CHAPTER 10

TAC とのサービス リクエストのオープン

シスコと正式なサービス契約を交わしているすべてのお客様、パートナー、および代理店は、Cisco Technical Support で 24 時間テクニカル サポートを利用することができます。Cisco Technical Support Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。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：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。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。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、Cisco TAC のエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

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

この項では、TAC に問い合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。

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。

- 「必要な予備的情報」
  - 「ネットワーク レイアウト」
  - 「問題の説明」
  - 「一般情報」
- 「TAC Case Open ツールのオンライン サービス」
- 「Cisco Live!」
- 「リモート アクセス」
- 「Cisco Secure Telnet」

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。

- 「ネットワーク レイアウト」
- 「問題の説明」
- 「一般情報」

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）。

- Cisco Unified Communications Manager
  - バージョン（Cisco Unified CM の管理で [詳細（Details）] を選択）
  - Cisco 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（Cisco Unified CM の管理から）
  - 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）
  - Cisco Unified Communications Manager の負荷（Skinny ゲートウェイ）
- スイッチ
  - 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。Cisco Live! セッションを利用すると、ホワイトボードを使用して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

一般情報

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
- Cisco Unified Communications Manager の古いバージョンのインストールである場合、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）

TAC Case Open ツールのオンライン サービス

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。

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 からアクセスします。

http://c3.cisco.com/

リモート アクセス

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、Integrated Services Digital Network（ISDN; 統合デジタル通信網）モデム、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）
- Network Address Translation（NAT; ネットワーク アドレス変換）：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 Private Internet Exchange（PIX; プライベート インターネット エクスチェンジ）

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

Cisco Service Engineer（CSE; シスコ サービス エンジニア）は、Cisco Secure Telnet を使用して、サイト上の Cisco 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、シスコシステムズ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、ファイアウォールの内側にある 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、Cisco 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。

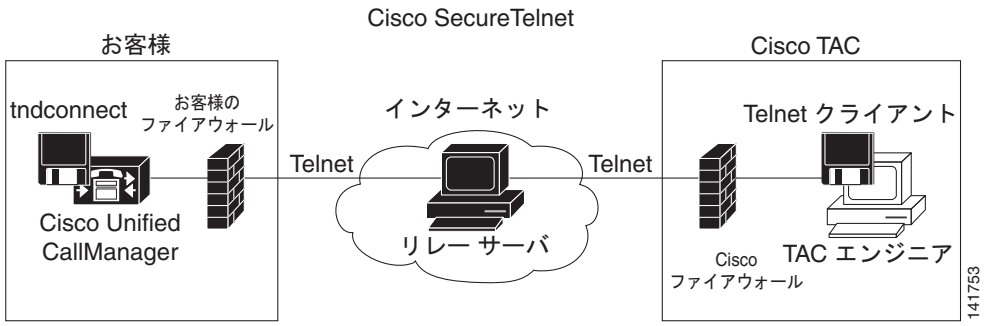
通常、企業ネットワークではパブリック インターネットとの通信が許可されますが、ファイアウォール内部から外部ホストに向けて開始される接続だけが許可されます。

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 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 10-1　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システムズとの間に Telnet トンネルが構築され、接続が確立されます。これにより、Cisco 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、Cisco 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 サービスアビリティを導入できます。

CSE が送信するコマンド、および Cisco Unified Communications Manager サーバから発行される応答を表示することはできますが、コマンドや応答はすべてが完全な形式で表示されるわけではありません。