



Web サイト改ざん検知システムのセキュア化

isAdmin と SSH Tectia ConnectSecure を
組み合わせた安全な FTP データ通信

Compatibility Note

2009 年 1 月

JNS 社製 isAdmin は Windows プラットフォームで動作する Web サイトの改ざん検知と自働復旧を行うためのアプリケーションとなっており、官公庁をはじめ多くの企業に導入されています。本書では、この isAdmin と SSH Tectia を組み合わせて、行われるデータ通信をセキュアにする方法についてご紹介します。

目次

1 シナリオ.....	2
1.1 はじめに.....	2
1.1.1 <i>isAdmin</i> とは.....	2
1.1.2 <i>SSH Tectia</i> の透過的トンネリング機能.....	3
1.2 <i>isAdmin</i> と <i>SSH Tectia</i>	4
1.3 利用シナリオ.....	5
1.3.1 既存の環境.....	5
1.3.2 <i>SSH Tectia</i> によるセキュアな環境.....	6
1.4 ハードウェア/ソフトウェア.....	6
2 設定.....	7
2.1 <i>isAdmin</i> の設定.....	7
2.2 <i>SSH Tectia</i> の設定.....	8
3 動作確認.....	15

1 シナリオ

1.1 はじめに

SSH Tectia ソリューションのバージョン 6 では新しい機能として既存の TCP アプリケーションの通信を SSH で透過的にトンネリングすることが可能となりました。これはさまざまな TCP アプリケーションに対して行うことが可能となっており、本書では JNS 社製の Web サイトの改ざん検知システムである isAdmin で利用される通信をセキュアにする方法について記載されています。

1.1.1 isAdmin とは

JNS 株式会社 (<http://www.jnsjp.com>) が開発した isAdmin は Web サイトの改ざんを検知、管理者にメール、SNMP、コマンド実行など様々な手法で通知を行う仕組みを提供しており、また必要に応じて自動で復旧操作を行うことも可能となっています。インストールや設定が容易で利用している Web サーバにも依存しません。現在でも Web サイトの改ざんは大きな社会問題となっており、この isAdmin を使うことで効果的に Web コンテンツを守り、個人情報を正確に保護することが可能です。

isAdmin 製品の種類

- isAdmin Standard: 小規模 Web サイト向け
- isAdmin Pro: 中規模 Web サイト向け
- isAdmin Enterprise: 大規模 Web サイト

機能概要

- Web 改ざん検知システム: コンテンツ改ざんの検知と稼働状態を監視
- Web 改ざん自動復旧システム: コンテンツ/Web アプリケーションの改ざんを自動で復旧。正規更新との見極めも可能 (Pro/Enterprise にて)
- ファイル改ざん検知システム: コンテンツ/Web アプリケーションの改ざんを検知

SSH Communications Security

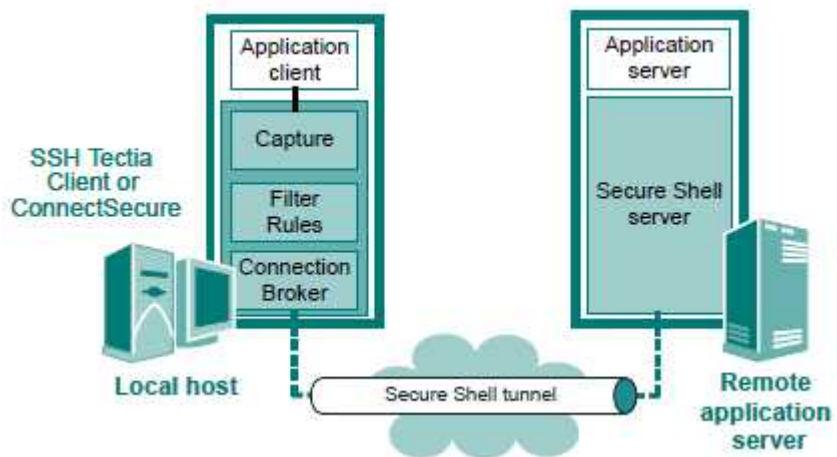
1.1.2 SSH Tectia の透過的トンネリング機能

SSH Tectia では Secure Shell が従来からもつポートフォワードの機能をさらに拡張し、クライアントアプリケーション側での“localhost”指定の必要がない (= 利用者にとって透過的) SSH によるトンネリング機能を提供します。

