SSH.COM

Tectia® Client/Server 6.6 (Windows)

クイック・スタート・ガイド

2024年12月04日

Tectia® Client/Server 6.6 (Windows): クイック・スタート・ガイド

2024年12月04日

SSH Communications Security Corporation
Karvaamokuja 2D, FI-00380 Helsinki, Finland

目次

第1章 本マニュアルについて

本マニュアルでは、Tectia Client 及び Server を使い始めるための簡単な手順について説明します。さまざまなプラットフォーム・アーキテクチャ用にクライアント/サーバ製品が用意されています。

- AIX、HP-UX、Linux、Solaris、及び Windows プラットフォーム用の Tectia Client/Server
- IBM メインフレーム用の Tectia Server for IBM z/OS 及び Tectia Server for Linux on IBM System z

本ガイドの手順は、Tectia Client を使用して Tectia Server に接続し、その両方が Windows オペレーティング・システム上で動作しているシステムを対象としています。

本クイック・スタート・ガイドの目的は、製品を評価できるように、Tectia client/server ソリューションをデフォルトの設定で起動及び実行する手順を示すことです。

本ガイドは、Tectia 製品を評価する必要のあるシステム管理者などの専門家を対象としています。本マニュアルで説明する情報を利用するためには、システム管理者レベルの知識を有し、Tectia Client 及び Server の用途を理解している必要があります。

Tectia の製品群には、Tectia Client が提供する基本的な Secure Shell クライアント・サービスに加え、より高度なファイル転送やアプリケーション接続サービスを提供できる Tectia ConnectSecure も含まれています。本ガイドの説明は、エントリーレベルの製品である Tectia Client に焦点を合わせて記述されています。

1.1. 参考文書

Tectia client/server ソリューションの説明と、ユーザ向けの詳細な説明は、以下の製品固有のマニュアルに記載されています。

- 『Tectia Client/Server Product Description』。製品、そのアーキテクチャ、主な機能、及び製品の構成に関する一般的な情報が記載されています。
- 『Tectia Client ユーザ・マニュアル』。Tectia Client のインストール、設定、及び使用に関する詳細な手順が記載されています。

- 『Tectia Server Administrator Manual』。Tectia Server のインストール、設定、及び使用に関する詳細な手順が記載されています。

Unix で Tectia Client 及び Server を評価する手順は、別のクイック・ガイド『Tectia Client/Server (Unix) Quick Start Guide』に記載されています。

1.2. 関連用語

以下の用語が本マニュアル中で使用されます。

クライアント・コンピュータ
: Secure Shell 接続を開始するコンピュータ。

接続ブローカー
: 接続ブローカー は Tectia Client、Tectia ConnectSecure、及び Tectia Server for IBM z/OS クライアント・ツールに含まれているコンポーネントです。接続ブローカー はすべての暗号化動作及び認証関連のタスクを処理します。

FTP-SFTP変換
: Tectia ConnectSecure はクライアント上の FTP 接続を自動的にキャプチャして SFTP に変換し、Tectia Server、Tectia Server for IBM z/OS、または別のベンダの Secure Shell サーバ・ソフトウェアが動作する SFTP サーバに接続をダイレクトすることができます。

ホスト鍵ペア
: Secure Shell サーバを識別するための公開鍵ペア。秘密鍵ファイルにアクセスできるのはサーバのみです。公開鍵ファイルは、サーバに接続するユーザに配布されます。

リモート・ホスト
: 接続の対向側。見る側の視点によってクライアント・コンピュータまたはサーバ・コンピュータのいずれかを指します。

Secure Shell クライアント
: Secure Shell プロトコル・バージョン 2 を使用するクライアント側アプリケーション (Tectia Client の **sshg3**、**sftpg3**、**scpg3** など)。

Secure Shell サーバ
: Secure Shell プロトコル・バージョン 2 を使用するサーバ側アプリケーション。

サーバ・コンピュータ
: Secure Shell サービスが稼動し、Secure Shell クライアントが接続するコンピュータ。

SFTP サーバ
: Secure Shell サーバのサブシステムとして、セキュアなファイル転送サービスを提供するサーバ側アプリケーション。

Tectia Client
: ワークステーションにインストールされるソフトウェア・コンポーネント。Tectia Client は、セキュアな対話的ファイル転送とターミナル・クライアント機能を、Tectia Server またはその他の Secure Shell プロトコルを使用したアプリケーションが稼動して

いるサーバへのアクセスをリモート・ユーザやサーバの管理を行うシステム管理者に提供します。また、(非透過的) 静的トンネリングもサポートします。

Tectia client/server ソリューション
: Tectia client/server ソリューションはTectia Client、Tectia ConnectSecure、Tectia Server、及びTectia Server for IBM z/OS (Tectia Server for IBM z/OS クライアント・ツールを含む) で構成されています。

Tectia コネクション設定　GUI
: Tectia Client 及び ConnectSecure には、リモート・サーバへの接続設定を行うためのグラフィカル・ユーザ・インターフェイス (GUI) があります。この GUI は Windows と Linux に対応しています。

Tectia ConnectSecure
: サーバ・ホストにインストールされるソフトウェア・コンポーネント。ただしこれは、Secure Shell クライアントとして機能します。Tectia ConnectSecure は FTP の置き換え用に設計されており、FTP-SFTP変換、透過的FTPトンネリング、透過的TCPトンネリング、及び高速ファイル転送サービスを提供します。Tectia ConnectSecure は標準の Secure Shell サーバに接続することができます。

Tectia セキュア・ファイル転送 GUI
: Windows 上の Tectia Client 及び ConnectSecure には、ファイル転送を対話的に処理及び実行するための専用のグラフィカル・ユーザ・インターフェイス (GUI) があります。

Tectia SFTP API
: Tectia ConnectSecure には、C 及び Java 用の専用のアプリケーション・プログラミング・インターフェイス (API) があります。開発者はこれらの API を使用して、セキュアなファイル転送アプリケーションを開発したり、Tectia 製品を他のシステムに統合したりできます。

Tectia Server
: Tectia Server は Secure Shell クライアントの接続先であるサーバ側コンポーネントです。Linux、Unix、及び Windows プラットフォーム用の Tectia Server、Tectia Server for Linux on IBM System z、及び Tectia Server for IBM z/OS という 3 つのバージョンの Tectia Server 製品を利用できます。

Tectia Server for IBM z/OS
: Tectia Server for IBM z/OS は一般的な Secure Shell 接続を提供し、IBM メインフレーム上の高機能ファイル転送 (EFT) 機能と透過的TCPトンネリングをサポートします。

Tectia Server for Linux on IBM System z
: Tectia Server for Linux on IBM System z は、IBM System z プラットフォームで動作する Linux 上で Secure Shell 接続を提供します。

Tectia Server 設定ツール
: Tectia Server には、設定ファイルを編集する代わりに、サーバの設定に使用できるグラフィカル・ユーザ・インターフェイスがあります。この GUI は Windows に対応しています。

透過的FTPトンネリング
: Secure Shell トンネルによって透過的に暗号化され、セキュアになっている FTP 接続。

透過的TCPトンネリング
: Secure Shell トンネルによって透過的に暗号化され、セキュアになっている TCP アプリケーション接続。

トンネルされたアプリケーション
: Secure Shell 接続によってセキュアになっている TCP アプリケーション。

ユーザ鍵ペア
: Secure Shell ユーザを識別するための公開鍵ペア。秘密鍵ファイルにアクセスできるのはユーザのみです。公開鍵ファイルは、ユーザが接続するサーバにコピーされます。

1.3. 本マニュアル中で使用される規則

Tectia のマニュアルでは、以下の表記規則が使用されています。

表1.1 マニュアルの規則表

規則	用途	例
太字	ツール、メニュー、GUI エレメント及びコマンド、コマンドライン・ツール、強調	**[適用]** または **[OK]** をクリックします。
→	連続するメニューの選択	**[ファイル]** → **[保存]** の順に選択します。
#	コマンドの前に付いた # は、そのコマンドが特権ユーザ (root) として実行されることを示します。	`# rpm --install package.rpm`
$	コマンドの前に付いた $ は、そのコマンドが特権のないユーザとして実行されることを示します。	`$ sshg3 user@host`
\	コマンド行の末尾にある \ は、その行を 1 行では表示できないため、次の行に続くことを示します。	`$ ssh-keygen-g3 -t rsa \` `  -F -c mykey`

注意

「注意」は、本文中の重要なポイントを強調または補足するための一般的な、または役に立つ情報を示します。またメモリの制限、装置の設定、またはプログラムの特定のバージョンなど、特殊な場合にのみ適用される情報を示します。

警告

「警告」はユーザに対して、特定の操作を行う、または避けることができなかった場合にデータが消失する可能性があることを示します。

1.3.1. オペレーティング・システムの名称

情報がオペレーティング・システムの複数のバージョンに適用される場合は、次の命名規則を使用します。

- 「**Unix**」は、サポートされる以下のオペレーティング・システムを指しています。
  - HP-UX
  - IBM AIX
  - Red Hat Linux、SUSE Linux
  - Linux on IBM System z
  - Solaris
  - IBM z/OS (Tectia Server for IBM z/OS が USS で動作中であり、Unix タイプのツールを使用している場合に該当。)
- 情報が IBM z/OS バージョンに直接関係する場合は、IBM z/OS に対して「**z/OS**」が使用されます。
- 「**Windows**」は、サポートされるすべての Windows バージョンを指しています。

1.4. カスタマー・サポート

Tectia の製品マニュアルはすべて、 https://www.ssh.com/manuals/ で入手できます。

Tectia の全製品の使用方法をまとめた FAQ は http://answers.ssh.com/ でご覧いただけます。

メンテナンス契約をご購入された場合、SSH Communications Security からテクニカル・サポートを受けることができます。契約書で具体的な条件をご確認のうえ、https://support.ssh.com/ にログインしてください。

サポート・リクエスト、機能リクエスト、またはバグ・レポートの送信、及びオンライン・リソースへのアクセスに関する情報は、 https://support.ssh.com/ でご確認いただけます。

第2章 インストール

本章では、Windows オペレーティング・システムに Tectia client/server ソリューション をインストールする手順について説明します。

Tectia　製品は他のプラットフォームでも動作します。サポートされているオペレーティング・システムの一覧と、それらに　Tectia　をインストールする手順については、『Tectia Client ユーザ・マニュアル』及び『Tectia Server Administrator Manual』を参照してください。

2.1. インストールの準備

Tectia Client 及び Server のインストールを開始する前に、以下の準備と確認を行ってください。

2.1.1. ハードウェア及びディスクの空き容量の要件

Tectia　製品には、ハードウェアに関する特別な要件はありません。サポートされているオペレーティング・システムのバージョンが動作し、ネットワーク接続機能を備えたコンピュータであればどれでもインストールできます。

Tectia Client のインストールには、約 100 MB のディスク空き容量が必要です。Tectia Client では、個々のユーザの設定は、そのユーザの個人ディレクトリに保存されます。

Tectia Server のインストールには、100 MB のディスク空き容量が必要です。

インストールの概要については、『Tectia Client ユーザ・マニュアル』及び『Tectia Server Administrator Manual』を参照してください。

前提条件

Tectia Server 製品をインストールする前に、TCP ポート 22 への着信がファイアウォールでオープンされていることを確認してください。

2.1.2. すでにインストール済みの Tectia ソフトウェアのアップグレード

Tectia Client 及び Tectia Server を同じマシンにインストールした場合は、常に同じバージョンにアップグレードする必要があります。これは共通コンポーネント間に依存関係があるためです。

Tectia の新しいバージョンをインストールする予定のマシン上で Secure Shell ソフトウェア (以前のバージョンの Tectia 製品やサードパーティ製の Secure Shell サーバまたはクライアントなど) が動作しているかどうか確認します。

Tectia Client 及び Server 6.6 にアップグレードする前にアンインストールする必要のある Tectia のバージョンを以下の表に示します。「上書きアップグレード」と記載されたバージョンは、インストール手順中に自動的にホストから削除されます。

以下の場合は、バージョン 6.6.5 をインストールする前に、既存バージョンの Tectia Client/Server をアンインストールする必要があります。

- 既存バージョンが 6.0 またはそれ以前の場合。
- 既存バージョンの Tectia Client には透過的トンネリング・コンポーネントが含まれている場合。

上記以外の場合は、最初に既存バージョンをアンインストールすることなく Tectia Client/Server 6.6.5 にアップグレードできます。既存バージョンは、インストール手順中に自動的にホストから削除されます。

設定ファイルのアクセス権

すでにインストールされている Tectia Server のバージョンをアップグレードする場合、アップグレード・インストール中に既存の設定ファイルのアクセス権が確認されます。

設定ファイル `ssh-server-config.xml` のアクセス権は、以下のようにする必要があります。

- ファイル所有者は管理者グループのメンバーである。
- 管理者と SYSTEM だけがファイルを完全に制御できる。
- ユーザはファイルを変更できない。
- 他のアカウントはこのファイルにアクセスできない。

アクセス権が安全でない場合、アップグレード・インストール中に **[Configuration File Permissions]** ダイアログボックスが表示されます。以下のいずれかの方法で対処してください。

- 設定ファイルの権限をデフォルトの安全な状態にリセットし (**[Reset]** を選択し)、インストールを続行します。(推奨)
- 不適切な権限は無視し (**[Ignore]** を選択し)、権限を修正せずにインストールを続行します。このように判断した場合、サーバが起動できなくなる可能性があります。権限は後から手動で修正できます。

- インストールをキャンセルします ([**Cancel**] を選択します)。

注意

以前にインストールされていた Tectia Server はすでに削除されているため、インストールをキャンセルすると、Tectia Server のどのバージョンもマシンにインストールされていない状態になります。

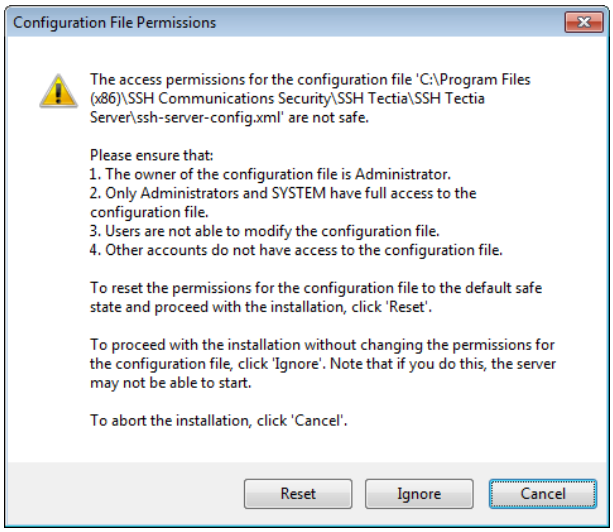

図2.1 安全ではない設定ファイルの権限

2.1.3. ライセンス・ファイル

Tectia Client and Server が機能するためには、ライセンスが必要です。 Tectia Client のライセンス・ファイル名は `stc66.dat`、Tectia Server のライセンス・ファイル名は `sts66.dat` です。

