CHAPTER 29

Cisco Secure Telnet の設定

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 の概要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。

Cisco Secure Telnet のコンポーネント

次の項では、Cisco Secure Telnet で使用されているコンポーネントについて説明します。

リレー サーバ

Cisco リレー サーバは、Windows NT プラットフォーム上で動作します。このリレー サーバは公衆インターネット上のノードで、マルチユーザ システムとして設定されています。このため、Cisco Secure Telnet サービスを使用するシスコのお客様はリレー サーバに自由にアクセスできます。

お客様はリレー サーバを専用デバイスとして使用することができます。またパイロット期間中であれば、必要なときだけ接続することもできます。

リレー サーバは、シスコシステムズのファイアウォールの外部に配置されていますが、その安全が確保されている被制御システムです。また、このサーバは、シスコが所有し、その運用と操作もシスコが行っています。

（注）　インターネットからリレー サーバに簡単にアクセスできない場合は、デバイスへのダイレクトなインターネット アクセスを許可している ISP に対するダイヤルイン接続を使用してください。

Telnet クライアント

Telnet クライアントは、UNIX ホストまたは Windows NT システム上のシスコのサイトで動作します。このクライアントは TCP/IP 上で端末エミュレーションを実行して、ユーザ サイトのサーバへの入力を可能にするリモート シェルを提供します。

Telnet クライアントは、Cisco リレー サーバを経由して、Cisco CallManager ホストにコマンドラインを使用してアクセスします。

Telnet サーバ

Telnet サーバはお客様のネットワーク上に常駐して、Cisco CallManager サーバ上で動作します。Windows 2000 オペレーティング システムは Cisco CallManager サーバ上で動作し、ローカル システムで使用されるテキスト ベースのコマンド実行をサポートします。

Telnet プロキシ **tndconnect** は、Cisco CallManager サーバ上で動作し、ユーザの Telnet サーバを Cisco リレー サーバにリンクします。

（注）　Windows 2000 システム上で実行される tndconnect ウィンドウは、シスコ TAC とユーザの Cisco CallManager システムの間で使用されるコマンドと応答を表示します。ただし、サポートされる端末タイプによっては、Windows 2000 Telnet デーモンが要素間のスペースを削除する場合があります。

Cisco Secure Telnet のアプリケーション

Cisco Secure Telnet システムは、4 つのソフトウェア コンポーネントから構成されています。

1. Telnet デーモン接続（**tndconnect**）プログラムは、ユーザ側のサイトにある Cisco CallManager サーバ上で実行されます。
2. リレー アプリケーション（**relayapp**）プログラムは、シスコのリレーまたは「接続」サーバ上で実行されます。
3. Windows 2000 Telnet デーモンは、ユーザ サイトにある Cisco CallManager サーバ上で実行される Microsoft のソフトウェアです。
4. 標準 Telnet クライアントは、シスコ TAC 側のファイアウォールの内側で実行されます。

Cisco Secure Telnet の実行可能プログラム

tndconnect コマンドライン実行可能プログラムは、Windows 2000 のコマンド プロンプト ウィンドウから呼び出します。

リモートの保守ユーザは、Cisco CallManager サーバ上のコマンド ウィンドウから **tndconnect** プログラムを呼び出します。このプログラムは、インターネット リレー サーバ上の **relayapp** アプリケーションとコンタクトを取ります。

ユーザ サイトで **tndconnect** が呼び出された後、CSE は Telnet を使用して **relayapp** に接続し、ユーザのシステムにアクセスします。そのシステムにログインすると Telnet セッションが一緒にマップされ、シスコ技術サポートはお客様のサイトにアクセスできるようになります。

それぞれの実行可能プログラムには、各プログラムの動作特性を制御するコマンドライン パラメータ（パスワードや TCP ポートなど）があります。

Telnet プロキシ

tndconnect プログラムは、お客様のサイトからリレー サーバ上にある外部アプリケーションへの接続を可能にするプロキシとして機能します。

このコネクタ プログラムを使用する場合は、特定のコマンドライン パラメータを指定する必要があります。オプションのパラメータが一部含まれています。

tndconnect のコマンドライン構文

tndconnect プログラムは、Cisco CallManager サーバ上の C:\Program Files\Cisco に保存されています。たとえば、コマンドラインから次のように呼び出します。

tndconnect -host relayservername -password cisco -file connect.log -port 80 -verbose -noecho

