トラブルシューティング

この章では、次の内容について説明します。

ネイバーとトラバーサルゾーンでの SIP TLS ネゴシエーションの失敗

TLS 検証モードが有効にされている場合、ゾーン構成の **[ピアアドレス（Peer address）]** フィールドに指定されたネイバーシステムのFQDNまたはIPアドレスがそのシステムで提示されたX.509証明書の証明書の所有者名と照合するために使用されます。（名前は証明書のSAN属性に含まれている必要があります）。証明書自体も有効であり、信頼された認証局によって署名されている必要があります。

そのため、証明書がピアまたはクラスタ FQDN で生成されている場合は、ゾーンの **[ピアアドレス（Peer address）]** フィールドが IP アドレスではなく FQDN で設定されていることを確認します。

8192 ビットキー長の証明書

証明書が 8192 ビットのキー長を使用する場合、SIP TLS ゾーンがアクティブになれない場合があります。4096 ビットのキー長を有する証明書を使用することを推奨します。

モバイルおよびリモートアクセスを使用する際のサービス障害

末尾の改行文字を含まない秘密キーファイルをアップロードした場合、証明書のエラーにより Unified Communications のモバイルおよびリモートアクセスサービスが失敗する場合があります。

秘密キーファイルに末尾の改行文字が含まれていることを確認してください。

SSH 障害および未対応 OID に関する問題

ssh トンネルの確立ができないなどの不明な ssh 障害が発生した場合は、証明書に不明な OID がないかを確認してください。これは、[発行者および件名（Issuer & Subject）] フィールドの CN に復号化されていない数値エントリがないかを確認することで対応できます（GUI の場合、**[メンテナンス（Maintenance）] > [セキュリティ証明書（Security Certificates）] > [サーバー証明書（Server Certificate）] > [表示（復号化）（Show (decoded)]** から確認。コンソールの場合、「`openssl x509 -text -noout -in /tandberg/persistent/certs/server.pem`」で確認）。

無効（Invalid）

```
subject=CN=blahdeblah,OU=IT

Security,O=BigBang,L=Washington,ST=District of

Columbia,C=US,1.3.6.1.4.1.6449.1.2.1.5.1 = #060C2B06010401B2310102010501
```

有効

```
subject=CN=blahdeblah,OU=IT

Security,O=BigBang,L=Washington,ST=District of

Columbia,C=US,jurisdictionOfIncorporationLocalityName=Dover
```

Expressway との Cisco Unified Communications Manager 暗号の相互運用性

Transport Layer Security（TLS）ハンドシェイク中のサーバーは、Rivest Shamir Adleman（RSA）/楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA）暗号を送信します。クライアントとしての Expressway は、これらの暗号を受け入れることができます。

（注） Expressway の新規インストールでは、デフォルトで ECDSA 暗号が使用されます。

Expressway は ECDSA 暗号要求をネゴシエートできます。

メモ

- RSA を使用した証明書暗号化、UCM は *CallManager* または *Tomcat* 証明書のいずれかを送信します。
- ECDSA を使用した証明書暗号、UCM は *CallMananager-ECDSA* または *Tomcat-ECDSA* 証明書のいずれかを送信します。
- ユーザーは、UCM から受信した証明書を検証するために、署名済み Unified Call Manager（UCM）証明書を信頼できる認証局（CA）として Expressway-C に順番にアップロードする必要があります。

参考情報

- **暗号構成の場合：**ECDSA を構成してから RSA 暗号を構成します。

```
ECDHE-ECDSA-AES128-GCM-SHAdefault:ECDHE-ECDSA-AES128-SHAdefault:ECDHE-ECDSA-
AES128-SHA:ECDHE-ECDSA-AESdefault-GCM-SHA384:ECDHE-ECDSA-AESdefault-
AES128-SHA:ECDHE-ECDSA-AESdefault-GCM-SHA384:ECDHE-ECDSA-AESdefault-
GCM-SHA384
```

- **Expressway での構成の場合**

  [メンテナンス（Maintenance）] > **[セキュリティ（Security）]** > **[暗号（Ciphers）]**の順に選択し、以下の暗号を追加します。

（注） ECDSA を高優先度として送信するには、次の暗号の変更が必要です。

```
EECDH:EDH:HIGH:-
AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH
```

トラブルシューティング

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。