



## TAC への問い合わせ

Cisco Technical Assistance Center (TAC) は、シスコのお客様、パートナー、および代理店に対してテクニカル サポート サービスを提供します。お客様のニーズに十分に対応するために、TAC では次の 2 タイプのサポートを用意しています。

- Cisco TAC Web サイト ([www.cisco.com/tac](http://www.cisco.com/tac)) でのオンライン サポート
- TAC Escalation Center による電子メールおよび電話でのサポート

TAC からの支援が必要になった場合は、次の 3 つの方法で TAC にお問い合わせいただけます。

### 1. Web による連絡

TAC Service Request Tool を使用すると、TAC へのお問い合わせプロセスが自動化されます。Service Request Tool は、<http://tools.cisco.com/ServiceRequestTool/create/launch.do> でいつでも入手することができます。

TAC Service Request Tool は、お問い合わせプロセスの中で、解決方法を自動的に提案します。このため、実際にお問い合わせいただく前に問題を解決できることがあります。お問い合わせが必要となる場合、TAC Service Request Tool は自身のステータスをチェックし、アップデートを追加することができます。

Technical Documentation & Support Web サイト (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) を使用して、一般的な問題を分析し、解決方法を見つけることもできます。次の URL からアクセスできます。<http://www.cisco.com/en/US/support/index.html>

### 2. 電子メールによる連絡

お問い合わせは、電子メールで行っていただくこともできます。メッセージの送付先は [tac@cisco.com](mailto:tac@cisco.com) です。

### 3. 電話による連絡

TAC にご連絡いただく場合の電話番号は複数あり、お客様の所在地に応じて異なります。現在の番号を次に示します。

地域	電話番号
アジア太平洋	+61 2 8448 7107
北米	1 800 553 2447
ヨーロッパ、中東、アフリカ	+32 2 704 5555

最寄り地域の電話番号があるかどうかについては、TAC の Web サイトもご確認ください。



(注) Web および電子メールでのお問い合わせは、デフォルトでは自動的にプライオリティ 3 または 4 の案件になります。  
プライオリティ 1 または 2 の案件については、GCC に電話でお問い合わせください。

## 必要な情報

Cisco TAC へのお問い合わせに際しては、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。お問い合わせをした後に、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 に問い合わ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
- 問題の説明
- 一般的な情報

## ネットワーク レイアウト

物理的な構成と論理的な構成に関する詳細な説明、および音声ネットワークに關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 Unified CallManager
  - バージョン（Cisco Unified CallManager の管理ページで [ヘルプ] > [バージョン情報] を選択して確認します）
  - Cisco Unified CallManager の数
  - 構成（スタンドアロン、クラスター）
- Unity
  - バージョン（Cisco Unified CallManager の管理ページで確認します）
  - 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 Unified CallManager ロード（Skinny ゲートウェイ）
- スイッチ
  - OS バージョン
  - VLAN 設定
- ダイアルプラン：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ールしているか。
- 古いバージョンの **Cisco Unified 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、それは通常の場合か、それとも特殊な状況か。
  - 再現不可能な場合、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 を利用した問い合わせは、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わせ（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、その問い合わせ内容を 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

問い合わ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に対して、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 Unified 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 Unified 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。

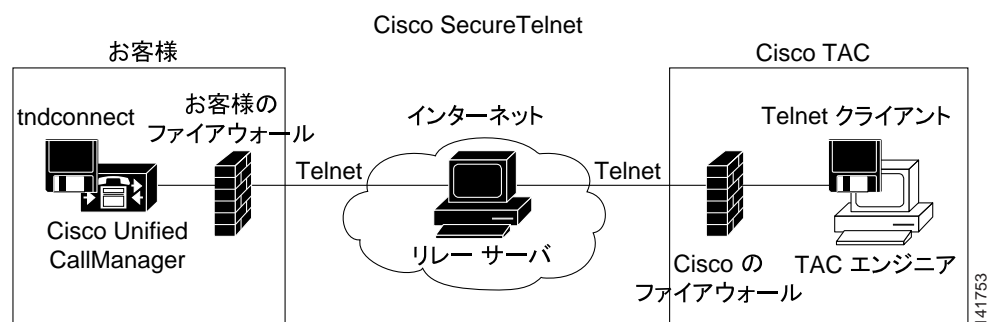
通常、企業ネットワークはパブリック インターネットとの通信を許可します。ただし、外部ホストへの接続がファイアウォールの内側で開始された場合に限りです。

## 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、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 Unified 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 サービスアビリティ機能を使用して、Cisco Unified 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 Unified 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 Unified 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。

