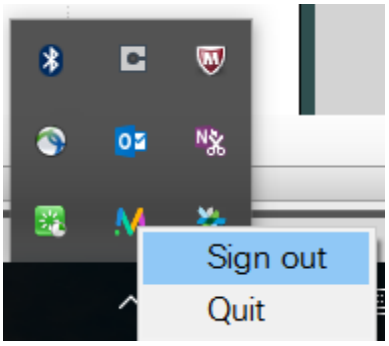
- XMPP 証明書
- MMP コマンド **`xmpp`** の出力結果
- **`_xmpp client._tcp.example.com`** で行った DNS ルックアップの出力結果

3　Cisco ミーティング アプリケーションからログアウトする際の問題

3.1　アプリが応答しない

アプリが応答しない場合はアプリを終了する必要があります。

Windows PC の場合、右下の隅にある Cisco ミーティング アプリケーションのアイコンを探して右クリックし、[**終了**（Quit）] を選択します。



Mac の場合、左上の隅にある Cisco ミーティング アプリケーションのアイコンを探して右クリックし、[シスコ　ミーティングの終了（Quit Cisco Meeting）] を選択します。

アプリのフォルダを探してフォルダ内のすべてのファイルを zip に格納し、zip ファイルをシスコサポートに送信します。

Windows PC の場合、クライアントのフォルダは **`C:\Users\<ユーザ名>\AppData\Roaming\cisco\client\`** です

Mac の場合、クライアントのフォルダは **`/Users/<ユーザ名>/Library/Caches/com.cisco.client/`** です

4　Cisco ミーティング アプリケーションにログインした後に発生する問題

App4.1　診断ログ

アプリケーションの診断ログは、問題の原因を特定するのに役立ちます。診断ツールの使用方法については、*ログの収集*を参照してください。

4.2　アプリのユーザーインターフェイスに欠けているものがある

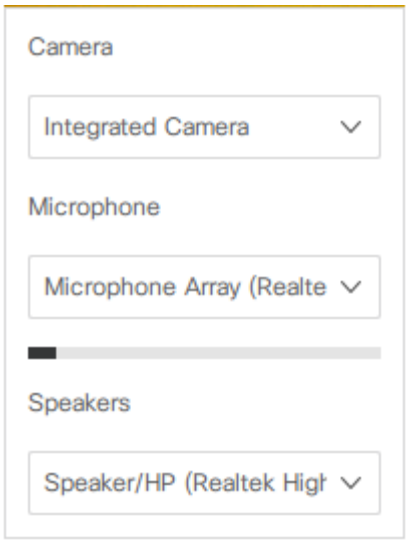
スペース、ボタンやアイコンが不足している場合や、チャット メッセージや連絡先が見つからない場合など、何らかの項目がかけている場合はスクリーンショットを取って [**診断**（Diagnostics）] ボタンをクリックします。シスコサポートにスクリーン ショットと xmppLog ファイルを送信します。

4.3　マイク、スピーカーおよびカメラのデバイスに関する問題

アプリでドロップダウンリストに載っているマイク、スピーカーやカメラのデバイスがすべて表示されない場合は、次の作業を行います。

- 外部デバイスが適切に接続されていることを確認します。
- ドライバが最新かどうか確認します。

問題が解決されない場合は、スクリーン ショットを取って [**診断**（Diagnostics）] ボタンをクリックします。シスコサポートにスクリーン ショットと xmppLog ファイルを送信します。



4.4　Call Bridge クラスタの使用中に大きな遅延が生じる、あるいはパケットが紛失する

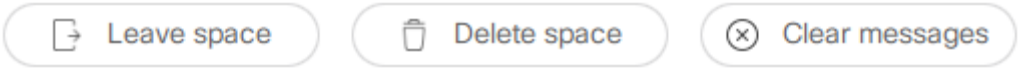
サーバのデプロイ環境に Call Bridge クラスタが含まれている場合、アプリに最も近いものではない Call Bridge がアプリをホストしていることが判明する場合があります。これによって遅延が生じたり、通話品質が下がったりすることがあります。これを回避する方法：

- ユーザはすべての Cisco ミーティング アプリからログアウトする必要があります。ホーミングの有効期限はアプリやバージョンによって異なるため、ホーミングされたアプリを削除する最も安全な方法は、対象のユーザのすべてのインスタンスから 2 ~ 3 時間以上ログアウトすることです。

4.5　チャット メッセージを削除できない

この機能は API 経由で有効化する必要があります。有効になっていない場合、[**メッセージのクリア**（Clear messages）] ボタンが表示されません。有効化したら、スペースを選択して ⎚ ボタンをクリックします。

その後 [**メッセージのクリア**（Clear messages）] をクリックします。すべてのメッセージを削除するかどうか確認されます。

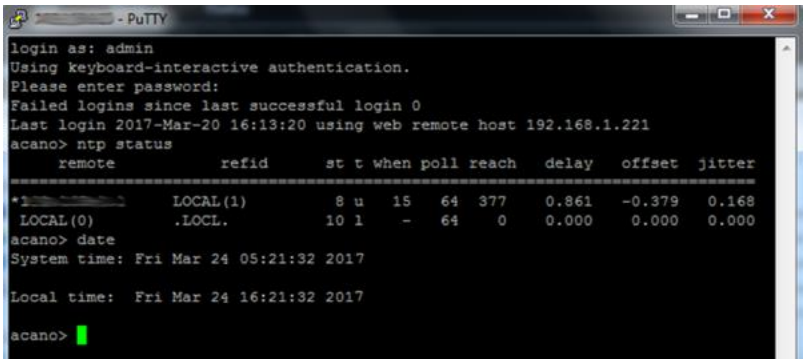


{b}注：{/b}個々のメッセージを削除することはできません。すべてのメッセージが永久に削除されます。メッセージを削除する際、全メンバーに通知が送信されます。

5　Cisco ミーティング アプリケーションを使用する際のスペースに関する問題

5.1　通話時間が負の値になる

NTP を使ってアプリの時間を Call Bridge タイマーと同期させます。NTP ステータスおよび Cisco Meeting Server の時間を確認します。



5.2　参加者の表示が消えない

自身がスペースの唯一の参加者でありながらリストにまだ参加者が表示されている場合は、参加者の通話接続に問題があります。

クライアント診断ログを作成して対応するサーバ側クライアントの診断ログを収集してください。また、Cisco Meeting Server からログファイルをダウンロードします。シスコのサポートにこれらすべてのファイルを送信してください。

6　音声の問題

会議中のユーザが音声の問題に直面している場合は、このセクションで問題を検索し、推奨手順に従います。

6.1　参加者に他の参加者の音声が届かない

送信側の参加者に次のことを確認してもらいます。

- マイクがミュートされていないこと。
- 別の参加者はこれらをミュートできません。
- 相手のマイクが選択されていること。遠端にあるマイク デバイスを変更してもらい、確認します。
- 送信側の参加者が iOS を使用している場合は、iPhone/iPad 設定に移動し、Cisco ミーティング アプリケーションにマイクを使用する権限が付与されていることを確認します。
- 会議と同じマイクを使用している他のアプリケーションがないこと。

受信側の参加者に次のことを確認してもらいます。

- スピーカーの音量が十分であること。
- [**スピーカーのテスト**（Test speakers）] ボタンをクリックすると、参加者が音声を聴くことができます。
- スピーカー デバイスが選択されていること。スピーカーを変更してもらいます。

6.2　特定の参加者の音声が非常に小さい

送信側の参加者に次のことを求めます。

- 相手のマイクが選択されていることを確認し、マイクを変更してもらいます。

受信側の参加者に次のことを求めます。

- スピーカー デバイスが選択されていることを確認してもらいます。
- スピーカーの音量が十分であることを確認してもらいます。

6.3　荒れた音声が参加者に届く

荒れた音声が一人のユーザにのみ届く場合は、参加者のスピーカーが機能しており、インターネット接続が正常であることを確認します。ネットワークの接続状態が悪い場合は、ビデオの画質も低くなります。

すべて、あるいは複数の参加者に荒れた音声が届く場合：

- 送信側の参加者のマイクを変更し、この問題の原因になっているかどうか確認します。
- 送信側の参加者のネットワーク接続が正常であることを確認します）（この場合、他の参加者が対象の参加者から受信するビデオの画質も悪くなります）。
- 診断ログを収集し、メディアの統計情報を確認します。*[ログ収集（Collecting Logs）]* のセクションを参照してください。

6.4　音声にエコーが生じる

ポイントツーポイントの通話では、エコーが聞こえない参加者がおそらくエコーを発生させています。スピーカーとマイクが近すぎないかどうか確認してもらいます。

マルチサイトの通話では、エコーが消えるまでマイクを一つずつミュートし、エコーを発生させている参加者を特定します。次に、スピーカーとマイクが近すぎないかどうか確認してもらいます。

6.5　バックグラウンド ノイズ

通話中にバックグラウンドでノイズが聞こえる場合は、ノイズが消えるまでマイクを一つずつミュートし、ノイズを発生させている参加者を特定します。

対象の参加者のマイクを変更し、この問題の原因になっているかどうか確認します。

参加者に静かな部屋に移動してもらいます。

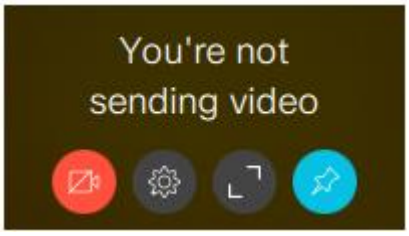
ユーザが発言中でない場合はマイクをミュートすることが常に推奨されます。

7　ビデオの問題

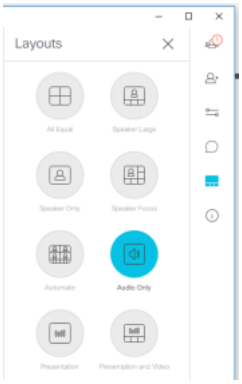
会議中のユーザがビデオの問題に直面している場合は、このセクションで問題を検索し、推奨手順に従います。

