の評価

Reflection for Secure IT Windows クライアント

Micro Focus

Reflection for Secure IT Windows クライアント

MICRO FOCUS

Reflection for Secure IT...
... サポートサービスの付いた Secure Shell

Reflection for Secure IT は、セキュリティ対策に真剣に取り組まれようとするお客様にお勧めの製品です。セキュアでない Telnet や FTP を信頼できる暗号化された通信手段 Secure Shell (SSH) に置き替えることによって、管理者は安全が保証されないネットワーク経由の環境でも、TCP/IP 上のアプリケーションを安全な転送トンネルを介して通信させたり、重要なデータを安全にファイル転送したり、リモートサーバを遠隔から安全に保守することができます。

なぜ Secure Shell なのか

Secure Shell (SSH) プロトコルは、転送中のデータを盗聴、改ざん、なりすましの不正行為から保護するために、セキュリティ要素技術を用いて、内部動作仕様を規定しています。具体的には、次の保護手段にて実現しています。今日、このような保護手段の重要性は高まる一方です。

- サーバ認証により、クライアントはなりすまし行為に欺かれることなく目的のサーバに接続します。
- ユーザ認証により、許可されたクライアントユーザのみがサーバに接続できます。
- データの暗号化により、転送中のデータやパスワード等の制御情報が盗聴されるのを防ぎます。接続のたびにクライアントとサーバが共通の鍵を生成し、この共通鍵でのみ受信データの復号化が可能になります。
- データの完全性保証検査により、転送中のデータの改ざんを検知し保護します。

なぜ Reflection for Secure IT なのか

高信頼なセキュリティシステムを構築するには、製品自体が高品質で、かつそれを正しく導入/運用することが肝要です。Attachmate 社の Reflection for Secure IT は、製品とサポートの両面からその期待に応える製品です。

- 高品質なソフトウェア製品

  最新技術を用いたソフトウェア開発環境で設計された Reflection for Secure IT は、安定性と脆弱性排除を極めた製品です。

- 多様なプラットフォームに対応

  Reflection for Secure IT クライアントおよびサーバには Windows と 各種 UNIX に対応し、32 ビットと 64 ビットのハードウェア環境で動作します。

- 迅速な技術サポート

  当社の技術サポートスタッフは、お客様の質問や問題に対して親密に接し、社内開発チームと緊密に連携しながら、迅速かつ適切に対応します。

- セキュリティアップデート

  当社のセキュリティスペシャリストは、潜在的なセキュリティの脆弱性に対する注意を怠りません。新たな脆弱性を発見した場合は、常に最新情報をお知らせし、お客様のセキュリティに関する懸念事項を速やかに解決することを最優先としています。

- 整備されたマニュアル類

  当社のマニュアル等のドキュメントは、製品に関する導入/設定/運用/製品仕様等について、技術的に正確な情報をお客様に提供します。

ご自分の目でお確かめください

評価版ソフトウェアでは、Reflection for Secure IT Windows クライアントのすべての機能を 60 日間お試しいただけます。まだ手元にご用意していない方は、http://www.attachmate.com/ja-jp/Evals/rsitclientwin/eval-form.htm にアクセスし、評価版申請フォームに必要事項を記入した上で入手してください。

1. 「評価版のダウンロード」ページで、該当パッケージへのリンクを選択し、パッケージを保存します。ダウンロードしたパッケージを起動し、インストールプログラムを実行します。
2. インストーラファイルの保存場所を選択し、**[OK]** をクリックします。

   指定した場所にファイルが展開され、Reflection インストーラが自動的に起動します。ダイアログに従いインストールを進行させます。

評価を始める前に

- Reflection for Secure IT Windows クライアントを評価するためには、接続先 Secure Shell サーバが必要です。すでにサーバをお持ちであればそれを使用し、無い場合は、Reflection for Secure IT Windows サーバまたは UNIX サーバの評価版を導入ください。
- 「Reflection for Secure IT Windows Client User Guide」(英文) をダウンロードして、このガイドの詳細確認として参照ください。次の場所にあります。

  http://support.attachmate.com/manuals/rsit_win_client.html

はじめに

この評価ガイドでは、Reflection for Secure IT の標準的な使い方を理解頂くために、まずいくつかのポイントを示します。説明に従い試したら、次に「さらにお試しください」の項目をお読みください。ここには、Reflection に備わっている豊富な機能を使用して、時間と費用を節約しながら、セキュリティレベルを最大限に高めるのに役立つヒントが記載されています。