（注）　**tndconnect** を終了するには、ウィンドウ内で Ctrl+C キーを押します。

次に、各パラメータの定義を示します。

`-host` <*relay hostname*>
host 引数はターゲット リレー サーバの DNS 名を定義します。このため、この引数は必須です。CSE は初期コール時にユーザにホスト名を提供します。

`-password` <*any 4+ character string*>
password 引数は、リレー サーバへのアクセスを可能にします。このため、この引数は必須です。CSE は初期コール時にパスワードを提供します。

`-file` <*logfile name*>
Telnet による情報交換は、後で確認するためにすべてログに記録されます。**-file** パラメータを使用して、ログ ファイル名を指定できます。ログ ファイルには、始動とコンソールのアクティビティの監査証跡が記録されます。システムは、コマンド ウィンドウに対するすべてのアクティビティをログに記録します。

-file 引数を使用しない場合、ファイル名はデフォルトの **tndconnect.log** になります。

`-port` <*optional port number*>
port 引数を指定すると、リレー サーバ上で Telnet ポート 23（デフォルト）以外のポートを選択できます。このオプションは、お客様のサイトのファイアウォールが Telnet ポートをブロックした場合に使用する必要があります。たとえば、サーバによってはファイアウォールを通過する HTTP 伝送だけを許可していることがあります。この場合は、-port 80 を使用します。

`-verbose`
verbose オプションは、接続の問題が起こることが予想される場合に使用します。このパラメータを指定すると、デバッグ メッセージとプログラム トレースの詳細がログ ファイルとコンソール ウィンドウに記録されます。

`-target` <*optional host name of Cisco CallManager system*>
このパラメータは、**tndconnect** が Cisco CallManager サーバ以外のシステム（たとえば、ユーザ サイトの Telnet サーバ）にある場合に限り使用します。

この場合は、Cisco CallManager システムのホスト名を指定する必要があります。この引数を使用しない場合は、値はデフォルトの localhost になります。

`-noecho`
リレーされたデータをコンソールに表示しないようにします。

すべてのオプションの表示

システム全体に関する情報を入手するには、コマンドラインに **/?** 引数を指定して **tndconnect** プログラムを呼び出します。

tndconnect /?

このコマンドは、すべてのコマンドライン オプションに関する情報を返します。

Telnet コネクタ プログラムの構造

tndconnect プログラムは、CSE がお客様の Cisco CallManager システムにログインできるように、必要な作業を実行します。

（注）　プログラムを実行するときに Telnet デーモンが実行されていない場合、**tndconnect** はコンソールにエラー メッセージを表示し、コマンドは終了します。

tndconnect プログラムを開始する時に、コマンド パーサはコマンドラインに指定された値を設定します。コマンドラインに明示的なパラメータが設定されていない場合、プログラムはデフォルト値を使用します（**-host** パラメータと **-password** パラメータを除く）。これらの値は、**tndconnect** を開始するたびに入力する必要があります。

CSE がリレー アプリケーションに接続すると、TCP/IP 構造を作成してローカル Telnet デーモンに接続するように **tndconnect** プログラムに指示するシグナルが出されます。

-target オプションを使用しない場合、**tndconnect** にはデフォルトでお客様のローカル Telnet サーバが指定されます。

（注）　DNS が Cisco リレー アプリケーション サーバを検出できない場合、ローカル システムの hosts ファイルにそのサーバの名前を追加する必要があります。この場合は、「*IP アドレス*」と「 *ホスト名*」を含む行をファイル C:\WINNT\system32\drivers\etc\hosts に追加して、そのホスト名を指定します。

tndconnect プログラムによって、CSE のログイン先の Cisco リレー サーバに情報が送信されます。CSE は、Cisco CallManager の IP アドレスとパスワードを指定し、リターンを入力して、ログイン画面が表示されるようにします。次に CSE は、お客様から提供されたパスワードを使用して Cisco CallManager システムにログインします。

