SSH の使い方 (3)

– Windows パソコンからの利用について –

赤坂 浩一 *　　平野 彰雄 *　　沢田 篤史 *

1　はじめに

近年、インターネットを安心して利用するために、暗号技術を用いた安全な通信方式である **SSH**(Secure SHell) が注目を集めています。

本センターでは平成 11 年 7 月に、まず汎用 UNIX 計算機 (sakura) にバージョン 1 の SSH(SSH Protocol Version 1) を導入し、その後、他の UNIX 系システム (spp,vpp) にも導入してサービスを開始し、平成 13 年 4 月から、より強度の高い暗号方式を用いるバージョン 2 の SSH(SSH Protocol Version 2) をサポートする OpenSSH へ移行してサービスを行なっています。

本稿では、前回の解説記事である本センター広報「SSH の使い方 (2) –OpenSSH への移行について –」 (Vol.34 No.2) で、紹介しきれなかった Windows パソコン (以下、 PC) からの利用について、簡単に紹介します。

2　PC 用の SSH クライアント

PC から SSH が導入されたサーバを利用するためには、 PC に SSH のクライアントソフトウェアをインストールする必要があります。

SSH のクライアントソフトウェアとしては、前々回の解説記事の「SSH の使い方 – より安全にネットワークを利用するために –」 (Vol.32 No.5) で紹介した **TTSSH** がありますが、 TTSSH は、バージョン 2 の SSH(SSH Protocol Version 2) には対応していませんので、ここでは、 SSH Communications Security 社の SSH クライアントソフトウェアである、 **SSH Secure Shell for Workstations** (以下、 SSHWin) の利用方法について紹介します。

2.1　SSHWin の入手方法

SSHWin は、 SSH Communications Security 社のホームページから入手することができますが、このソフトウェアはライセンスの管理されているソフトウェアです。利用するためにはライセンスが必要ですが、大学関連 (教員・学生・職員) の利用に関しては、無料のライセンスが提供されています。また、個人での利用に関しては、非商用ライセンスが必要となっており、非商用ライセンスに該当するかは、各自で確認してください。

SSH Communications Security 社のホームページは、以下の URL となっています。

- English Site
  `http://www.ssh.com/`
- Japanese Site
  `http://www.ipsec.co.jp/`

なお、京都大学では KUINS(京都大学学術情報ネットワーク機構) が、京都大学における非営利目的に限定したサイトライセンスを取得しており、京都大学に所属されている利用者の方は、 KUINS のホームページから入手することができますので、こちらを利用ください。

`http://www.kuins.kyoto-u.ac.jp/download/`

本稿では、英語版の SSHWin を例に紹介します。なお、本稿執筆中の最新バージョンは、SSH2(Secure Shell Ver.2.4.0) です。

* あかさか ひろかず , ひらの あきお , さわだ あつし (京都大学大型計算機センター)

2.2 SSHWin のインストール

SSHWin のインストールは簡単です。入手した実行ファイル (SSHWinSecureShell24.exe) のアイコンを PC でダブルクリックすると自動的にインストーラが起動しますので、表示されるウィンドウに従って進めば、インストールが完了します。

デフォルトでは、デスクトップにアイコンを作成するようになっているので、インストールが完了すると、デスクトップに**図 1**のような二つのアイコンが作成されます。

図 1. SSHWin のアイコン

3 SSHWin の使い方

「**SSH Secure Shell Client**」は端末エミュレータで、こちらを使って SSH サーバが動作しているリモートホストにログインします。

また「**SSH Secure File Transfer Client**」はファイル転送用のクライアントで、バージョン 2 の SSH(SSH Protocol Version 2) からサポートされた SFTP サーバが動作しているリモートホストとファイル転送を行ないます。

それでは、SSHWin による本センターの UNIX 系システムの利用方法を説明します。環境設定やカスタマイズは、後から説明します。

3.1 端末エミュレータを使う

デスクトップの「**SSH Secure Shell Client**」アイコンをダブルクリックするとターミナルウィンドウが起動します。

図 2のようにメニューバーの「**File**」をクリックし、メニューから「**Connect...**」を選択するか、**図 3**のようにメニューバーの下のツールバーのボタンをマウスでクリックすると、接続するリモートホストを指定するダイアログボックスが表示されます。

