TAC とのケースのオープン

この項では、TAC に問い合わせる場合に必要な情報の詳細、および TAC の担当者と情報を共有する方法について説明します。

シスコテクニカルサポートでは、有効なシスコ サービス契約を保有しているすべてのお客様、パートナー、リセラー、およびディストリビュータ向けに、24時間対応の高い評価を得ているテクニカル サポートを用意しています。Cisco Technical Support Web サイトでは、シスコ製品やシスコ テクノロジーに関する技術的な問題を解決するためのオンラインのドキュメントやツールをご利用いただけます。この Web サイトは、24 時間 365 日、いつでも利用可能です。URL は次のとおりです。*http://www.cisco.com/techsupport*

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3 と S4 の問題とは、ネットワークの障害が軽微である場合、あるいは製品情報が必要な場合を意味します）。状況をご説明いただくと、TAC Service Request ツールが自動的に推奨する解決方法を提供します。これらの推奨手段で問題を解決できない場合は、Cisco TAC のエンジニアが対応します。次の URL で TAC サービスリクエストツールを検索してください。 *http://www.cisco.com/techsupport/servicerequest*

S1 または S2 に関して、またはインターネット アクセスがない場合は、電話で Cisco TAC にご連絡ください。（S1 または S2 の問題とは、運用中のネットワークがダウンした場合、あるいは重大な障害が発生した場合を意味します）。S1 および S2 の問題には Cisco TAC の技術者がただちに対応し、業務を円滑に実行できるよう支援します。

電話でサービス リクエストを開く場合は、次の番号にご連絡ください。

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

米国：1 800 553 2447

詳細な Cisco TAC の連絡先については、次の URL を参照してください。
http://www.cisco.com/techsupport/contacts

- 必要な情報 （2 ページ）
- 必要な予備的情報 （2 ページ）
- オンライン ケース （4 ページ）
- Serviceability Connector （4 ページ）

- Cisco Live! （5 ページ）
- Remote Access （6 ページ）
- Cisco Secure Telnet （6 ページ）
- リモート アカウントの設定 （8 ページ）

必要な情報

Cisco TAC に対してサービス リクエストをオープンする場合は、問題を特定し、その内容を把握しやすくするための予備的情報をご提供いただく必要があります。問題の内容によっては、追加の情報をご提供いただく必要があります。次に示す情報をエンジニアから要求されなくても遅滞なく収集してください。サービス リクエストをオープンし、エンジニアから要求されたあとに収集を開始すると、問題の解決が遅くなります。

関連トピック

Cisco Live! （5 ページ）
Cisco Secure Telnet （6 ページ）
全般情報 （3 ページ）
ネットワーク レイアウト （2 ページ）
オンライン ケース （4 ページ）
問題の説明 （3 ページ）
Remote Access （6 ページ）
必要な予備的情報 （2 ページ）

必要な予備的情報

すべての問題において、必ず次の情報を TAC に提供してください。この情報を収集および保存して TAC サービス リクエストをオープンするときに使用できるようにし、変更があった場合には定期的に更新します。

関連トピック

全般情報 （3 ページ）
ネットワーク レイアウト （2 ページ）
問題の説明 （3 ページ）

ネットワーク レイアウト

物理セットアップおよび論理セットアップの詳細な説明、および音声ネットワークに関連する次のすべてのネットワーク要素をお知らせください（存在する場合）。

- Unified Communications Manager
  - バージョン（Unified Communications Manager Administration で **[詳細]** を選択）

- Unified Communications Manager の数
- セットアップ（スタンドアロン、クラスタ）
    - Unity
- バージョン（Unified Communications Manager Administration から）
- 統合のタイプ
    - アプリケーション
- インストールされているアプリケーションのリスト
- 各アプリケーションのバージョン番号
    - IP/音声ゲートウェイ
- OS のバージョン
- show tech コマンド（IOS ゲートウェイ）
- Unified Communications Manager の負荷（Skinny ゲートウェイ）
    - スイッチ（Switch）
- OS のバージョン
- VLAN の設定
    - ダイヤル プラン：番号付け方式、コール ルーティング

Visio や JPG などで作成した詳細な図を提出すると理想的です。ホワイトボードを使用して、Cisco Live! セッションから図を提供することもできます。

問題の説明

問題が発生したときにユーザが実行した処理について、手順ごとの詳細を提供します。詳細情報には、次の内容を含める必要があります。

- 予想される動作
- 実際に観察された動作の詳細

全般情報

次の情報を準備する必要があります。

- 新しいインストールかどうか

- 以前のバージョンのUnified Communications Managerがインストールされている場合、最初からこの問題が発生していたかどうか（最初から発生していない場合は、最近システムに対して行った変更）
- この問題は再現可能かどうか
  - 再現可能である場合は、通常の環境で発生するか、または特別な環境で発生するか
  - 再現不可能である場合は、問題発生のタイミングが特別であったかどうか
  - 発生の頻度
- 影響のあるデバイス
  - ランダムなデバイスではなく、特定のデバイスが影響を受ける場合、影響を受けるデバイスの共通点は何か
  - 問題に関連するすべてのデバイスの DN または IP アドレス（ゲートウェイの場合）
- コール パス上のデバイス（存在する場合）

