MRA のトラブルシューティング

一般的なテクニック

アラームとステータスメッセージ

トラブルシューティングを行うときは、最初にアラームが発生していないかどうかを確認します（**[ステータス（Status）] > [アラーム（Alarms）]**）。アラームが発生している場合、**[アクション（Action）]** 列の指示に従います。Cisco Expressway-C と Cisco Expressway-E の両方でアラームを確認します。

次にステータスの概要と構成情報を表示します（**[ステータス（Status）] > [Unified Communications]**）。Cisco Expressway-C と Cisco Expressway-E の両方でステータスページを確認します。必要な構成がないか、無効な場合、エラーメッセージと関連構成ページにアクセスするリンクが表示されます。

Cisco Expressway で次の項目を変更すると、無効なサービスまたはエラーが表示される場合があります。この場合、構成変更を有効にするため、システムを再起動する必要があります。

- サーバーまたは CA 証明書
- DNS 構成
- ドメインの設定

Collaboration Solutions Analyzer の使用

TAC が提供するCollaboration Solutions Analyzer（CSA）ツール 一式を使用して、MRA の展開とトラブルシューティングを行うことができます。（CSA にアクセスする方法については、Cisco Expressway リリースノートを参照してください。）

ステップ 1 CollabEdge **バリデータ ツール**を使用して、MRA 展開を検証します。

これは、Jabber クライアントのサインインプロセスをシミュレートし、結果に関するフィードバックを送信します。

ステップ 2 CollabEdge バリデータが問題を識別できない場合は、サインインの試行中に Cisco Expressway からログを収集することをお勧めします。次に、CSA の**ログ分析**コンポーネントを使用してログを分析します。

診断ログ

Jabber for Windows 診断ログ

Jabber for Windowsログファイルは、`C:\Users\<UserID>\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs` で `csf-unified.log` として保存されます。

Cisco Expressway 診断ログ レベルの構成

Cisco Expressway の診断ロギングツールは、システムの問題をトラブルシューティングするために使用できます。また、長時間に渡ってシステムアクティビティの診断ログを生成し、ログをダウンロードすることができます。

始める前に

診断ログを実行する前に、適切なロギングモジュールのログレベルを設定する必要があります。

ステップ 1 **[メンテナンス（Maintenance）] > [診断（Diagnostics）] > [詳細設定（Advanced）] > [サポートログの構成（Support Log configuration）]** の順に選択します。

ステップ 2 発生している問題に対して推奨されるログを選択します。これらは、Log Advisor ツールを使用して見つけることができます。https://logadvisor.cisco.com/logadvisor/collaboration/unifiedcommunications/mra を参照してください。

ステップ 3 **[デバッグに設定（Set to debug）]** をクリックします。

診断ログキャプチャの作成

Cisco Expressway 診断ログ レベルを構成したら、診断ログキャプチャを開始できます。

ステップ 1 **[メンテナンス（Maintenance）]** > **[診断（Diagnostics）]** > **[診断ロギング（Diagnostic logging）]** の順に選択します。

ステップ 2 （任意） **[ロギング中にtcpdumpを取る（Take tcpdump while logging）]** を選択します。

ステップ 3 [Start new log] をクリックします。

ステップ 4 （任意） **マーカー**テキストを入力して、**[マーカーの追加（Add Marker）]** をクリックします。

- 特定のアクティビティが実行される前にマーカー機能を使用して、ログ ファイルにコメント テキストを追加することができます。これは、ダウンロードされた診断ログ ファイルで該当するセクションを識別するのに役立ちます。
- 診断ログの進行中に、必要に応じた数のマーカーを追加できます。
- マーカーのテキストは「**DEBUG_MARKER**」タグでログに追加されます。