7.1　参加者に映像が届かない

参加者が映像を受信しない場合：

1. 送信側の参加者のセルフビューを確認します。
2. ビデオが停止している場合、その参加者に  をクリックしてビデオ送信を開始してもらいます。 

3. 受信側の参加者のレイアウト設定を確認します。

   [**音声のみ**（Audio only）] が選択されている場合は、別のレイアウトに変更するよう参加者に求めます。 

7.2　ビデオの画質が悪い

1. ビデオの画質が悪い参加者が Cisco ミーティング アプリケーションを使用している場合は、  をクリックして [**設定**（Settings）] ページを開いてもらいます。[**詳細**（Advanced）] をクリックして [**帯域幅**（Bandwidth）] 設定を調整します。高い帯域に変更してもらい、もう一度ビデオの画質を確認します。[**ビデオ品質**（Video quality）] の設定も確認します。
2. Cisco ミーティング アプリケーションがエンドポイントである場合は、必要に応じて帯域幅の設定を調整するよう参加者に求めます。

{b}注：{/b}会議でミーティング アプリケーションを使用すると、使用するビデオの解像度と帯域幅がネットワークの状態に基づいて自動的に調整されます。ネットワークの状態に基づいてアプリが自動的に調整を行うため、帯域幅をデフォルトの設定から変更する必要はありません。

上記の手順を実行しても問題が解決しない場合は、ネットワークのパケット損失や遅延が原因で、通話中に通話速度が低速になっているおそれがあります。別の場所にあるエンドポイントを使ってさらにテストを実施します。常に特定の場所や特定のエンドポイントで問題が発生するかどうかを確認します。

[診断ログ（diagnostic log）] を取ってメディアの統計情報を確認し、シスコサポートの連絡先に送信します。

7.3　ビデオが大きく荒れる

1. ネットワークの問題でパケット損失が発生していないか確認します。別の場所にあるエンドポイントから通話を行い、ネットワーク パスに応じて問題が変化するかどうか確認します。
2. QoS によるパケット損失を確認します。
    a. 通話速度を低くして通話を行ってみます。

b. ミーティングを使用している場合は  をクリックして [**設定**（Settings）] ページを開きます。[**詳細**（Advanced）] をクリックして [**帯域幅**（Bandwidth）] 設定を低くします。再びテストします。

{b}注：{/b}会議でミーティング アプリケーションを使用すると、使用するビデオの解像度と帯域幅がネットワークの状態に基づいて自動的に調整されます。ネットワークの状態に基づいてアプリが自動的に調整を行うため、帯域幅をデフォルトの設定から変更する必要はありません。

3. エンコード/デコードの問題を確認します。可能であれば、異なるエンドポイントや別のソフトウェア バージョンを実行している同じエンドポイントを使用して、通話を複数回実行します。問題が発生しない通話もある場合は、特定のエンドポイントやソフトウェア バージョンが原因である可能性があります。
4. ビデオを送信するカメラを確認します。末端の参加者に別のエンドポイントあるいはカメラを使って通話してもらいます。
5. [診断ログ（diagnostic log）] を取ってシスコサポートの連絡先に送信します。

7.4　レイアウトの問題

選択していないレイアウトが表示される場合、あるいは意図していない縦横比で表示される場合は、ネットワーク帯域幅が低く、通話速度が低速になっているおそれがあります。イーサネット ケーブルで有線接続し、場所を変えてみます。

問題が解決しない場合は通話中にクライアント診断ログを取得し、対応するサーバー側のクライアント診断ログを収集します。シスコのサポートにこれらすべてのファイルを送信します。

7.5　コンテンツの共有/受信に関する問題

参加者が次のようなコンテンツの共有に関する問題に直面している場合：

- コンテンツの共有開始時、あるいは共有中にコンテンツを受信できない
- コンテンツがはっきり見えない
- コンテンツのストリーミングがドロップされる

をクリックして [**設定**（Settings）] ページを開きます。[**詳細**（Advanced）] をクリックし、十分な帯域幅が許可されていることを確認します。帯域幅のデフォルト設定は 1200 Kbps です。

{b}注：{/b}会議でミーティング アプリケーションを使用する際、使用するビデオの解像度と帯域幅がネットワークの状態に基づいて自動的に調整されます。ネットワークの状態に基づいてアプリが自動的に調整を行うため、帯域幅をデフォルトの設定から変更する必要はありません。

また、ネットワーク デバイスもチェックし、パケット損失や帯域幅の枯渇が発生していないかどうか確認します。

Cisco Meeting Server の設定をチェックし、コンテンツ共有が有効になっていることを確認します。

問題が解決しない場合は、共有時やコンテンツがドロップされる際にアプリの送信側と受信側の両方でクライアント診断ログを取ります。また、該当するサーバ側のクライアント診断ログも収集してシスコサポートにログを送信します。

8　サインイン時の機能に関する問題

8.1　招待ボタンが表示されない

スペースのゲスト アクセスが無効になっていると、[**招待**（Invite）] ボタンが表示されません。スペースの編集権限を持っている場合は、  をクリックして非メンバーによるアクセスを許可します。メイン画面で をクリックしてヘルプを参照してください。

8.2　招待に関する詳細情報が表示されない

{b}注：{/b}coSpace は現在、スペースと呼ばれています。しかし、スクリプトが動作するよう、API では引き続き coSpace の用語が使われています。

何らかの詳細情報がスペースの招待状に表示されない場合は、次の確認を行います。

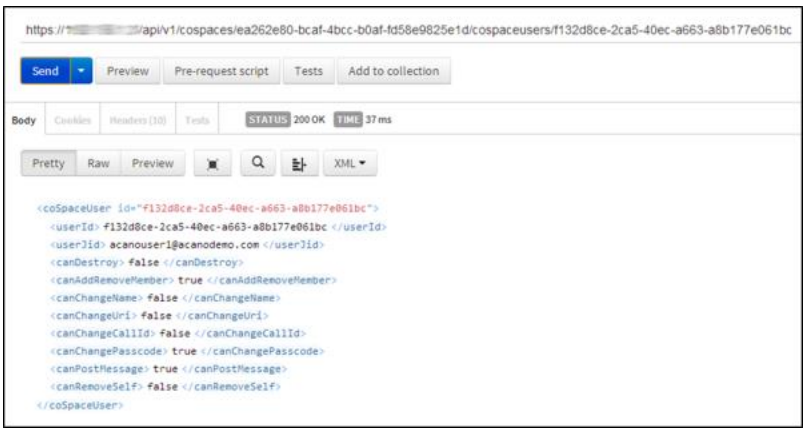
- ビデオ URL が欠落している場合は、Web 管理インターフェイスにサインインし、[**構成**（Configuration）] > [**スペース**（Spaces）] で対象のスペースの [URI ユーザ部分（URI user part）] を確認します。
- 電話番号が欠落している場合は、Web 管理インターフェイスにサインインし、[**構成**（Configuration）] > [**一般**（General）] で [IVR 識別番号（IVR numeric ID）] を確認します。
- 通話 ID が欠落している場合は、Web 管理インターフェイスにサインインし、[**構成**（Configuration）] > [**スペース**（Spaces）] でこの coSpace の [通話 ID（Call ID）] を確認します。
- ウェブ リンクが欠落している場合は、Web 管理インターフェイスにサインインし、[**構成**（Configuration）] > [**一般**（General）] でこのスペースの [ゲスト アカウント クライアント URI (Guest account client URI)] を確認します。

8.3　通話中に参加者を削除できない

通話中、ユーザがビデオ ペインをクリックして[**削除**（Remove）] を選択することで、参加者を削除できる場合があります。参加者が別の参加者を削除できない場合：

- ユーザがスペースのメンバーであるかどうか確認します。
- Cisco ミーティング アプリケーションにサインインしているものの、ゲストとしてのみ通話に参加しているユーザは、参加者を追加・削除できません。ユーザがメンバーである場合は、参加者を追加・削除する権限があるかどうかを確認してください。これを行うための API の URL フォーマットは **`https://<server_IP_address>/api/v1/cospaces/<coSpace_id>/cospaceusers/<user_id >`** です。**`<CanAddRemoveMember>`** が true に設定されている場合、ユーザは通話に参加している他の参加者を削除する権限を持っています。

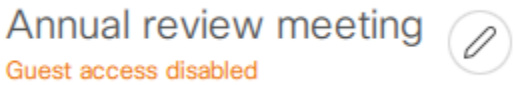
以下が例（Postman ツールを使用）になります。ここでは、**`<canAddRemoveMember>`** パラメータが true に設定されているため、参加者を削除/追加できることが分かります。



8　ゲストに関する問題

8.4　ゲスト アクセスが無効になっている

ゲスト アクセスが無効な場合は、スペースを検索・選択する際にスペース名の下にメッセージが表示されます。



スペースの編集権限を持っている場合、スペースを編集したりゲスト アクセスを許可したりできます。詳細については、ヘルプ アイコンをクリックしてヘルプを参照してください。

8.5　Chrome ブラウザを使用してゲストとして通話に参加できない

誰でもゲスト ユーザとして Chrome で通話に参加できます（ゲスト ユーザ用ウェブ リンクを通じて、あるいは会議 ID を提示）。ゲストに関する問題が発生している場合は、次を確認します。

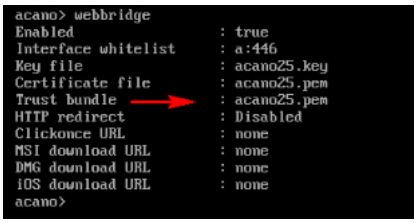
ユーザに Unable to connect – try again later というメッセージが表示されるかどうか

1. ウェブ管理画面でウェブ ブリッジが設定されている場合、ウェブ管理インターフェイスにサインインして [**構成**（Configuration）] > [**一般**（General）] で [**ゲスト アカウント** JID **ドメイン**（Guest Account JID Domain）] を確認します。これは XMPP サーバで設定されているドメインと一致する必要があります。

ユーザに Unable to connect to server というというメッセージが表示される場合：

1. MMP コマンドライン インターフェイスを使用して Web Bridge の信頼できる証明書の設定を確認します。Web Bridge が Call Bridge 証明書を信頼する必要があります。詳細については、Cisco Meeting Server 導入ガイドを参照してください。

   次の例ではトラスト バンドルを使用します。これは、Call Bridge が使用する証明書でなければなりません。



   さらに、こちらの FAQ トラブルシューティング Web Bridge の接続に関する問題を参照してください。

8.6　インテリジェントなペアリングが付近のビデオ システムを検出しない

ミーティング アプリケーションではインテリジェントなペアリングが常に有効になっています。圏内にあるシスコのビデオ システムのソフトウェア バージョンが CE8.0 以降でなければなりません。ビデオ システムが圏内にあり、ミーティング アプリケーションが検出できることを確認します。

