TAC への問い合せ

Cisco TAC へのお問い合せに際しては、問題点を識別して限定しやすくするために、予備情報をご提供いただく必要があります。問題の性質によっては、追加情報をご提供いただく場合もあります。お問い合せをした後に、エンジニアが求める次の情報を収集した場合には、必然的に解決が遅れます。

- 必要な予備情報
  - ネットワーク レイアウト
  - 問題の説明
  - 一般的な情報
- TAC Web
- CCO の利用
- 添付ファイル
- Cisco Live!
- リモート アクセス

必要な予備情報

すべての問題について、次の情報は必ず TAC に提供してください。TAC に問い合せを行う際に使用できるように、これらの情報を収集および保存しておき、変更については定期的に更新してください。

ネットワーク レイアウト

物理的な構成と論理な構成に関する詳細な説明、および音声ネットワークに関与する次のネットワーク要素（該当する場合）に関する詳細な説明です。

- Cisco CallManager
  - バージョン（Cisco CallManager Administration で **Details** を選択して確認します）
  - Cisco CallManager の数
  - 構成（スタンドアロン、クラスタ）
- Unity
  - バージョン（Cisco CallManager Administration で確認します）
  - 統合タイプ
- 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 バージョン
  - Show tech（IOS ゲートウェイ）
  - Cisco CallManager ロード（Skinny ゲートウェイ）
- スイッチ
  - OS バージョン
  - VLAN 設定
- ダイヤル プラン：番号付け方式、コール ルーティング

可能な場合は、Visio またはその他の詳細な図（JPG など）を提出してください。Cisco Live! セッションで、ホワイトボードを使用して図を用意することもできます。

問題の説明

問題発生時にユーザが実行した操作を順序どおりに説明した詳細な情報を用意してください。その中には次の項目を含めてください。

- 予想した動作
- 実際の動作の詳細

一般的な情報

次の情報をすぐに提示できるようにしておいてください。

- 新しいバージョンをインストレールしているか。
- 古いバージョンの Cisco CallManager をインストールしている場合、この問題は当初から発生していたか（当初は発生していなかった場合、システムに対して最近どのような変更を行ったか）。
- この問題は再現可能か。
  - 再現可能な場合、それは通常の状況か、それとも特殊な状況か。
  - 再現不能な場合、問題が実際に発生した状況に関して何か特別な情報はあるか。
  - 問題が発生する頻度はどのくらいか。
- 影響を受けるデバイスは何か。
  - 特定の複数デバイスが影響を受ける場合（影響を受けるデバイスがいつも決まっている場合）、それらのデバイスに共通することは何か。
  - 問題に関与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）。
- Call-Path 上にあるデバイスは何か（該当する場合）。

TAC Web

TAC Web（各種ツールや TAC エンジニアが作成した技術文書を豊富に収集したサイト）は、一般的な問題を分析し、解決方法を見いだすために使用します。TAC Web ツールとその使用方法を説明するコンテンツについては、次の URL を参照してください。

http://www.cisco.com/public/support/tac/home.shtml

CCO の利用

CCO を利用した問い合せは、その他のすべての方法に優先して取り扱われます。優先度の高い問い合せ（P1 および P2）は、この規則の例外となります。

CCO を利用して問い合わせを行う際は、問題を正確に記述する必要があります。その記述により、それに応じた解決方法を提供すると考えられる URL リンクが返されます。

問題の解決方法が見つからない場合は、その問い合せ内容を TAC エンジニアに送信するプロセスに進みます。

添付ファイル

問い合せ内容に添付するレポートは、電子メールでエンジニアに送信します。100 KB よりも大きい文書の場合は zip ファイルを添付します。

次の URL で、*Manage a TAC Case* セクションを使用してください。*please login* リンクを使用して、登録ユーザとしてログインします。

http://www.cisco.com/public/support/tac/contact.shtml

Cisco Live!

暗号化されたセキュアな Java アプレットである Cisco Live! では、Collaborative Web Browsing および URL 共有、ホワイトボード、Telnet、およびクリップボードの各ツールを利用することによって、Cisco TAC エンジニアと協力して、より効果的に作業を進めることができます。

Cisco Live! には、次の URL でアクセスします。

http://c3.cisco.com/

リモート アクセス

リモート アクセスにより、必要なすべての機器対して、Terminal Services（リモート ポート 3389）、HTTP（リモート ポート 80）、および Telnet（リモート ポート 23）の各セッションを確立できます。

注意　ダイヤルインを設定するときは、**login:cisco** および **password:cisco** を使用しないでください。これらは、システムに脆弱性をもたらす要因となります。

次のいずれかの方法により、デバイスに対するリモート アクセスを TAC エンジニアに許可することで、多くの問題を非常に迅速に解決できます。

- パブリック IP アドレスを持つ機器
- ダイヤルイン　アクセス：（優先順位の高いものから）アナログ　モデム、Integrated Services Digital Network（ISDN; サービス総合デジタルネットワーク）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 アドレスを持つ機器に対するアクセスを許可する IOS および Private Internet Exchange（PIX）