ステップ 5 診断ログにトレースするシステムの問題を再現します。

ステップ 6 [Stop Logging] をクリックします。

ステップ 7 [ログの収集（Collect Logs）] をクリックします。

ステップ 8 ログの収集が完了したら、**[ログのダウンロード（Download log）]** をクリックして、ローカル ファイル システムに診断ログ アーカイブを保存します。

アーカイブを保存するように促されます（実際の表現はブラウザによって異なります）。

ログの作成後

ログを再度ダウンロードする場合は、**[ログ収集（Log Collection）]** ボタンを使用することで再度収集できます。ボタンがグレー表示されている場合は、まず、ブラウザでページを更新してください。

診断ログを完了した後、**[サポートログの構成（Support Log configuration）]** ページに戻り、*INFO* レベルに変更されたロギングモジュールをリセットします。

ドメインネームシステム（DNS）レコードの確認

Cisco Expresswayのドメインネームシステム（DNS）ルックアップ ツールを使用すると、システムの問題をトラブルシューティングできます。

[メンテナンス（Maintenance）] > **[ツール（Tools）]** > **[ネットワークユーティリティ（Network utilities）]** > **[ドメインネームシステム（DNS）ルックアップ（DNS lookup）]** の順に選択します。

SRV レコードのルックアップには、H.323、SIP、Unified Communications、および TURN サービスに固有のものが含まれます。

（注） Cisco Expressway-C からドメインネームシステム（DNS）ルックアップを実行すると、企業内からのビューが返され、Cisco Expressway-E で実行すると、DMZ 内から表示できる内容が返されます。これは、必ずしもパブリックインターネットのエンドポイントで使用可能なレコードと同じレコード一式であるとは限りません。

ドメインネームシステム（DNS）ルックアップには、Unified Communications に使用する次の SRB サービスが含まれます。

- _collab-edge._tls
- _cisco-uds._tcp

Cisco Expressway-E が到達可能であることを確認します

この手順では、 Cisco Expressway-E が到達可能であることを確認する方法について説明します。

Cisco Expressway-E の FQDN がパブリック ドメインネームシステム（DNS）で解決可能であることを確認します。

[システム（System）] > **[ドメインネームシステム（DNS）（DNS）]** で FQDN を **<System host name>.<Domain name>** として構成します。

通話状況の確認

通話状況情報には、現在の通話と完了した通話の両方を表示できます。

コール ステータス情報の同じセットは、「**登録ごとのコール（Calls by registration**）」ページ（「**登録の詳細（Registration details**）」ページ経由でアクセス可能）でも表示できます。

Cisco Expressway がクラスタの一部の場合、リストが各ピアに対して最新の 500 通話に制限されていても、クラスタ内でピアに適用できるすべての通話が表示されます。

ステップ 1 現在の通話に関する情報を取得する場合は、**[通話状態（Call status）]**ページ（**[状態（Status）]** > **[通話（Calls）]** > **[通話（Calls）]**）にアクセスします。

[通話状態（Call status）] ページには、現在進行中のすべての通話または Cisco Expressway で登録されているデバイスからの通話、または Cisco Expressway をパススルーしている通話が一覧されます。

ステップ 2 完了した通話に関する情報を取得する場合は、 **[通話履歴（Call history）]** ページ（**[状態（Status）]** > **[通話（Calls）]** > **[履歴（History）]**）にアクセスします。

[通話履歴（Call history）] ページには、非アクティブのすべての通話が一覧されます。このリストは、最新の 500 通話に制限されており、 Cisco Expressway が最後に再開されてから発生した通話が含まれます。

モバイルおよびリモートアクセス通話 ID

[通話状態（Call Status）] と [通話履歴（Call History）] ページには。Unified CM リモートセッション（モバイルおよびリモートアクセスが有効な場合）と Cisco Expressway RMS セッションを含むすべての通話タイプが表示されます。

コール タイプを区別するにはコール コンポーネントをドリルダウンする必要があります。モバイルおよびリモートアクセス通話には、通話が Cisco Expressway-C または Cisco Expressway-E で表示されているかによって、異なるコンポーネントの特性があります。