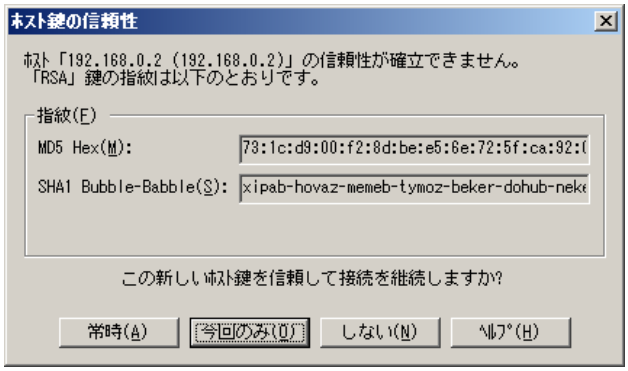
接続操作

インストール完了後、リモートホストに接続開始可能な状態になっています。まずは、デフォルトの構成設定状態のまま接続を試行してみます。

1. Reflection for Secure IT クライアントを起動します。(**[スタート]** - **[すべてのプログラム]** - **[Attachmate Reflection]** - **[SSH クライアント]** の順に選択します)
2. ツールバーから、**[接続/切断]** ボタンをクリックします。

3. **表示した[ホストに接続]** ダイアログボックス上で、ホスト名 (または IP アドレス) とユーザ名を入力して、**[OK]** をクリックします。

   注記: リモートホストに初回接続時、次のような **[ホスト鍵の信頼性]** ダイアログボックスが表示されます。



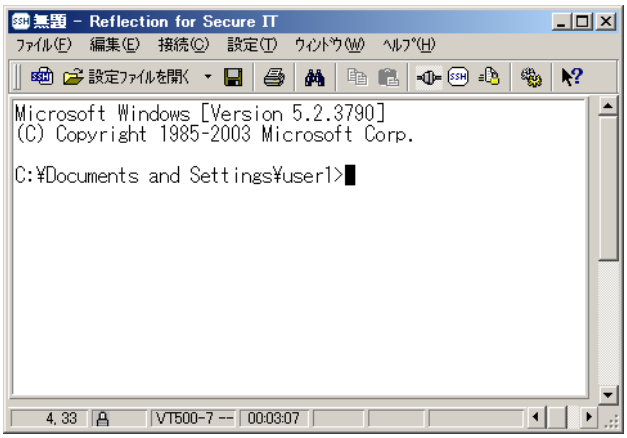
   画面内にサーバのホスト鍵の指紋(ダイジェストコード)を 2 つの形式で表示しますので、内容を目視確認します。サーバのシステム管理者に事前に確認しておくことで、確かに接続しようとしたサーバかを厳密に確認できます。

4. このホスト鍵を信頼して既知のホスト一覧に追加する場合、**[常時]** をクリックします。

   一覧にホスト鍵を追加後は、クライアントプログラムが自動的にホスト認証するので、以後の接続では、**[ホスト鍵の信頼性]** のプロンプトは表示されなくなります。

5. ログインのためのパスワードを入力して、**[OK]** をクリックします。

   認証が成功すると、端末ウィンドウにリモートホスト上のシェルセッションが表示されます。このシェルセッションを使用して、サーバ上で UNIX シェルコマンドまたは Windows DOS コマンドを実行します (実行コマンドはリモートサーバに依存します)。