SSH Tectia でサポートしているトンネリング機能は以下のとおりです。

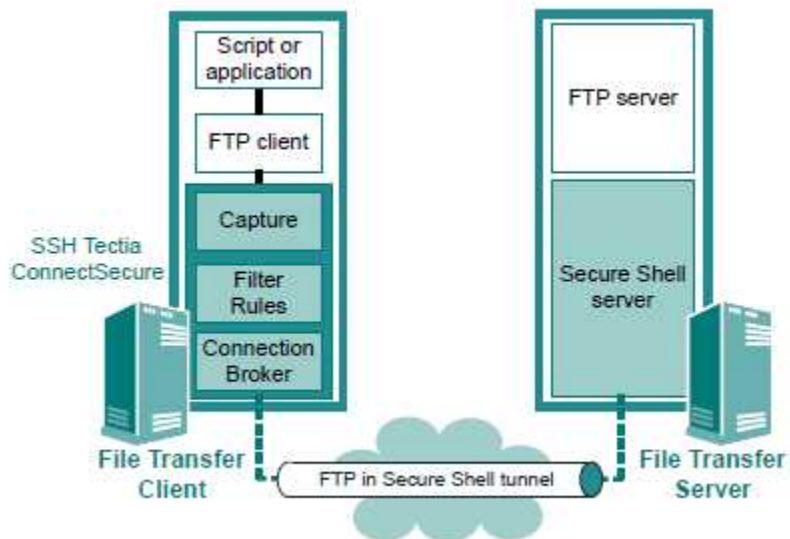
- Transparent TCP トンネリング

主要な TCP アプリケーション通信を透過的にトンネリング。ただし FTP のみは以降の機能にて対応。



- Transparent FTP トンネリング (要 ConnectSecure)

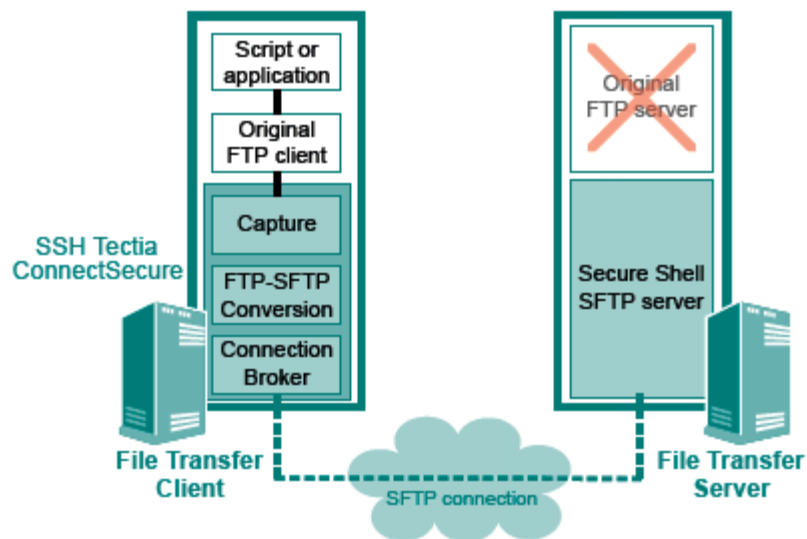
主要な FTP 通信を透過的にトンネリング。



SSH Communications Security

- FTP-SFTP 変換(要 ConnectSecure)

FTP の通信を SFTP へと自動的に変換。サーバ側には FTP サーバは不要



1.2 isAdmin と SSH Tectia

isAdmin の Web 改ざん自動復旧システム/ファイル改ざん検知システムは FTP 通信を利用して行われています。当然ながら FTP の通信は ID/パスワードをはじめ、その通信内容がネットワーク上を平文として流れるためセキュリティ上大きな問題があります。



