CHAPTER 16

Cisco Secure Telnet

この章の内容のサービスは、日本では提供されていません。米国などこのサービスの提供国でご利用のお客様だけ参照してください。ここでは、Cisco Secure Telnet について説明します。この章の構成は、次のとおりです。

Cisco Secure Telnet の機能は、シスコ サービス エンジニア（CSE）が使用し、ファイアウォール経由でお客様のサイトに配置してある Cisco CallManager サーバに透過的にアクセスします。

この Cisco Secure Telnet 機能により、シスコシステムズのファイアウォール内のシスコ Telnet クライアントは、お客様のファイアウォールの内側にある Telnet デーモンにトンネルを構築して接続します。このトンネルでセキュアに保護された接続により、ファイアウォールを変更せずにお客様の Cisco CallManager サーバに対してリモート モニタリングとメンテナンスを行うことができます。

（注）　シスコでは、お客様の承諾を得たうえでお客様のネットワークにアクセスしています。また、作業を始めるときは、お客様のネットワーク管理者のご協力をお願いしています。

システム設計

Cisco Secure Telnet システム設計は、サイト上にある Cisco CallManager インストレーションとの通信の基準を提供します。

ここでは、各コンポーネントおよびアプリケーションについて、使用方法のシナリオの概要とともに説明します。

リモート アクセスの方法

CSE は、Cisco Secure Telnet 以外の技術を使用してお客様のサイトへのリモート接続を提供できますが、他の方法では、望ましくない状態になる場合があります。

ダイヤルイン アクセスの場合は、専用電話回線とモデムをサイトに設置する必要があります。したがって、ダイヤルイン アクセスは現実的な方法ではありません。Telnet を直接使用すると、TCP/IP 接続を確立できますが、ファイアウォールを開く必要が生じます。そのため、セキュリティが低下し、サービスに遅延が生じる可能性があります。

ファイアウォールの保護

事実上、すべての内部ネットワークはファイアウォール アプリケーションを使用して外部から内部のホスト システムへの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、ネットワークと公衆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ます。

ファイアウォールは、アクセスを許可するようにソフトウェアを再設定しない限り、外部から開始された TCP/IP 接続を自動的にブロックして機能します。

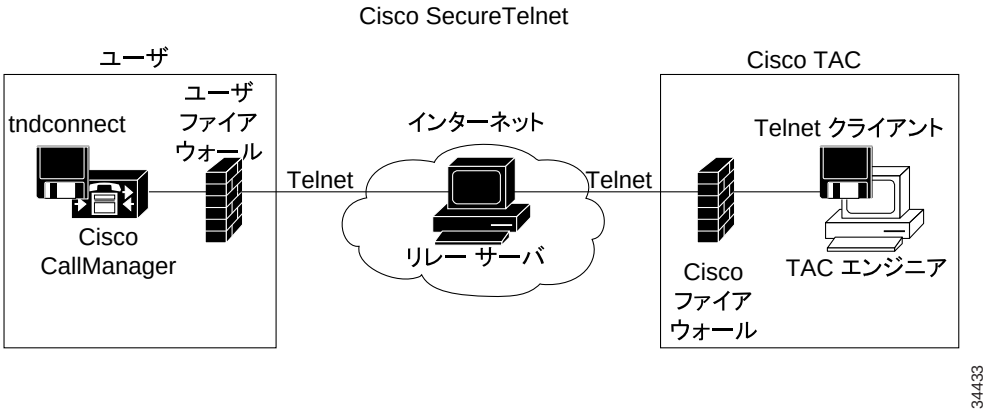
企業ネットワークでは、通常、公衆インターネットとの通信が許可されていますが、接続がファイアウォールの内部から外部のホストへ発信された場合に限られています。

Cisco Secure Telnet の設計

Cisco Secure Telnet は、Telnet 接続がファイアウォールの後方から簡単に開始できるという事実を利用します。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後方から Cisco Technical Assistance Center（TAC）にある別のファイアウォールの後方のホストに TCP/IP のメッセージをリレーします。

保護されたリモート システム間のセキュアな通信をサポートすると同時に、このリレー サーバを使用して両方のファイアウォールの整合性を維持します。図 16-1 を参照してください。

図 16-1　Cisco Secure Telnet システム



Cisco Secure Telnet 構造

外部リレー サーバは、Telnet トンネルを構築して、ネットワークとシスコシステムズとの通信を確立します。これにより、Cisco CallManager サーバの IP アドレスとパスワード識別情報を CSE へ送信できます。

（注）　パスワードは、管理者と CSE が互いに同意したテキスト文字列から構成されています。

管理者は、Telnet トンネルを開始することにより処理を開始します。これにより、ファイアウォールの内側から、外側の公衆インターネット上のリレー サーバへの TCP 接続を確立します。Telnet トンネルは、もう 1 つの接続をローカル Telnet サーバに対して確立し、エンティティ間に双方向のリンクを作成します。

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

サイトの Cisco CallManager がパスワードを受け入れた後、Cisco TAC で動作中の Telnet クライアントは、ファイアウォールの後方で動作中している Telnet デーモンに接続します。その結果として生じる透過的な接続により、マシンをローカルで使用している場合と同様にアクセスできます。

Telnet 接続が安定したら、CSE はすべてのリモート保守機能を実装して、Cisco CallManager サーバ上で、メンテナンス、診断、トラブルシューティングなどの作業を実行できます。

CSE が送信したコマンドと、Cisco CallManager サーバが発行した応答は表示できます。ただし、コマンドと応答は、完全にフォーマットされているとは限りません。

Cisco Secure Telnet 設定のチェックリスト

表 16-1 は、Cisco Secure Telnet を設定する手順の概要を示しています。

表 16-1　Cisco Secure Telnet 設定のチェックリスト

設定手順		関連する手順と項目
ステップ 1	Cisco Secure Telnet のコンポーネントを取得します。	『*Cisco CallManager Serviceability アドミニストレーション ガイド*』の「Cisco Secure Telnet のコンポーネント」
ステップ 2	Cisco Secure Telnet のアプリケーションを取得します。	『*Cisco CallManager Serviceability アドミニストレーション ガイド*』の「Cisco Secure Telnet のアプリケーション」
ステップ 3	tndconnect プログラムを実行します。	『*Cisco CallManager Serviceability アドミニストレーション ガイド*』の「Cisco Secure Telnet の実行可能プログラム」
ステップ 4	tndconnect コマンドを使用して、Cisco CallManager サーバにアクセスします。	『*Cisco CallManager Serviceability アドミニストレーション ガイド*』の「tndconnect のコマンドライン構文」

参考情報

関連項目

- 『*Cisco CallManager Serviceability アドミニストレーション ガイド*』の第 29 章「Cisco Secure Telnet の設定」

参考資料

- *Cisco CallManager トラブルシューティング ガイド*