ライセンスに関する以下の点を考慮してください。

- 解凍したパッケージからインストールするときに、インストール・ウィザードによって適切なディレクトリにライセンス・ファイルが自動的にコピーされます。

  インストール後、ライセンス・ファイルは以下のデフォルトのインストール・ディレクトリにあります。

  - "`C:\Program Files (x86)\SSH Communications Security\SSH Tectia\SSH Tectia AUX\licenses`" (64 ビット Windows バージョンの場合)

- オンライン・インストール・パッケージでは、ライセンス・ファイルは、リリース・ノート (`.txt`) ファイルや PDF 形式のマニュアルとともに圧縮ファイル (`.zip`) に含まれています。

- Tectia の評価版パッケージにライセンス・ファイルは含まれていません。評価版は、ライセンス・ファイルなしで 45 日間使用できます。 ユーザにライセンスの期限切れまでの日数を示すバナー・メッセージが表示されます。

- 評価版または標準商用バージョンから Tectia Quantum Safe Edition へのアップグレードは、ライセンスファイルをライセンス・ディレクトリにコピーし、 Tectia Client and Server ソフトウェアを再起動するだけです。

2.1.4. オペレーティング・システムのユーザ・アカウントの作成

Tectia Server 自体にユーザ管理プログラムはありません。ユーザ・アカウントは標準的なオペレーティング・システムのツールで作成します。

Windows でのユーザ・ログインには、ローカルにログオンする権限と、ネットワークからリモート・コンピュータにアクセスする権限が必要です。ドメイン・コントローラでは、これらの権限はデフォルトで無効になっています。Tectia Server がドメイン・コントローラにインストールされている場合、ローカルにログオンする権限と、ネットワークからコンピュータにアクセスする権限をドメイン・コントローラ上で Domain Users グループに対して有効にする必要があります。

2.2. Tectia ソフトウェアのインストール

本項では、Windows に Tectia Client 及び Server をインストールする方法について説明します。

2.2.1. インストールの完了

インストールに成功すると、Tectia Client 及び Tectia Server は再起動時に自動的に起動し、手動で停止するか、またはホストをシャットダウンするまでバックグラウンドで動作し続けます。

Tectia Client 及び Tectia Server の機能は、デフォルトの設定で試すことができます。初めてセキュアな接続を開く方法については、第3章 を参照してください。

また、Tectia client/server ソリューション の動作をニーズに合わせてカスタマイズすることもできます。目的に応じた Tectia 設定の変更については、本マニュアルの後続の章を参照してください。

- 第4章 では、認証方法の設定について説明します。
- 第5章 では、セキュアなファイル転送について説明します。
- 第6章 では、アプリケーション接続をセキュアにする方法について説明します。

2.3. Tectia ソフトウェアの削除

Tectia Client 及び Server ソフトウェアを削除する必要がある場合は、以下の手順に従ってください。

注意

このアンインストール手順では、ソフトウェアのインストール時に作成されたファイルだけが削除されます。設定ファイルは、各ユーザの `%APPDATA%\SSH` ディレクトリと、以下のインストール・ディレクトリから手動で削除する必要があります。

- "`C:\Program Files (x86)\SSH Communications Security\SSH Tectia\SSH Tectia Server`" (64 ビット Windows バージョンの場合)

2.3.1. Windows からの Tectia Client 及び Server の削除

Windows 環境から Tectia Client 及び Server を削除するには、以下の手順に従ってください。

1. Windows の [**スタート**] メニューから [**コントロール パネル**] を開き、[**プログラムと機能**] をクリックします。
2. インストール済みのプログラム一覧から [**Tectia Server**] または [**Tectia Client**] を選択し、[**アンインストール**] をクリックします。

   ### 注意

   Tectia Server と一緒に Tectia Client がインストールされている場合、Tectia Server をアンインストールすると Tectia Client も削除されます。
3. [**はい**] をクリックして確認します。
4. Tectia Server のアンインストールが完了すると、システムによって Windows の再起動が求められます。

第3章 リモート・サーバへの接続

本項では、デフォルト設定でパスワード認証を使って Tectia Client から Tectia Server にログインする方法について説明します。Tectia Client 及び Server のデフォルト設定では、パスワード、公開鍵、GSSAPI、及びキーボード・インタラクティブでログインできます。デフォルトでは、ユーザ認証にはパスワードが使用され、サーバ認証には公開鍵が使用されます。

接続先のリモート・サーバにユーザ・アカウントがあり、そのサーバ上で Secure Shell サーバが稼動している必要があります。ここから説明する例では、サーバのアドレスがわかっていることと、Tectia Server が稼動していることが確実な、ローカル・マシン内で接続するだけでも構いません。

3.1. パスワードによる最初の接続

Windows では、Tectia SSHターミナル GUI を次のように使用して、リモート・ホストに接続することができます。

1. デスクトップ上の Tectia SSH ターミナルのアイコンをクリックして開きます。

図3.1 Tectia SSH ターミナルのアイコン

2. 以下のいずれかの手順を実行して、Secure Shell 接続を開きます。

   - ツールバー上の **[接続]** アイコン をクリックします。
   - **[ファイル]** メニューで **[接続]** をクリックします。
   - まだ接続していない状態でターミナル・ウィンドウがアクティブになっているときに、キーボードの **Enter** キーまたは **Space** キーを押します。

3. これにより **[サーバへ接続]** ダイアログボックスが開き、そこで接続するホストを定義できます。

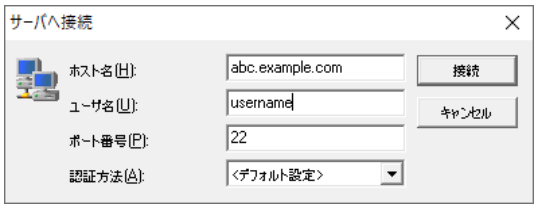

図3.2 [サーバへ接続] ダイアログボックス

以下の情報を定義して、**[接続]** をクリックします。

- **[ホスト名]** – FQDN、短いホスト名、またはリモート・ホストの IP アドレス。(同じマシンにインストールされている Tectia Server への接続をテストするには、「`localhost`」と入力します。)
- **[ユーザ名]** – リモート・ホストでのユーザ名
- **[ポート番号]** – 22 がデフォルトの Secure Shell リスナー・ポートです。
- **[認証方法]** – パスワードで認証するには、**<デフォルト設定>**を使用します。

同じ非接続時ターミナル・ウィンドウ内からのこれ以降のセッションでは、前の接続で使用された値があらかじめ入力されています。

4. サーバの認証が始まります。リモート・サーバ・ホストがローカル・コンピュータにホスト公開鍵を提供します。ホスト鍵によってサーバ・ホストが識別されます。

   Tectia Client により、この鍵についての情報がすでにユーザのホスト鍵ディレクトリに保存されているかどうか確認されます。保存されていない場合は、次に、コンピュータ上のすべてのユーザに共有のホスト鍵ディレクトリが確認されます。このホスト鍵についての情報が見つからない場合は、新しい鍵を検証するよう要求されます。

   サーバの認証に公開鍵認証が使用される場合、最初の接続が非常に重要です。 Tectia Client が新しいサーバ・ホスト鍵を受信すると、ホスト識別メッセージが表示されます。

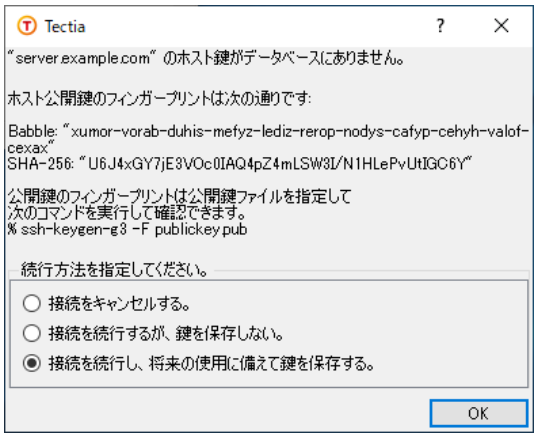

図3.3 ホスト識別ダイアログ – リモート・ホストへの最初の接続

メッセージは、ホストの公開鍵のフィンガープリントが SSH Babble 形式で表示されます。この形式は、ダッシュで区切られた英小文字 5 文字からなる読み上げ可能な一連の単語で構成されています。

5. フィンガープリントの有効性を確認してください。可能であればリモート・ホスト・コンピュータの管理者に電話で問い合わせてください。フィンガープリントを検証したら、将来使用するためにホスト鍵に関する情報を保存しておくと安全です。また、接続をキャンセルすることも、ホスト公開鍵の情報を保存せずにこの接続を続行することもできます。

   警告

   ホスト公開鍵の信頼性を検証せずに保存することは絶対に避けてください。

6. **[OK]** をクリックしてホスト識別ダイアログを閉じます。

   サーバ公開鍵の情報は、クライアントが後でこの鍵を検証できるように、クライアント側のマシンに保存されます。 Tectia Client では、公開鍵情報は「`%APPDATA%\SSH\HostKeys`」ディレクトリに保存されます。

   `%APPDATA%` は以下のディレクトリに相当します。

   - "`C:\Users\<username>\AppData\Roaming`"

   最初の接続の後は、ローカルに保存されたサーバ公開鍵に関する情報のみがサーバ認証に使用されます。

7. ユーザの認証が始まります。パスワードを使って、 サーバへの認証を受けるよう要求されます。必要な認証方法はサーバ設定によって異なります。

   サーバによって認証されると、サーバへの Secure Shell 接続が確立されます。

3.2. 接続プロファイルの作成

Windows 上の Tectia Client では、接続する各 Secure Shell サーバに対して別々の接続設定を行えます。また、同じサーバに対して、たとえば異なるユーザ・アカウントで複数のプロファイルを作成することもできます。

以下のビューで接続プロファイルを追加できます。

- **Tectia SSHターミナル GUI** を起動し、**[プロファイル]** ボタンをクリックします。下図に示すように、ドロップダウン・メニューから **[プロファイルの追加]** を選択します。

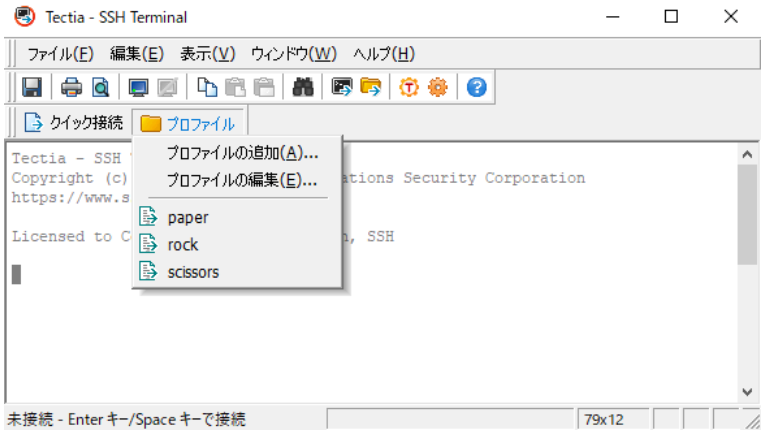

図3.4 接続プロファイルの追加

- Tectia SSHターミナル GUI を起動し、ツールバーの Tectia アイコン をクリックして **Tectia コネクション設定　GUI** を開きます。

  (Windows タスクバーの通知領域にある Tectia アイコン を右クリックし、ショートカット・メニューから **[設定]** を選択しても、Tectia コネクション設定　GUI を開くことができます。)

  Tectia コネクション設定　GUI で **[接続プロファイル]** ページに移動し (下図を参照)、**[プロファイルを追加]** をクリックします。

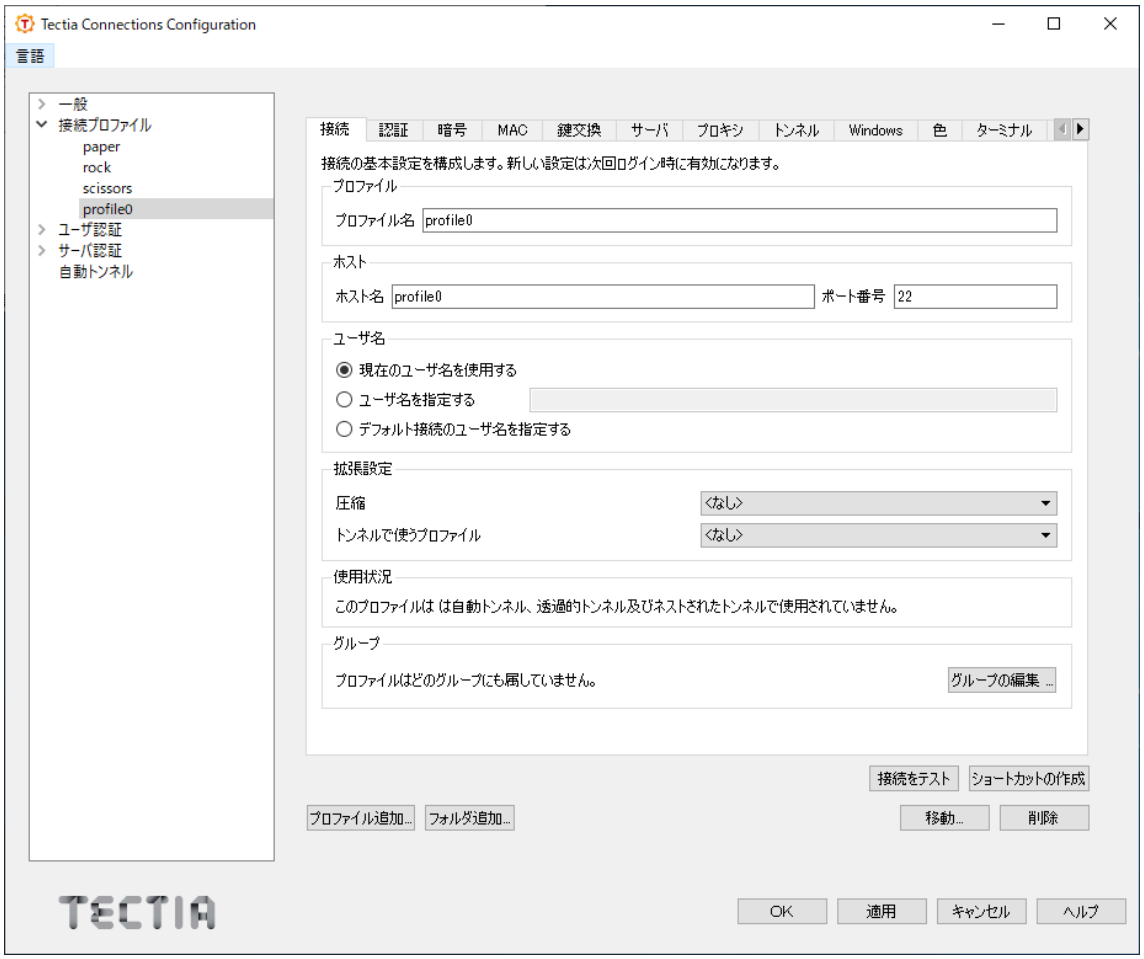

図3.5 接続プロファイルの追加

新しく作成された接続プロファイルは、**[一般]** → **[デフォルト接続]** ページで定義された認証、暗号、MAC、鍵交換、トンネリング、及び詳細なサーバ設定のデフォルト値を継承します。これらの値は、プロファイル固有のタブを使ったページでカスタマイズできます。図 3.6 を参照してください。