ビデオ システムの近接性のトラブルシューティングと設定の詳細については、エンドポイントのドキュメントを参照してください。

8　通知

8.7　画面が非表示である際に iOS が通知を表示しない

アプリがフォア グラウンドにある場合（起動して表示中）のみ通知が表示されます。こちらの FAQ iOS デバイスの Cisco ミーティング アプリケーションの特定のバージョンで通知を受信できないのはなぜですか？を参照してください。

9　スペースの管理に関する問題

9.1　ビデオ アドレスがスペースの名前と一致しない

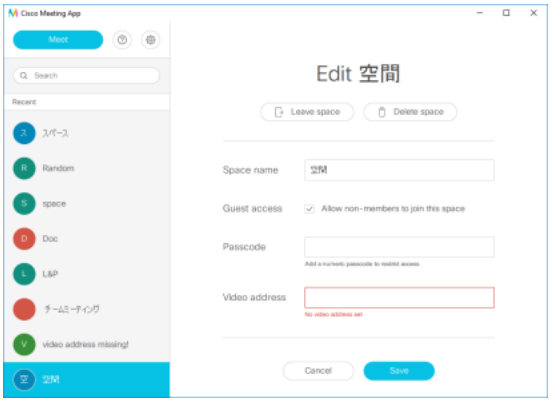
これは問題ではありません。ビデオ アドレスをスペース名と一致させられない場合があります。同じ名前のスペースを複数作ることはできますが、ビデオ アドレスは一意でなければなりません。

アプリでスペース名を入力する際、できるだけスペース名と似た一意のビデオ アドレスを Cisco ミーティング アプリケーションが自動で作成します。スペースの編集権限を持つユーザは必要に応じてビデオ アドレスを編集できます。詳細については、[**スペースの編集**（Edit space）] 画面からヘルプを参照してください。

9.2　ビデオ アドレスが設定されない

ゲスト アクセスが有効になっている場合のみ、スペースのビデオ アドレスを編集することができます。スペース名に ASCII 文字が含まれている場合は、スペース名に基づいてアプリが自動的にスペース アドレスを生成します。

スペース名に ASCII 文字が含まれていない場合は、スペースのアドレスが設定されず、フィールドが空になります。[**スペースの編集**（Edit space）] 画面でゲスト アクセスを有効化しようとする際、アドレスが設定されていない場合はミーティング アプリケーションに次のメッセージが表示されます。



編集権限を持っている場合は、任意のスペースで をクリックして ASCII 文字を使ってビデオ アドレスを入力します。アプリは入力したアドレスを利用できることを示すか、検索内容によく似たものを提案します。[**保存**（Save）] をクリックして変更内容を保存し、この画面を閉じます。

9.3　スペースのメンバーが不足している

ユーザ アカウントを誤って削除すると、以前はメンバーだったスペースからユーザが削除されます。スペースにユーザをメンバーとして追加し直すには、まずはユーザを再作成し、次のいずれかの操作を行います。

- そのスペースのメンバーとしてミーティング アプリケーションにサインインし、削除されたユーザを追加します。
- API 経由でユーザを追加します。API の URL フォーマットは **`https://<cisco_meeting_server_IP_address>/api/v1/cospaces/<coSpace_id>/cospaceusers`** です。

API 経由でメンバーを追加する例を次に示します。

https://<cisco_meeting_server_IP_address>/api/v1/cospaces/e843dbf5-4945-43b0-afe3-93175de37d34/cospaceusers

これで、ユーザがミーティング アプリケーションにログインし、スペースを閲覧できる状態になっているはずです。

10　SIP エンドポイントに関する問題

ユーザが SIP 通話の問題に直面している場合は、このセクションで問題を検索し、推奨手順に従います。

10.1　通話を確立できない

発信後すぐに発信者の接続が解除される場合：

1. ミーティング アプリケーションから発信している場合は、Cisco Meeting Server でアウトバウンド コールのダイヤル プランを確認します。一致したダイヤル プラン ルールが発信コールをルーティングする設定になっていなければなりません。

2. 外部の SIP エンドポイントから発信している場合は、外部の SIP 通話制御デバイスのダイヤル プランを確認してください。一致したダイヤル プラン ルールが外部の Meeting Server に向けてコールをルーティングする設定になっていなければなりません。正しい場合は、Meeting Server のダイヤル プランを確認します。一致した着信コールのダイヤル プラン ルールが着信コールをルーティングする設定になっていなければなりません。

3. 外部の SIP 通話制御デバイスの SIP トランクがアクティブであることを確認します。

コールを発信したにも関わらず、発信側で発信音が聞こえず、受信側に着信がない場合：

1. ミーティング アプリケーションから発信している場合は、Cisco Meeting Server で発信コールのダイヤル プランを確認します。一致したダイヤル プラン ルール

が外部の適切なコール制御デバイスに向けてコールをルーティングする設定になっていなければなりません。

2. 外部の SIP エンドポイントから発信している場合は、外部の SIP コール制御デバイスでダイヤル プランを確認します。一致したダイヤル プラン ルールがコールを Meeting Server にルーティングする設定になっていなければなりません。
3. Meeting Server と外部の SIP コール制御デバイスを確認します。ダイヤル プランの誤った設定によりコール ループが発生していないことを確認します。

受信側で着信があり着信音が聞こえるものの、発信側には聞こえない場合、あるいは受信側が電話に出たにも関わらず発信側で発信音が消えない場合や、受信側が電話に出た直後に接続が切れる場合は、次の作業を行います。

1. 別の場所から、さらに適切な場合は別の SIP トランク経由で SIP エンドポイントに発信してみます。
2. 両方向から発信を試みてください。
3. テスト発信の一部が上手くいく場合は、SIP コール制御デバイスと SIP エンドポイントのソフトウェア バージョンやモデルなどを含め、上手くいく場合と行かない場合を比較してください。ネットワークの場所と設定を比較します。デバイスの互換性、ネットワーク接続、設定の誤りなどの原因が考えられます。

Cisco Meeting Server で有効になっている詳細な SIP トレーシングを使って上記の手順を再現し、ログを確認してシスコサポートに送信します。

10.2 通話を終了できない

ある参加者が電話を切ると他の参加者が通話中に固まり、通話の接続が解除されない場合は、単一のテスト発信を行って次の情報を収集します。

- Cisco Meeting Server のソフトウェア バージョン
- デプロイした仮想環境あるいはサーバのタイプ
- コンピュータのオペレーティング システムとブラウザのタイプおよびバージョン
- MMP コマンド **webbridge** の出力
- Live.json ファイル（付録 A を参照してください）
- ログ（付録 A を参照してください）
- 診断ログ（クライアント側とサーバ側、 付録 A を参照してください）
- Call Bridge およびコンピュータ上の pcap。

情報をシスコサポートに送信します。

10.3 参加者が音声/ビデオを受信できない

単一の参加者が音声やビデオを受信できない場合：

1. ファイアウォールの設定を確認します。

   ファイアウォールがメディア ポートをブロックしている可能性があります。導入ガイドと外部の SIP ソリューションのメディア ポートの範囲を確認します。

ファイアウォールメがメディアをブロックしていない場合は、単一のテスト コールを行って次の情報を収集します。

- Cisco Meeting Server のソフトウェア バージョン
- デプロイした仮想環境あるいはサーバのタイプ
- コンピュータのオペレーティング システムとブラウザのタイプおよびバージョン
- MMP コマンド **webbridge** の出力
- Live.json ファイル（付録 A を参照してください）
- ログ（付録 A を参照してください）

- 診断ログ（クライアント側とサーバ側、 付録 A を参照してください）
- Call Bridge およびコンピュータ上の pcap。

10.4 参加者に荒れた音声/ビデオが届く

単一の参加者に荒れた音声やビデオが届く場合：

1. 低帯域幅を使用してテスト コールを発信してみます。

   パケット損失またはネットワーク遅延が原因で音声/ビデオが荒れる可能性があります。低帯域幅を使用すると音声/ビデオが向上するかどうかを確認します。

2. 可能であれば、SIP エンドポイントで各種のコーデックを使用します。

   エンコード/デコードの問題も考えられます。オーディオ/ビデオ コーデックを変更し、問題が解決するかどうか確認してください。

問題が解決しない場合は、単一のテスト コールを行って次の情報を収集します。

- Cisco Meeting Server のソフトウェア バージョン
- デプロイした仮想環境あるいはサーバのタイプ
- コンピュータのオペレーティング システムとブラウザのタイプおよびバージョン
- MMP コマンド **`webbridge`** の出力
- Live.json ファイル（付録 A を参照してください）
- ログ（付録 A を参照してください）
- 診断ログ（クライアント側とサーバ側、 付録 A を参照してください）
- Call Bridge およびコンピュータ上の pcap。

この情報をサポートにメールで送信します。

10.5 デュアル ストリーム/プレゼンテーションの問題

参加者がデュアル ストリームのビデオ/プレゼンテーションを受信しない場合。

1. ファイアウォールの設定を確認します。

   ファイアウォールがメディア ポートをブロックしている可能性があります。Cisco Meeting Server 導入ガイドとデュアル ストリームのメディア ポートの範囲を扱う外部の SIP ソリューションのドキュメントを確認します。

2. 可能であれば、SIP エンドポイントで各種のコーデックを使用します。

   エンコード/デコードの問題も考えられます。デュアル ストリーム/プレゼンテーションのオーディオ/ビデオ コーデックを変更し、問題が解決するかどうか確認してください。

問題が解決しない場合は、単一のテスト コールを行って次の情報を収集します。

- Cisco Meeting Server のソフトウェア バージョン
- デプロイした仮想環境あるいはサーバのタイプ
- コンピュータのオペレーティング システムとブラウザのタイプおよびバージョン
- MMP コマンド **`webbridge`** の出力
- Live.json ファイル（付録 A を参照してください）
- ログ（付録 A を参照してください）
- 診断ログ（クライアント側とサーバ側、 付録 A を参照してください）
- Call Bridge およびコンピュータ上の pcap。
- クライアント コール用に API calllegs/<calllegid>/calllegdetailed トレースに GET 送信