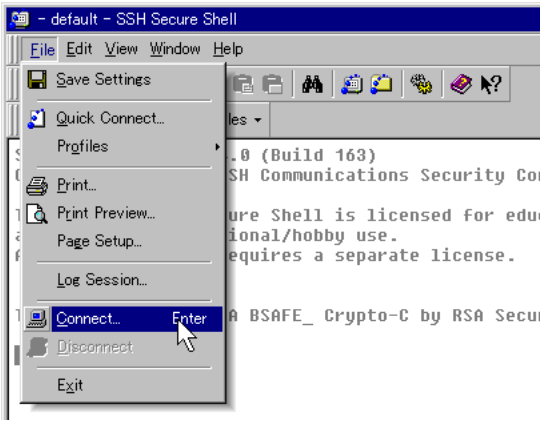

図 2. ターミナルウィンドウ (接続 1)

図 3. ターミナルウィンドウ (接続 2)

ダイアログボックスでは、**接続するリモートホスト名**と**ログイン名**、**ポート番号**、**認証方法**を指定します。ここでは、リモートホストとして sakura を例に説明します。

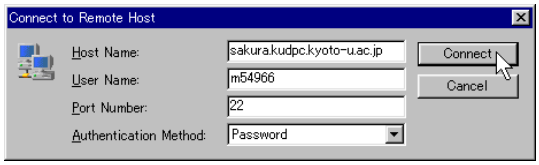

図 4. 接続用のダイアログボックス

図 4のように、「Host Name」に sakura.kudpc.kyoto-u.ac.jp 、「User Name」に本センターの利用番号 (この例では m54966) を入力します。

「Port Number」は、リモートホストの SSH サーバが任意のポート番号で動作している場合は、そのポート番号を指定する必要がありますが、通常、デフォルト (22) のままで構いません。

「Authentication Method」では、リモートホストの接続時に利用する認証方法を選択します。良く使う認証方式として、**パスワード認証**と**公開鍵認証**があります。この例では、パスワード認証で接続しますので、password を選択します。

正しく指定して、Connect をマウスでクリックします。

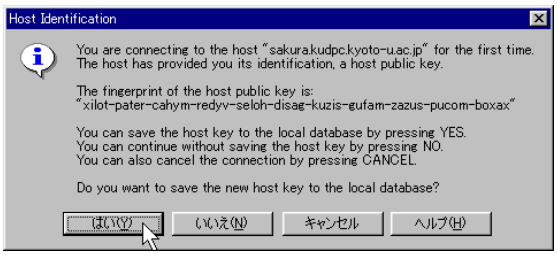

図 5. ホスト識別のダイアログボックス

初めて接続するリモートホストの場合は、送られてきたリモートホストの公開鍵が PC に保存されていないため、**図 5**のようにホスト識別のダイアログボックスが表示されますので、リモートホストの公開鍵を PC に保存する場合は**はい**を、保存しない場合は**いいえ**をクリックします。この例では、**はい**をクリックします。

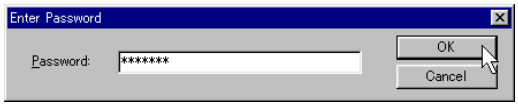

図 6. パスワード入力用のダイアログボックス

次に、**図 6**のようにリモートホストのパスワードを入力するダイアログボックスが表示されますので、正しいパスワードを入力して、OKをクリックします。

パスワードの認証に成功すると、**図 7**のように接続が完了します。

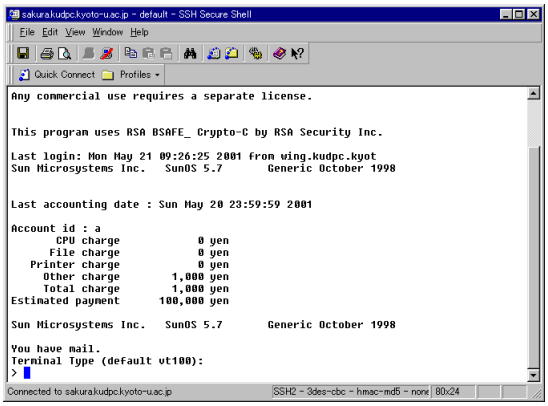

図 7. ターミナルウィンドウ (接続完了)