接続プロファイルの名前を変更するには、**[接続プロファイル]** リストでプロファイル名を右クリックし、**[名前の変更]** をクリックします。新しい名前を入力します。

接続プロファイルを削除するには、プロファイルを選択し、**[削除]** をクリックします。確認を求められます。**[はい]** をクリックして削除を実行します。

3.2.1. 接続プロファイル設定の定義

[接続プロファイル] ページの **[接続]** タブでは、接続で使用するプロトコル設定を定義できます。変更された接続設定は次回のログイン時に有効になります。

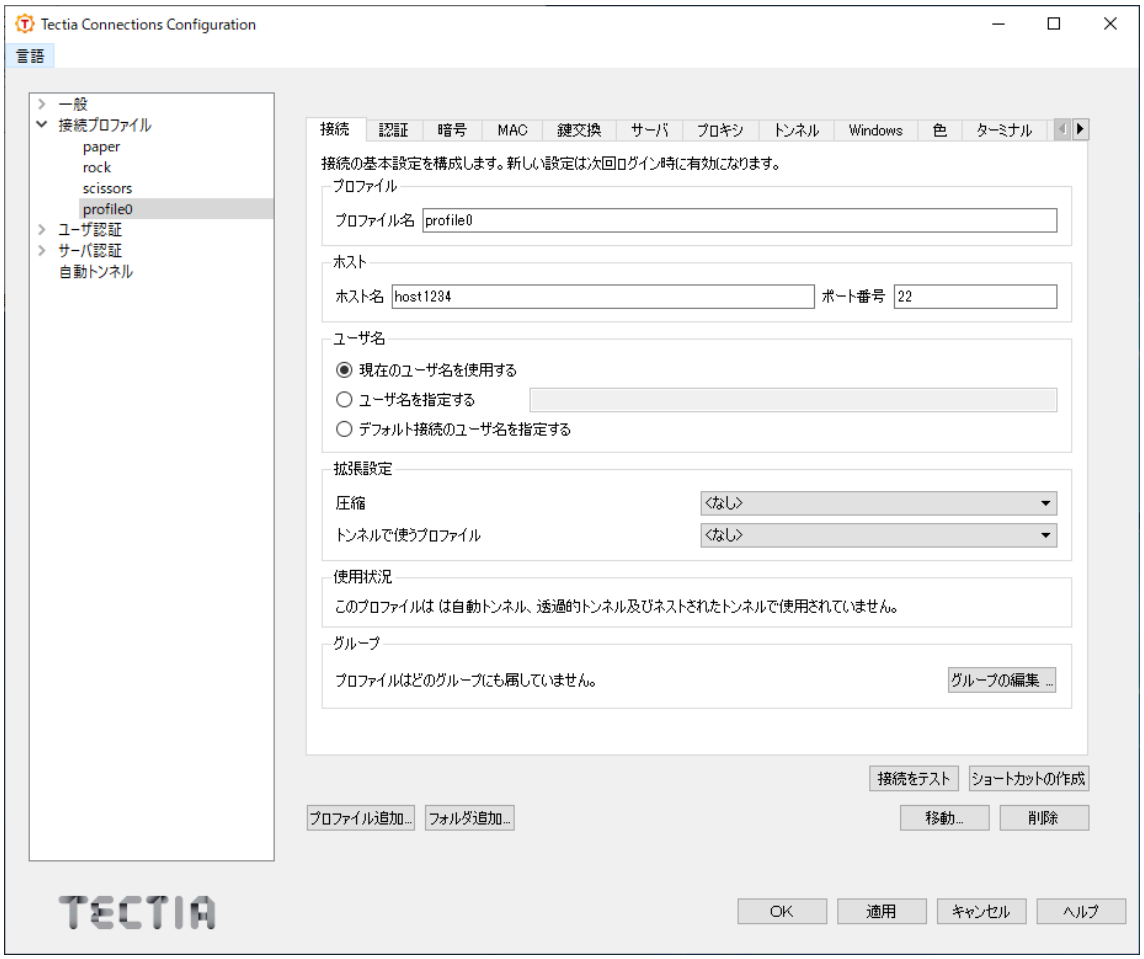

図3.6 接続プロファイルの設定

[プロファイル]

[プロファイル名] にプロファイルの名前を入力します。

[ホスト]

[ホスト名] には、このプロファイルで接続するリモート・ホスト・コンピュータの名前を入力します。

[ポート番号] には、Secure Shell 接続に使用するポート番号を入力します。デフォルトのポートは 22 です。

注意

Secure Shell サーバ・プログラムは、リモート・ホスト・コンピュータ上の指定されたポートをリッスンしている必要があり、そうでない場合は接続試行に失敗します。リモート・ホスト・コンピュータがリッスンしているポートが不明な場合は、リモート・ホストのシステム管理者に問い合わせてください。

[ユーザ名]

現在ログインしている Windows ユーザ名を使用して常に接続を確立する場合は、**[現在のユーザ名を使用する]** を選択します。この設定は、ユーザ名として %USERNAME% (パーセント記号に注意) を定義するのと同じような働きをします。

リモート・ホスト・コンピュータへの接続時に使用するユーザ名を定義する場合は、**[ユーザ名を指定する]** を選択してユーザ名を入力します。ユーザ名に %USERNAME% (パーセント記号に注意) を指定すると、接続時に現在の Windows ユーザ・アカウントの名前に置き換えられます。

[拡張設定]

現在は不要: **[圧縮]** では、使用する圧縮設定をドロップダウン・メニューから選択します。**[zlib]** または **[なし]** を選択できます。圧縮はデフォルトでは無効です。

現在は不要: **[トンネルで使うプロファイル]** では、使用する接続プロファイルをドロップダウン・メニューから選択します。ネストされたトンネルはすべて、プロファイルを使って作成されます。トンネリング機能については、『Tectia Client User Manual 』を参照してください。

第4章 認証方法の設定

Tectia client/server ソリューションには、サーバとユーザを認証するための別々の認証手順があります。認証は相互に行われます。つまり、クライアントはサーバを認証し、サーバはユーザを認証します。

サーバの設定では、どの認証方法を許可するかを定義し、クライアントの設定では、認証方法を試行する順序を定義します。

このガイドでは、リモート Tectia Server ホストの認証に公開鍵認証がどのように使用されるのかについて紹介します。ユーザ認証については、デフォルトで設定されているパスワード認証方法と、より強固なセキュリティを実現し、非対話型ログインをセキュアに利用できる公開鍵の両方について説明します。

4.1. サーバ認証方法

サーバは、RSA、DSA、ECDSA、または Ed25519 の公開鍵アルゴリズムに基づくデジタル署名で認証されます。

サーバのインストールプロセス中に、RSA 鍵ペア (ファイル名は `hostkey` 及び `hostkey.pub`) が 1 つ生成され、サーバ・ホストの以下のディレクトリに保存されます。

- "`C:\Program Files (x86)\SSH Communications Security\SSH Tectia\SSH Tectia Server`" (64 ビット Windows バージョンの場合)

デフォルトでは、この鍵ペアがサーバ認証に使用されます。

リモート・サーバに初めて接続する方法については、第3章 を参照してください。

4.2. パスワードによるユーザ認証

Tectia Client 及び Server ではどちらも、パスワードと公開鍵の認証方法はデフォルトで設定されています。パスワードはサーバ側で設定する必要がないため、最も簡単にユーザを認証できる方法です。また、すべての通信が暗号化されているため、パスワードは盗聴者から守られています。

Windows のパスワード認証では、ログイン時に使った Windows のパスワードによりユーザを認証します。

ローカル・アカウントとドメイン・アカウントでのユーザ名の扱いの違いについては、『Tectia Server Administrator Manual』の「User Authentication with Passwords」を参照してください。

4.3. 公開鍵によるユーザ認証

公開鍵認証はデジタル署名の使用に基づいており、非常に優れた認証セキュリティを提供します。

公開鍵をユーザ認証に使用するためには、まずクライアント側で鍵ペアを作成する必要があります。作成された鍵ファイルの 1 つは公開鍵であり、もう 1 つはユーザの秘密鍵です。

鍵ペアのセキュリティ・レベルは、鍵の複雑さ (またはビット長) に依存します。鍵は大きいほどよりセキュアになりますが、それとともに生成と使用の時間が長くなります。

注意

デフォルトの RSA鍵長 (3072ビット) は 128ビットのセキュリティを、デフォルトの ECDSA鍵長 (384ビット) は 192ビットのセキュリティを提供します。サードパーティ製品との互換性のためであっても 2048ビット未満の RSA または DSA 鍵の生成は推奨しません。

注意

SSH 鍵については、最低でも 2 年に一度は新しい鍵に交換することをお勧めします。

サーバはユーザの公開鍵を把握している必要があるため、公開鍵はサーバにアップロードする必要がありますが、秘密鍵は他人に知らせないでください。

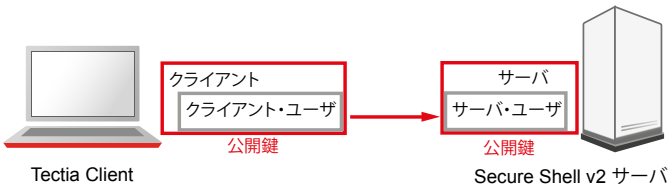

図4.1 公開鍵を使用したユーザ認証

リモート・サーバへのログインを開始すると、クライアントはサーバに署名を送信し、サーバは一致する公開鍵の有無を確認します。鍵がパスフレーズで保護されている場合、クライアントはパスフレーズの入力を要求します。

秘密鍵は自分自身の認証に使用されることを忘れないでください。秘密鍵は安全な場所に保管し、他の誰からもアクセスできないようにしてください。他の誰かがその秘密鍵にアクセスできた場合は、本人になりすましてリモート・ホスト・コンピュータへのログインを試行

することが可能になります。できる限り、秘密鍵を保護するためのパスフレーズを定義してください。

警告

鍵の生成は、他の誰もアクセスできない自分自身のパーソナル・コンピュータだけで行ってください。他のユーザと共有しているコンピュータには秘密鍵を保存しないでください。

公開鍵認証の使用を開始するときには、以下の手順を実行してください。

1. 鍵ペアを生成します。組み込みの **[公開鍵認証ウィザード]**を使用して (4.3.1 を参照) して独自の鍵ファイルを生成できます。

   Tectia コネクション設定　GUIの **[鍵と証明書]** ページで既存の鍵をインポートすることもできます。

2. 公開鍵をリモート・ホスト・コンピュータ (Tectia Server を実行している) に自動的にアップロードします (4.3.2 を参照)。

注意

Tectia Server は、OpenSSH で生成されたユーザ公開鍵にも対応しています。Tectia Server は、Tectia の `authorized_keys` ディレクトリや `authorization` ファイルに加えて、OpenSSH の `authorized_keys` ファイルもチェックするように設定できます。Tectia の場所で定義された公開鍵と同じ鍵が OpenSSH ファイルでも定義されている場合、前者の鍵が優先されます。

この手順では、クライアント・ユーザがパスワード認証を使用して、Tectia Server が実行されているリモート・ホストへのログインを許可されていることを前提としています。

4.3.1. 公開鍵認証ウィザードによる鍵の作成

Windows では、Tectia の **[公開鍵認証ウィザード]** を使用して鍵ペアを生成できます。このウィザードでは、秘密鍵と公開鍵の 2 つの鍵ファイルが生成され、ローカル・コンピュータの `%APPDATA%\SSH\UserKeys` ディレクトリに保存されます。公開鍵ファイルの拡張子は `.pub` で、秘密鍵ファイルの基本のファイル名は公開鍵と同じですが、拡張子はありません。

公開鍵ペアは、コマンドライン・ツール **ssh-keygen-g3** を使用して生成することもできます。手順については、『クライアント・ユーザ・マニュアル』を参照してください。