次にこの情報をシスコサポートに送信します。

10.6 アプリからエンドポイントに通話を移動する際の問題

ユーザがエンドポイントに通話を移動しようとすると、エンドポイントが呼び出されない場合：

1. Web 管理インターフェイスの[**発信コール**（Outbound calls）] の設定をチェックし、通話を移動するのに使用するドメインと共にアウトバウンド ルールが設定されているかどうかを確認します。たとえば、endpoint@conference.example.com に通話を移動する場合は、アウトバウンド ルール（以下を参照）の [**ドメイン**（Domain）] が conference.example.com でなければなりません。

2. アプリからエンドポイントに発信して接続を確認します。テスト コールで接続できるものの通話を移動できない場合は、この問題を再現し、Cisco Meeting Server の SIP トレースを取ってください。Cisco Support に問題の説明とログを送信します。

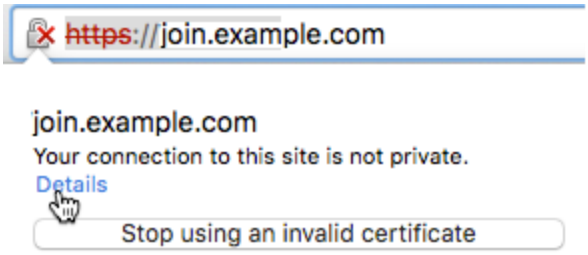
11　WebRTC ブラウザ証明書の問題

ユーザが WebRTC ブラウザ証明書の問題に直面している場合は、このセクションで問題を検索し、推奨手順に従います。

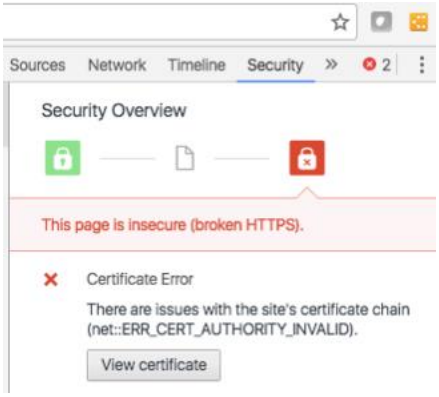
11.1　Google Chrome - 「Cannot connect to the real join.example.com」または「Your connection is not private」

Chrome ブラウザで「Cannot connect to the realjoin.example.com」あるいは「Your connection is not private」のエラーが発生する場合は、次の作業を試みてください。

1. アドレス フィールドの鍵をクリックし、さらに [**詳細**（Details）] をクリックします。

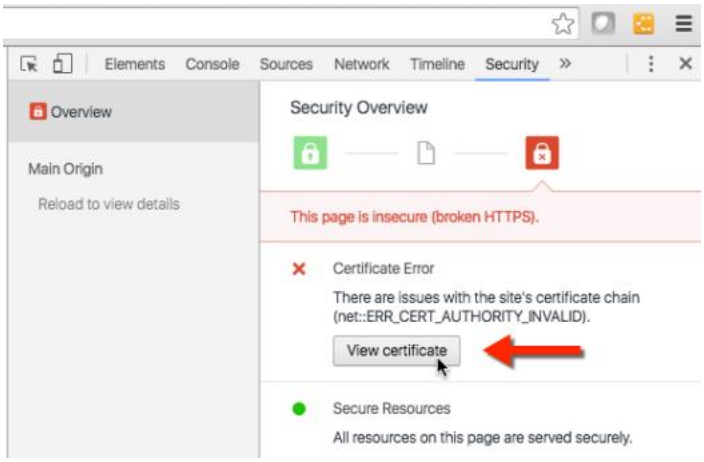


2. 表示されたエラーメッセージを確認します。この例では、コンピュータが信頼していない認証局によって証明書が署名されています。

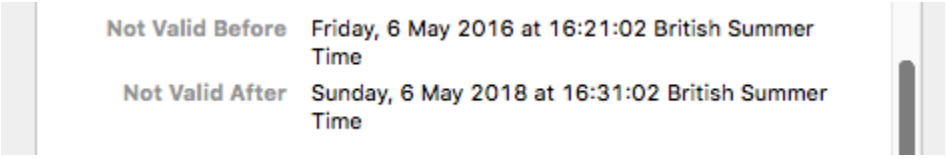


これは、証明書が自己署名されているか、ブラウザが信頼していない認証局によって証明書が署名されていることを意味します。また、証明書バンドルがアップロードされておらず、Web Bridge に正しく割り当てられていないことを意味する場合もあります。

3. 詳細については、[**証明書の表示**（View certificate）] をクリックします。



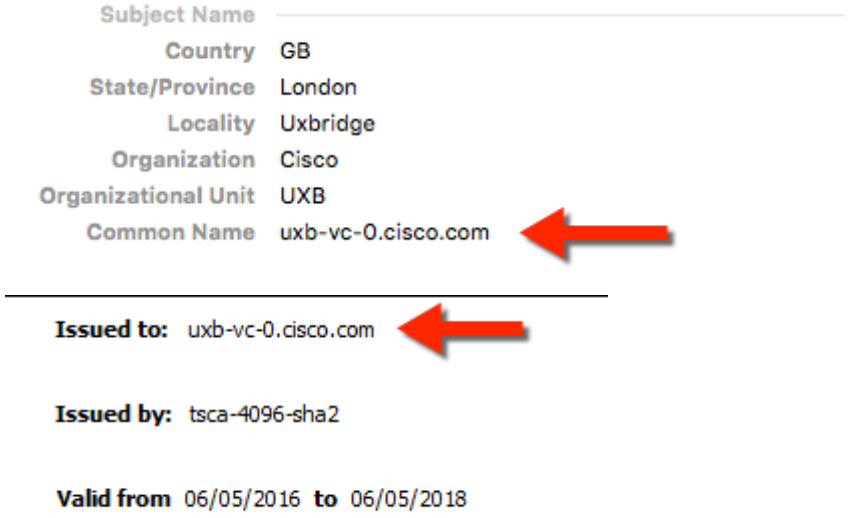
4. [**詳細**（Details）] を開き、証明書が有効かどうか確認します。



ブラウザは証明書の詳細情報をコンピュータと比較し、コンピュータの日時設定が正しいかどうか確認します。

証明書が期限切れである場合、Cisco Meeting Server で更新して期限切れの証明書と交換します。

5. アドレス フィールドで入力した URL に対して証明書が発行されていることを確認します。OS X 用の Chrome の場合、[**サブジェクト名**（Subject Name）] > [**共通名**（Common Name）] を検索します。PC 用の Chrome の場合、[**発行先**（Issued to）] を検索します。

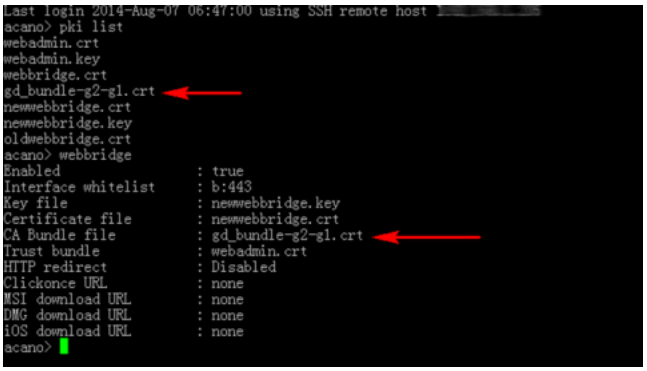


証明書が誤った名前（誤った URL）で発行されている場合、Cisco Meeting Server で適切な証明書を再発行する必要があります。

11.2　証明書バンドルに関する問題

署名者が信頼されていない場合は、証明書バンドルの問題が考えられます。たとえば Firefox は、「The certificate is not trusted because no issuer chain was provided」と報告します。次のことを試してください。

1. MMP 認証情報を使用して、SSH を使って Cisco Meeting Server にログインします。**`pki list`** および **`webbridge`** のコマンドを実行し、CA バンドルファイルがアップロードされており、Web Bridge に割り当てられていることを確認します。そうでない場合はバンドル証明書をアップロードし、**`webbridge certs < private_key > < cert > < bundle_cert >`** コマンドを実行して Web Bridge に証明書を割り当てます。



2. バンドル証明書をアップロードして Web Bridge に割り当てたら、この問題が解決したかどうか確認してください。

証明書バンドルの詳細については、http://en.wikipedia.org/wiki/Intermediate_certificate_authorities を参照してください。証明書の種類や中間署名局の使用などに関する情報が記載された当社の証明書のガイドラインも役立ちます。

12　WebRTC クライアントの問題

12.1　WebRTC クライアントの接続の問題

WebRTC クライアントで会議への参加や音声/ビデオの送信が難しい場合、まずはブラウザの WebRTC サポートをテストします。

1. Chrome を使用して https://apprtc.appspot.com に移動します。別のタブを開いて **`chrome://webrtc-internals/`** と入力すると、ICE 情報が表示されます。セルフ ビューが表示される場合、Chrome がカメラとマイクにアクセスでき、対象のサイトを訪問するネットワークの部分で STUN パケットがブロックされておらず、デバイスの能力が適切だということになります。
2. 下部に表示されるリンクをコピーして仕事仲間に送信し、音声およびビデオの双方向通信をライブで行うポイントツーポイントの通話に招待します。

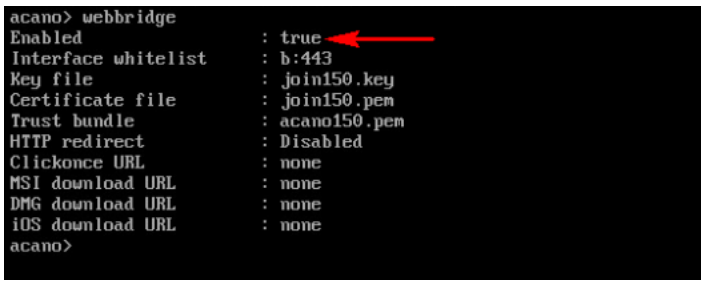
Cisco Meeting Server とブラウザ間のファイアウォールの構成が通話で使用した 2 つのブラウザ間の構成と同じであるなら、これらのテストが成功した場合、Cisco ミーティング アプリケーション（ウェブ）による通話も成功したということになります。

