SSH Communications Security

指紋認証をプラスしたセキュアな通信

PUPPY と SSH Tectia を組み合わせた 強固なユーザ認証とセキュアなデータ通信

Compatibility Note

2008 年 12 月

Sony 社製 PUPPY は指紋によって保護されるセキュアな USB メモリであり、昨今の情報漏洩問題を解決する非常に強力なツールとなっています。SSH Tectia ソリューションを PUPPY と組み合わせることで認証に指紋認証システムをプラスし、確実な本人確認を実現させることが可能です。

本書では、SSH Tectia のトークンによる証明書認証の機能を使い、PUPPY の指紋認証との組み合わせにより強力なユーザ認証とセキュアなデータ通信を実現する方法を紹介しています。

CONTENTS

1　シナリオ

1.1　はじめに

SSH Tectia ソリューションでは、Tectia Client から Tectia Server への接続時に必要となるユーザ認証として証明書が格納されているスマートカードおよび USB キーによる認証をサポートしています。

本書では、Sony 社製 PUPPY を使用した場合についてご紹介します。

1.1.1　PUPPY とは

指紋認証機能付きトークン『PUPPY』は、持ち運びしやすいスティックタイプの形状に指紋認証、USB トークン、ストレージの機能を一体化した個人毎に利用する認証デバイスです。ソニー独自のアルゴリズムを開発することで、高速で高性能な照合を実現しています。

PUPPY の主な機能

- 指紋認証ソリューション
- PKI トークン機能
- 情報漏えい防止ソリューション
- Windows ログオン

詳細は、下記 PUPPY のページをご参照ください。
http://www.sony.co.jp/Products/Media/puppy/index.html

1.1.2　Tectia の強力な暗号化技術と PKI 機能

世界中の政府調達基準である FIPS140-2 認定を取得した強力な暗号化と認証技術を利用することにより、SSH Tectia ソリューションはセキュアなリモートアクセスとファイル転送を実現します。

SSH Tectia でサポートしている PKI 機能は、以下のとおりです。

- X.509 v3 証明書
- HTTP、LDAP、オフライン経由の X.509 v2 CRL フェッチング
- OCSP
- PKIX CMPv2
- PKCS#7 および PKCS#12
- PKCS#8 および PKCS#11 鍵
- Windows での MSCAPI

1.2 PUPPY を使用した時の優位性について

SSH Tectia にて PUPPY を利用することにより、他の認証方法よりも、次のような点で非常に優れており、強力なセキュリティを保つユーザ認証が可能となります。

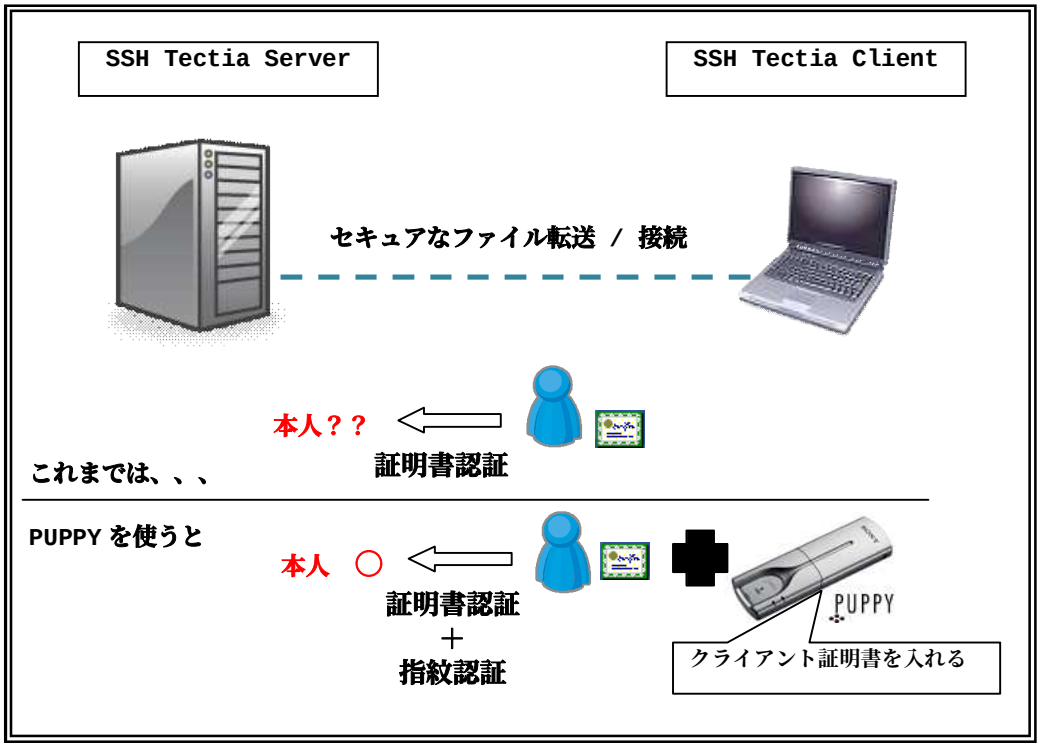
- 証明書が USB トークンのみに保持される為、Windows マシンごとに証明書をインポートする必要がなくマシンに証明書が残らない。
- 指紋認証を利用することが可能である為、セキュリティの強化が図れる。
- PUPPY の機能である Windows ログイン認証機能との併用が可能である。