SSHWin では、頻繁に接続するリモートホストが複数ある場合、リモートホスト毎にプロファイルを作成し設定を保存しておくことができます。

リモートホストへの接続完了時に、**図 8**のようなプロファイルを追加するためのダイアログボックスが表示されます。

図 8. プロファイル追加のダイアログボックス

このダイアログボックスは、しばらくすると自動的に閉じますが、後からプロファイルを作成 (追加) することができますので、ここではそのままにしておきます。

3.2 ファイル転送クライアントを使う

デスクトップの「**SSH Secure File Transfer Client**」アイコンをダブルクリックするとファイル転送ウィンドウが起動します。

ファイル転送を行なうリモートホストへの接続は、先ほど説明した「**3.1 端末エミュレータを使う**」と同様ですが、既にリモートホストに接続しているターミナルウィンドウが起動している場合は、**図 9**のようにターミナルウィンドウのメニューバーの「**Windows**」をクリックし、メニューから「**New File Transfer**」をクリックするか、**図 10**のように、メニューバーの下のツールバーのボタンをクリックして、ファイル転送ウィンドウを開くことができます。

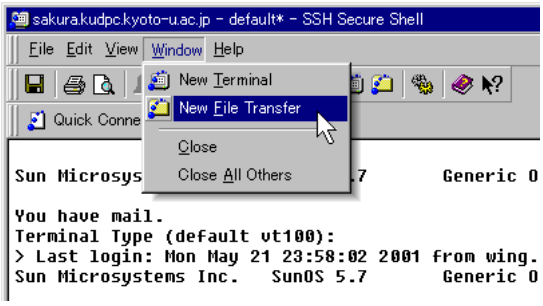

図 9. ファイル転送ウィンドウの起動 1

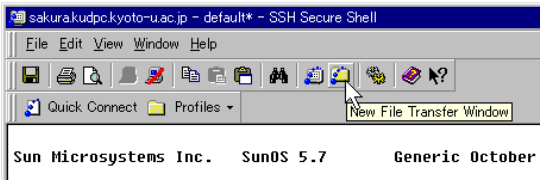

図 10. ファイル転送ウィンドウの起動 2

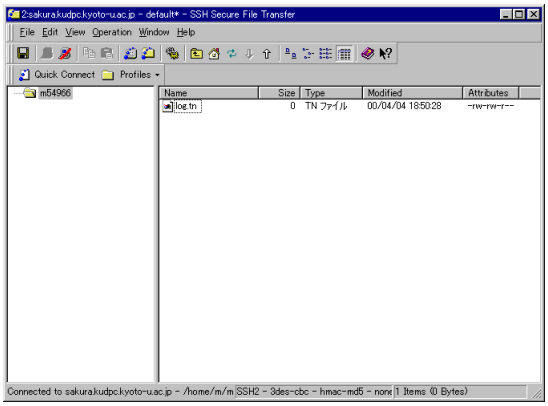

図 11. ファイル転送ウィンドウ

図 11のようにファイル転送ウィンドウでは、リモートホストのファイルが表示され、 PC からのリモートホストへのファイル転送 (Upload) やリモートホストから PC へのファイル転送 (Download)、リモートホストに新しくディレクトリ (フォルダ) を作成したり、ファイルやディレクトリの削除や名前の変更などが安全な通信経路で簡単に行なうことができます。

また、 PC とリモートホスト間のファイル転送には、コピー (Copy) &ペースト (Paste) も利用でき、ある程度、 PC を使い熟れた方には、操作しやすいと思います。更に、ファイルやディレクトリ (フォルダ) のパーミッションも変更できるので、 UNIX のファイル操作コマンドを使わずにファイルを管理することができます。