- Cisco Expressway-C では、Unified CMリモートセッションには、（メディア暗号化を強制するために B2BUA が使用されるため）3 つのコンポーネントがあります。 Cisco Expressway コンポーネントの 1 つは、 Cisco Expressway と Unified CM 間で自動生成されたネイバーゾーン（名前の前に **CEtcp** または **CEtls**が付きます）の 1 つを介して通話をルートします。
- Cisco Expressway-E では、1 つのコンポーネントがあり、これは **CollaborationEdgeZone** を介して通話をルートします。

両方のエンドポイントが企業外（つまりオフプレミス）にある場合は、2 つの独立したコールとして扱われます。

リッチメディアセッション（ Cisco Expressway のみ）

システムにリッチ メディア セッション キーがインストールされ、Business-to-Business（B2B）コール、サードパーティ製ソリューションへのインターワーク コールまたはゲートウェイ コールなどをサポートする場合、これらのコールは、コール状態やコール履歴のページに記載されています。

Cisco Expressway 経由で Unified CM に登録されたデバイス

Unified CM のアイデンティティデバイス

この手順では、 Cisco Expressway を介して Unified CM にアイデンティティデバイスを登録する方法を説明します。

ステップ 1 Unified CM で、**[デバイス（Device）]** > **[電話機（Phone）]** の順に選択し、**[検索（Find）]** をクリックします。

ステップ 2 **[IP アドレス（IP Address）]** 列をチェックします。

Cisco Expressway 経由で登録されたデバイスが、Cisco Expressway-C で登録された IP アドレスを表示します。

Cisco Expressway-C でのプロビジョニングセッションを識別

この手順では、Cisco Expressway-C を経由してプロビジョニングされるセッションの識別方法について説明します。

ステップ 1 Cisco Expressway-C で、**[ステータス（Status）] > [Unified Communications]** の順に選択します。

ステップ 2 **[詳細ステータス情報（Advanced status information）]** セクションで、**[プロビジョニングセッションの表示（View provisioning sessions）]** をクリックします。

これは、現在および最近の（赤色で表示）すべてのプロビジョニングセッションのリストを表示します。

Cisco Expressway-C が Unified CM と同期されていることを確認してください。

Unified CM クラスタまたはノード構成を変更すると、Unified CM と Cisco Expressway-C 間で通信の問題が発生する場合があります。これには、次の項目への変更が含まれます。

- Unified CM クラスタ内のノード数
- 既存クラスタのホスト名または IP アドレス
- リスニングポート番号
- セキュリティ パラメータ
- 電話機セキュリティプロファイル

そのような変更が Cisco Expressway-C で反映されることを確認する必要があります。手順は次のとおりです。

ステップ 1 Cisco Expressway で、**[構成（Configuration）] > [Unified Communications]** の順に選択します。

ステップ 2 すべての Unified CM と IM and Presence Service ノードで再検出します。

MRA 認証ステータスとトークンの確認

この手順では、MRA 認証ステータスとトークンを確認する方法について説明します。

ステップ 1 （任意） 標準（更新無し）OAuth ユーザートークンを確認してクリアするには、**[ユーザー（Users）] > ビューを選択し、トークン所有者を更新せずに OAuth を管理します。**

これは、特定のユーザーの OAuth アクセスに関する問題を特定するのに役立ちます。

ステップ 2 （任意） MRA 認証の統計を確認するには、**[状態（Status）] > [Unified Communications] > [詳細なMRA認証統計を表示（View detailed MRA authentication statistics）]** の順に選択します。