Cisco Secure Telnet セッションの終了

接続が確立されるとタイマーがスタートし、トラフィックが検出されなくなると、最終的に接続を終了します。**tndconnect** によって確立されたお客様のサイトへのトンネルは、アイドル状態が 30 分間続くと自動的に終了します。ユーザが意図的に接続解除を行った場合は、Telnet コネクタ プログラムを使用するたびに手動で再起動する必要があります。

ソケットに障害が発生した場合もセッションは終了し、シスコまたはお客様のサイトからの接続もクローズされます。CSE が接続解除を行うか、リレー プログラムが終了するか、または Telnet デーモンが終了すると、クローズが発生します。TCP に接続障害が検出された場合、どちらかの Telnet セッションがクローズされた場合、または *Ctrl* キーを押した状態で C キーを押して **tndconnect** プログラムを終了した場合にも、接続は終了します。

接続が終了するとプログラムは終了し、Cisco CallManager の Telnet サーバとリレー サーバの間に作成されたトンネルは切断されます。

Telnet デーモンとの接続

Cisco Secure Telnet システムのもとでは、Telnet クライアントとデーモンは更新されることのない標準のコンポーネントであり、直接接続されている場合と同じようにデータを交換します。

Cisco CallManager を実行するシステムは、標準の Windows 2000 Telnet デーモン サービスを実行する必要があります。CSE 側のクライアントがこのプログラムに接続する必要があるため、Telnet デーモンに接続する目的、および企業ネットワークから Telnet リレー プログラムへの接続を確立する目的で、**tndconnect** の追加ソフトウェア コンポーネントが必要になります。Telnet デーモンと **tndconnect** は協調して動作し、Telnet セッションのトラフィックの通路になるエンドツーエンドの接続を提供します。

Telnet サーバ コンポーネントは、Cisco CallManager Windows 2000 システム上でバックグラウンドのサービスとして動作します。デーモンの主な機能は、接続要求に応答することです。Telnet セッションが確立された後では、コマンドライン プログラムを実行できます。

Telnet デーモン ソフトウェアを選択する際には、ここで説明した項目を考慮してください。

Windows NT Telnet デーモンの計画

Telnet デーモンおよび FTP サーバは、Windows 2000 の標準機能です。したがって、リモートから保守を行う場合は、この接続方式を使用します。

Cisco Secure Telnet の使用方法のシナリオ

お客様のシステム管理者は、Cisco CallManager サーバの問題でリモート診断が必要と判断したときは、Cisco Secure Telnet をアクティブにして、CSE に問題の診断を求めることができます。通常の要請手順を次に示します。

ステップ 1　Windows 2000 Telnet デーモンの設定では、UNIX ホストからの Telnet アクセスを許可しておきます。Windows 2000 のコマンド **tndadmn** を使用すると、Telnet デーモンの操作特性を設定できます。

（注）　ローカル Telnet セッションが正常に機能することを確認しておきます。また、シスコ TAC のログイン用ユーザ ID とパスワードが適切であるかどうかも確認しておきます。

ステップ 2　お客様のシステム管理者には、コミュニケーションを開始するときに使用するワンタイム パスワードと Cisco リレー サーバの DNS 名がシスコの CSE から提供されます。

ステップ 3　Telnet デーモンがまだ実行されていない場合は、Windows 2000 システムのコントロール パネルの Services オプションを使用して、デーモンを開始します。

ステップ 4　次に **tndconnect** を実行して、Telnet デーモンと Cisco リレー サーバとの間でトンネル セッションを開始します。コマンドライン構文を使用して、ワンタイム パスワードを送信します。このパスワードは、リレー サーバへの接続時に CSE から提供されたパスワードと相互に関連しています。

（注）　トンネルにより、ネットワーク間のデータ ストリームはセキュアに伝送され、ルーティングは透過的に行われます。トンネルを作成するには、宛先ネットワークを保護するファイアウォールを介して通信を行うソフトウェアを使用します。

ステップ 5　ビットを操作して伝送用のワンタイム パスワードを暗号化した後、**tndconnect** はパスワードの識別のために **relayapp** に送信します。

伝送が完了すると、お客様のシステムは Cisco TAC 診断用にセットアップされます（**tndconnect** ウィンドウでサポート エンジニアのコマンドと応答を確認することができます)。

シスコ TAC エンジニアが接続を解除すると、**tndconnect** プログラムは終了します。