オンライン ケース

Cisco.com から TAC Case Open ツールのオンライン サービスを使用すると、他のすべてのサービス リクエスト オープン方法よりも優先的に処理されます。ただし、高優先度のサービス リクエスト（P1 および P2）は例外です。

サービス リクエストをオープンする場合は、問題についての正確な説明を提供してください。問題の説明を提供すると、すぐに解決策として使用できる可能性がある URL リンクが返されます。

リンクを参照しても問題の解決策が見つからない場合は、プロセスを続行して、サービス リクエストを TAC エンジニアに送信してください。

Serviceability Connector

Serviceability Connector の概要

Webex Serviceability サービスを使用すると、ログの収集を容易にすることができます。このサービスでは、診断ログや情報を検索、取得、保管するタスクを自動化します。

この機能は、お客様の社内に導入された *Serviceability Connector* を使用します。Serviceability Connector は、ネットワーク内の専用ホスト（「コネクタ ホスト」）で実行されます。次のいずれかのコンポーネントにコネクタを取り付けできます。

- Enterprise Platform (ECP) の利用: 推奨

ECP は、Docker コンテナを使用してサービスを分離、保護、管理します。ホストとサービスアビリティ コネクタ アプリケーションがクラウドからインストールされます。最新の状態で安全な状態を確保するために、手動でアップグレードする必要はありません。

重要 ECP の使用を推奨します。私たちの将来の開発は、このプラットフォームに焦点を当てます。Expressway に有用性コネクタをインストールすると、一部の新機能が使用できなくなります。

- Cisco Expressway

Serviceability サービスは、次の目的で使用できます。

- サービス要求のログおよびシステム情報の自動取得
- クラウド接続型 UC 導入内の Unified CM クラスタのログ収集

Serviceability サービスを使用する利点

サービスには次の利点があります。

- ログの収集速度を上がります。TAC エンジニアは、問題の診断を実行する際に関連するログを取得できます。追加のログ リクエストや手動による収集と配送の待機の遅延を回避できます。この自動化により、問題解決に要する時間を数日短縮できる可能性があります。
- TAC のコラボレーション ソリューション 解析ツールおよび診断署名データベースと連携します。システムは、ログを自動的に分析し、既知の問題を特定し、既知の修正または回避策を推奨します。

Serviceability Connector の TAC サポート

Serviceability Connector の詳細については、https://www.cisco.com/go/serviceability を参照するか、TAC の担当者に問い合わせてください。

Cisco Live!

安全で暗号化された Java アプレットである Cisco Live! を利用すると、コラボレーティブ Web ブラウジング、URL 共有、ホワイトボード、Telnet、クリップボードツールを使用することによって、Cisco TAC のエンジニアとより効率的に協同して作業できます。

Cisco Live! には次の URL からアクセスできます。

```
http://c3.cisco.com/
```

Remote Access

リモート アクセスを使用すると、必要なすべての装置に対して Terminal Services セッション（リモート ポート 3389）、HTTP セッション（リモート ポート 80）、および Telnet セッション（リモート ポート 23）を確立できます。

注意 ダイヤルインを設定する場合は、システムに対する脆弱性となるため、**login:cisco** または **password:cisco** は使用しないでください。

TAC エンジニアが次のいずれかの方法を使用してデバイスにリモート アクセスすることを許可すると、多くの問題を非常に迅速に解決できます。

- パブリック IP アドレスが設定された装置
- ダイヤルイン アクセス：（プリファレンスの高い順に）アナログ モデム、統合デジタル通信網（ISDN）モデム、バーチャル プライベート ネットワーク（VPN）
- ネットワーク アドレス変換（NAT）：プライベート IP アドレスが設定された装置へのアクセスを可能にする IOS およびプライベート インターネット エクスチェンジ（PIX）。

エンジニアの介入時にファイアウォールによってIOS トラフィックと PIX トラフィックが遮断されないこと、およびサーバ上で Terminal Services などの必要なすべてのサービスが開始されていることを確認してください。

（注） TAC では、すべてのアクセス情報は厳重に管理されます。また、お客様の同意なしにシステムを変更することはありません。

Cisco Secure Telnet

シスコ サービス エンジニア（CSE）は、Cisco Secure Telnet を使用して、サイト上のUnified Communications Managerサーバに対して透過的にファイアウォール アクセスを実行できます。