このページでの予期しないリクエストまたは応答は、構成または承認の問題を特定するのに役立つ場合があります。

Registration Issues

Unified CM にエンドポイントを登録できない

次の理由でエンドポイントが登録できない場合があります。

- Unified CM と Cisco Expressway-C の間で SIP トランクが構成されている場合、Unified CM にエンドポイントを登録できない場合があります。SIP トランクが構成されている場合、Unified CMUnified CM への SIP 回線登録に使用されるポートとは別のリスニング ポートを Unified CM で使用する必要があります。詳細については、Unified CM と Expressway-C 間の SIP トランクを参照してください。

- Cisco Expressway-C のサーバー証明書に、Subject Alternate Name リスト、暗号化された TLS に対して構成された Unified CM のすべての電話機セキュリティプロファイルの名前、リモートアクセスに必要なデバイスに使用するすべての電話機セキュリティプロファイルの名前が含まれていない場合、登録を安全にできない場合があります（「SSL 接続確立の失敗」メッセージ）。Unified CM と Cisco Expresswayの証明書の両方にあるこれらの名前は、FQDN フォーマットにしなければなりません。

  Expressway-C の既存のクラスタに新しい Expressway-C ノードを追加する間は、新しいノードの証明書署名要求（CSR）を生成する必要があります。CUCM でモバイルおよびリモートアクセス（CUCM）クライアントの安全な登録が必要な場合、CUCM に安全なプロファイル名を付ける必要があります。「Unified CM Phone のセキュリティプロファイル名」が CUCM デバイスのセキュリティプロファイルの名前またはホスト名だけである場合、新しいノードでの CSR の作成は失敗します。これにより、管理者は **[安全な電話機プロファイル（Secure Phone Profile）]** ページの下で、CUCM で 「Unified CM Phone のセキュリティプロファイル名」の値を変更する必要があります。

  X12.6 から、Unified CM のセキュリティプロファイル名は完全修飾ドメイン名（FQDN）である必要があります。名前、ホスト名、または値だけでは使用できません。

  たとえば、`jabbersecureprofile.domain.com`、`DX80SecureProfile.domain.com`

（注） FQDN は複数レベルで構成できます。各レベルの名前に使用できるのは文字、数字、ハイフンのみで、各レベルはピリオド（ドット）で区切ります。レベル名はハイフンで開始または終了できません。また、最後のレベル名は文字で開始する必要があります。

Cisco Expressway 証明書と TLS 接続の問題

Cisco Expressway のサーバー証明書または信頼できる CA 証明書を変更するには、変更を有効にするために Cisco Expressway を再起動する必要があります。

セキュアなプロファイルを使用している場合、Cisco Expressway-C 証明書に署名した認証局のルート CA を CallManager の信頼証明書（**[Cisco Unified OS の管理（Cisco Unified OS Administration）]** アプリケーションの **[セキュリティ（Security）]** > **[証明書管理（Certificate Management）]**）としてインストールする必要があります。

CiscoSSL 5.4.3 が 1024 ビット未満の Diffie-Hellman キーを拒否する

バージョン 9.x 以前、または Unified CM または Unified CM IM and Presence Service の Cisco Expressway バージョン X8.7.2 以降を実行している場合、2 つのシステム間の SSL ハンドシェイクはデフォルトで失敗します。

これは、 Cisco Expressway X8.7.2 以降にアップグレードした後、すべての MRA エンドポイントが登録または呼び出しに失敗する症状です。

これは、CiscoSSL コンポーネントを 5.4.3 以降にアップグレードしたことが原因です。このバージョンは、D-H キー交換を使用するときに Unified CM が提供するデフォルト（768 ビット）キーを拒否します。

インフラストラクチャをアップグレードするか、Cisco Technical Assistance Center に問い合わせて、Unified CM や Unified CM IM and Presence Service のデフォルト設定を修正し、 TLS をサポートできるかを確認する必要があります（CSCuy59366）。