Windows サーバに接続した直後の端末画面例

6. 接続終了後に **[ファイル]** - **[保存]** コマンドをクリックして、設定ファイルをこのセッション構成で保存します。

次回からは、保存した設定ファイルを開くだけで、同じホストに接続が自動的に開始されます。

さらにお試しください

デフォルト構成設定状態での接続が成功したら、さまざまな機能を試してください。次に例を挙げます。

- **表示をカスタム設定する**

  [設定] - **[表示]** コマンドをクリックして、表示色、フォントなどの表示オプションをカスタム設定できます。

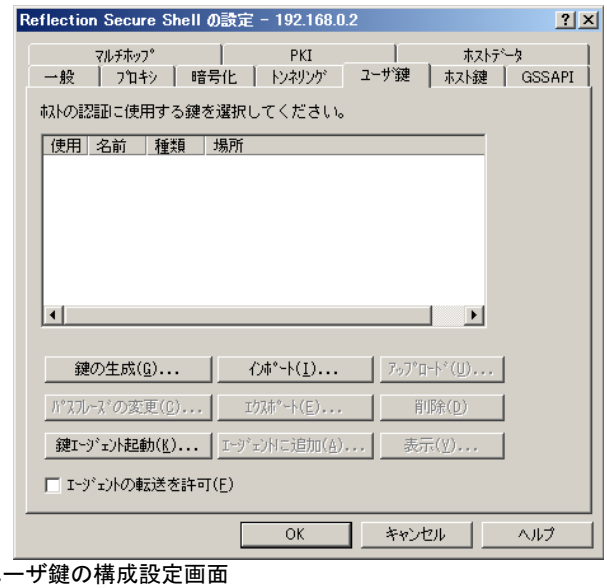
- **[セッション設定の構成] ツールバーを使用して、設定画面をすばやく表示する**

  [セッション設定の構成] ボタンをクリックします。

- **公開鍵認証を構成する**

  公開鍵ユーザ認証を使用すると、Secure Shell サーバは、固有のデジタル署名を使用してクライアントユーザを認証します。公開鍵認証を構成するには、クライアント側で鍵ペアを作成し、対応する公開鍵をリモートサーバにアップロードします。公開鍵認証では、認証に使用する鍵ペア情報がネットワーク上を送信されず、かつ物理的に秘密鍵ファイルを所有しないと認証されないため、セキュリティ水準が向上します (パスワード認証では、ユーザが認証を行うたびに暗号化したパスワードがネットワーク上を送信されます)。

  公開鍵認証を構成するには、**[セッション設定の構成]** ボタンをクリックします。端末ウィンドウの左画面で **[ユーザ鍵]** を選択することで、次の図のように **[ユーザ鍵]** タブが開いた状態で表示されます。詳細は「Reflection for Secure IT Windows Client User Guide」を参照ください。



ユーザ鍵の構成設定画面

- **ユーザ鍵をサーバにアップロードする**

  ユーザ鍵をサーバにアップロードするには、SSH 接続中に、上記 **[ユーザ鍵]** 設定画面において、生成した鍵ペアを選択し **[アップロード]** ボタンをクリックします。Reflection によって、サーバの正しい場所に正しい形式で鍵が自動的にアップロードされます。

- **証明書認証を構成する**

  証明書認証は、公開鍵認証に伴う問題の一部を解決します。例えば、ユーザ認証に公開鍵を使用している場合、各クライアントの公開鍵をサーバにアップロードし、その鍵を認識するようにサーバを構成する必要があります。証明書認証の場合は、1 つの CA (証明局) のルート証明書を使用して、複数のクライアントユーザを認証できます。デフォルトでは、Reflection for Secure IT は、Microsoft の証明書格納場所にある証明書を使用します。また、Reflection 証明書マネージャを使用して、Reflection セッションごとに別個の証明書格納場所を保持できます。このようにすることで、SSH 接続において一層高度なセキュリティを実現できます。

  Reflection 証明書マネージャを開くには、**[セッション設定の構成]** ボタンをクリックします。端末ウィンドウの左画面で、**[PKI]** - **[Reflection 証明書マネージャ]** ボタンをクリックします。