自動復旧元に対して、正しい Web コンテンツを置く。

更新された情報を FTP を利用して自動復旧先に自動的に反映します。

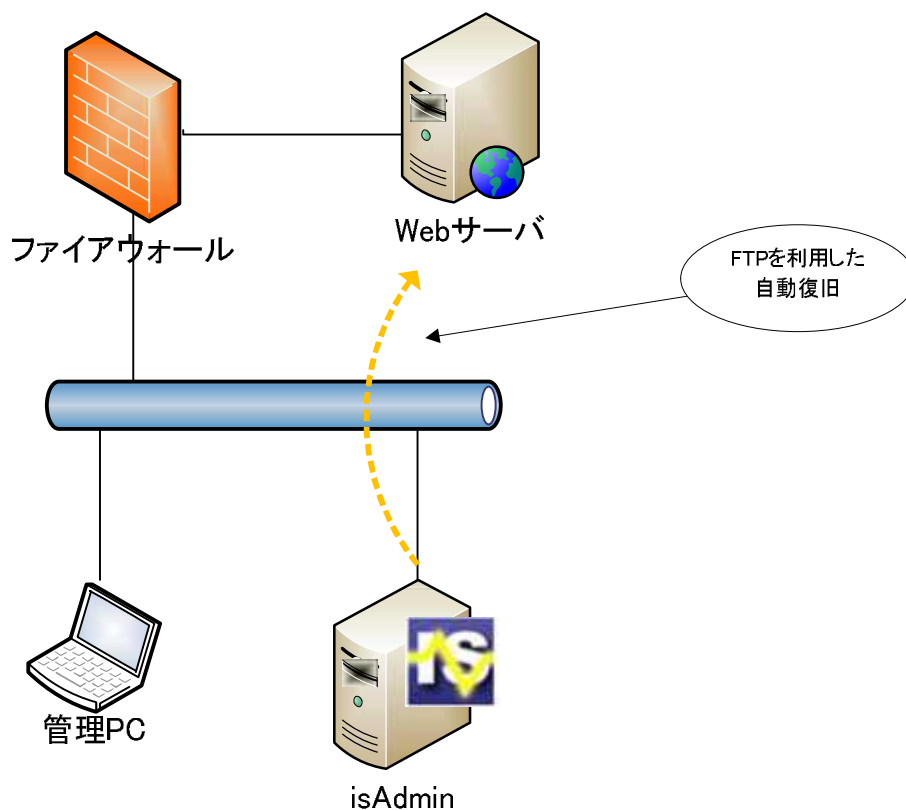
SSH Communications Security

以降の章では SSH Tectia の持つ透過的トンネリング機能を利用して、isAdmin の通信をセキュアにする方法についてご紹介します。

1.3 利用シナリオ

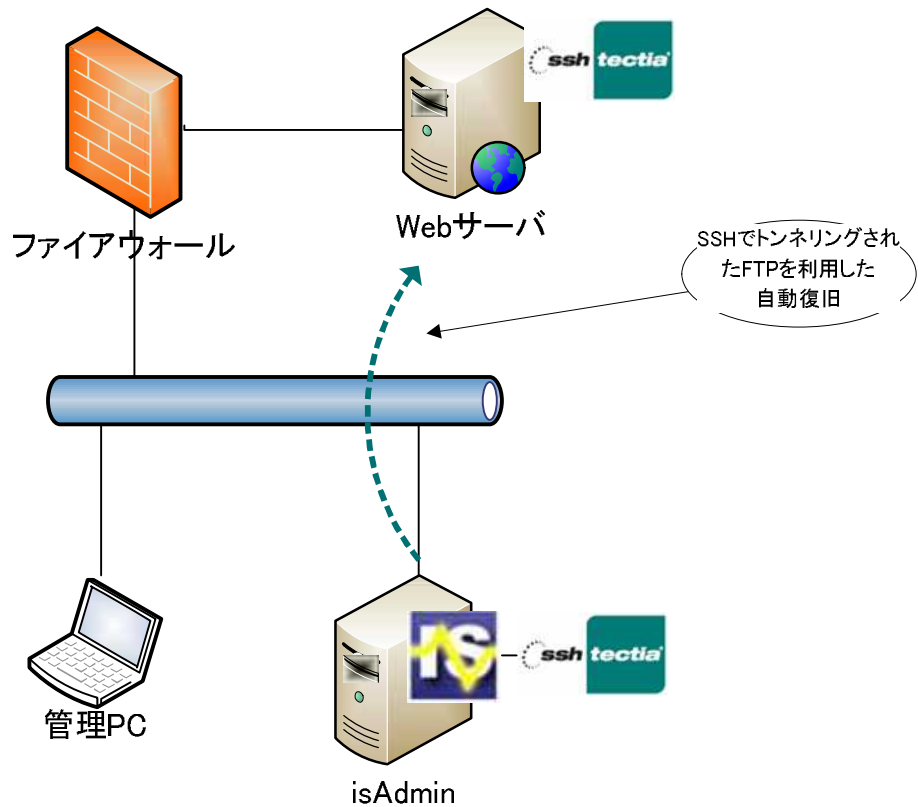
isAdmin の機能としてある自動復旧サービス/ファイルシステム改ざん監視サービスはいずれも FTP 通信が利用されていますが、SSH Tectia を導入してこれをセキュアなものへと置き換えます。この時、isAdmin への特別な設定変更は必要ありません。

1.3.1 既存の環境



SSH Communications Security

1.3.2 SSH Tectia によるセキュアな環境



1.4 ハードウェア/ソフトウェア

本書は以下の環境を元に記載されています。

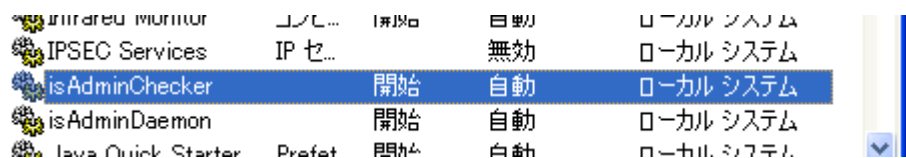
	クライアント	サーバ
OS	Windows XP SP3	Redhat Enterprise Linux 4
ソフトウェア	SSH Tectia ConnectSecure 6.0.7 isAdmin Enterprise 2.6.3	SSH Tectia Server 6.0.7
IP アドレス	192.168.1.1/24	192.168.1.100/24