Cisco Jabber サインインの問題

Jabber が自動侵入保護をトリガーする

条件（Conditions）

- MRA ソリューションは、OAuth トークンによる認証用に構成されています（更新の有無にかかわらず）。

- Jabber ユーザーのアクセストークンの有効期限が切れた
- Jabber は、次のいずれかを行います。
  - デスクトップの休止状態からの再開
  - ネットワーク接続の回復
  - 数時間サインアウトした後の高速ログインの試行

動作

- 一部の Jabber モジュールは、有効期限切れのアクセストークンを使用して Cisco Expressway-E で認証を試行します。
- Cisco Expressway-E がこれらのリクエストを（正しく）拒否する
- 特定の Jabber クライアントからそのようなリクエストが 5 つ以上ある場合、Cisco Expressway-E は、（デフォルトで）10 分間、IP アドレスをブロックします。

Symptoms

影響のある Jabber クライアントの IP アドレスは、*HTTP* プロキシ認証障害カテゴリにある Cisco Expressway-E の **[ブロックされたアドレス（Blocked addresses）]** リストに追加されます。**[システム（System）]** > **[保護（Protection）]** > **[自動検出（Automated detection）]** > **[ブロックされたアドレス（Blocked addresses）]** の順に選択すると、これらを表示できます。

回避策

この問題に対処するには、2 つの方法があります。1 つ目は、特定のカテゴリに対して検出しきい値を増加させる方法、2 つ目は、影響のあるクライアントに対して例外を作成する方法です。例外は実際の環境で実用的ではない場合があるので、ここではしきい値オプションについて説明します。

1. **[システム（System）]** > **[保護（Protection）]** > **[自動検出（Automated detection）]** > **[設定（Configuration）]**の順に選択します。
2. **[HTTPプロキシの認証の失敗（HTTP proxy authorization failure）]** をクリックします。
3. **トリガーレベル** を *5* から *10* に変更します。期限が切れたトークンを提示する Jabber モジュールを容認するには 10 で十分です。
4. 設定を保存すると、すぐに有効になります。
5. 影響を受けるクライアントのブロックを解除します。

ネットワーク外からの接続時、Jabberポップアップが無効な証明書を警告する

これは、Cisco Expressway-E 上で正しく構成されていないサーバー証明書の症状です。証明書が自己署名されているか、サブジェクトの別名（SAN）としてリストされている組織の外部ドメインネームシステム（DNS）ドメインがない可能性があります。

これは、Jabber で想定されている動作です。Jabber が信頼する CA が発行した証明書をインストールし、その証明書に Jabber が使用しているドメインが SAN のリストに含まれていることをお勧めします。「証明書の要件」を参照してください。

Jabber が電話サービスに登録しない

Cisco Expressway と ユーザーデータサービス（UDS）の間には不一致を処理するケースがあり、提供されたユーザー ID が保存されている ID のケースと一致しない場合、電話サービスに Jabber を登録できなくします。Jabber は、継続してサインインできますが、電話サービスは使用できません。

ユーザーは、UDS で保存されているとおりのユーザー ID でサインインすることで、この問題を回避できます。

ユーザーは、サインアウトして Jabber をリセットすることで、この問題を解決できます。「CSCux16696」を参照してください。

XMPP のバインド障害が原因で Jabber がサインインできない

XMPP のバインド障害が原因で、Jabber クラインとにサインインできない場合があります（「サーバーに通信できない」エラーメッセージ）。

これは、Jabber クライアントログのリソース バインド エラーによって示されます。次に例を示します。

```
XmppSDK.dll #0, 201, Recv:<iq id='uid:527a7fe7:00000cfe:00000000' type='error'><bind
xmlns='urn:ietf:params:xml:ns:xmpp-bind'/><error code='409' type='cancel'><conflict
xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/></error></iq>

XmppSDK.dll #0, CXmppClient::onResourceBindError

XmppSDK.dll #0, 39, CTriClient::HandleDisconnect, reason:16
```