Reflection 証明書マネージャ

- **特定のホストまたはホストのグループに対して Secure Shell 設定を構成する**

  接続先ホストごとに設定ファイルを保存します。その結果、複数のホストで同一構成設定内容を共有する場合でも、個別に異なる設定とする場合でも、適切に対応できます。

新しい構成セクションを作成するには、**[接続の設定]** ダイアログボックス (**[接続]** - **[接続の設定]**) を開き、ホスト名を指定します。**[SSH 構成セクション]** は空白のままか、既に構成保存した SSH 構成セクションを指定します。(空白の場合、セクション名は現在のホスト名と同一になります。)

次に、**[セキュリティ]** をクリックし、Reflection Secure Shell 設定を構成して、**[OK]** をクリックします。Reflection Secure Shell 設定に加えた変更は、すべて現在のセクション名の下にあるクライアント構成ファイルに保存されます。以後の接続では、この保存構成ファイルの内容に従います。

- **ウィンドウレイアウトを保存する**
  一度に複数の端末セッションを使用して作業することが多い場合や、各端末セッションで FTP クライアントセッションを自動的に開く場合は、レイアウトを使用して、複数の Reflection セッションをグループとしてまとめて保存できます。レイアウトに含める各 Reflection 設定ファイルを開き、**[ファイル]** - **[レイアウト]** コマンドをクリックします。
- **コマンドラインから操作する**
  Reflection for Secure IT Windows クライアントは、コマンドプロンプト画面を通じたコマンドラインユーティリティを用意しています。**ssh**、**scp**、**sftp**、および **ssh-keygen** コマンドに対応しています。

安全なファイル転送

Reflection FTP クライアントを使用することで、ドラッグアンドドロップ等の簡単な操作でファイル転送の指示が行えます。転送の対象は、個々のファイル、複数のファイル、フォルダ全体と適宜選択して指定します。以下に手順を示します。

1. Windows の **[スタート]** メニューから、**[Attachmate Reflection]** - **[Reflection FTP クライアント]** をクリックします。

   [FTP サイトに接続] ダイアログボックスが自動的に開きます。

2. **[新規サイト]** をクリックします。

   [FTP サイトの追加] ウィザードが起動します。このウィザードは、デフォルトで SFTP 接続を開始するようになっています。この後 SFTP 接続を行うためには、接続先ホストに Secure Shell サーバが稼働している必要があります。

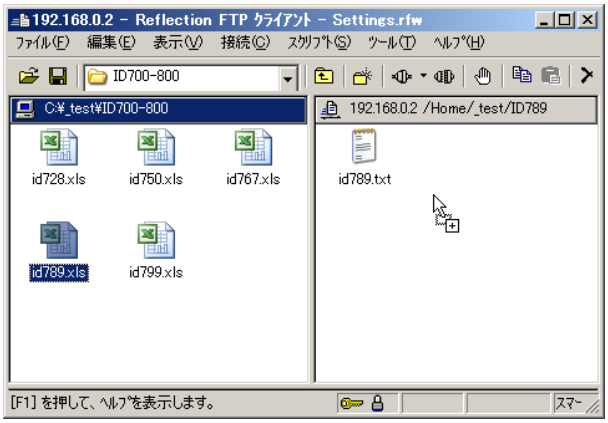
3. ウィザードに示される手順に従って、ホスト名およびユーザ名を入力します。

4. 最後の画面で、FTP サイトに接続するかどうかを尋ねられます。**[はい]** (既定) を選択し、**[完了]** をクリックしてウィザードを終了し、接続を確立します。

   注記: 既に同一サーバに接続実績があれば、**[ホスト鍵の信頼性]** ダイアログボックスは表示されません。新規に接続するサーバの場合は、**[ホスト鍵の信頼性]** ダイアログボックスにて確認し既知のホスト一覧に追加してください。