1. Windows タスクバーの通知領域または Tectia Client ツールバーで Tectia アイコン  をクリックして、**Tectia コネクション設定　GUI** を開きます。

2. **[ユーザ認証]** に進み、**[鍵と証明書]** ページを選択します。**[鍵生成]** をクリックします。

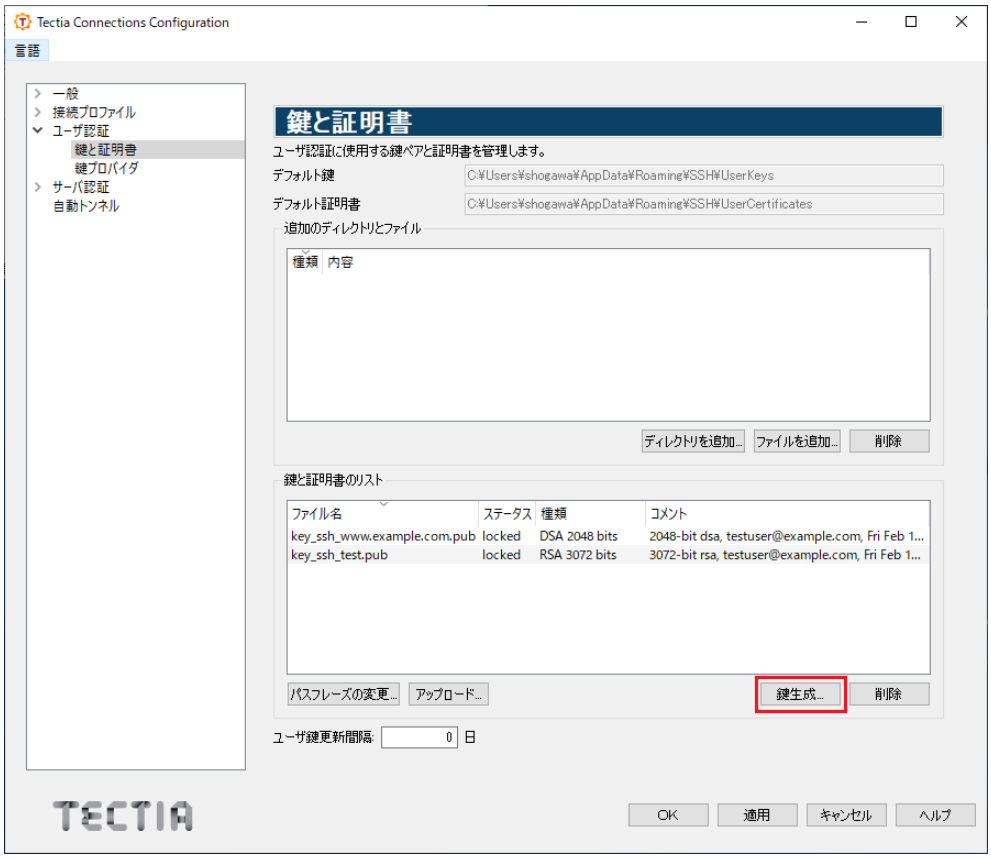

図4.2 Tectia コネクション設定　GUI の [鍵と証明書] ビュー

3. **[公開鍵認証ウィザード]** が起動します。

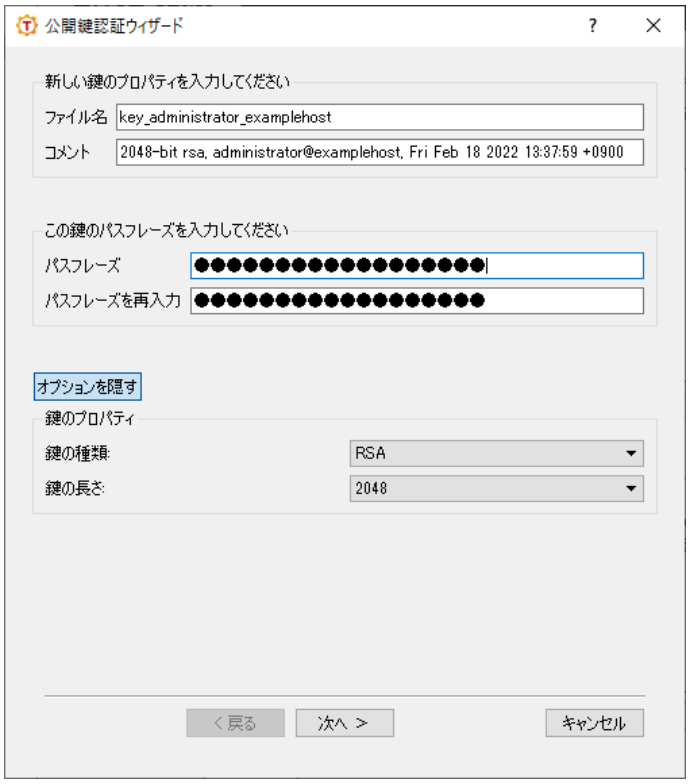

図4.3 [公開鍵認証ウィザード]

4. 鍵ペアを保護するために、鍵のプロパティと必要なパスフレーズを定義します。

   [ファイル名]

   鍵ファイルに付ける一意の名前を入力します。ウィザードでは、ユーザ名とホスト名を組み合わせた名前が提案されます。

   [コメント]

   鍵ペアについて説明する、短いコメントを記入します。たとえば、その鍵が使用される接続について説明します。ウィザードでは、鍵の長さと種類、ユーザ名とホスト名、及び現在の日時を組み合わせたコメントが提案されます。このフィールドは必須ではありませんが、後で鍵を特定するのに役立ちます。

   [パスフレーズ]

   推測するのが難しいフレーズを入力します。理想はアルファベットと数字の両方を使用した 20 文字以上です。句読文字も使用できます。 パスフレーズも秘密鍵もネットワークに送信されることはありませんが、ローカルでアクセスできる場合は辞書攻撃が使用できます。使いやすさのためには、パスフレーズを空白にするのではなく認証エージェントの使用を推奨します。ssh-groker-g3　はデフォルトで認証エージェントとして機能します。

注意

FIPS モードでは、暗号化されていない秘密鍵を FIPS モジュールからエクスポートすることが FIPS 規定において禁じられているため、パスフレーズなしでユーザ鍵を生成することはできません。

自動化されたジョブに鍵ペアを使用する場合は、パスフレーズのフィールドを空にすることで、パスフレーズなしで鍵を生成できます。

鍵を使用して認証するときには、常にパスフレーズの入力が求められます。パスフレーズには、パスワードに似た機能があり、秘密鍵をある程度保護します。

パスフレーズはしっかりと記憶し、書き留めないようにしてください。

[パスフレーズを再入力]

パスフレーズを再入力します。これにより、入力ミスがないことが確認できます。

5. 生成する鍵の種類や長さをデフォルトとは異なるものに定義したい場合は、**[詳細オプション]** をクリックします。デフォルトでは、Tectia Client は 3072 ビットの RSA 鍵のペアを生成します。

   [鍵のプロパティ] 領域では、以下のことを定義できます。

   [鍵の種類]

   生成する鍵の種類を選択します。利用可能なオプションは Ed25519、RSA、ECDSA、及び DSA です。

   

   ### 注意

   FIPS モードでは (FIPS 186-5 に準拠し) RSA、 ECDSA および Ed25519 がサポートされます。DSA は非推奨です。

   [鍵の長さ]

   生成する鍵の長さ (複雑さ) を選択します。以下のオプションから選択できます。

   - DSA/RSA 鍵: 2048、3072、4096、5120、6144、7168、8192 ビット
   - ECDSA 鍵: 256、384、521 ビット
   - Ed25519 鍵: 256 ビット

   同じ種類の鍵でも、大きいほどよりセキュアになりますが、それとともに生成時間が長くなります。256 ビットの ECDSA 鍵と 3072 ビットの RSA 鍵は同等のセキュリティを提供します。

6. **[次へ]** をクリックして、鍵のアップロードに進みます。ウィザードは4.3.2 の手順 3 に続きます。

既存の公開鍵を新しいリモート・サーバにアップロードする方法については、4.3.2 で説明します。

4.3.2. 公開鍵の自動アップロード

公開鍵は、SFTP サブシステムが有効になっているサーバに自動的にアップロードできます。Tectia Server では SFTP がデフォルトで有効になっています。**[公開鍵認証ウィザード]** では、選択したリモート・ホストに新しい公開鍵がそれぞれ自動的にアップロードされます。また既存の鍵はすべて、**Tectia コネクション設定** GUI の **[鍵と証明書]** ページに一覧表示され、いつでも鍵を選択してリモート・サーバにアップロードできます。

公開鍵は、リモート・サーバ上のデフォルトのユーザ・ホーム・ディレクトリ (Windows では `%USERPROFILE%\.ssh2`) にアップロードされます。

注意

鍵ユーザは、サーバ上の鍵ディレクトリへの `write` 権限を持っている必要があり、そうでない場合は自動アップロードに失敗します。リモート・ホスト・コンピュータの管理者がユーザ・アクセスを制限している場合、サーバ設定で公開鍵認証が許可されていても、ユーザ自身が公開鍵認証を設定できないようになっていることがあります。

1. **[公開鍵認証ウィザード]** にアクセスするには、ツリー・ビューで **[ユーザ認証]** → **[鍵と証明書]** の順にクリックします。
2. **[鍵と証明書のリスト]** から鍵を選択し、**[アップロード]** をクリックします。
3. ウィザードの **[公開鍵をアップロード]** ビューが表示されます。

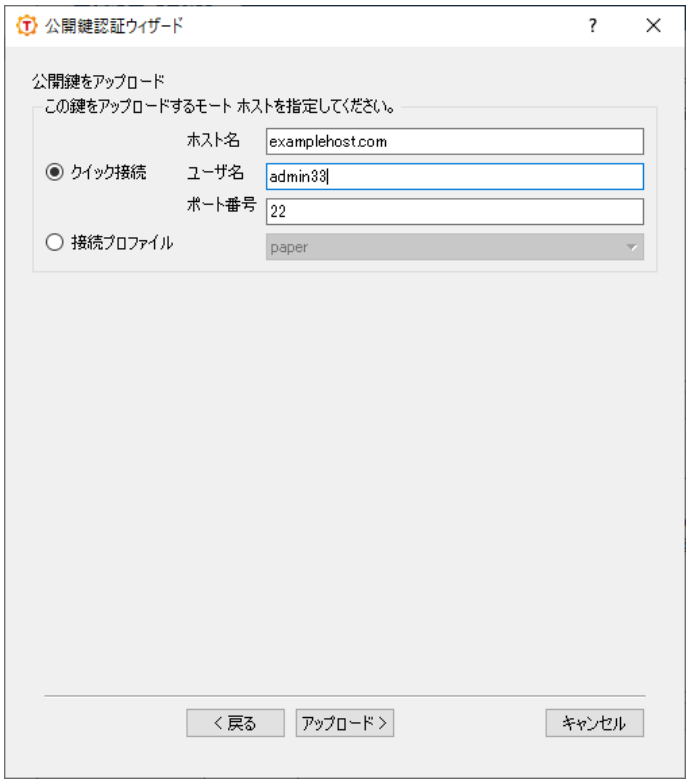

図4.4 鍵のアップロード

鍵をアップロードしたいリモート・ホストを、以下のように定義します。

[クイック接続]

このオプションを選択して、リモートの **[ホスト名]** と、そこで使用する自分の **[ユーザ名]** を定義します。デフォルトの Secure Shell **[ポート番号]** は 22 です。

[接続プロファイル]

目的のリモート・ホストとユーザ名を規定する **[接続プロファイル]** をドロップダウン・リストから選択します。

4. **[アップロード]** をクリックして、選択したサーバに鍵を転送します。すでにリモート・サーバ・ホストに接続されている場合は、鍵のアップロードがすぐに開始されます。接続されていない場合は、サーバ上での認証が求められます (デフォルトではパスワードが必要です)。

4.4. 自動化スクリプトのための非対話型認証の設定

Tectia Server を自動ファイル転送に使用する場合、ファイル転送用に別々のユーザ・アカウントを作成できます。そのようなユーザ・アカウントを非対話型のファイル転送にのみ使用する場合は、サーバ側でターミナル・アクセスを無効にすることをお勧めします。5.2.5 の手順を参照してください。

SFTP アカウントには、公開鍵やスクリプト・コマンドによる非対話型認証を設定できます。非対話型のバッチ・ジョブの場合、パスフレーズなしの公開鍵認証を使用できます。

クライアントを非対話的に実行するには、サーバのホスト公開鍵をクライアントに保存し、ユーザ認証に非対話的な方法を設定しておく必要があります。非対話的な使用にはコマンドライン・ツールのバッチ・モードを使用する必要があります。

1. RSA 鍵ペアを生成し、パスフレーズのフィールドは空にします。4.3.1 の手順を参照してください。

2. 鍵のアップロードについては、4.3.2 の手順を参照してください。

警告

秘密鍵は、他人がアクセスできないようにしてください。これは、パスフレーズなしで鍵を保存する場合に特に重要です。

その他の非対話型認証方法の詳細については、『Tectia Server Administrator Manual』の「Authentication」の章を参照してください。

第5章 セキュアなファイル転送の使用

Secure File Transfer プロトコル (SFTP) は、プレーンテキスト・ベースの FTP サービスに代わるセキュアなサービスです。SFTP サービスでは、転送時にすべてのファイルを暗号化します。

本章では、セキュアなファイル転送がどのように使用されるかを示し、使用事例と必要な設定変更について説明します。

5.1. Tectia Client での SFTP の使用

Tectia Client の SFTP のデフォルト設定はほとんどの場合に適切なため、すぐにファイル転送の実験を開始できます。SFTP サービスはコマンドラインまたは Tectia セキュア・ファイル転送 GUI から使用できます。GUI には、ガイドとなるツールチップが含まれています。

5.1.1. コマンドラインでの SFTP の使用

sftpg3 コマンドは、SFTP サーバ・サブシステムが有効な Secure Shell バージョン 2 サーバを実行しているホストに接続するために、コマンドラインで使用します。

sftpg3 の基本構文は以下の通りです。

```
sftpg3 username@remotehost
```

これにより、リモート・ホストにログインします。たとえば、ログインに成功した後、次のようなコマンドでリモート・ホストからローカル・ホストにファイルを取得できます。

```
sftp> get filename
```

sftpg3 で利用できるコマンドを表示するには、SFTP プロンプトで `help` と入力します。

```
sftp> help
```

sftpg3 の詳細については、『Tectia Client ユーザ・マニュアル』を参照してください。

5.1.2. Tectia セキュア・ファイル転送 GUI の使用

Windows の Tectia Client には、セキュアなファイル転送を行うためのグラフィカル・ユーザ・インターフェイスがあります。セキュアなファイル転送 GUI を開くには、デスクトップ上の Tectia セキュア・ファイル転送 GUI アイコンをクリックします。

図5.1 Tectia セキュア・ファイル転送 GUI のアイコン

Tectia セキュア・ファイル転送 GUI では、接続ブローカー 設定で定義された接続プロファイルを使用して ([**プロファイル**] をクリック)、または [**クイック接続**] オプションを使用して、リモート・ホストへの接続を開くことができます。