これらのテストが失敗した場合は、Wireshark トレースをコンピュータ上で取って PC あるいはネットワークの問題を調査する必要があります。

12.2　ウェブクライアントのランディング ページに到達できない

1. Web Bridge が実行されており、有効であることを確認します。

   MMP に SSH で接続し、**webbridge** コマンドを入力して Web Bridge が有効であるか確認します。

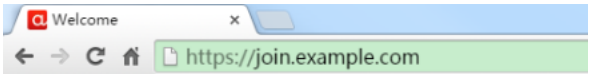


2. DNS サーバのアドレスが設定されていることを確認します。

   a. Windows のコマンド プロンプトで **ipconfig/all** コマンドを入力します

   b. Mac のターミナルの場合は **scutil--dns** コマンドを入力します。DNS サーバのアドレスは、必要な A レコードが設定された、あるいはこのクエリを処理できる別の DNS サーバに DNS クエリを転送する DNS でなければなりません。

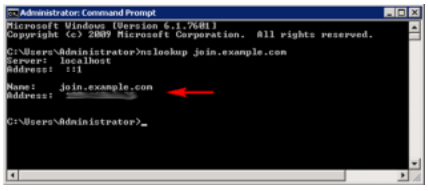
3. Web URL の FQDN が解決する IP アドレスが正しいことを確認します: web URL の例：https://join.example.com。



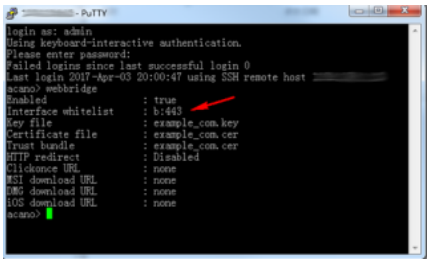
   Windows のコマンド プロンプトで次と同様の内容を入力します。

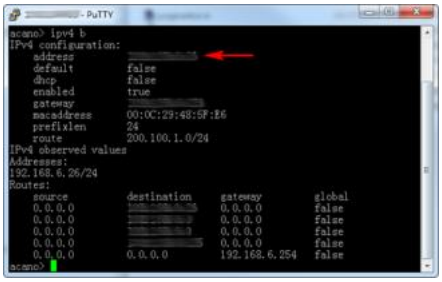
   nslookup join.example.com

   解決された IP アドレスに注目してください。



4. この IP アドレスが Web Bridge がリッスンしているインターフェイスに関連付けられていることを確認します。MMP に SSH で接続し、**webbridge** コマンドを入力して Web Bridge がリッスンしているインターフェイスを表示します。次に Cisco Meeting Server で **ipv4 b** に相当するコマンドを入力し、IP アドレスを確認します。

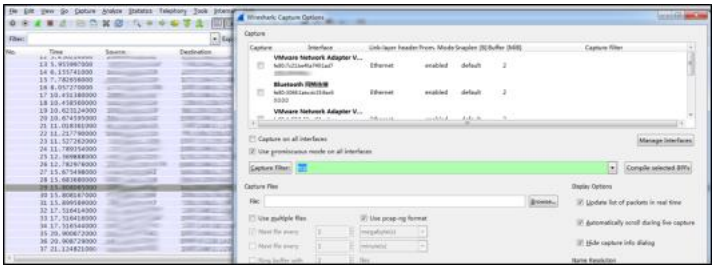




12.3　WebRTC クライアントのコール ドロップ

このような問題の原因の 1 つは、TCP 接続を閉じるファイアウォールです。

問題を再現することができない場合は、Chrome を実行している PC 上で Wireshark トレースを取りますが、キャプチャ フィルタとして「tcp」を使用し、UDP メディア トラフィックをすべてキャプチャすることを避け、ネットワーク レベルでこれを発生させている問題があるかどうか確認します。



また、Chrome の Javascript コンソールを有効化します（Windows では Ctrl-Shift-J）。これを右クリックし、[**ナビゲーションのログを保持**（Preserve Log on Navigation）] が選択されていることを確認します。通話のネクスト ドロップの際、Cisco Support にログおよび Wireshark トレースを送信します。

13　カスタマイズの問題

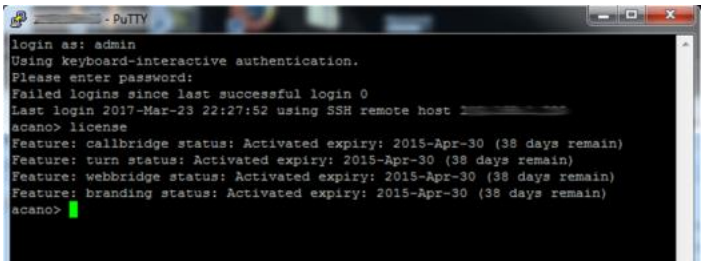
13.1　カスタマイズされた機能が動作しない

カスタマイズされた背景画像を取得することができない、ログや音声プロンプトが表示されない、あるいは聞こえない場合は、ライセンスとカスタマイズ ファイルが存在することを確認します。

{b}注：{/b}カスタマイズされた画像は webRTC アプリ上でのみ表示され、ネイティブ アプリでは表示されません。

---

1. ライセンスが有効であることを確認するには、MMP で **[ライセンス（license）]** コマンドを実行します。ライセンス ファイルのアップロード後、Call Bridge を再起動する必要があります。



{b}注：{/b}コンポーネントを 2 つのサーバ（Core と Edge）にかけてデプロイするスプリット配置の場合、ブランディング ライセンスは Core サーバでのみ必要であり、Edge サーバでは不要です。

---

2. WebRTC のカスタマイズの場合、すべてのカスタマイズ ファイルを単一の zip ファイルに配置する必要があります。Cisco Meeting Server のカスタマイズ ガイドラインに従ってください。

3. カスタマイズ ファイルのサイズ、プロパティ、名前がカスタマイズ ガイドラインの要件を満たしていることを確認します。エラーはイベントログで確認できます。

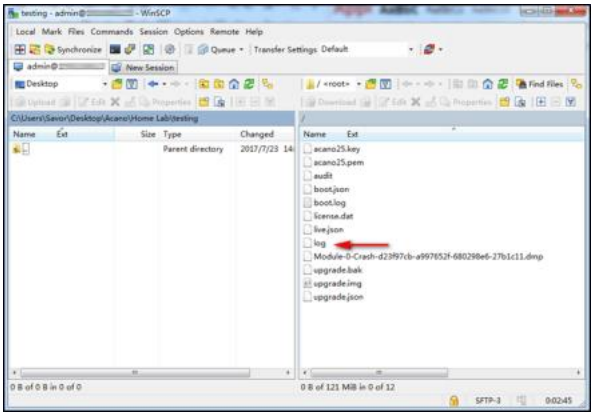
{b}注：{/b}IVR および コール ブリッジは SIP 通話用であり、クライアントには関連しません。

ふ付録 A　ログの収集

前のセクションの手順で問題が解決しない場合は、シスコサポートの連絡先にファイルをメールで送信する必要があります。また、ログを添付することをお勧めします。このセクションでは、それらを収集する方法を説明します。

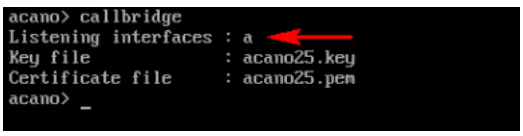
ログの収集

1. WinSCP と MMP ログイン認証情報を使用して Cisco Meeting Server にログインします。
2. ルート ディレクトリ直下にある「log」という名前のファイルを探し、ローカル PC にドラッグします。これは、シスコサポートに送信するログです。



pcap ファイルの収集

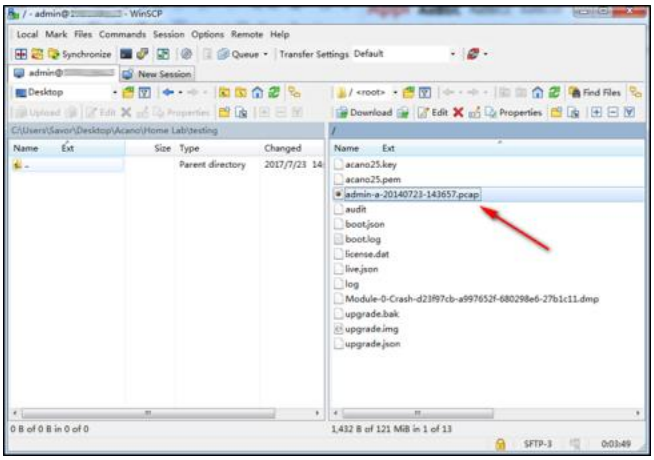
1. SSH とウェブ管理インターフェイスのログイン認証情報を使用して Cisco Meeting Server にログインします。
2. **callbridge** コマンドを実行し、Call Bridge がどのインターフェイスをリッスンしているのか確認します。



3. pcap インターフェイス>（例：**pcap a**）コマンドを実行し、このインターフェイス上でパケット キャプチャを開始します。
4. この問題を再現します。
5. Ctrl+C を押してキャプチャを停止します。
6. pcap ファイルが作成され、ファイル名が表示されます。この例では、ファイル名は **admin-a-20140723-143657.pcap** です。

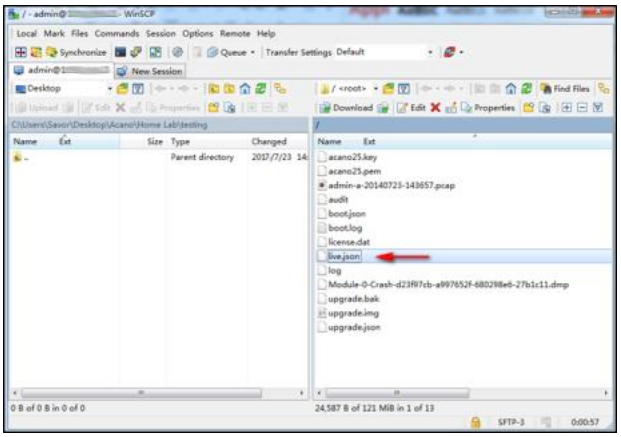
```
acano> pcap a
Packet capture running: press Ctrl-C to stop
Packet capture available in admin-a-20140723-143657.pcap
acano>
```