1.3 利用シナリオ

SSH Tectia の証明書認証に PUPPY を利用して、強力なユーザ認証を行うまでを想定します。

1.3.1 利用イメージ

以下が PUPPY を利用したイメージです。



あらかじめ指紋登録した PUPPY に証明書をインポートすることで、登録したユーザのみが証明書を利用できるようになり、PUPPY を使用した SSH Tectia のユーザ認証を実現します。

SSH Tectia と PUPPY の組み合わせで、この機能を利用いただく事は簡単な設定で実施できます。次章以降この設定方法を具体的に示します。

1.4 ハードウェア/ソフトウェア

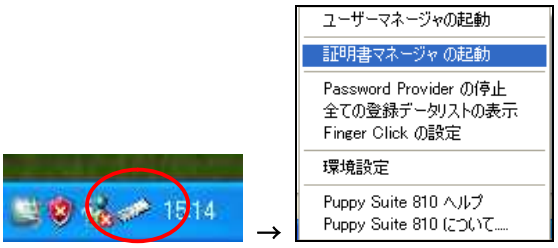
本書は、以下の環境を想定しています。

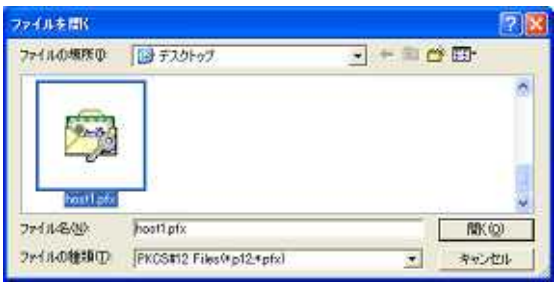
	クライアント	サーバ
OS	Windows XP SP2	Windows サーバ、Unix サーバ
ソフトウェア	SSH Tectia Client 6.0.5 PuppySuite シリーズ	SSH Tectia Server 6.0.5
ハードウェア	PUPPY FIU-850	—

2　設定

2.1 PUPPY の設定

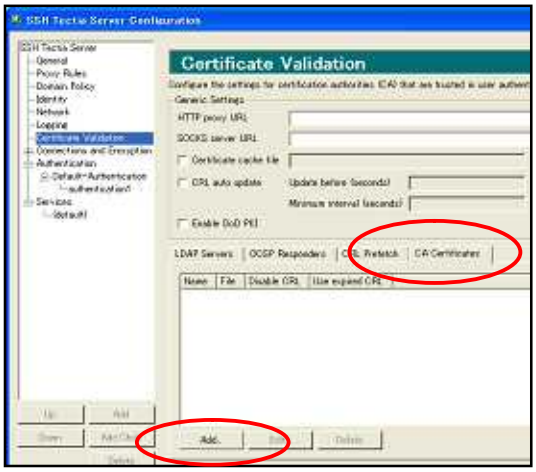
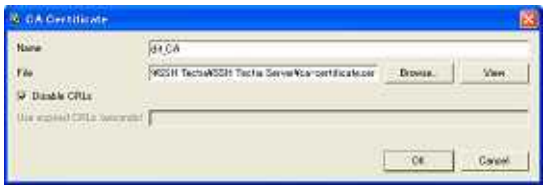
SSH Tectia のユーザ認証で使用する証明書をあらかじめ PUPPY にインポートする方法について、説明します。尚、PUPPY FIU-850 のハードウェア設定およびユーティリティソフト PuppySuite のインストール方法は、製品付属のマニュアル「PUPPY850 クイックスタートガイド」をご参照ください。また、本マニュアルは、PUPPY が PC に挿入されている状態を前提としています。