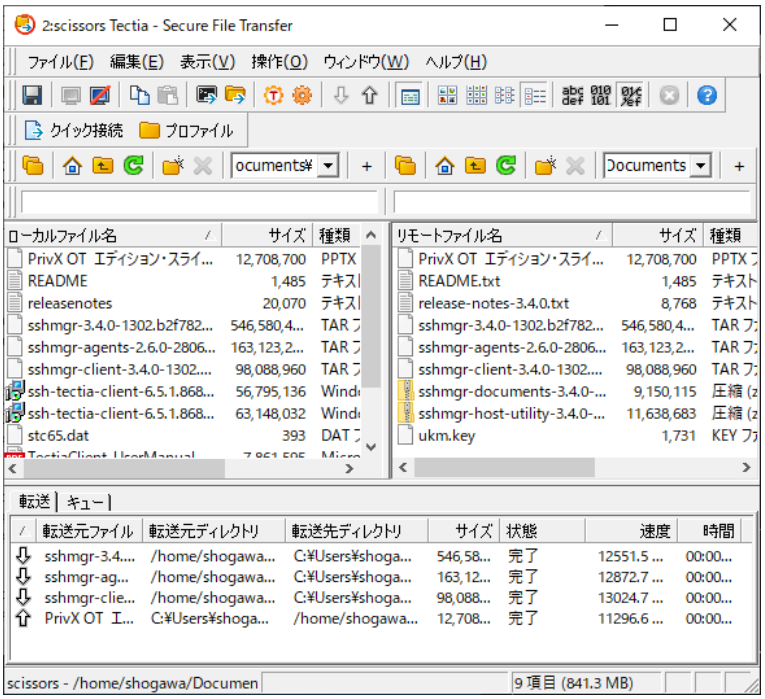

図5.2 Tectia セキュア・ファイル転送 GUI

Tectia セキュア・ファイル転送 GUI を使用すると、リモート・ホスト・コンピュータからローカル・コンピュータにファイルをダウンロードしたり、リモート・ホストにファイルをアップロードしたりすることが簡単にできます。Tectia セキュア・ファイル転送 GUI は Windows エクスプローラと似た作動をします。

5.2. セキュアな自動ファイル転送のための Tectia Server の設定

Tectia Server はセキュアな自動ファイル転送に使用できます。この使用事例では、そのための Tectia Serverの 設定方法について説明します。Tectia Client の設定変更は必要ありません。

Tectia Server の設定を変更する目的は、自動ファイル転送に向けてシステムのセキュリティを向上させることです。そのためには、SFTP の使用について、いくらかユーザ制限を設ける必要があります。この使用事例では、Tectia Server に以下の制限が定義されています。

1. 公開鍵が許可された唯一の認証方法です。5.2.2 の手順を参照してください。

2. SFTP サービスは、特別に作成されたユーザ・グループである `SFTP-users` 及び `admin` にのみ許可されます。それ以外のユーザに対して、SFTP サービスは拒否されます。5.2.3、5.2.4、及び5.2.5 の手順を参照してください。

3. `SFTP-users` のメンバーは、ユーザ固有のホーム・フォルダへのみアクセスできます。これは仮想フォルダで定義できます。5.2.4 及び 図 5.15 の手順を参照してください。

4. ターミナル・アクセスは管理者にのみ許可され、それ以外のユーザは拒否されます。5.2.3 及び 5.2.5 の手順を参照してください。

5.2.1. Tectia Server Configuration GUI の起動

Windows では、Tectia Server の設定はグラフィカル・ユーザ・インターフェイスを介して行います。

[スタート] → **[(すべての) プログラム]** → **[Tectia Server]** → **[Tectia Server Configuration]** の順にクリックして、**[Tectia Server Configuration GUI]** を起動します。

必要な Tectia Server の設定にアクセスするには、**[Tectia Server]** ビューの **[GUI Mode]** にある **[Advanced]** をクリックして、拡張設定を有効化します。

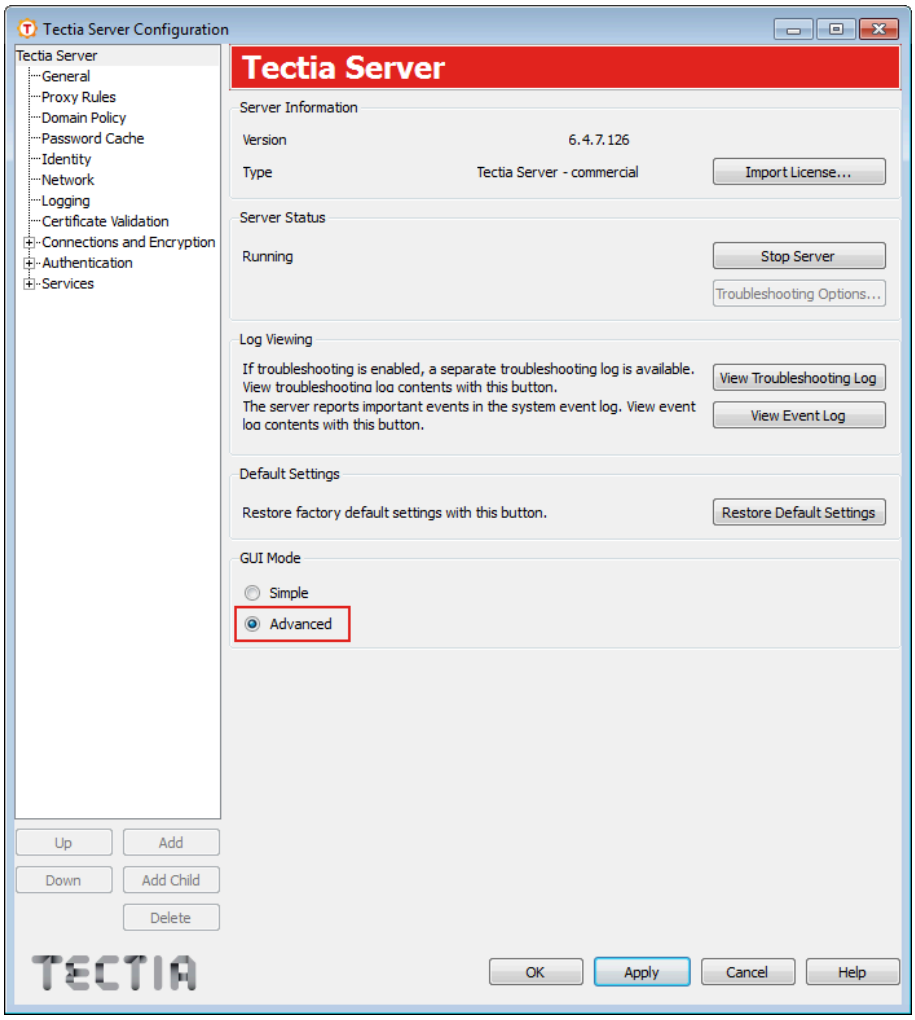

図5.3 [GUI Mode] の [Advanced] の有効化

ここからは、実際の設定に進みます。以下のビュー例を参照してください。

5.2.2. 公開鍵認証の有効化

[Authentication - Default-Authentication] ページの **[Parameters]** タブで、許可される唯一の認証方法として公開鍵認証を定義します。

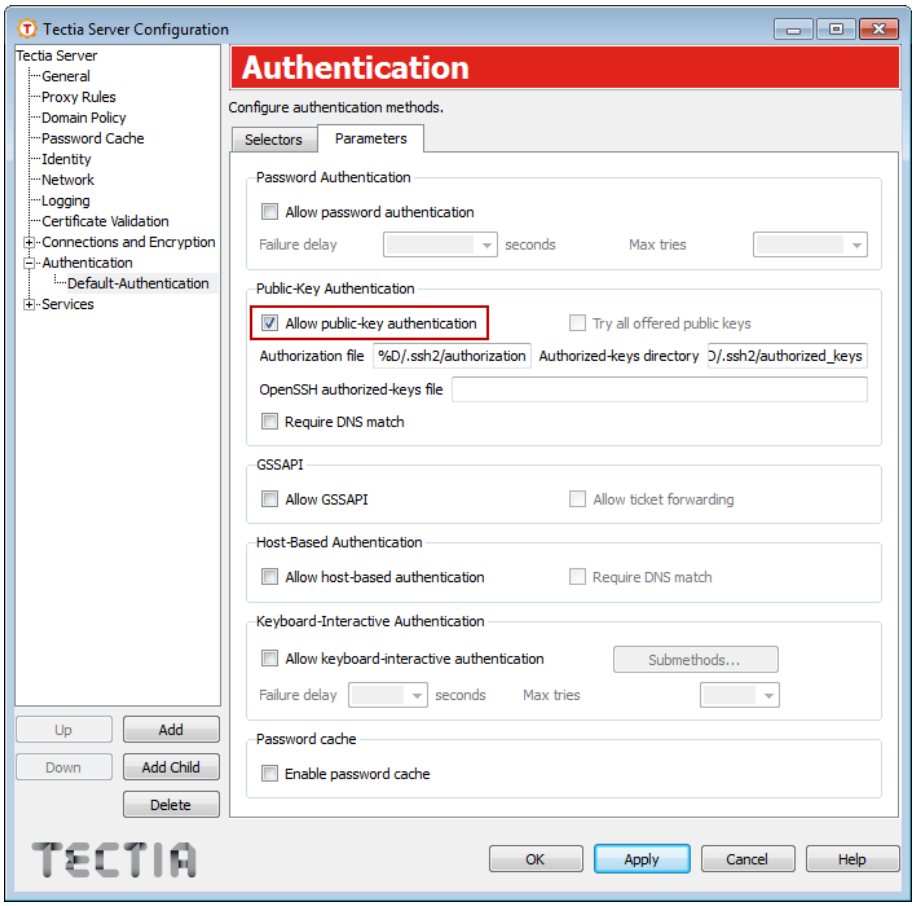

図5.4 公開鍵認証のみの有効化

5.2.3. 管理者グループの設定

管理者権限を持つユーザ・グループを作成し、そのグループのメンバーに対してすべてのアクションとサービスを許可します。

1. **[Services]** ページで **[Add]** をクリックして、管理者用のグループを作成します。

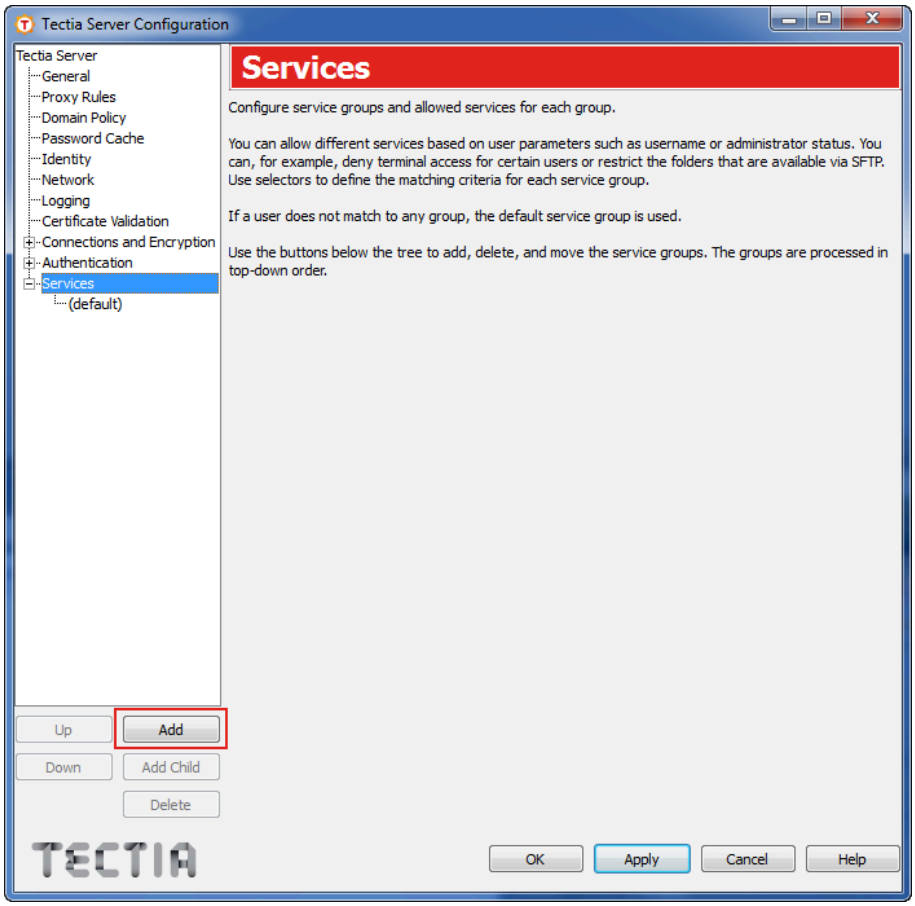

図5.5 ユーザ・グループの作成開始

Tectia Server は、新しく作成されたグループに対して `group1` というプレースホルダ名を使用します。

2. **[Basic]** タブで、グループの名前を `admin` とし、**[Terminal]**、**[Commands]**、**[Local Tunnels]**、及び **[Remote Tunnels]** のすべてのサービスについて **[Allow]** または **[Allow all]**を選択します。

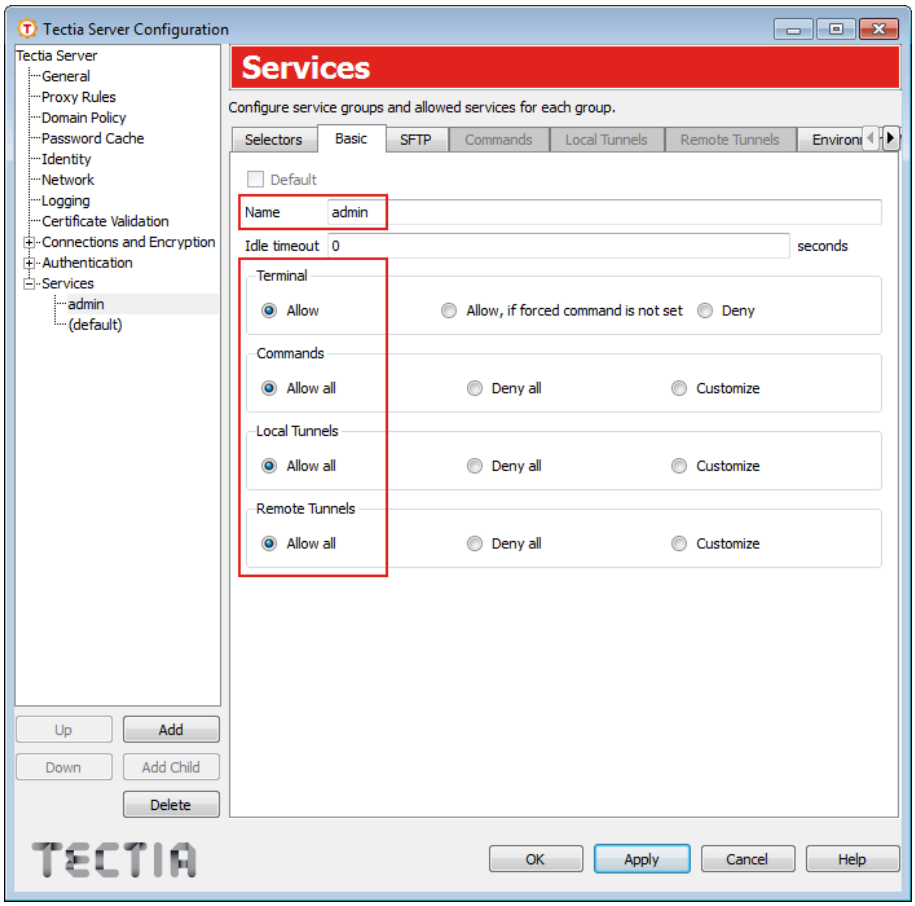

図5.6 「admin」グループの命名及びすべてのサービスの許可

3. **[Selectors]** タブに移動し、**[Add Selector]** をクリックします。**[Add Selector]** タブで、セレクタの種類に **[Administrator]** を選択し、**[OK]** をクリックします。