これは通常、IM and Presence Intercluster Sync Agent が正しく実行されない場合に発生します。詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html の『Cisco Unified Communications Manager 構成ガイド』の「*IM and Presence* 情報」を参照してください。

SSH トンネル障害が原因で Jabber がサインインできない

SSH トンネルが確立できないことが原因で、Jabber がサインインできない場合があります。Cisco Expressway-C と Cisco Expressway-E の間のトラバーサルゾーンは、他のすべての点で正常に機能します。 Cisco Expressway は、「アプリケーションに障害発生 – `portforwarding.pyc` で予期しないソフトウェアエラーが検出されました」と報告します。

これは、Cisco Expressway-E ドメインネームシステム（DNS）ホスト名に下線を含めると発生する場合があります。**[システム（System）] > [ドメインネームシステム（DNS）（DNS）]**の順に選択し、**システムホスト名**に、文字、数字、ハイフンのみが含まれていることを確認します。

Cisco Expressway-E のクラスタ内の異なるピアに接続すると Jabber がサインインできない

Cisco Expressway-E ピア間でドメインネームシステム（DNS）ドメイン名に不整合があると、Jabber がサインインできない場合があります。ドメイン名は、クラスタ内のすべてのピアで、大文字と小文字の区別も含めて同一である必要があります。

各ピアで、**[システム（System）] > [ドメインネームシステム（DNS）（DNS）]**の順に選択し、ドメイン名が、すべてのピアで同じであるか確認します。

特定の問題

Cisco Expressway が 「401 Unauthorized」 のエラーメッセージを返します。

Cisco Expressway が、エンドポイントクライアントが提示したログイン情報を認証しようとした場合、「401 Unauthorized」 のエラーメッセージが表示される場合があります。エラーの理由には次のものが挙げられます。

- SAML アサーションで提供される IDP の userid にソリューションを構成する必要があることに注意してください。これは、トークン（アクセス/更新）に対して検証するために、Cisco Unified Communications Manager userid の sAMAccountName と一致する必要があります。
- クライアントが不明なユーザー名または間違ったパスワードを入力した。
- クラスタ間ルックアップサービス（ILS）がすべての Unified CM クラスタに設定されていない。これは、UDS クエリがクライアントのホームクラスタを検出するために Cisco Expressway が使用する Unified CM ノードに応じて、断続的な障害の原因となる場合があります。

「「407 Proxy Authentication Required」」または「「500 Internal Server Error」」のエラーによる通話障害

通話障害は、 Cisco Expressway のトラバーサルゾーンが *[*ログイン情報の確認（*Check credentials*）*]* の **[認証ポリシー（Authentication policy）]** で構成されていると発生する場合があります。モバイルおよびリモートアクセスに使用されているトラバーサルゾーンの **[認証ポリシー（Authentication policy）]** が *[*ログイン情報を確認しない（*Do not check credentials*）*]* に設定されていることを確認します。

通話のビットレートが 384 kbps に制限されているまたは、BFCP（プレゼンテーション共有）使用時のビデオの問題

これは、Unified CM で構成された地域内のビデオビットレート制限によって生じる可能性があります。

地域間と地域内で、**[ビデオ コールの最大セッション ビット レート（Maximum Session Bit Rate for Video Calls）]**（**[システム（System）]** > **[リージョン情報（Region Information）]** > **[リージョン（Region）]**）が 6000 kbps などのシステムの適切な上限に設定されていることを確認します。

IM and Presence Service レルムの変更

IM and Presence Service レルムが変更され、Cisco Expressway-C のレルムデータが更新されていない場合、プロビジョニングエラーが発生する可能性があります。

たとえば、これは、IM and Presence Service ノードのアドレスが変更された場合、または新しいピアが IM and Presence Service クラスタに追加された場合に発生する可能性があります。

診断ログには、Cisco Expressway-C でレルムが見つからないため、「`Failed to query auth component for SASL mechanisms`」のような 情報メッセージが含まれる場合があります