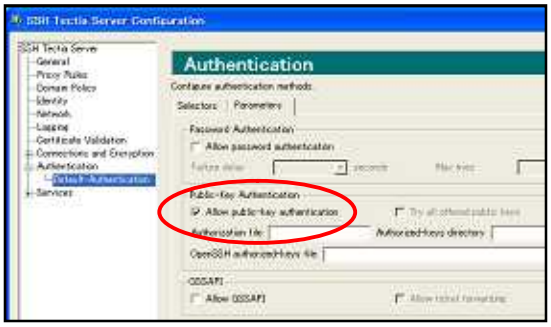
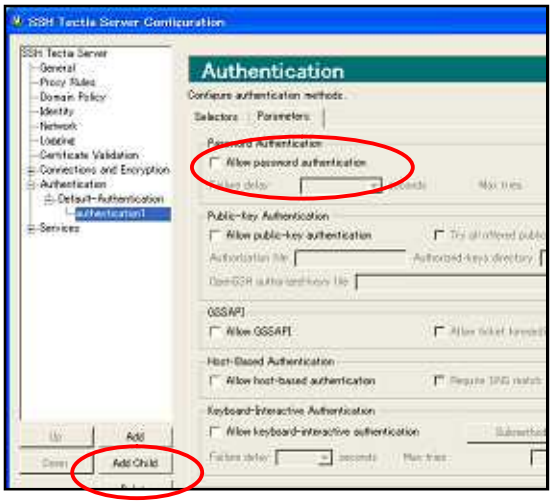
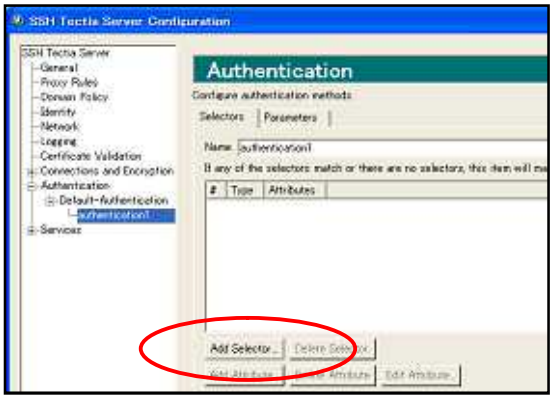
1		・タスクトレイの PUPPY アイコンを右クリックし、「証明書マネージャの起動」を選択します。
2		・PUPPY の認証画面に従い、認証を行います。
3		・問題なく認証されると、証明書マネージャが起動します。 ・「インポート」をクリックします。

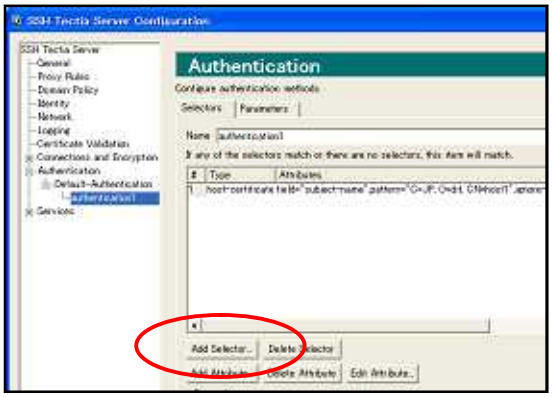
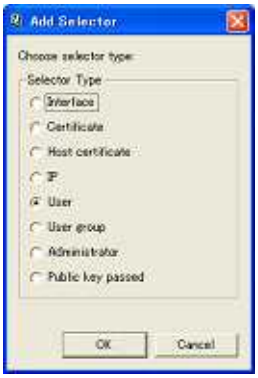
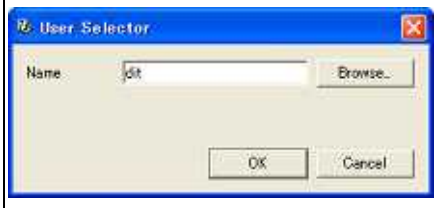
4		・インポートする証明書を選択し、「開く」をクリックします。
5		・証明書にパスワードが設定されている場合は、パスワードを入力し、「OK」をクリックします。
6		・「いいえ」をクリックします。
7		・「OK」をクリックします。
8		・証明書がインポートされたことを確認し、「閉じる」をクリックします。
		・証明書のインポートは完了です。