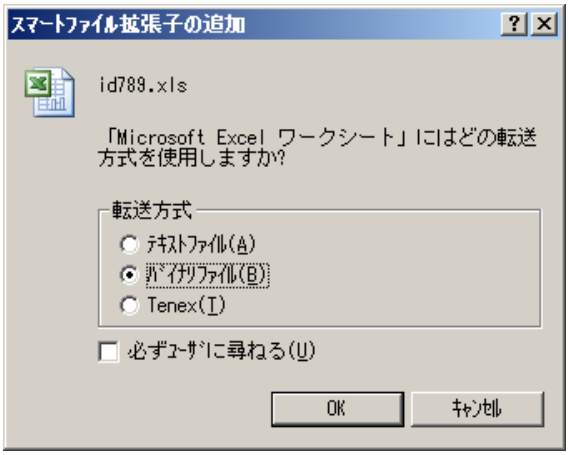
5. 接続に成功すると **[Reflection FTP クライアント]** 画面の左右にファイルまたはフォルダが表示されます。左側がローカルホスト、右側がリモートホストです。それぞれディレクトリを上下移動し、対象ファイルやディレクトリを選択します。

6. 対象ファイルまたはフォルダを選択し、それをローカルからリモートへ、あるいはリモートからローカルへドラッグアンドドロップし転送操作をします。



[Reflection FTP クライアント] 操作画面
～ドラッグアンドドロップ操作にて、ローカルホスト(左)からリモートホスト(右)に転送指示をする

注記: 主な拡張子についてはファイルの種類に応じて転送方式が決められていますが、その他の拡張子を持つファイルの転送時には、次に示すように転送方式を指定するオプションを表示します。



.xls ファイルに対するファイル転送方式の設定

7. 処理終了後に設定ファイルを保存するために、メニューの **[ファイル]** - **[保存]** を選択するか、**[Reflection FTP クライアント]** 画面を閉じる際に変更内容の保存を確認するダイアログにて、変更を設定ファイルに保存します。

保存したサイトは、FTP クライアントを起動するたびに **[FTP サイトに接続]** ダイアログボックスの一覧に表示されます。その後の処理で設定を保存した場合は、セッションの間に加えた変更内容が保存されます。

さらにお試しください

基本的なファイル転送操作ができたら、次のような機能を試してください。

- **フォルダ全体をドラッグアンドドロップする**

  フォルダをドラッグすると、そのフォルダ内のすべてのファイルが転送されます。

- **サイト固有のホームディレクトリを設定する**

  開始時に使用頻度の高いディレクトリから開始して操作手順を簡略化するために、サイト固有の起動ディレクトリを構成できます。**[FTP サイトに接続]** ダイアログボックスから、**[プロパティ]** をクリックし、**[ディレクトリ]** タブにアクセスします。サーバとローカルの両方の起動ディレクトリを構成できます。ただし、サーバのディレクトリへのアクセスは、サーバ側の構成によって制限される場合があります。

- **コマンドウィンドウを使用して、コマンドの詳細情報を表示する**

  [表示] - **[コマンドウィンドウ]** をクリックすると、新たにコマンドウィンドウ欄を表示します。この欄には、操作内容や転送内容がコマンド行として逐次表示されます。

- **スクリプトの収録を使用してスクリプトを作成する**

  操作内容をスクリプトとして自動収録し、その後で再生することで、転送指示を容易に自動化できます。**[スクリプト]** - **[収録の開始]** コマンドを使用します。

- **scp および sftp コマンドラインユーティリティのバッチモード処理で転送を自動化する**

  scp および **sftp** コマンドラインユーティリティにてのバッチモードオプションにて、ファイル転送を自動化できます。これらのユーティリティについては、アプリケーションヘルプを参照してください。

- **自動化 API を使用して、他のアプリケーションからファイルを転送する**

  FTP クライアント自動化 API を使用すると、Visual Basic プログラムや、Microsoft Office アプリケーションをはじめとする他の外部アプリケーションからの FTP 転送をスクリプト化することができます。詳細については、FTP クライアントのアプリケーションヘルプを開き (**[ヘルプ]** - **[トピックの検索]**)、目次で「FTP クライアントオートメーション API のヘルプ」を検索します。