2 設定

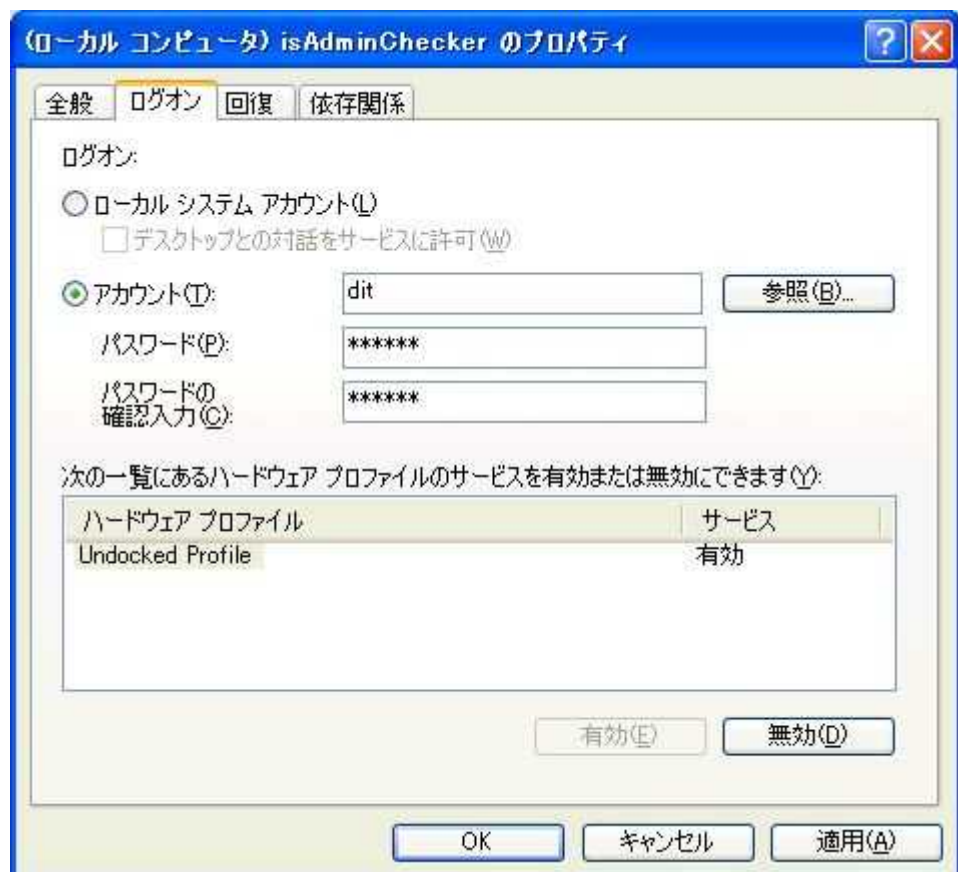
2.1 isAdmin の設定

isAdmin のアプリケーションは Windows サービスとして動作し、そのユーザ権限はデフォルトでは「ローカル システム アカウント」となっています。このままでは SSH の透過的トンネリング機能は利用できないため、あらかじめ Windows にログオンしているユーザアカウントに変更しておく必要があります。

1. スタートメニュー 設定 コントロールパネルを選択。
2. 続いて管理ツール サービスを選択してダブルクリックで開く。
3. isAdminChecker を選択、ダブルクリックで開く。



4. ログオンタブからアカウントを現在、Windows にログオンしているユーザアカウントに変更する。アカウント変更後は、サービスの再起動が必要となります。



SSH Communications Security

5. 以下のようにユーザが変更され、サービスの稼働状態が“開始”であることを確認してください。

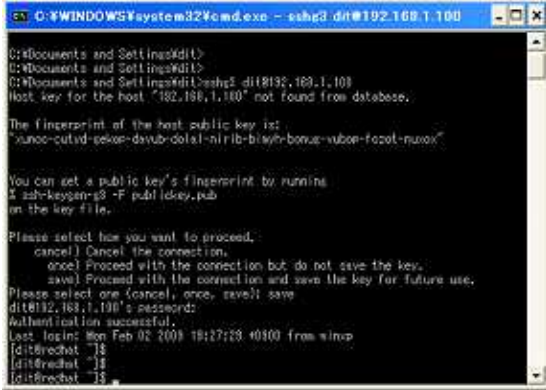
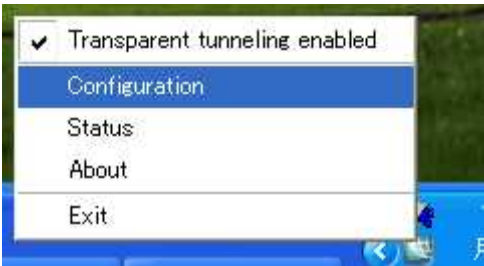
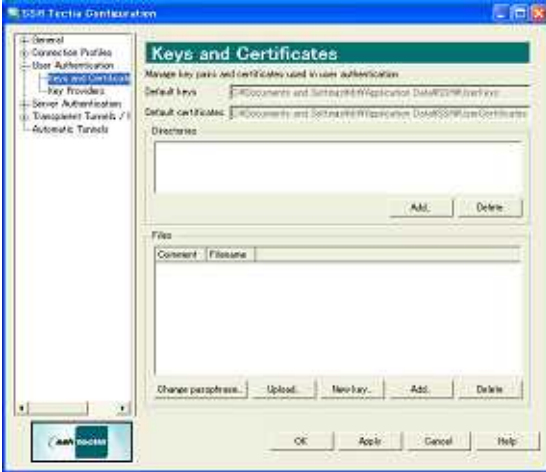