7. WinSCP とウェブ管理インターフェイスのログイン認証情報を使用して Cisco Meeting Server にログインします。ファイルをローカル PC にドラッグします。



live.json ファイルの収集

1. WinSCP を使用して Cisco Meeting Server にログインします。ログイン認証情報は MMP の認証情報と同じです。
2. ルート ディレクトリ直下にある「live.json」という名前のファイルを探し、ローカル PC にドラッグします。



Cisco ミーティング アプリケーションから診断情報を収集

アプリの使用注に問題が発生した場合、次の手順に従います。

1. シスコサポートから提案された場合は、 をクリックして設定画面を開きます。
2. [**診断**（Diagnostics）] をクリックします。
3. ファイルを保存または送信します。
    - Windows と OS X : [**診断ファイルの保存**（Save diagnostics file）] ウィンドウが表示されます。ログファイルを保存するコンピューター上の場所を選択します。問題の説明をシスコサポートの連絡先にメールで送信してトラブルシューティングを行います。
    - Web アプリ：新しいタブで診断情報を使用できます。ファイルを保存し、問題の説明と共にシスコサポートの連絡先にメールで送信します。
    - iOS：アプリが新規メールを開き、トラブルシューティングに必要なすべての情報を自動入力して診断ファイルを添付します。メールアドレスを入力し、シスコサポートの連絡先に送信します。

Windows と OS X のアプリで会議を行う際、ユーザは次のいずれかの方法でログファイルを保存できます。

- 会議中のメニューオプションから をクリックします。
- Ctrl+d（ Windows）あるいは cmd+d（OS X）を押します。これは、コンテンツを共有している際に診断を送信する唯一の方法です。

[**診断ファイルの保存**（Save diagnostics file）] ウィンドウが表示され、ファイルを保存することができます。問題の説明と共にファイルをシスコサポートの連絡先にメールで送信します。

Cisco Meeting Server から診断情報を収集

通話中のアプリで診断ログを生成する際、Cisco Meeting Server もサーバ側の診断ログを自動的に生成します。

1. ウェブ管理インターフェイス、[**ステータス**（Status）] > [**一般**（General）] の順に移動します。ページの下部にタイムスタンプが付いた診断ログがあります。適切なタイムスタンプのものをダウンロードします。

Windows または OS X アプリのログおよびクラッシュ ファイルを取得

Windows のクラッシュ ファイルは **`C:\Users\ < ユーザ名 > \AppData\Roaming\cisco`** にあります。

OS X のクラッシュ ファイルは **`~Library/Caches/com.cisco.client/`** にあります。

連絡先の詳細情報すべてと一緒に最新のファイルをシスコサポートの連絡先にメールで送信します。イベント毎にタイムスタンプが同じファイルが複数ある場合がありますが、それらをすべて送信してください。

IOS アプリのクラッシュ ファイルを取得

log/crash ファイルをダウンロードするには、iPad または iPhone を PC や Mac の iTunes と同期します。すると、次の場所にクラッシュ レポートが保存されます。

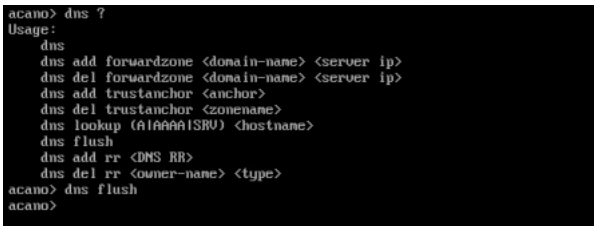
- Windows 7 の場合：**C:\Users\<user_name>\AppData\Roaming\Apple computer\Logs\CrashReporter/MobileDevice**
- Mac の場合：**~/Library/Logs/CrashReporter/MobileDevice**

連絡先の詳細情報すべてと一緒に最新のファイルをシスコサポートの連絡先にメールで送信します。イベント毎にタイムスタンプが同じファイルが複数ある場合がありますが、それらをすべて送信してください。

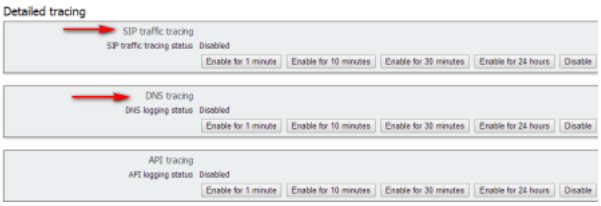
SIP と DNS トレースの収集

1. テスト通話が復号化されていることを確認します。Web 管理インターフェイスにログインし、[**設定**（Configuration）] > [**通話設定**（Call settings）] に移動します。
2. Cisco Meeting Server または仮想デプロイ環境で DNS キャッシュをフラッシュします。MMP にサインインしてから **dns mmp flush** および **dns app flush** コマンドを実行します。

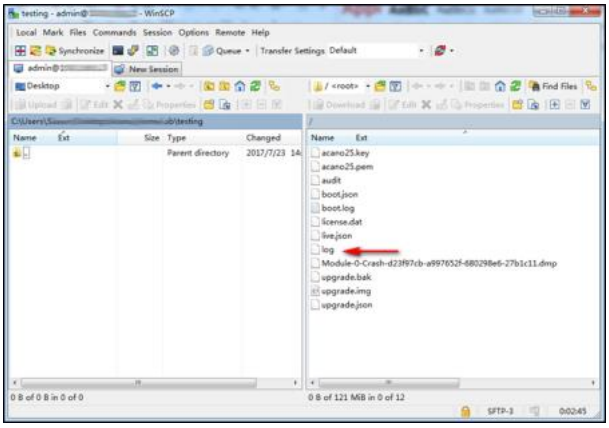
3. 仮想デプロイ環境で MMP にサインインし、 **dns flush** コマンドを実行します。



4. SIP トレースと DNS トレースを有効にします。
   a. ウェブ管理インターフェイスで [**ログ**（Logs）] > [**詳細なトレース**（Detailed Tracing）] の順に移動します。
   b. SIP トラフィック トレースと DNS トレースを有効にします。ほとんどの場合、30 分有効化すれば十分です。



5. 単一のテスト通話を行って問題を再現します。
6. 問題を再現したら、できるだけ早くトレースを無効にします。
7. WinSCP とウェブ管理インターフェイスのログイン認証情報を使用して Cisco Meeting Server にログインします。
8. ルート ディレクトリにある「log」という名前のファイルを探し、ローカル PC にドラッグします。



9. ログファイルを zip に格納してシスコサポートに送信します。

XMPP ログファイルの収集

ミーティング アプリケーションを閉じてから XMPP ログを収集する必要があります。これは、アプリケーションの終了時にしかログが更新されないためです。ログはこちらにあります。

Mac の場合は **`~Library/Caches/com.cisco.client/`**

Windows の場合は **`C:\Users<user_name>\AppData\Roaming\cisco`**

iOS の場合、通話画面を 3 回タップして診断を送信します。これにより、メールに xmpp ログイン情報が含まれます。

あるいは、[**設定**（Settings）] 画面にある [**診断**（Diagnostics）] ボタンを使用します。

または、すでにデバイス上にあるログを使用する場合は、デバイスを Mac や PC に接続し、iTunes を使用してログをダウンロードします（iTunes で iDevice を選択してからアプリに移動し、下にスクロールすると共有ファイルがあります）。

付録 B　クライアント診断ログの分析

メディア ネゴシエーション、パケット損失、ジッター、キーフレーム リクエスト（高 速更新要求）などの一般的な問題を調査する際に役に立つ診断ログに関する情報が記載されています。

この付録では、この情報をログで探すためのヒントを説明します。

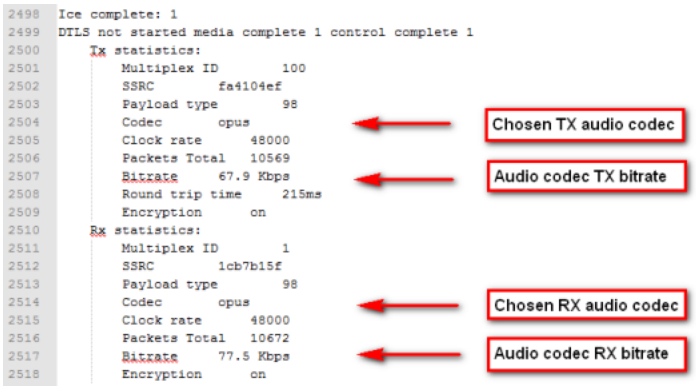
メディア セッション情報（音声セッション）

[メディア セッション情報（Media session info）] のセクション（以下を参照）で、Audiosession から始まる行を探します。

```
=== Media sessions info ==========================
==== Media session FE48560 ====
  Change object awaiting 0 responses
-- Message counter --
Session offers sent 2 response 2, pending 0
Session answers received 2
Selections sent 2 response 2, pending 0
Selections received 1
Advertisement sent 1 response 1, pending 0
Configures sent 0 response 0, pending 0
Configures received 0
Streams advertised:
Audio: 25703630-d8ef-4e88-bbe9-8d3129d3016f
Main video: de6ac16d-ec14-4fc1-9297-a83afc6bc6b7
Streams requested from far end:
    bdc7d5b4-5a73-419b-8d09-ead2ff8c00ac with multiplexId 2 @ 1010x688; aspect ratio 1010:688; layout 3
    4e1a1422-0984-45a4-9577-dfc3c304d472 with multiplexId 1
Audio session: 25703630-d8ef-4e88-bbe9-8d3129d3016f
Remote media: 209.9.228.135:3478; control: 209.9.228.135:3478
  215 seconds ago: media -:50139; control: -:50391
  215 seconds ago: media 209.9.228.135:3478; control: 209.9.228.135:3478
  215 seconds ago: media 209.9.228.135:3478; control: 209.9.228.135:3478
Estimated bandwidth: Unknown
Interfaces:
  10.86.8.11 media 51164 control 51165
  ::1 media 51166 control 51167
  127.0.0.1 media 51168 control 51169
  2001::9d38:6ab8:3890:efe:8380:bbfb media 51170 control 51171
  fe80::3890:efe:8380:bbfb media 51172 control 51173
```