\

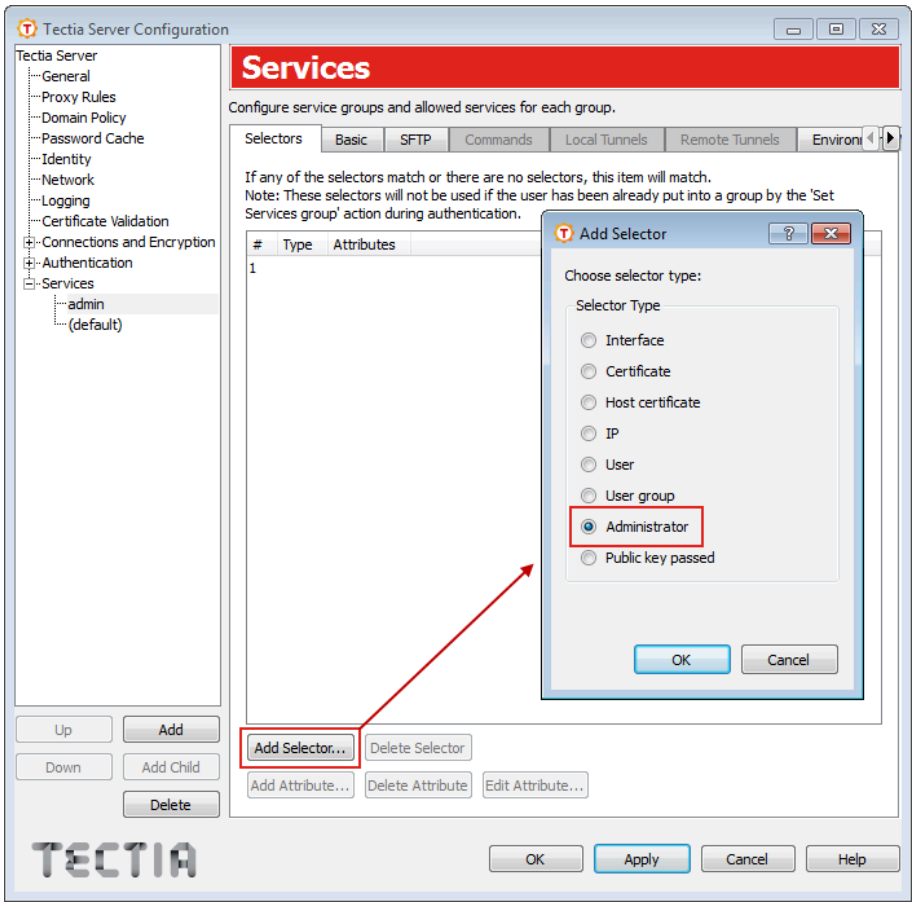

図5.7 管理者としてのグループ・セレクタの定義

4. **[Administrator Selector]** ビューが開いたら、**[Is Administrator]** を選択し、**[OK]** をクリックします。

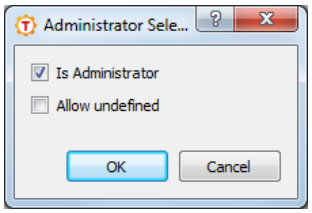

図5.8 管理者グループとしてのユーザ・グループの定義

5. **[SFTP]** タブで、`admin` グループの SFTP サービスを許可し、デフォルト設定のままにします。

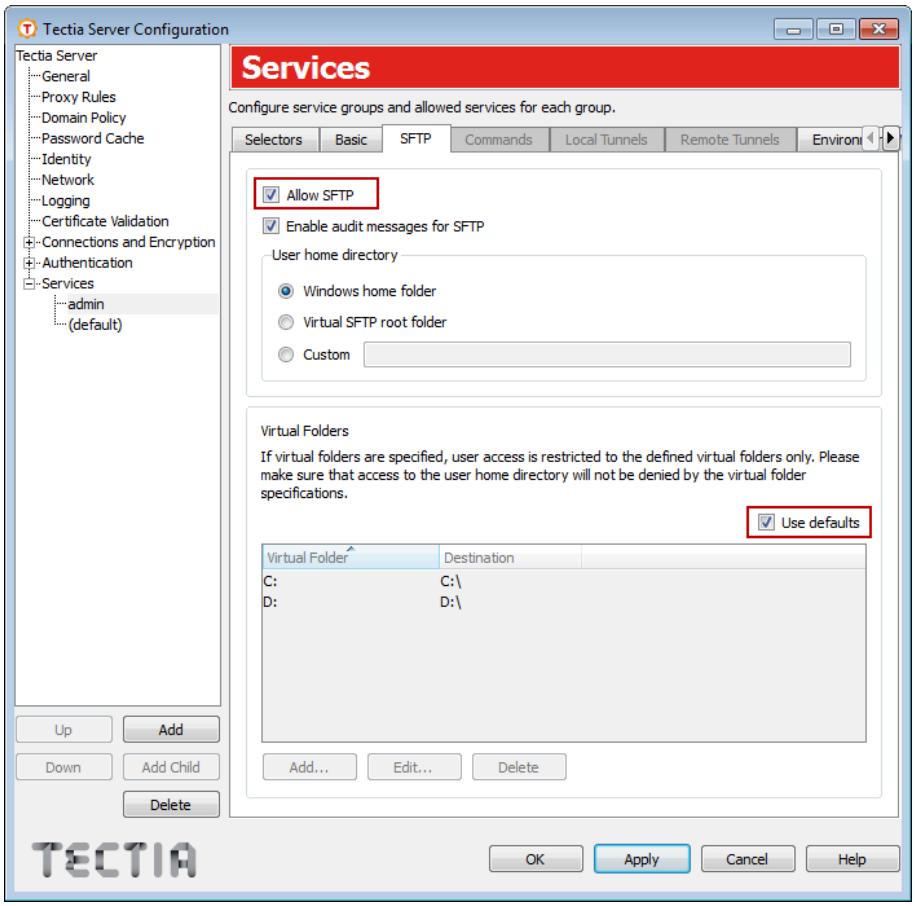

図5.9 「admin」グループに対する SFTP の許可

5.2.4. SFTP-users グループの設定

セキュアなファイル転送を行うユーザ専用のユーザ・グループを作成します。Tectia SFTP グループには既存のオペレーティング・システム関連のユーザ・グループが所属し、ユーザ固有のホーム・フォルダへのアクセスのみが許可されます。

1. **[Services]** ページで **[Add]** をクリックして、SFTP ユーザ用のグループを作成します。

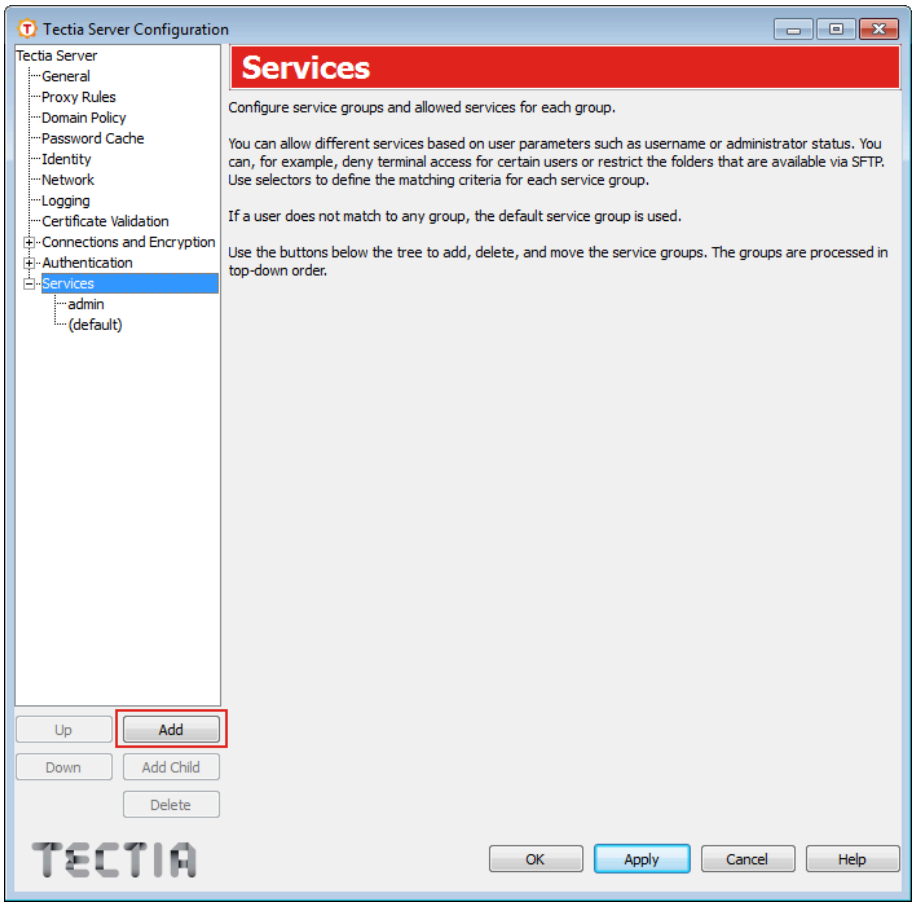

図5.10 SFTP ユーザ・グループの作成開始

2. **[Basic]** タブで、グループの名前を `SFTP-users` とし、**[Terminal]**、**[Commands]**、**[Local Tunnels]**、及び **[Remote Tunnels]** のすべてのサービスについて **[Deny]** または **[Deny all]**を選択します。ターミナル・アクセスの制限の詳細については、5.2.5 を参照してください。

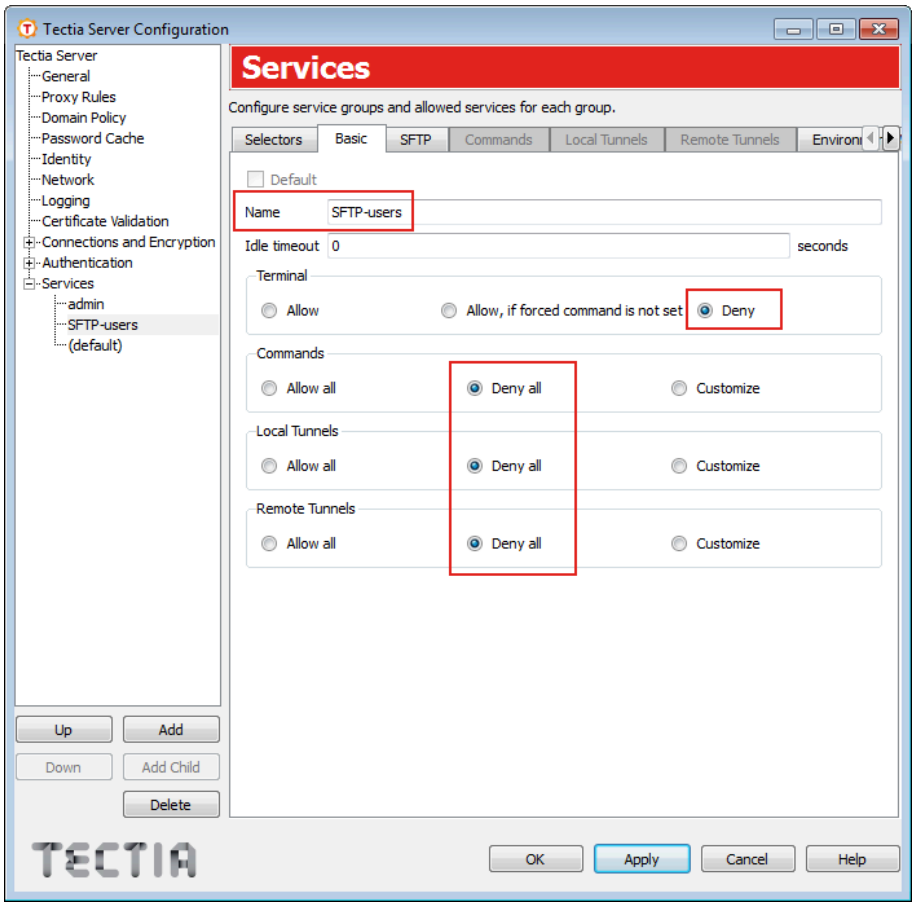

図5.11 「SFTP-users」グループの命名及びすべてのサービスの拒否

3. **[Selectors]** タブで、**[Add Selector]** をクリックし、セレクタの種類に **[User Group]** を選択して、**[OK]** をクリックします。