エンジニアの介入時にファイアウォールが IOS トラフィックおよび PIX トラフィック を遮断しないこと、および Terminal Services などの必要なすべてのサービスがサーバ上で起動していることを確認してください。

（注）　TAC は、すべてのアクセス情報の取り扱いに最大限の注意を払います。また、お客様の同意なしにシステムに変更を加えることはありません。

Cisco Secure Telnet

Cisco Secure Telnet を使用すると、Cisco Service Engineer（CSE; シスコ サービス エンジニア）は、ファイアウォールを介してお客様のサイトの Cisco CallManager サーバに透過的にアクセスできます。

Cisco Secure Telnet が機能するためには、シスコシステムズのファイアウォールの内側にある Telnet クライアントが、お客様のファイアウォールの内側にある Telnet デーモンに接続できるようにする必要があります。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、お客様の Cisco CallManager 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、必ずお客様の許可を得た上で、お客様のネットワークにアクセスします。作業を開始する場合は、お客様のサイトでネットワーク管理者のご協力をお願いしています。

ファイアウォール保護

ほぼすべての内部ネットワークでは、ファイアウォール アプリケーションを使用して、内部ホスト システムに対する外部アクセスを制限しています。これらのアプリケーションは、ネットワークとパブリック インターネット間の IP 接続を制限することで、ネットワークを保護しています。

ファイアウォールの機能は、外部で開始された TCP/IP 接続を許可するように設定が変更されない限り、そのような接続を自動的にブロックすることです。

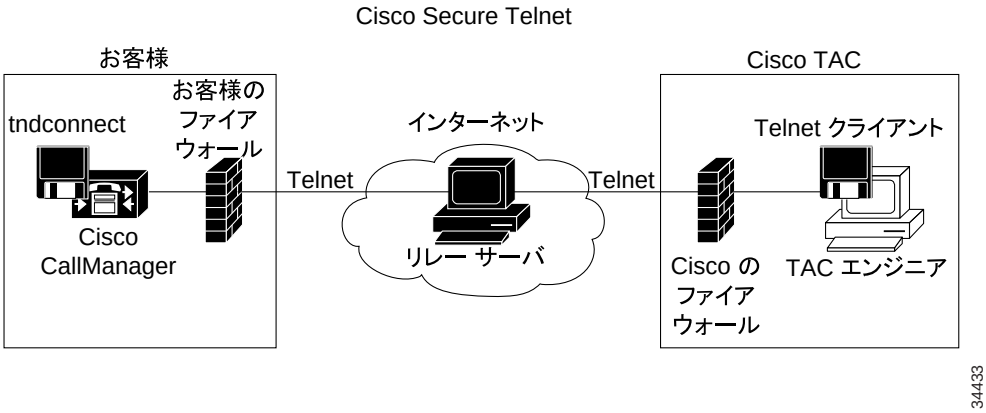
通常、企業ネットワークはパブリック インターネットとの通信を許可します。ただし、外部ホストへの接続がファイアウォールの内側で開始された場合に限ります。

Cisco Secure Telnet の設計

Cisco Secure Telnet では、Telnet 接続がファイアウォールの内側から簡単に開始できるという点を利用しています。外部のプロキシ マシンを使用して、システムはファイアウォールの内側から 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 TCP/IP 通信をリレーします。

このリレー サーバを使用することで、保護されたリモート システム間のセキュアな通信がサポートされるとともに、両方のファイアウォールの整合性が維持されます。

図 A-1　Cisco Secure Telnet システム



Cisco Secure Telnet の構造

外部リレー サーバは Telnet トンネルを構築することにより、お客様のネットワークとシスコシステムズ間の接続を確立します。この処理によって、Cisco CallManager サーバの IP アドレスとパスワード識別情報を CSE に送信できるようになります。

（注） パスワードは、お客様側の管理者と CSE が相互に同意したテキスト文字列で構成されます。

管理者は Telnet トンネルを起動してプロセスを開始します。この操作により、お客様側のファイアウォールの内側からパブリック 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。その後、Telnet トンネルによって、お客様のローカル Telnet サーバへの別の接続が確立され、エンティティ間に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 上のシステムまたは UNIX オペレーティング システムのもとで動作します。

お客様のサイトの Cisco CallManager がパスワードを受け入れた後、Cisco TAC で動作している Telnet クライアントは、お客様側のファイアウォールの内側で実行されている Telnet デーモンに接続します。その結果、透過的な接続が実現するので、ローカルでマシンを使用している場合と同様のアクセスが可能になります。

Telnet 接続が安定すると、CSE はすべてのリモート サービサビリティ機能を使用して、Cisco CallManager サーバに対してメンテナンス、診断、およびトラブルシューティングの各作業を実行できます。

CSE によって送信されたコマンドおよび Cisco CallManager サーバからの応答を表示することができますが、これらのコマンドおよび応答は必ずしも完全にフォーマットされているとは限りません。

その他の情報

詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。