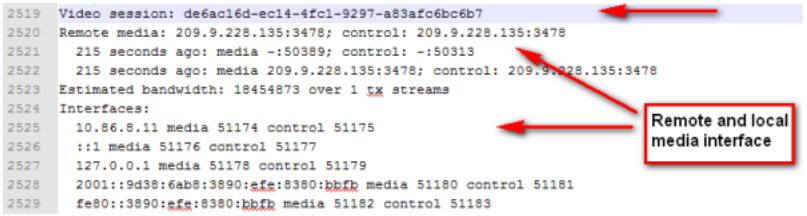

そこには、各ケースで使用する IP アドレスとポートなど、リモートおよびローカルのメディア インターフェイスが記載されています。

同じ音声セクションのさらに下には、選択したコーデックと音声のビットレートの情報があります（以下を参照）。



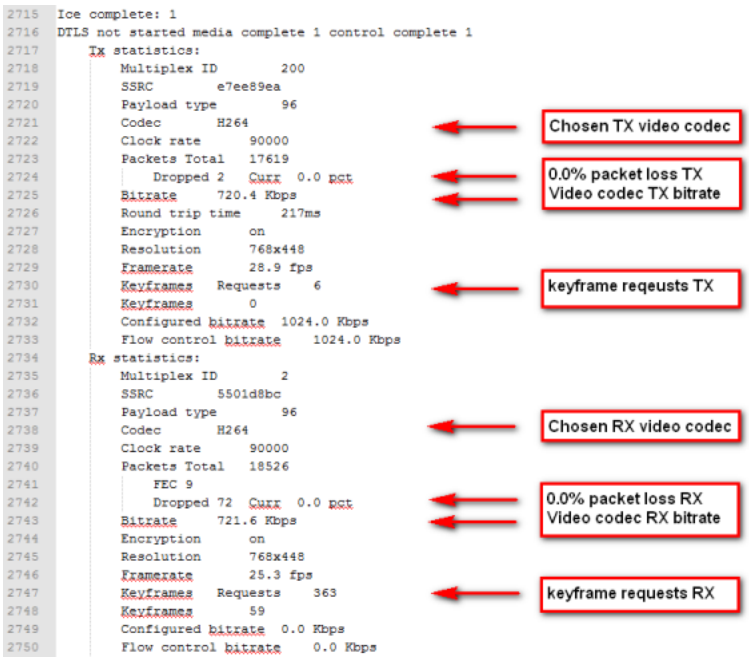
メディア セッション情報（ビデオ セッション）

さらに下にはビデオ セッションのセクションがあります。



ここには、各インターフェイスの IP アドレスとポートなど、リモートおよびローカルのメディア インターフェイスが記載されています。

同じビデオ セッションのセクションのさらに下には、選択したコーデック、音声のビットレート、キーフレーム リクエストの情報があります（以下を参照）。パケット損失によってキーフレーム リクエストが発生する場合があります。



メディアの診断

[メディア診断（Media Diagnostics）] の情報が役立つ場合があります。次の例では、音響エコー、利用できる CPU の枯渇、パケット損失などの問題を確認できます。

```
======== Media Diagnostics =========

1 848 1 0 0 audio echo
```

```
======== Media Diagnostics =========

2 468 40 0 1005 low available CPU
```

```
======== Media Diagnostics =========

1 448 1 2 0 audio echo
34 2790 50 1 24 packet loss
38 308 50 1 35 packet loss
```

Call Bridge の選択

[XMPP 情報（XMPP info）] セクションには、Call Bridge 選択作業後にアプリをホーミングする Call Bridge があります。

```
813  === XMPP info ====================================
814  Connected to 200.100.1.79
815  Choosing from 3 servers after 500ms
816   Server ukcore1.example.com (score 3710886328):
817    RTT direct: Unreachable
818    RTT via 200.100.1.80: 2ms local + 0ms remote
819    RTT via 200.100.1.25: 3ms local + 1ms remote
820    RTT via 200.100.1.77: 2ms local + 1ms remote
821    RTT via 200.100.1.79: 2ms local + 0ms remote
822   Server ukcore2.example.com (score 3251570200):
823    RTT direct: Unreachable
824    RTT via 200.100.1.80: 2ms local + 0ms remote
825    RTT via 200.100.1.25: 3ms local + 0ms remote
826    RTT via 200.100.1.77: 2ms local + 1ms remote
827    RTT via 200.100.1.79: 2ms local + 0ms remote
828   Server uscore1.example.com (score 1782068193):
829    RTT direct: Unreachable
830    RTT via 200.100.1.80: 2ms local + 0ms remote
831    RTT via 200.100.1.25: 3ms local + 0ms re
832    RTT via 200.100.1.77: 2ms local + 1ms re
833    RTT via 200.100.1.79: 2ms local + 0ms remote
834   Chosen best server ukcore1.example.com with RTT 2
835  === End XMPP info ================================
```

Homed by ukcore1

サーバのリクエストによって選択されている場合、この特定のユーザがすでに Call Bridge によってホーミングされており、そのホーミング セッションのタイマーが切れていないということになります。そのため、Call Bridge 選択作業は関与しません。

```
815  === XMPP info ====================================
816  Connected to 200.100.1.79
817  Choosing from 3 servers after 0ms
818   Server ukcore1.example.com chosen by request of server
819  === End XMPP info ================================
```

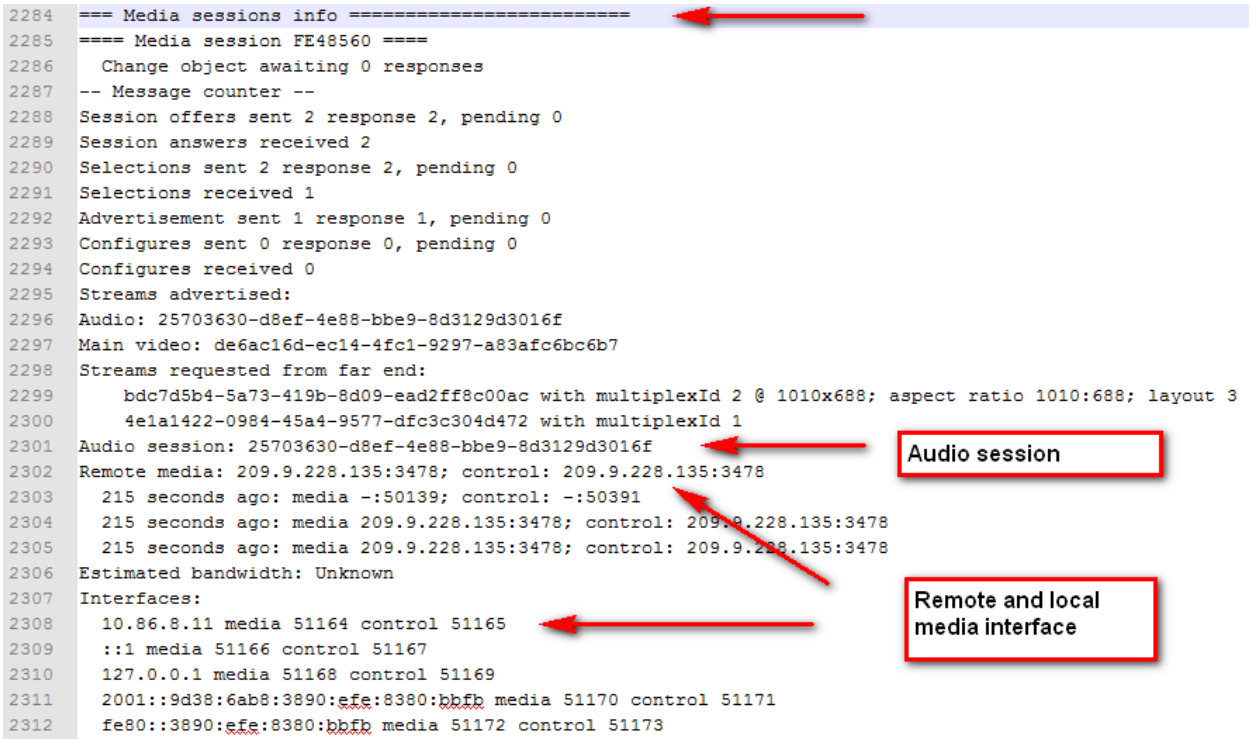
Homed by ukcore1

付録 C　サーバ診断ログの分析

メディア ネゴシエーション、パケット損失、ジッター、キーフレーム リクエスト（高速更新要求）などの一般的な問題を調査する際に役に立つ診断ログに関する情報が記載されています。

この付録では、この情報をログで探すためのヒントを説明します。

最近のログ メッセージ




```
=== Media sessions info ========================
==== Media session FE48560 ====
  Change object awaiting 0 responses
-- Message counter --
Session offers sent 2 response 2, pending 0
Session answers received 2
Selections sent 2 response 2, pending 0
Selections received 1
Advertisement sent 1 response 1, pending 0
Configures sent 0 response 0, pending 0
Configures received 0
Streams advertised:
Audio: 25703630-d8ef-4e88-bbe9-8d3129d3016f
Main video: de6ac16d-ec14-4fc1-9297-a83afc6bc6b7
Streams requested from far end:
    bdc7d5b4-5a73-419b-8d09-ead2ff8c00ac with multiplexId 2 @ 1010x688; aspect ratio 1010:688; layout 3
    4e1a1422-0984-45a4-9577-dfc3c304d472 with multiplexId 1
Audio session: 25703630-d8ef-4e88-bbe9-8d3129d3016f
Remote media: 209.9.228.135:3478; control: 209.9.228.135:3478
  215 seconds ago: media -:50139; control: -:50391
  215 seconds ago: media 209.9.228.135:3478; control: 209.9.228.135:3478
  215 seconds ago: media 209.9.228.135:3478; control: 209.9.228.135:3478
Estimated bandwidth: Unknown
Interfaces:
  10.86.8.11 media 51164 control 51165
  ::1 media 51166 control 51167
  127.0.0.1 media 51168 control 51169
  2001::9d38:6ab8:3890:efe:8380:bbfb media 51170 control 51171
  fe80::3890:efe:8380:bbfb media 51172 control 51173
```

対応するクライアント ログの検索

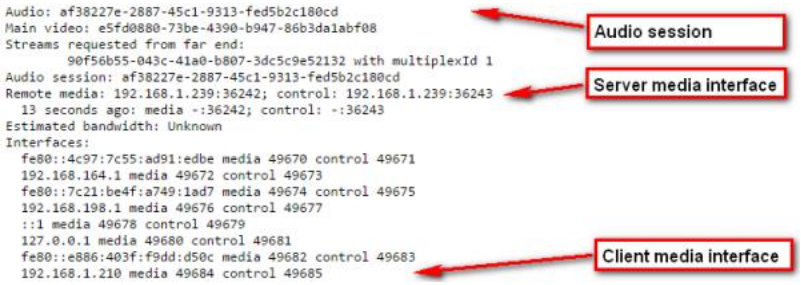
Core サーバ ログはクライアント ログの作成時に生成されるため、通話の両端で発生する問題をトラブルシューティングする際に役立つログのペアが存在します。