2.2 SSH Tectia Server の設定

証明書を使用したユーザ認証を行う場合の Tectia Server 設定について、説明します。
尚、Tectia Server のインストールはマニュアル
「SSHTectiaServer_AdminManual.pdf」をご参照ください。

1		・「スタート」-「すべてのプログラム」から「SSH Tectia Server」-「SSH Tectia Server Configuration」を選択します。 ・Configuration 画面の「GUI Mode」で”Advanced”を選択します。
2		・項目 Certificate Validation を選択します。 ・CA Cerificate タブを選択し「Add..」をクリックします。
3		・Name に名前(任意)を入力します。 **Name** | **dit_CA** ・「Browse...」をクリックし使用する CA の証明書を選択します。 ・”Disable CRLs”にチェックを入れます。 （本設定は CRL リストを使用しない場合）

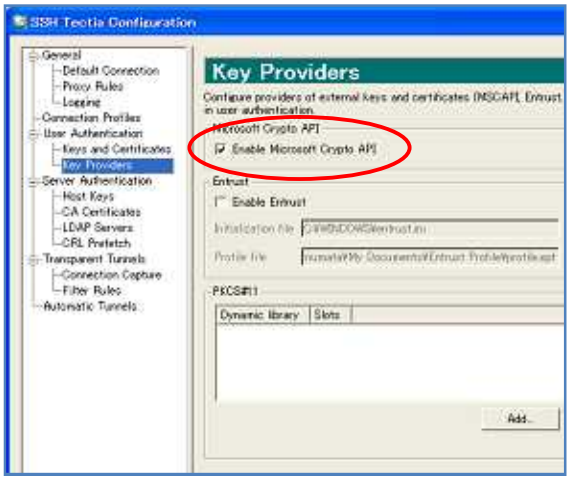
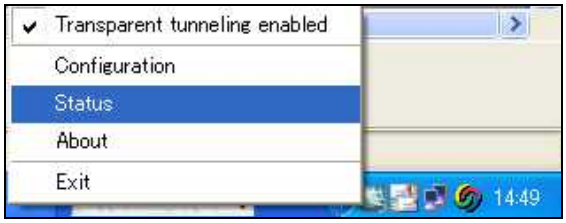
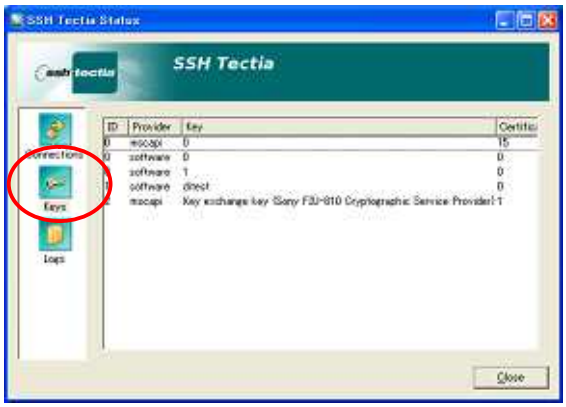
4		・項目 Authentication で Default-Authentication を選択します。 ・「Public-Key Authentication」の”Allow public-key authentication”にチェックを入れます。
5		・「Add Child」をクリックし設定項目を追加します。 ・追加された authentication1 の「Parameters」タブでデフォルトで設定されている”Allow password authentication”のチェックをはずします。
6		・次に「Selector」タブを選択し、「Add Selector..」をクリックします。
7		・「Certificate」を選択し「OK」をクリックします。