2.2 SSH Tectia の設定

これより SSH Tectia の設定を行っていきます。なお、サーバ側である SSH Tectia Server については特にアクセス制御など細かな設定を行わない限りはデフォルト設定のままです。

1	<p>The screenshot shows a Windows command prompt window titled 'O:\WINDOWS\system32\cmd.exe'. The prompt is at 'C:\Documents and Settings\fdit>' and the user has entered 'cmd'.</p>	<ul style="list-style-type: none">・スタートメニューからファイル名を指定して実行で cmd と入力し、コマンドプロンプトを立ち上げます。
2	<p>The screenshot shows a Windows command prompt window titled 'O:\WINDOWS\system32\cmd.exe - sshg3.dit@192.168.1.100'. The prompt is at 'C:\Documents and Settings\fdit>' and the user has entered 'sshg3'. The output shows a warning about a host key fingerprint not found in the database and a prompt to select how to proceed.</p>	<ul style="list-style-type: none">・sshg3 コマンドを実行してサーバとの接続性を確認します。・初めてサーバに接続する場合は、左図のように表示されますので、save と入力します。

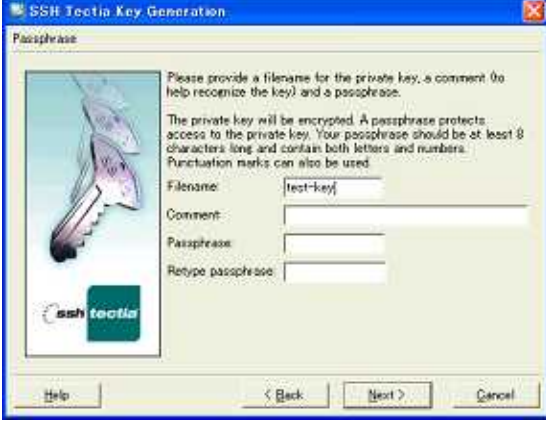
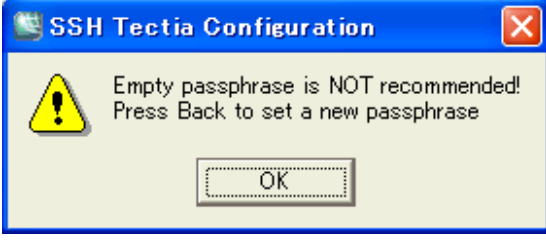
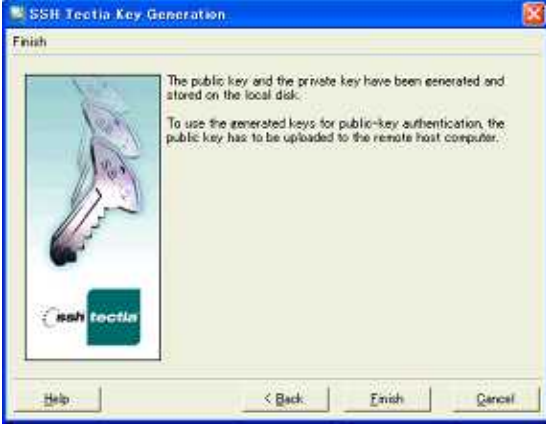
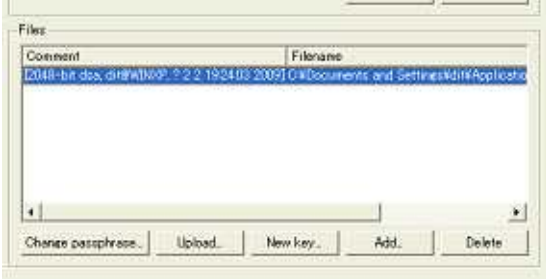
SSH Communications Security