どのサーバ ログが特定のクライアント ログに一致するか判断できるよう、同じ情報が両方に表示されます。次のスクリーン ショットは、サーバ側とクライアント側の両方で情報が同じである例です。

```
client diagnostics:
Acano PC Client version 1.1.2.3
== User interface info ================
Video display D9D898
  Video stream 0
Video display 63681F0
  Call: DFECE8
  Video stream D6E05C
== End user interface info ============
```

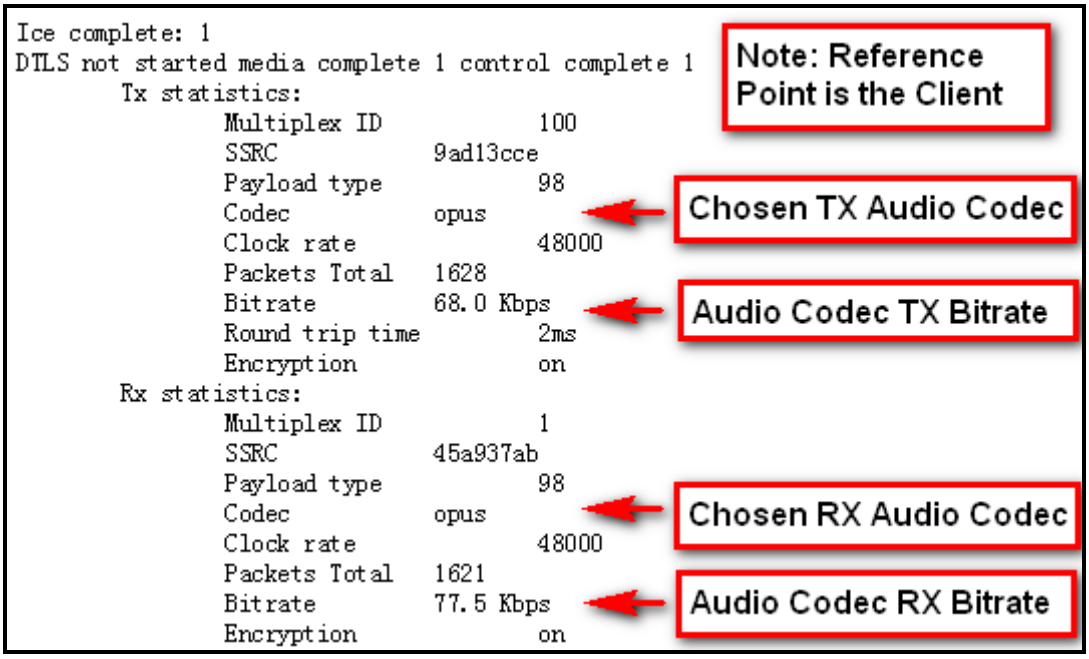
音声メディア セッション

次のスクリーン ショットは両方ともサーバ ログのものです。最初のものは、サーバおよびクライアント上で選択されたメディア インターフェイスを示しています。



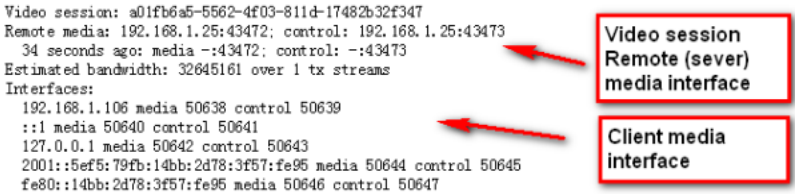
2 番目のスクリーン ショットは、通話で使用するコーデックとビットレートを示しています。コーデックは通話をセットアップする際にネゴシエートされます。

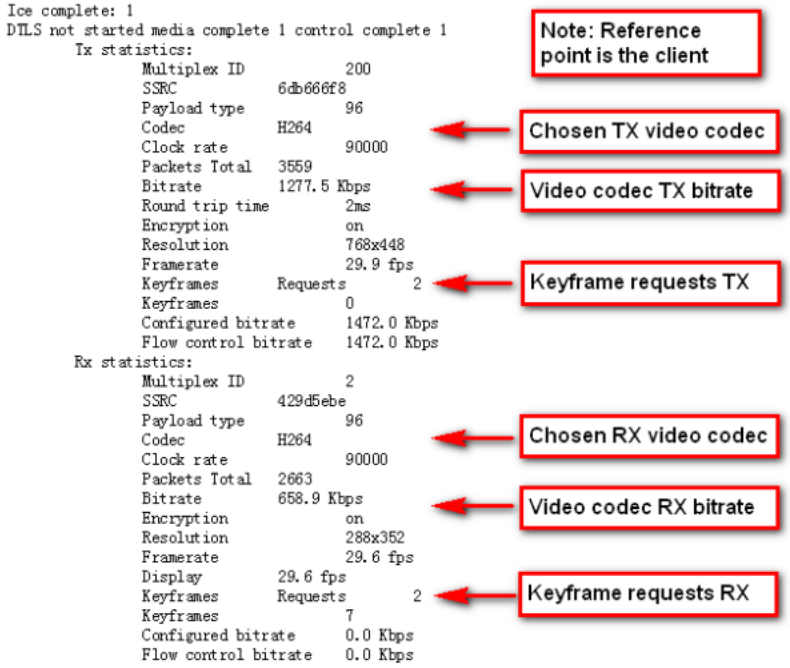
{b}注：{/b}これはサーバ ログですが、TX はサーバが受信するビットレートです。基準点はサーバではなくクライアントになります。



ビデオ メディア セッション

次の例はサーバ ログのものです。

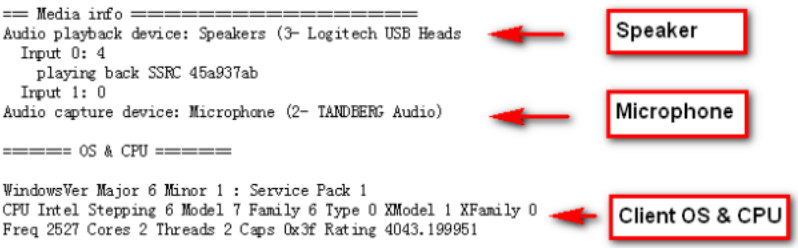




{b}注：{/b}普通、キーフレーム リクエストは 1、2 件しかない（通常は通話開始時）ため、これらが複数ある場合は問題を示唆している可能性があります。通常、デバイス（サーバやクライアント）がパケット損失を受信していることを検出した際にキーフレーム リクエストが送信されます。

クライアント デバイスの情報

次のスクリーン ショットはサーバ ログのものです。



付録 D　ログの分析

Cisco ミーティング アプリケーションのサインイン、通話への参加、通話からの退出や通話のドロップなど、良くあるいくつかの問題を調査する際に役立つログに関する情報が記載されています。

この付録では、この情報をログで探すためのヒントを説明します。

Acanouser1 が Cisco ミーティング アプリケーションからログインしました。

Sep 21 05:57:03 user.info acano host:server: INFO : new session created for user acanouser1@example.com

Acanouser1 がスペースに参加

```
Sep 21 05:57:04 user.info acano host:server:  INFO : call 8: allocated for
acanouser1@example.com "Windows PC client" conference participation

 Sep 21 05:57:04 local0.info acano host:server:  INFO : participant
"acanouser1@example.com" joined coSpace 373d13a0-da03-4137-9c56-1cf83eff6a0b
(acanouser1.cospace)
```

Acanouser1 がユーザによってスペースを退出

```
Sep 21 05:57:11 user.info acano host:server:  INFO : acanouser1@example.com
resource user "67b8d47dc57fe63d": deactivating due to session resource
teardown

 Sep 21 05:57:11 user.info acano host:server:  INFO : call 8: tearing down
("acanouser1@example.com" conference media)
Sep 21 05:57:11 local0.info acano host:server:  INFO : participant
"acanouser1@example.com" left coSpace 373d13a0-da03-4137-9c56-1cf83eff6a0b
(acanouser1.cospace)
```

Acanouser1 がネットワーク接続の問題でスペースを退出

```
Sep 21 05:58:00 user.info acano host:server:  INFO : call 9: inactivity
notification; tearing down...

 Sep 21 05:58:00 user.info acano host:server:  INFO : resource 0:0 for
"acanouser1@example.com"; deactivating due to call drop

 Sep 21 05:58:00 user.info acano host:server:  INFO : resource 0:0 for
"acanouser1@example.com"; sending stream failure indication, size 98

 Sep 21 05:58:00 user.info acano host:server:  INFO : user
"acanouser1@example.com", ephemeral invitation no longer valid due to call
drop
```

```
 Sep 21 05:58:00 local0.info acano host:server:  INFO : participant
"acanouser1@example.com" left coSpace 373d13a0-da03-4137-9c56-1cf83eff6a0b
(acanouser1.cospace)
```

タイムアウトによって Acanouser1 を Cisco Meeting Server から削除

```
Sep 14 11:00:20 user.info acano host: server: INFO : destroying client
instance for "user1@example.com" on keep-alive timeout

 Sep 14 11:00:20 user.info acano host: server: INFO : deinstantiating user
user1@example.com
```

大きな遅延と通話のドロップに関する報告

```
Sep 14 12:47:57 user.warning acano host: server: WARNING : call 9068
(acanouser1): video round trip time of 1643 ms observed...

 Sep 14 13:20:09 user.info acano host: server: INFO : call 9068: inactivity
notification; tearing down...

 Sep 14 13:20:09 user.info acano host: server: INFO : user
"user1@example.com", ephemeral invitation no longer valid due to call drop

 Sep 14 13:20:09 local0.info acano host: server: INFO : participant
"acanouser1@example.com" left coSpace 373d13a0-da03-4137-9c56-1cf83eff6a0b
(acanouser1.cospace)
```

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。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムを適応したものです。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 番号については、シスコの Web サイトをご覧ください（www.cisco.com/go/offices）。

シスコの商標または登録商標