8		・Field: で"subject-name"を選択します。 ・証明書に設定されている subject の内容を Pattern: に入力します。 **Pattern**: **C=JP, O=dit, CN=host1** ・“Allow undefined”にチェックを入れ、「OK」をクリックします。
9		・更に「Add Selector...」をクリックします。
10		・「User」を選択し、「OK」をクリックします。
11		・接続先サーバのユーザ名を Name: に入力します。 **Name**: **dit**
12		・Tectia Server の再起動を行います。

2.3 SSH Tectia Client の設定

トークンを使用したユーザ認証を行う場合の Tectia Client 設定について、説明します。

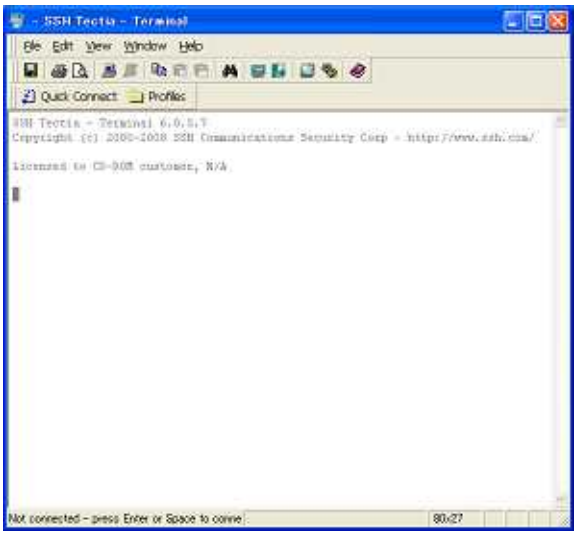
尚、Tectia Client のインストールは、マニュアル
「SSHTectiaClient_UserManual.pdf」をご参照ください。

1		・タスクトレイの broker を右クリックし、「Configuration」を選択します。 ・項目 User Authentication の Key Providers を選択します。 ・Microsoft Crypto API で”Enable Microsoft Crypto API”にチェックを入れます。 ・「OK」をクリックします。
2		・タスクトレイの broker を右クリックし、「Status」を選択します。
3		・「Keys」をクリックし、key が正常に読み込まれていることを確認します。

3　動作確認

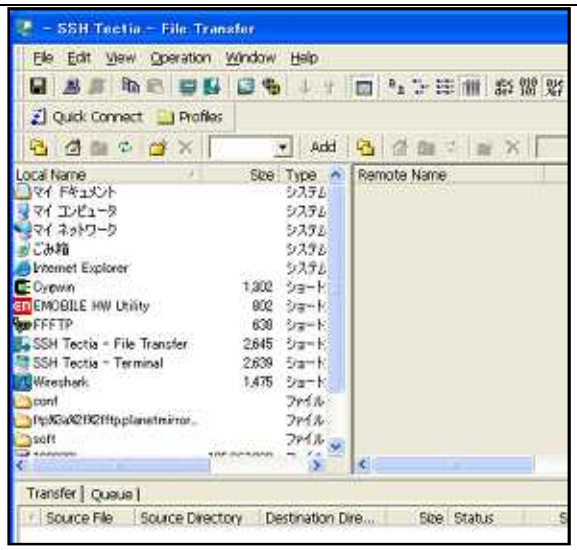
実際に PUPPY を使って、保持された証明書と指紋認証を組み合わせて、ssh または sftp 接続ができるか確認します。

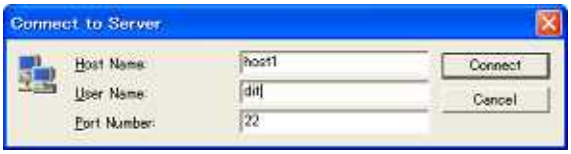
3.1 ターミナルによる ssh 接続（GUI）

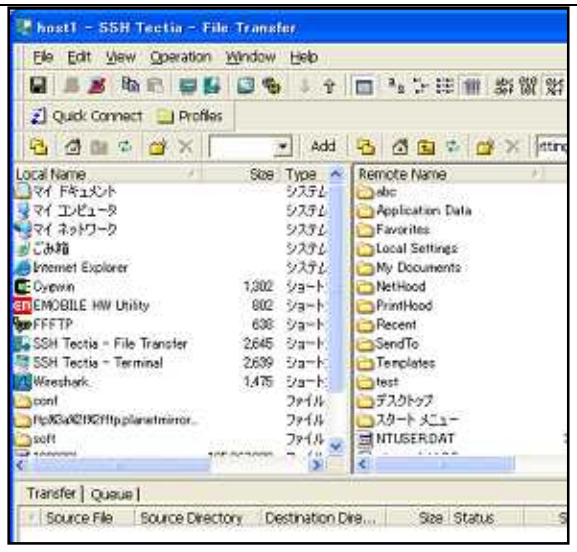
<table>
<tr><td>1</td><td> 
</td><td>・SSH Terminal を実行します。