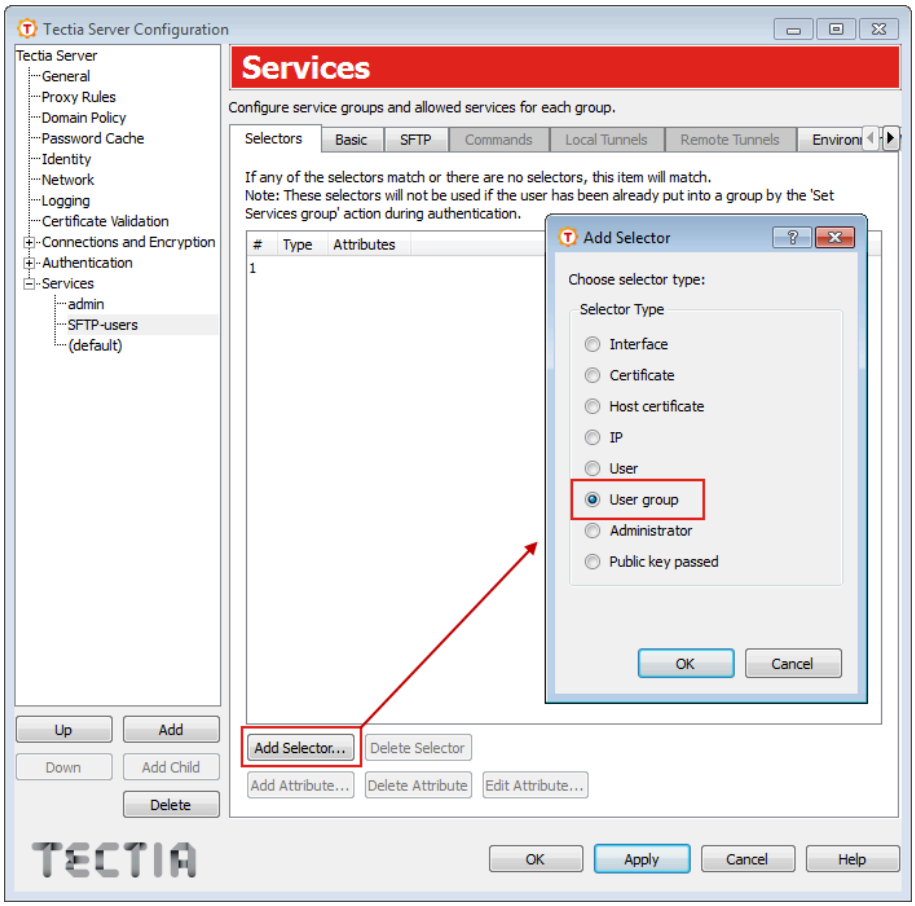

図5.12 ユーザ・グループとしてのグループ・セレクタの定義

4. **[User Group Selector]** ビューが開いたら、関連する既存のオペレーティング・システム関連のユーザ・グループ (この例では `staff` という名前) をグループに所属させます。

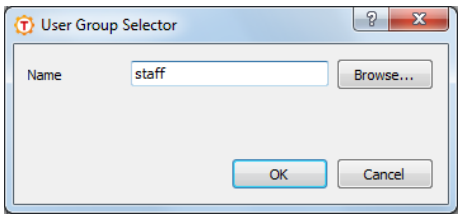

図5.13 「staff」ユーザ・グループの所属設定

新しく作成されたグループ・セレクタのデータが **[Selectors]** タブに表示されます。

5. **[SFTP]** タブで、`SFTP-users` に SFTP サービスを許可し、ユーザ・グループの **[User Home Directory]** を定義します。これは SFTP の開始ディレクトリです。下図のように、デフォルトの `%USERPROFILES%` を使用します。

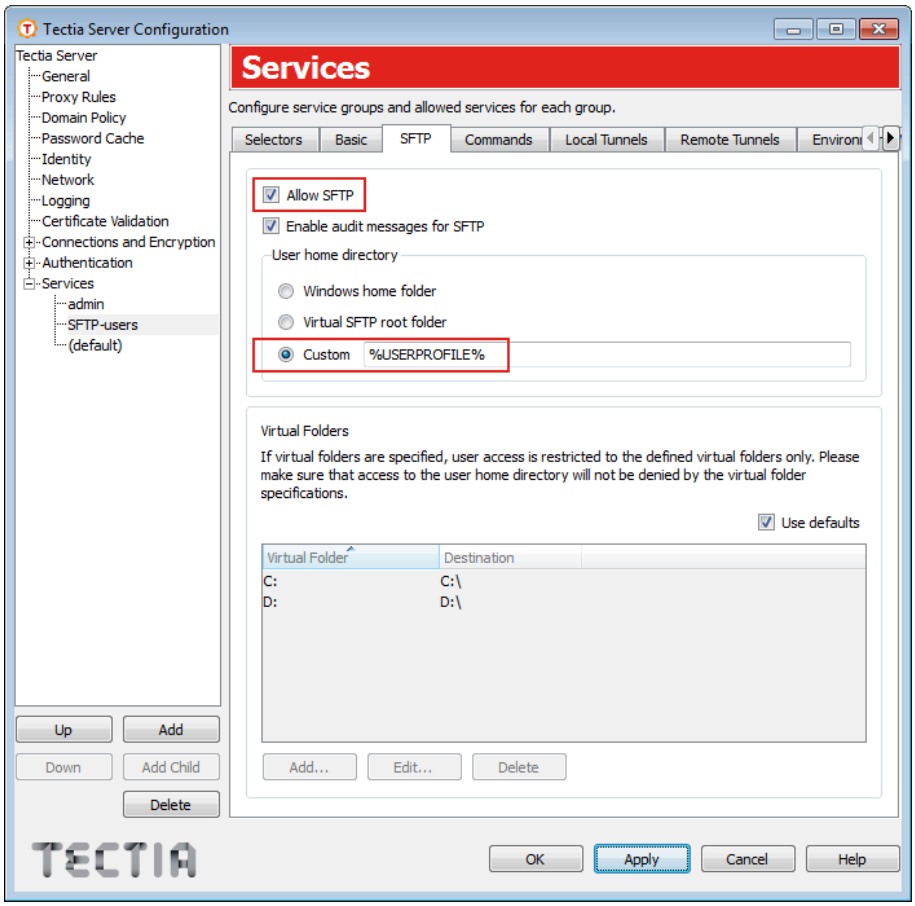

図5.14 SFTP-users グループに対する SFTP サービスの許可

6. ユーザ・グループの **[Virtual Folders]** を定義するには、まず **[SFTP]** タブの **[Use defaults]** チェックボックスを選択解除します。次に、**[Virtual Folder]** リストから `C:` を選択し、**[Edit]** ボタンをクリックします。**[SFTP Virtual Folder]** ダイアログが開いたら、仮想フォルダを `C:` と定義し、その保存先を `C:` ドライブの `SFTP` ディレクトリの下のユーザ固有のサブディレクトリにします (ユーザが `C:` にディレクトリを変更すると、実際にはユーザ固有の SFTP ディレクトリに移動します)。ユーザのホーム・ディレクトリでセッションが開始されます。それ以外のディレクトリには SFTP でアクセスできません。

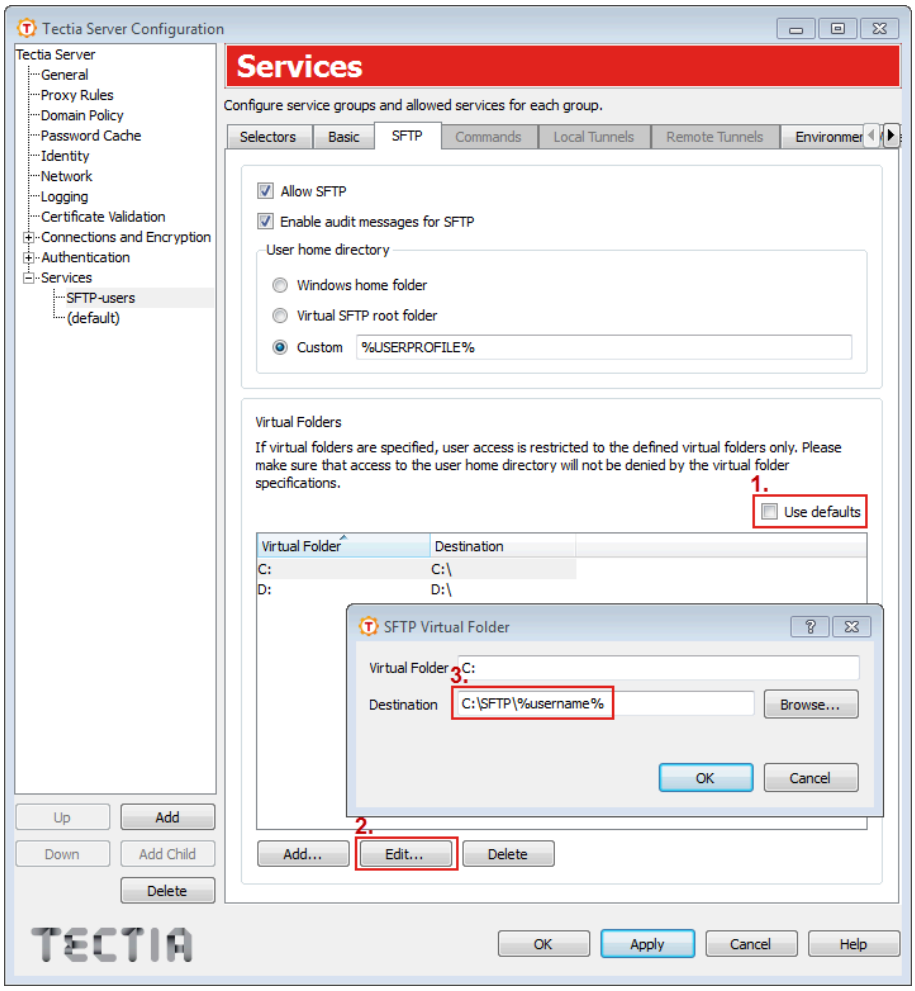

図5.15 グループ SFTP-users 用の仮想フォルダを定義する

デフォルトでは、SFTP　サブシステムを使用するユーザによるファイル・アクセスは、ファイル・システムのアクセス制御によって制限されます。Windows　上で仮想フォルダを定義することで、より多くの制限を定義できます。

デフォルトでは、仮想フォルダが設定に明示的に定義されていない場合、ユーザは　SFTP 及び SCP 操作ですべてのドライブにアクセスでき、ユーザの SFTP セッションは `C:\SFTP\%username%` ディレクトリで開始し、これが SCP 操作のターゲット・ディレクトリになります。

仮想フォルダが定義されている場合、ユーザのアクセスは、指定されたフォルダだけに制限されます。ユーザのホーム・ディレクトリは、定義された仮想フォルダのいずれかに含まれている必要があることに注意してください。

注意

仮想　SFTP　ルート・ディレクトリはディスク上の実際のディレクトリではないため、そこにファイルを書き込むことはできません。

仮想フォルダの値には、ホームの値と同じ特殊文字列 (`%username%`、`%username-without-domain%`、`%homedir%`、及び `%hostname%`) を指定できます。

5.2.5. その他のユーザの設定

`default` のサービス設定は、管理者グループまたは SFTP グループに所属していないすべてのユーザに適用されます。そのようなユーザからのすべてのサービスの拒否は、**[Basic]** タブと **[SFTP]** タブで行います。

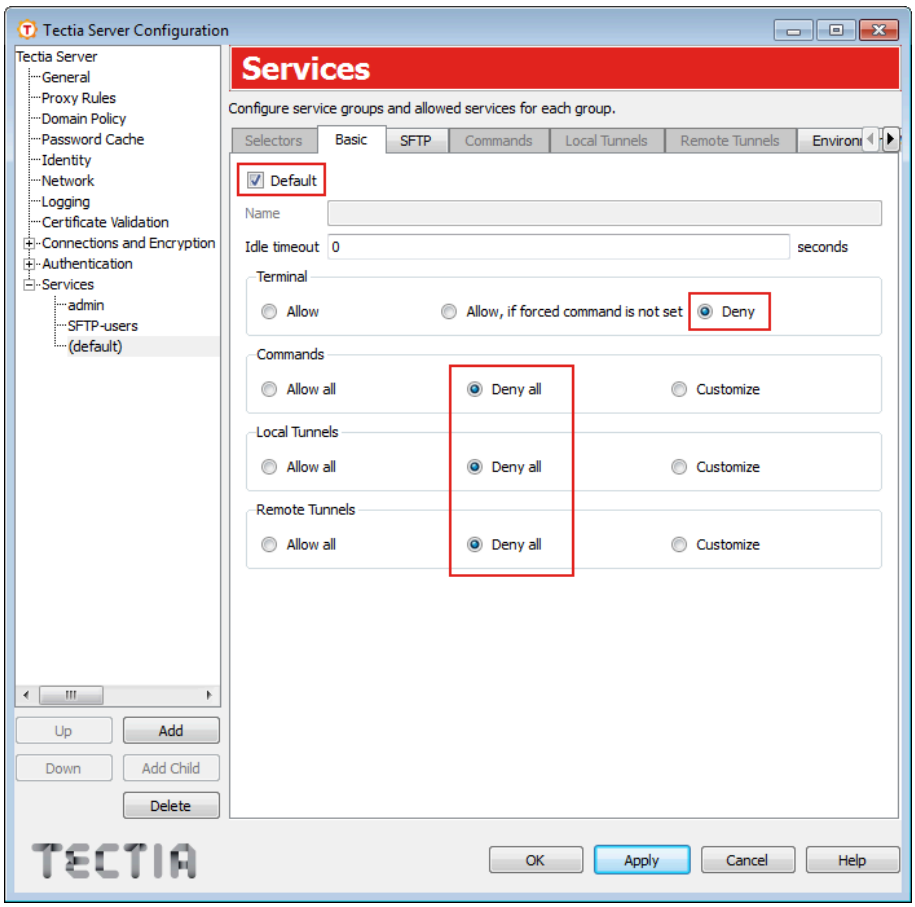

図5.16 デフォルトのグループからのすべてのサービスの拒否

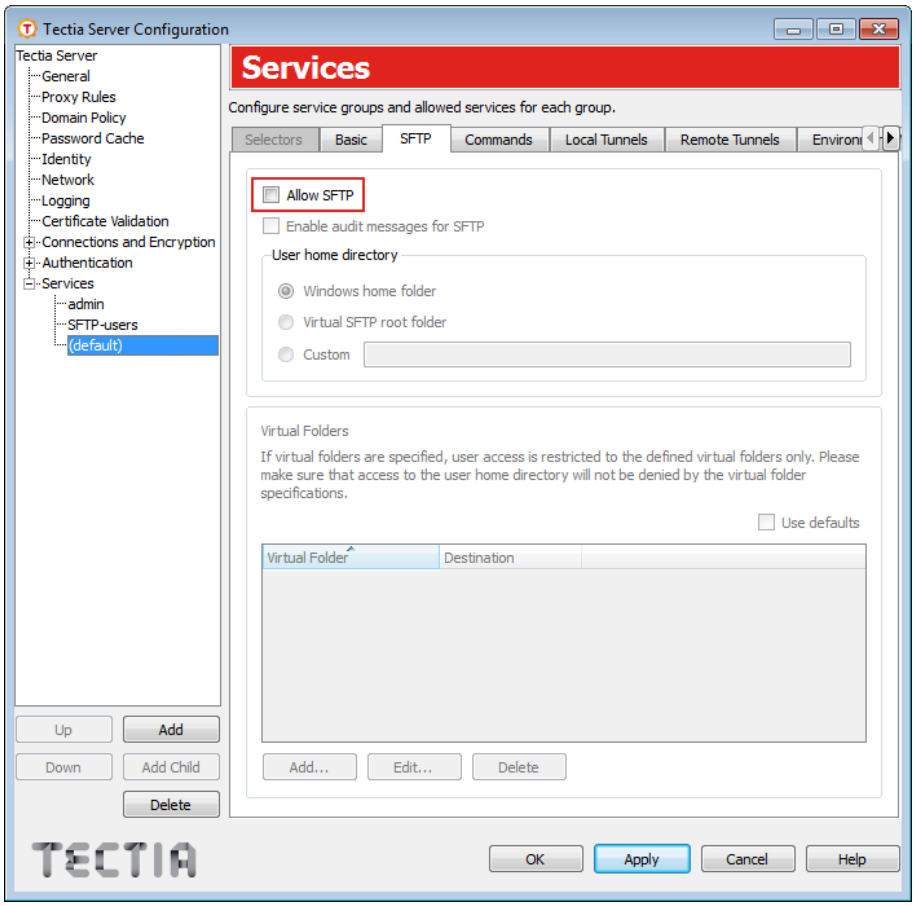

図5.17 デフォルトのグループからの SFTP サービスの拒否

ターミナル・サービスを拒否すると、指定されたグループの　X11、エージェント転送、及びシェル・コマンドも拒否されることに注意してください (一部のコマンドが明示的に許可されている場合を除きます)。