Cisco Secure Telnet は、シスコのファイアウォール内部で Telnet クライアントをイネーブル化することによって、ファイアウォールで稼働する Telnetデーモンに接続します。このセキュアな接続により、ファイアウォールを変更せずに、Unified Communications Managerサーバの監視およびメンテナンスをリモートで行うことができます。

（注） シスコは、許可があった場合にだけお客様のネットワークにアクセスします。サイトに、このプロセスの開始を支援するネットワーク管理者を配置する必要があります。

ファイアウォールによる保護

ほとんどすべての内部ネットワークでは、外部から内部のホストシステムへのアクセスを制限するためにファイアウォールアプリケーションが使用されています。これらのアプリケーションでは、ネットワークとパブリックインターネットとの間のIP接続を制限することによって、ネットワークが保護されます。

ファイアウォールでは、許可するように明示的に再設定しないかぎり、外部から開始されるTCP/IP 接続が自動的にブロックされます。

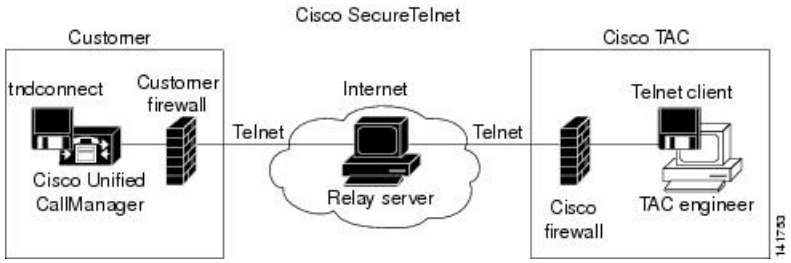
通常、企業ネットワークではパブリックインターネットとの通信が許可されますが、ファイアウォール内部から外部ホストに向けて開始される接続だけが許可されます。

Cisco Secure Telnet の設計

Cisco Secure Telnet では、ファイアウォールの内側から簡単に Telnet 接続を開始できるという技術を活用しています。外部のプロキシ マシンを使用して、ファイアウォールの内側からのTCP/IP 通信が *Cisco Technical Assistance Center* (TAC) にある別のファイアウォールの内側のホストへとリレーされます。

このリレー サーバを使用することによって、両方のファイアウォールの完全性が維持され、また保護されたリモート システム間の安全な通信がサポートされます。

図 *1 : Cisco Secure Telnet* システム



Cisco Secure Telnet の構造

外部のリレー サーバによって、お客様のネットワークとシスコとの間に Telnet トンネルが構築され、接続が確立されます。これにより、Unified Communications Managerサーバの IP アドレスおよびパスワード識別子を CSE に送信できます。

（注） パスワードは、管理者と CSE が相互に同意した文字列です。

管理者は、Telnet トンネルを開始することによって、プロセスを開始します。これにより、ファイアウォールの内部からパブリック インターネット上のリレー サーバへの TCP 接続が確立されます。次に、Telnet トンネルによって、ローカルの Telnet サーバへの別の接続が確立され、エンティティ間の双方向のリンクが作成されます。

（注） Cisco TAC の Telnet クライアントは、Windows NT および Windows 2000 上で動作するシステム、または UNIX オペレーティング システムに準拠して動作します。

ローカル サイトの Cisco Communications Manager がパスワードを受け入れると、Cisco TAC で実行されている Telnet クライアントは、ローカル ファイアウォールの内側で動作する Telnet デーモンに接続します。この結果確立される透過的接続によって、マシンがローカルで使用されている場合と同様にアクセスできるようになります。

安定的な Telnet 接続が確立されると、CSE は、Unified Communications Managerサーバに対してメンテナンス タスク、診断タスク、およびトラブルシューティング タスクを実行するためのあらゆるリモート有用性機能を導入できます。

CSE が送信するコマンドおよびUnified Communications Managerサーバから発行される応答を確認することはできますが、コマンドや応答が常に完全な形式で表示されるとは限りません。

リモート アカウントの設定

シスコ サポートがトラブルシューティングのためにご使用のシステムに一時的にアクセスできるよう、Unified Communications Manager でリモート アカウントを設定します。

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] で、**[サービス（Services）]** > **[リモート サポート（Remote Support）]** を選択します。

ステップ 2 [アカウント名（Account Name）] フィールドに、リモート アカウントの名前を入力します。

ステップ 3 [アカウントの有効期限（Account Duration）] フィールドに、アカウントの有効期限を日数で入力します。

ステップ 4 **[保存]** をクリックします。
システムは、暗号化パス フレーズを生成します。

ステップ 5 シスコのサポート担当者に連絡して、リモート サポート アカウント名とパス フレーズを提供します。