・「Quick Connect」をクリックします。</td></tr>
<tr><td>2</td><td> 
</td><td>・接続先の Host Name、User Name を入力します。
<table><tr><td>Host Name:</td><td>host1</td></tr><tr><td>User Name:</td><td>dit</td></tr></table></td></tr>
<tr><td>3</td><td> 
</td><td>・PUPPY の認証画面に従い、認証を行います。</td></tr>
<tr><td>4</td><td> 
</td><td>・認証が行われ、セキュアな方法で対象サーバへ接続します。</td></tr>
</table>

3.2 ファイル転送（GUI）

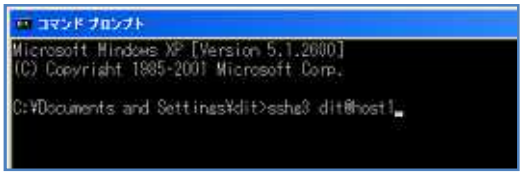
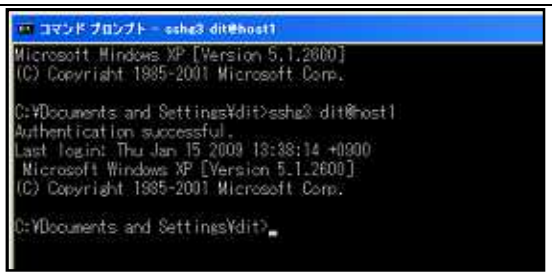
<table>
<tr><td>1</td><td> 
</td><td>・SSH File Transfer を実行します。

・「Quick Connect」をクリックします。</td></tr>
<tr><td>2</td><td> 
</td><td>・接続先の Host Name、User Name を入力します。

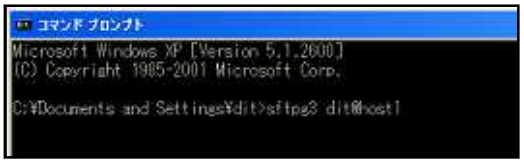
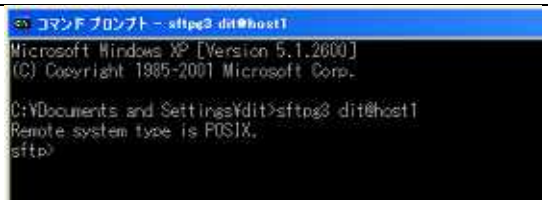
<table><tr><td>Host Name:</td><td>host1</td></tr><tr><td>User Name:</td><td>dit</td></tr></table></td></tr>
<tr><td>3</td><td> 
</td><td>・PUPPY の認証画面に従い、認証を行います。</td></tr>
<tr><td>4</td><td> 
</td><td>・認証が行われ、対象サーバへ接続します。

・セキュアなファイル転送が可能となります。</td></tr>
</table>

3.3 ssh 接続（コマンド）

1		・コマンドプロンプトを実行し次のコマンドを実行します。 >sshg3 dit@host1
2		・PUPPY の認証画面に従い、認証を行います。
3		・認証が行われ、セキュアな方法で対象サーバへ接続します。

3.4 sftp 接続（コマンド）

1		・コマンドプロンプトを実行し次のコマンドを実行します。 >sftpg3 dit@host1
2		・PUPPY の認証画面に従い、認証を行います。
3		・認証が行われ、セキュアな方法で対象サーバへ接続します。

問題なく動作確認が終了すれば、生体認証を利用したよりセキュアな方法で、リモートアクセスやファイル転送を実施する事ができます。これにより、ユーザは ID 管理のわずらわしさから解放され、セキュアな暗号化されたデータ転送が可能となります。