3	 <pre> C:\Documents and Settings\ddt> C:\Documents and Settings\ddt> C:\Documents and Settings\ddt>ssh -C ddt@192.168.1.100 Host key for the host "192.168.1.100" not found from database. The fingerprint of the host public key is: "xunoo-cutid-ekoe-dvub-dolal-nirib-blayr-bonuz-vubor-fozol-nuxox" You can set a public key's fingerprint by running: % ssh-keygen -F publickey.pub on the key file. Please select how you want to proceed. cancel) Cancel the connection. once) Proceed with the connection but do not save the key. save) Proceed with the connection and save the key for future use. Please select one (cancel, once, save): ddt@192.168.1.100's password: Authentication successful. Last login: Mon Feb 02 2009 19:27:28 +0800 from winip [ddt@rechat ~]\$ [ddt@rechat ~]\$ [ddt@rechat ~]\$ </pre>	<ul style="list-style-type: none"> 次にパスワードを入力して、サーバにログオンを行います。 入力したパスワードは表示されません。
4		<ul style="list-style-type: none"> SSH 接続を自動的に行えるように公開鍵認証を設定します。 タスクトレイにある Broker アイコンを右クリックして、Configuration を選択してください。
5		<ul style="list-style-type: none"> User Authentication Keys and Certificate を選択します。 New Key... を選択して、鍵生成を開始します。



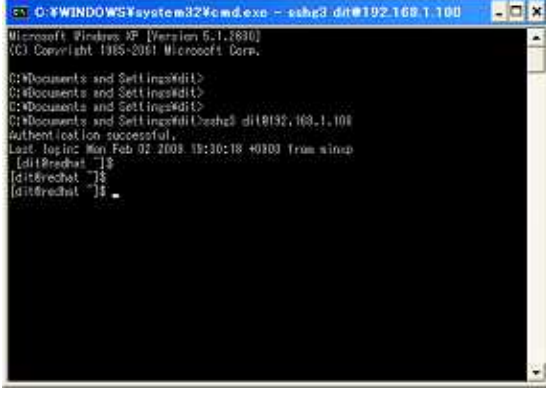
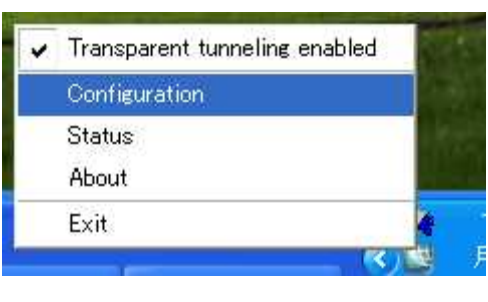
SSH Communications Security

6		<ul style="list-style-type: none">• Next を選択して、続けます。
7		<ul style="list-style-type: none">• 鍵の種類と長さを設定します。長さは大きければ大きいほど強度が高くなります。
8		<ul style="list-style-type: none">• 鍵生成が行われています。