ポート転送を使用した安全な通信

ポート転送はトンネリングとも呼ばれ、接続中のセッションの Secure Shell チャネルを介して TCP/IP 通信をトンネリングしフォワードする効果的な機能です。この機能を使用すると、ポート転送対象のトラフィックをファイアウォール内の安全な 1 ポートを介してルーティングできます (SOCKS のしくみと似ていますが、暗号化については異なります)。次の手順では、ポート転送を使用して、リモートサーバを安全に管理する方法を示します。

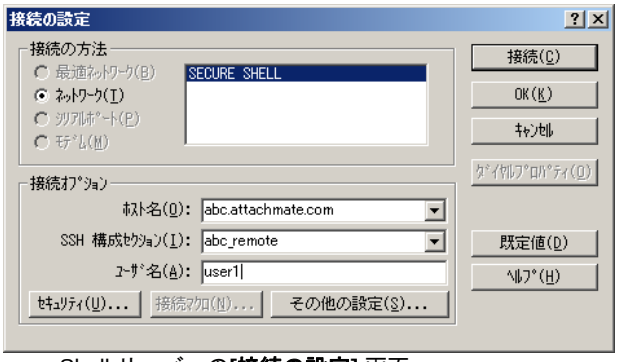
安全なリモート管理の構成

Secure Shell トンネルを介して送信できるプロトコルの 1 つに RDP (Remote Desktop Protocol) があります。RDP は、Microsoft 社が Windows Server 2003 において「リモートデスクトップ」、Windows 2000 Server において「ターミナルサービス」と呼ぶ機能のベースとなるプロトコルです。RDP を使用すると、Windows コンピュータにリモートでログオンし、ローカルコンソールを前にしているかのように操作できます。

リモートデスクトップを使用するためには、ファイアウォールに新たにポート (通常はポート 3389) を開く必要がありますが、セキュリティに注意を払っている企業であれば、これは避けたいところです。Secure Shell トンネルを介して RDP を実行すると、通信を暗号化すると同時に、ファイアウォールのポートも SSH 用を使います。次にしくみを説明します。

1. 対象の Windows サーバに Secure Shell サーバをインストールし、Reflection for Secure IT クライアントをローカル PC にインストールします。
2. Secure Shell サーバでポート転送が有効になっていることを確認します (Reflection for Secure IT サーバの場合、これがデフォルトです)。
3. Windows サーバでリモートデスクトップまたはターミナルサービスを有効にし、所有しているアカウントでリモートアクセスが可能であることを確認します。
4. Reflection for Secure IT クライアントを起動します (**[スタート]** - **[すべてのプログラム]** - **[Attachmate Reflection]** - **[SSH クライアント]**)。
5. **[接続]** - **[接続の設定]** コマンドを選択し、ホスト名およびユーザ名を入力します。

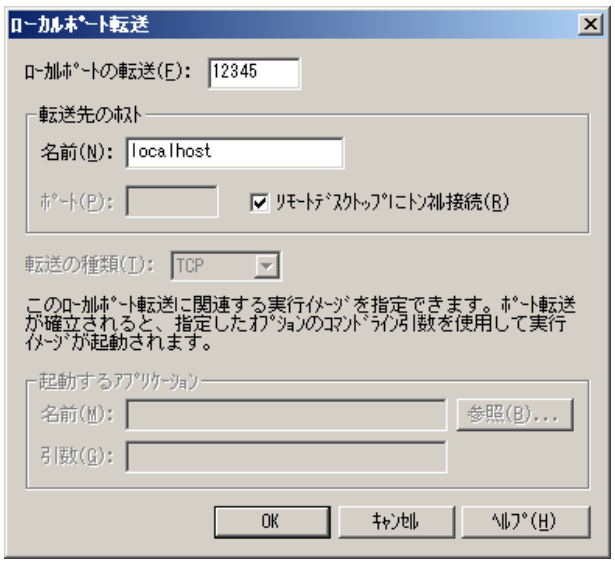
   注記: **[SSH 構成セクション]** に値を指定することもできます。値を指定すると、リモートデスクトップ接続を開始する時にはこのセクションを選択し、同じホストに他の Secure Shell 接続を行う時には異なるセクションを使用できます。



