CHAPTER 1

Cisco Unity Connection 9.x のトラブルシューティングの概要

『*Cisco Unity Connection トラブルシューティング ガイド*』には、Connection での問題を解決する方法が記載されています。Connection システムに、このトラブルシューティング ガイドに記載されている現象がみられる場合は、推奨されるトラブルシューティング手順を実行してください。現象がこのトラブルシューティング ガイドに記載されていない場合、または推奨されるトラブルシューティングを行っても問題が解決しない場合は、次の手順を実行し、問題の原因が SELinux Security ポリシーでないことを確認します（Connection サーバでは、Cisco Security Agent（CSA）の代わりに SELinux が使用されます）。

ガイドに記載のトラブルシューティング手順では解決できない問題をトラブルシューティングする方法

ステップ 1 Connection サーバで SELinux のステータスを確認するには、コマンドライン インターフェイス（CLI）**utils os secure status** を実行します。

ステップ 2 SELinux が Enforcing モードの場合は、CLI コマンド **utils os secure permissive** を実行し、Connection サーバを Permissive モードに切り替えます。CLI コマンド **utils os secure permissive** の詳細については、適切な『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。このガイドは、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html から入手可能です。

ステップ 3 Permissive モードの SELinux で現象を再現します。現象が再現可能な場合は、問題の原因は SELinux ではありません。

ステップ 4 現象が再現できない場合は、次の手順を実行し、Cisco TAC に接続する前にログを収集します。

a. SFTP サーバにテスト ディレクトリを作成し、そこに監査ログの診断ファイルを保存します。

b. CLI コマンド **utils os secure enforce** を実行し、Connection サーバを Enforcing モードに切り替えます。

c. 現象を再現します。

d. CLI コマンド **utils create report security** を実行し、監査ログの診断ファイルを作成します。このコマンドにより、診断ファイル security-diagnostics.tar.gz が作成されます。コマンド **file get activelog syslog/security-diagnostics.tar.gz** を実行し、手順 4（a）で作成した SFTP ディレクトリに診断ファイルをコピーします。CLI コマンドの詳細については、適切な『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』（http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html）を参照してください。

ステップ 5　Cisco TAC に連絡してください。

たとえば、Unity Connection 8.6 から新しいバージョンへのアップグレードの一環として、バージョン切り替えの障害をトラブルシューティングするには、次の手順を実行します。

Cisco Unity Connection 8.6 から新しいバージョンへのアップグレードの一環として、バージョン切り替えの障害をトラブルシューティングする方法

ステップ 1　Connection サーバで SELinux のステータスを確認するには、コマンドライン インターフェイス（CLI）**utils os secure status** を実行します。

ステップ 2　SELinux が Enforcing モードの場合は、CLI コマンド **utils os secure permissive** を実行し、Connection サーバを Permissive モードに切り替えます。CLI コマンド **utils os secure permissive** の詳細については、適切な『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。このガイドは、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html から入手可能です。

ステップ 3　Permissive モードの SELinux でバージョン切り替えを再試行します。バージョン切り替えの障害が再現可能な場合は、問題の原因は SELinux ではありません。

ステップ 4　バージョン切り替えの障害が再現できない場合は、次の手順を実行し、Cisco TAC に接続する前にログを収集します。

a. SFTP サーバにテスト ディレクトリを作成し、そこに監査ログの診断ファイルを保存します。

b. CLI コマンド **utils os secure enforce** を実行し、Connection サーバを Enforcing モードに切り替えます。

c. 現象を再現します。

d. CLI コマンド **utils create report security** を実行し、監査ログの診断ファイルを作成します。このコマンドにより、診断ファイル security-diagnostics.tar.gz が作成されます。コマンド **file get activelog syslog/security-diagnostics.tar.gz** を実行し、手順 4（a）で作成した SFTP ディレクトリに診断ファイルをコピーします。CLI コマンドの詳細については、適切な『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』（http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html）を参照してください。

ステップ 5　Cisco TAC に連絡してください。

Connection 8.6.（x）からアップグレード中にフェイルセーフ メッセージをトラブルシューティングする方法

クラスタ内で Connection 8.6.（x）からアップグレード中にフェイルセーフ メッセージを受け取った場合は、CLI コマンド **utils os secure permissive** コマンドを実行し、バージョン切り替え手順が完了するまでシステムを Permissive モードに切り替えます。システムを Permissive モードに切り替えるために使用される CLI モードについては、適切な『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。このドキュメントは、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html から入手可能です。