5.3. セキュアな自動ファイル転送スクリプト

Tectia Client 及び Server ホスト間の自動ファイル転送は、スクリプトを使用して設定できます。

Tectia Server を自動ファイル転送に使用する場合、ファイル転送ユーザ用に専用のユーザ・アカウントを作成できます。その上で、それらのアカウントに対して公開鍵による非対話型認証とスクリプト・コマンドが設定され、カレント・ユーザとしてファイル転送が実行されます。

以下のスクリプトの例では、まず　Tectia　Client　から　Tectia　Server　に `testfile` を転送し、その後ファイルを逆方向に転送します。スクリプトはコマンドと戻り値をファイルに記録します。

```
@echo off
REM Transfer file from localhost to sftpserver.example.com and back
```

```
set SRV=sftpserver.example.com
set logfile=C:\SCP-logs\scpg3_%SRV%

echo Script started %date% %time% >> %logfile%

REM This 'scpg3 put' command transfers the file from client to server.
echo scpg3.exe -B -q testfile.dat %SRV%:test >> %logfile%
scpg3.exe -B -q testfile.dat %SRV%:test
echo Result: %ERRORLEVEL% >> %logfile%

REM This 'scpg3 get' command fetches the file from server to client.
echo scpg3.exe -B -q %SRV%:test test >> %logfile%
scpg3.exe -B -q %SRV%:test test
echo Result: %ERRORLEVEL% >> %logfile%

echo Script ended %date% %time% >> %logfile%
echo *** >> %logfile%
```

第6章 セキュアなアプリケーション接続の使用

本章では、セキュアな電子メール・サーバ・アクセス用にあらかじめ設定した自動トンネルを使って、簡単にアプリケーション・トンネリングを設定する方法について説明します。電子メール・アプリケーションが動作しているクライアント・マシンには Tectia Client が必要です。

Tectia のトンネリング機能は、たとえば会社の従業員が社外で仕事をしているときに、電子メールや社内イントラネットのページ、共有ファイルにセキュアにアクセスできるようにする機能です。

トンネリング (ポート・フォワーディング) とは、そのままではセキュアではない TCP アプリケーション・トラフィックを、暗号化されたセキュアな形式で、Tectia 経由で転送する方法です。たとえばPOP3 や SMTP、HTTP 接続など、そのままではセキュアではない接続をセキュアにすることができます。

トンネリングを利用することで、モデムや GPRS、3G、DSL 回線、ケーブル接続、ホテルのインターネット・サービスといったアクセス方法に関係なく、あらゆるタイプのインターネット・サービスから電子メールにアクセスできるようになります。インターネットに TCP/IP 接続さえしていれば、世界中のどこからでもセキュアに電子メールを受信したり、他のリソースにアクセスしたりできます。

Tectia 接続ブローカー はバックグラウンドでトンネリングを処理します。接続ブローカー は起動時に、定義済みの自動トンネルのリスナーを開き、パスワードまたはパスフレーズを入力するようユーザに要求します。接続が、空のパスフレーズを持つ公開鍵を使って認証される場合、ユーザは何もする必要がありません。実際のトンネルは、リスナー・ポートに初めて接続されたときに形成されます。

注意

トンネルを使用するユーザ・アプリケーションは、暗号化トンネルを使用しない場合と同様に、独自の認証手順を実行します (存在する場合)。

自動トンネルはローカル (発信) トンネルです。つまり、ローカル・コンピュータの指定されたローカル・ポートから接続先のリモート・ホスト・コンピュータの指定されたポートへの

転送に使用する TCP 接続を保護します。リモート・ホスト・コンピュータを越えて接続を転送することも可能ですが、その場合の接続は Tectia Client と Secure Shell サーバ間でのみ暗号化されます。

図 6.1 は、Secure Shell サーバが DMZ ネットワークに存在する場合の例です。この場合の接続は、Tectia Client から Secure Shell サーバまでは暗号化されますが、その後、企業ネットワーク内では IMAP サーバまで暗号化されません。

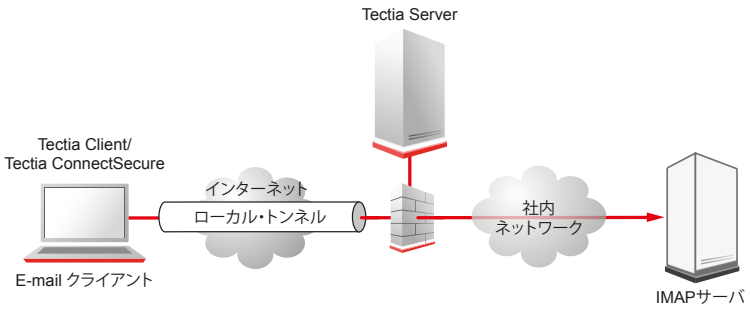

図6.1 IMAP サーバまでのローカル・トンネル

6.1. 自動トンネルの定義

自動トンネルは、あらかじめ設定されたサーバへのセキュアな接続で、接続は Tectia Client の起動時 (通常はセッションの開始時) に自動的に開かれます。実際のトンネルは、アプリケーションがリスナー・ポートに初めて接続したときに形成されます。その時点でサーバへの接続が開かれていない場合は、その接続も自動的に開かれます。

自動トンネリングには Tectia Client とアプリケーションでの設定が必要です。Tectia Client の自動トンネルを定義する手順については、6.1.1 を参照してください。

トンネリングするアプリケーションの自動トンネルを定義する手順については、6.1.2 を参照してください。

6.1.1. Tectia Client での設定

自動トンネルは **Tectia コネクション設定** GUI で設定します。

Windows タスクバーの通知領域で Tectia アイコン を右クリックし、**[設定]** を選択してツールを開きます。

ツリー・メニューで **[自動トンネル]** を選択し、**[追加]** をクリックして、**[自動トンネル]** ダイアログボックスを表示します。

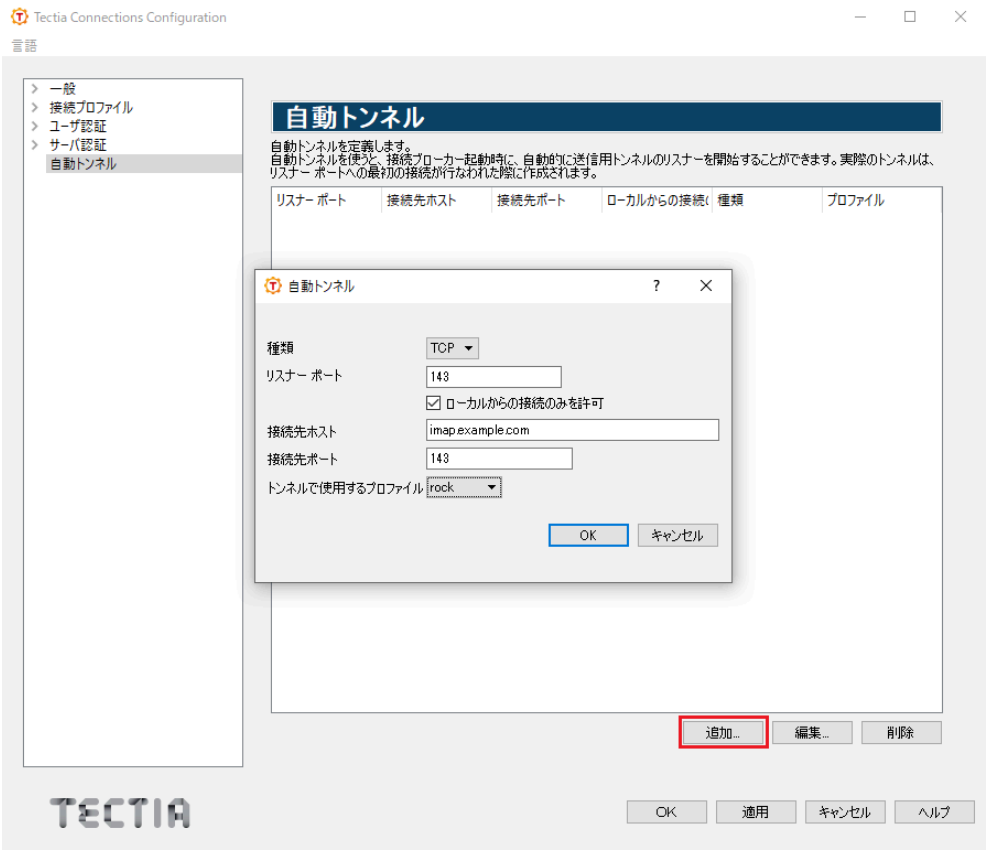

図6.2 自動トンネルの定義

以下のようにフィールドに入力します。

- **[種類]:** トンネルの種類をドロップダウン・リストから選択します。TCP 及び FTP から選択できます。
- **[リスナー ポート]:** Tectia Client がリッスンし、アプリケーションが接続するローカル・ポートの番号を定義します。予約されたポート番号は使用しないでください。

> **注意**
>
> トンネルを作成する対象のプロトコルまたはアプリケーションには、正常に接続するために使用する必要がある固定のポート番号 (IMAP の場合は 143、SMTP の場合は 25 など) が存在する場合があります。その他のプロトコルまたはアプリケーションについても、オフセット (VNC の場合は 5900 など) を考慮に入れなければならない場合があります。

- **[ローカルからの接続のみを許可]:** ローカル接続に限って確立を許可する場合は、このオプションを選択したままにします。この場合、作成されたトンネルは他のコンピュータでは使用できません。デフォルトでは、ローカル接続のみが許可されます。これはほとんどの状況に適した選択です。外部からの接続も許可する場合は、それに伴うセキュリティへの影響も十分に検討してください。

- **[接続先ホスト]**: このフィールドでは、トンネルの接続先ホストを定義します。

> **注意**
>
> 接続先ホストのアドレスは、Secure Shell 接続が確立された後に解決されるため、ここでの `localhost` は接続先の Tectia Server ホストを指します。

- **[接続先ポート]**: 接続先ポートは、接続先ホスト上でトンネル接続されるポートを定義します。
- **[トンネルで使用するプロファイル]**: トンネルを作成するときに使用する接続プロファイルを選択します。接続プロファイルを作成する手順については、3.2 を参照してください。

自動トンネルを編集するには、リストからトンネルを選択して **[編集]** をクリックします。

自動トンネルを削除するには、リストからトンネルを選択して **[削除]** をクリックします。

6.1.2. トンネルされたアプリケーションの設定

アプリケーション (Microsoft Outlook などの IMAP や SMTP メール) は、アプリケーション・サーバ・ポートではなく、`localhost` ポートに接続するよう設定する必要があります。

図 6.3 は、Microsoft Outlook 2007 の電子メール・アカウント設定の例です。

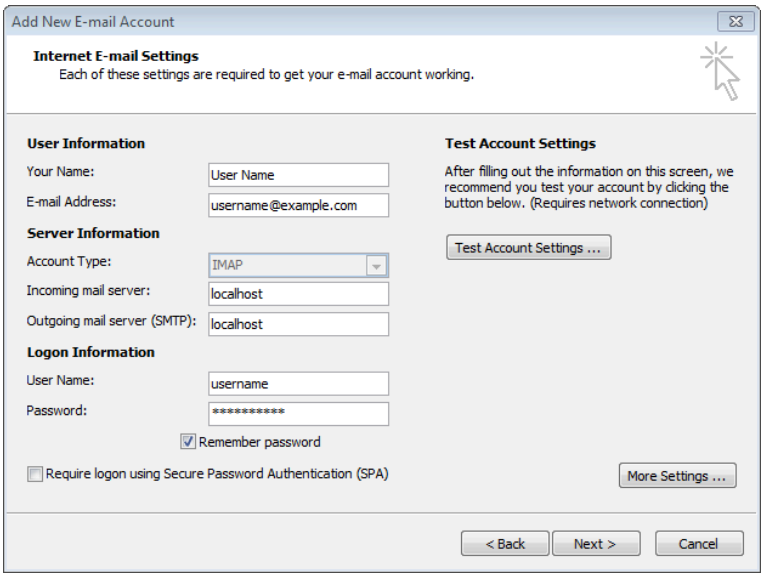

図6.3 Microsoft Outlook 2007 での電子メール設定の定義

トンネルされたアプリケーションが `localhost` ポートに接続すると、接続は暗号化された形式で Tectia Server に転送され、そこから暗号化されていない状態でアプリケーション・サーバに転送されます。

索引