[構成（Configuration）] > **[Unified Communications]** > **[IM and Presence Service ノード（IM and Presence Service nodes）]**の順に選択し、**[サーバーを更新（Refresh servers）]** をクリックして、更新した構成を保存します。プロビジョニングエラーが解決されない場合は、IM and Presence Service ノード構成を確認して再度更新します。

ボイスメールサービスがありません（「403 Forbidden」 応答）

Cisco Unity Connection（CUC）のホスト名が Cisco Expressway-C の HTTP サーバー許可リストに含まれていることを確認します。

サービスリクエストに対する「403 Forbidden」 応答

Cisco Expressway-C および Cisco Expressway-E が信頼できる NTP サーバーに同期されていない場合、サービスに障害が発生する場合があります（「403 Forbidden」 応答）。すべての Cisco Expressway システムが信頼できる NTP サービスと同期されていることを確認してください。

Cisco Expressway がクライアント HTTPS リクエストをドロップする

Cisco Expressway-E の自動侵入保護機能によって、HTTP プロキシ経由でリソースにアクセスするクライアント IP アドレスから、不正な試行（404 エラー）が繰り返し検出された場合に発生することがあります。

クライアント アドレスがブロックされないようにするには、**[HTTP プロキシのリソース アクセスの失敗（HTTP proxy resource access failure）]**（**[システム（System）]** > **[保護（Protection）]** > **[自動検出（Automated detection）]** > **[構成（Configuration）]**）が無効になっていることを確認します。

失敗：アドレスが IM and Presence サーバーではない

このエラーは、リモートアクセスに使用する IM and Presence Service サーバーを構成しようとした場合に発生する可能性があります（**[構成（Configuration）]** > **[Unified Communications]** > **[IM and Presence サーバー（IM and Presence servers）]**）。これは IM and Presence Service サーバーに CA 証明書がないことが原因で、9.1.1 を実行するシステムに該当します。詳細と推奨ソリューションは、「CSCul05131」を参照してください。

無効な SAML アサーション

クライアントが SSO を介した認証をできなかった場合の 1 つの可能性のある理由として、Cisco Expressway-C が IDP からの無効なアサテーションを拒否した場合が挙げられます。

無効な `SAML 応答` のログを確認します。

1 つの例として、ユーザーの ID を Cisco Expressway-C に送信するクレームルールが ADFS にない場合が挙げられます。この場合、ログに `[IdPからのアサテーションにuid属性がありません（No uid Attribute in Assertion from IdP）]` と表示されます。

Cisco Expressway は、**`uid`** と呼ばれる属性にアイデンティティを持つ ADFS からのクレームがアサートされるユーザー ID を想定します。ADFS に移動して、各信頼当事者証明でクレームルールを設定し、「uid」 としてユーザーの E メールアドレス（または展開に応じて sAMAccountName）を他の信頼当事者に送信します。

「502 Next Hop Connection Failed」 メッセージ

Cisco Expressway-E の 502 メッセージは、次のホップに障害が発生したことを示します（一般的には Cisco Expressway-C）。次の手順を実行します。

1. Cisco Expressway-E で、**[ステータス（Status）]** > **[Unified Communications]** の順に選択します。Cisco Expressway-E レポートで問題が発生しましたか?
2. ステータスが正常に見える場合は、[ステータス（Status）] ページの下部にある **[SSH トンネルステータス（SSH tunnel status）]** リンクをクリックします。Cisco Expressway-C ノードへの 1 つ以上のトンネルがダウンしている場合、502 エラーが原因である可能性があります。

着信側エンドポイントが Expressway-E から 15 ホップ以上離れている場合、MRA コールは失敗します

Unified Communications トラバーサルゾーンのデフォルトのホップカウントは 15 です。これが原因であると思われる場合は、すべての MRA Expressway にサインインし、ホップカウントを 70 などの非常に大きな数に増やしてテストします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。