Secure Shell サーバへの**[接続の設定]** 画面

6. **[セキュリティ]** をクリックします。
7. **[トンネリング]** タブの **[ポートのローカル転送]** で、**[追加]** をクリックします。

   [ローカルポート転送] ダイアログボックスが開きます。



[ローカルポート転送] 画面上のリモートデスクトップ転送の設定

8. **[ローカルポートの転送]** に、任意のポート (1024 より大きい、使用できる任意の値) を入力します。

   ローカルホスト側でこのポートに送信されたデータが、安全なトンネルを介してサーバに転送されます。

9. **[転送先のホスト]** で、**[リモートデスクトップにトンネル接続]** をオンにします。

   この設定により、クライアントは、指定されたポートを使用して RDP プロトコルを転送し、Secure Shell 接続が確立されると、リモートデスクトップを自動的に起動するように構成されます。

10. **[転送先のホスト]** で、**[名前]** に「localhost」と指定します。この場合、安全なトンネルを介して転送されたデータの Secure Shell サーバから先の転送先が、同一サーバであることを意味します。
11. **[OK]** をクリックして、**[接続の設定]** ダイアログボックスに戻ります。
12. **[接続]** をクリックし、資格情報を使用して Windows サーバにログオンします。

    Secure Shell セッションが確立されると、リモートデスクトップセッションまたはターミナルサービスセッションが自動的に起動されます。

13. ログオンして、安全なリモートセッションを完了します。
14. **[ファイル]** - **[保存]** コマンドをクリックして、このセッション構成を保存します。

保存した設定ファイルを開くことで、保存した構成を基に安全なリモートセッションが自動的に起動されます。

さらにお試しください

ポート転送の例を以下に示します。

- **任意の TCP/IP 上のアプリケーションをクライアントとサーバ間でトンネリングする**

  TCP/IP プロトコルを使用する任意のアプリケーションについて、クライアントとサーバ間の通信を安全にトンネリングします。 Telnet、HTTP、SMTP、POP、および IMAP 通信等が対象です。ポート転送の構成設定をしたら、TCP/IP アプリケーションを転送されるポートに接続するように設定するだけです。転送の設定の詳細については、「Reflection for Secure IT Windows Client User Guide」を参照してください。