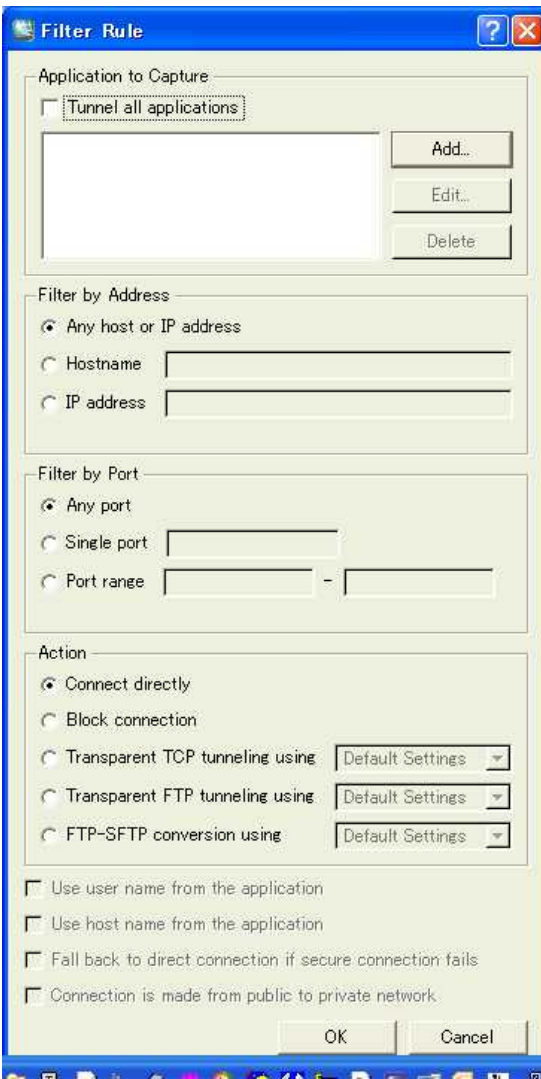
SSH Communications Security

9	 <p>The dialog box is titled "SSH Tectia Key Generation" and has a "Passphrase" sub-header. It contains a key icon on the left. The main text reads: "Please provide a filename for the private key, a comment (to help recognize the key) and a passphrase. The private key will be encrypted. A passphrase protects access to the private key. Your passphrase should be at least 8 characters long and contain both letters and numbers. Punctuation marks can also be used." Below this text are four input fields: "Filename:" with "test-key" entered, "Comment:" (empty), "Passphrase:" (empty), and "Retype passphrase:" (empty). At the bottom are buttons for "Help", "< Back", "Next >", and "Cancel".</p>	<ul style="list-style-type: none">• Filename としてファイル名 (任意) を入力します。• 通常は Passphrase を設定しますが、ここでは入力しません。
10	 <p>The dialog box is titled "SSH Tectia Configuration" and features a yellow warning triangle icon. The text says: "Empty passphrase is NOT recommended! Press Back to set a new passphrase". At the bottom center is an "OK" button.</p>	<ul style="list-style-type: none">• 警告が出ますが左のように出ますが無視してください。
11	 <p>The dialog box is titled "SSH Tectia Key Generation" and has a "Finish" sub-header. It contains a key icon on the left. The main text reads: "The public key and the private key have been generated and stored on the local disk. To use the generated keys for public-key authentication, the public key has to be uploaded to the remote host computer." At the bottom are buttons for "Help", "< Back", "Finish", and "Cancel".</p>	Finish で終了します。
12	 <p>The dialog box is titled "Files" and shows a list of files with two columns: "Comment" and "Filename". The first row is selected and highlighted in blue. The "Comment" column contains the text: "[2048-bit rsa, dsa@160: 2 192403 2005] C:\Documents and Settings\kiki\Appl...". The "Filename" column is empty. At the bottom are buttons for "Change passphrase...", "Upload...", "New key...", "Add...", and "Delete".</p>	<ul style="list-style-type: none">• 選択した鍵を選択し、Upload をクリックします。

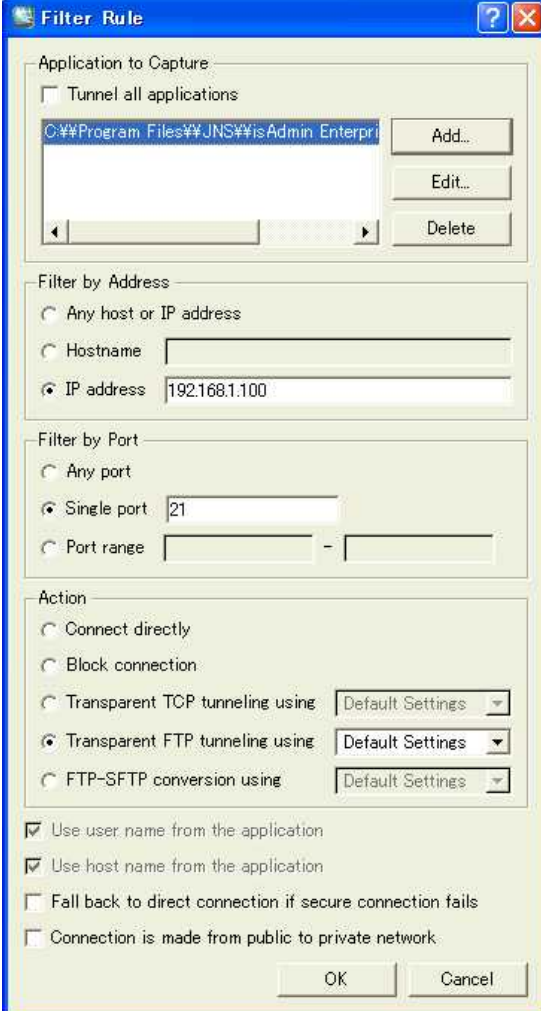
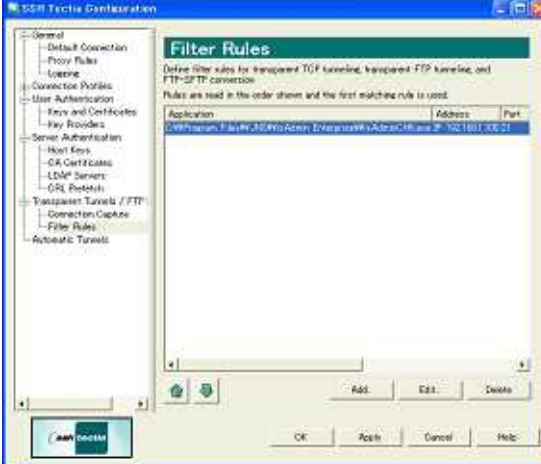
SSH Communications Security

13		<ul style="list-style-type: none">• Host name と User name を入力して、Upload をクリックします。
14		<ul style="list-style-type: none">• アップロードが終了すると、左図のように表示されます。
15		<ul style="list-style-type: none">• コマンドから接続を行い、自動的に接続できるか確認します。• すでにログインしていた場合は一度ログオンし直して確認してください。
16		<ul style="list-style-type: none">• 次に、トンネリングの設定を行います。• 再度、タスクトレイアイコンから Configuration を選択します。