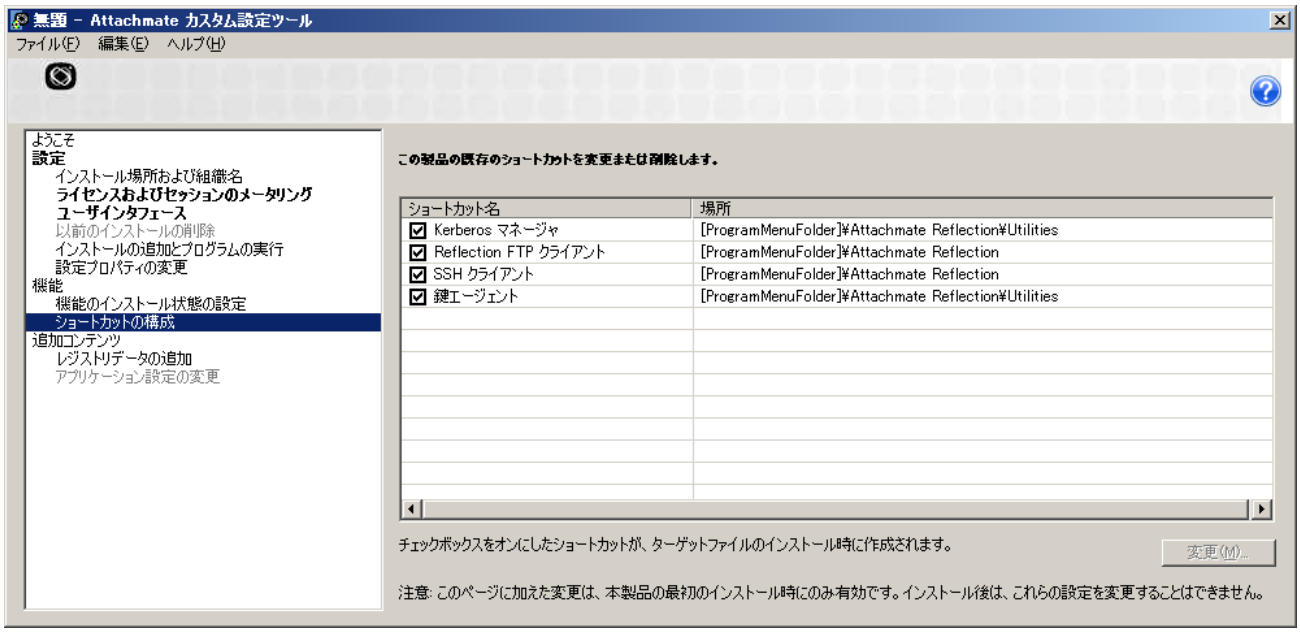
- **FTP プロトコルをクライアントとサーバ間でトンネリングする**

  デフォルトでは、Reflection for Secure IT は、安全なファイル転送のために SFTP プロトコルを使用します。一方で、お客様事情により FTP プロトコルをそのまま使用したい状況も起こり得ます。Reflection for Secure IT では、FTP プロトコルのポート転送を容易に構成でき、FTP プロトコルのコマンドチャネルとデータチャネルの両方を安全なトンネルを介して転送可能です。

  FTP クライアントの **[FTP サイトに接続]** ダイアログボックスでサイトを選択し、**[セキュリティ]** - **[Secure Shell]** で **[ポート転送を使用した FTP コマンドのトンネリング]** をオンにします。

- **コマンドラインを使いポート転送を構成する**

  Reflection for Secure IT には、ユーザインタフェースからポート転送を構成するほかに、**ssh** コマンドラインユーティリティのオプション指定、またはクライアント構成ファイルを編集した上で、ポート転送を構成できます。



[Attachmate カスタム設定ツール] 画面例

インストールのカスタム設定

Attachmate セットアッププログラムは、通常のインストール方法のほかに、Attachmate カスタム設定ツールを使用して Reflection for Secure IT のインストールをカスタム設定できます。

- Attachmate カスタム設定ツールを実行するには、コマンドラインに「`setup.exe /admin`」と入力します。

新しいカスタム設定ファイルを作成したり、コンパニオンインストーラを作成したりすることもできます。コンパニオンインストーラでは、例えばこのツールの **[ファイルの追加]** 機能を使用して、リモートホストのホスト鍵を事前にインストールし、初回接続時から **[ホスト鍵の信頼性]** ダイアログボックスを表示させずに接続を開始することも可能です。

Attachmate カスタム設定ツールの詳細については、「Reflection for Secure IT Windows Client User Guide」を参照してください。

Reflection for Secure IT Windows クライアントの詳細確認

1. マニュアルについて

下記製品マニュアルサイトを参照下さい。

http://support.attachmate.com/manuals/rsit_win_client.html

(日本語マニュアルについては別途作成予定です。)

2. 技術的お問合せ先について

1) ご購入前の評価版内容に関するお問合せは、下記メールアドレスまでご連絡下さい。

j-info@attachmate.com

下記テクニカルサポートページに FAQ も掲載しております。

http://attachmate.okweb3.jp

2) 購入されサポートサービス又は保守契約をされているお客様は、下記テクニカルサポート窓口を通じてお問合せ下さい。

http://attachmate.okweb3.jp

日本支社
Micro Focus
〒160-0023 東京都新宿区西新宿 6-3-1 新宿アイランド･ウィング 13 階
TEL 03-5909-5641 FAX 03-5909-5401
E-mail j-info@attachmate.com
URL www.attachmate.jp