SSH Communications Security

17		<ul style="list-style-type: none"> • Transparent Tunneling/FTP Security 中の Filter Rules を選択します。 • ついで Add を選択します。
18		<ul style="list-style-type: none"> • ここでは透過的トンネリングを行うためのルールを設定します。 <p>Tunnel all applications トンネルを行うアプリケーションの実行ファイルを指定。</p> <p>Filter by Address 宛先ホスト情報を入力</p> <p>Filter by Port トンネルを行うアプリケーションが使うポート番号を指定します。</p> <p>Action 透過的トンネリングの種類を設定します。FTP の場合は Transparent FTP か FTP-SFTP でなくてはなりません。</p>

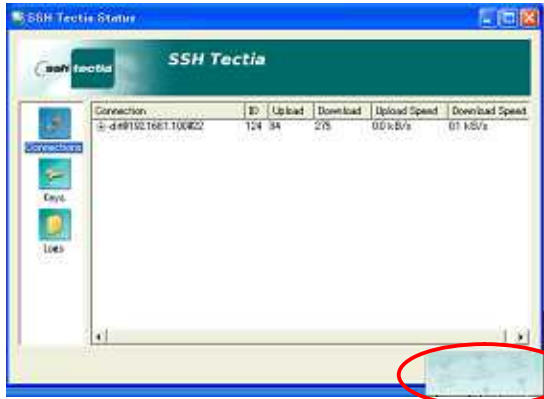
SSH Communications Security

19	 <p>Application to Capture</p> <p><input type="checkbox"/> Tunnel all applications</p> <p>C:\\Program Files\\JNS\\isAdmin Enterprise Add... Edit... Delete</p> <p>Filter by Address</p> <p><input type="radio"/> Any host or IP address</p> <p><input type="radio"/> Hostname</p> <p><input checked="" type="radio"/> IP address 192.168.1.100</p> <p>Filter by Port</p> <p><input type="radio"/> Any port</p> <p><input checked="" type="radio"/> Single port 21</p> <p><input type="radio"/> Port range</p> <p>Action</p> <p><input type="radio"/> Connect directly</p> <p><input type="radio"/> Block connection</p> <p><input type="radio"/> Transparent TCP tunneling using Default Settings</p> <p><input checked="" type="radio"/> Transparent FTP tunneling using Default Settings</p> <p><input type="radio"/> FTP-SFTP conversion using Default Settings</p> <p><input checked="" type="checkbox"/> Use user name from the application</p> <p><input checked="" type="checkbox"/> Use host name from the application</p> <p><input type="checkbox"/> Fall back to direct connection if secure connection fails</p> <p><input type="checkbox"/> Connection is made from public to private network</p> <p>OK Cancel</p>	<p>・今回のケースを設定すると左のようになります。トンネル対象のアプリケーション名は、isAdminCHK.exeです。</p>						
20	 <p>SSH Tectia Configuration</p> <p>Filter Rules</p> <p>Define filter rules for transparent TCP tunneling, transparent FTP tunneling, and FTP-SFTP conversion.</p> <p>Rules are read in the order shown and the first matching rule is used.</p> <table border="1"><thead><tr><th>Application</th><th>Address</th><th>Port</th></tr></thead><tbody><tr><td>C:\\Program Files\\JNS\\isAdmin Enterprise</td><td>192.168.1.100</td><td>21</td></tr></tbody></table> <p>OK Apply Cancel Help</p>	Application	Address	Port	C:\\Program Files\\JNS\\isAdmin Enterprise	192.168.1.100	21	<p>・以上で設定は終了です。最後にOKを選択し、ウィンドウを閉じてください。</p>
Application	Address	Port						
C:\\Program Files\\JNS\\isAdmin Enterprise	192.168.1.100	21						

3 動作確認

通信の暗号化は isAdmin の動作間隔で行われます。実際に通信が発生した場合、デスクトップ画面の右下にポップアップが表示されます。

1



Connection	ID	Upload	Download	Upload Speed	Download Speed
id#91021661.100022	124	34	275	0.0 KB/s	61.1 KB/s

isAdminCHK.exe to 192.168.1.100:21 Secure FTP tunnel to 192.168.1.100 created.

- ・アプリケーションがトンネリングされるタイミングでポップアップメッセージが右下に都度表示されます。
- ・また、タスクトレイにある Broker アイコンからステータス（接続状態、ログなど）の確認が可能です。

上記により、コンテンツ改ざんが検知された後の自動での復旧サービスのデータ転送が ID、パスワードを含め暗号化が行われるため、トラストネット DMZ 間の通信がセキュアになります。また、ファイル転送の整合性チェックなども行われるため宛先サーバに対して確実なファイル転送を行うことが出来ます。