なお、デフォルトでは、 "."で始まるファイルやディレクトリ (フォルダ) は隠しファイルとして取り扱われ表示されません。

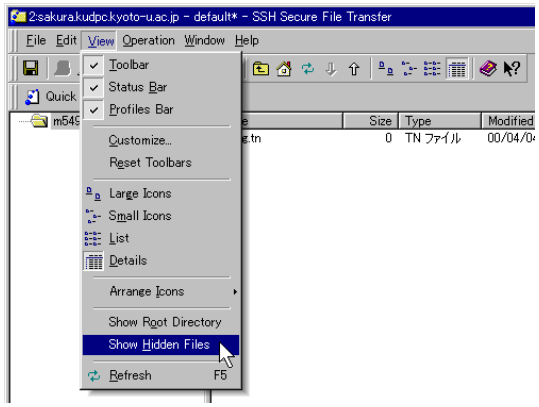

図 12. 隠しファイルの表示

隠しファイルを表示するには、**図 12**のようにメニューバーの「**View**」をクリックし、メニューから「**Show Hidden Files**」を選択します。

常に隠しファイルを表示させたい場合は、環境設定で指定し、保存しておく必要があります。

3.3 SSHWin の環境設定

ここまでで、 SSHWin の二つのアプリケーションの使い方を簡単に説明しました。

初期設定のままでも SSHWin を十分に活用できますが、ここでは、設定しておくと良いと思われる環境設定について簡単に紹介します。

環境設定を行なうには、ターミナルウィンドウもしくはファイル転送ウィンドウで、**図 13**のようにメニューバーの「**Edit**」をクリックし、メニューから「**Setting**」をクリックするか、**図 14**のようにメニューバーの下のツールバーのボタンをクリックすると、環境設定のダイアログボックスが表示されます。

環境設定のダイアログボックスでは、**図 15**のように接続するリモートホスト毎の**プロファイル設定**と全ての接続に関係する**グローバル設定**があります。

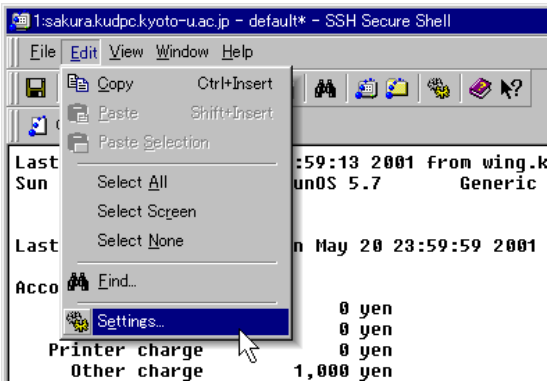

図 13. 環境設定の起動 1

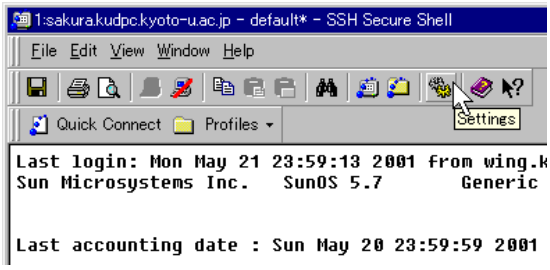

図 14. 環境設定の起動 2

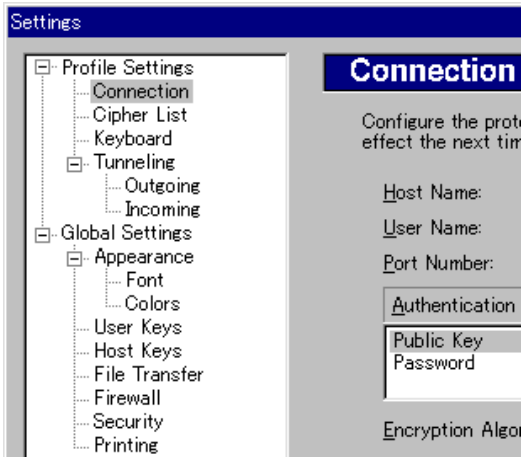

図 15. 環境設定のダイアログボックス

グローバル設定では、ターミナルウィンドウの外観、フォント・色の設定やユーザ鍵・ホスト鍵の管理、ファイル転送の設定、ファイアウォール、セキュリティ、印刷などの設定を行なうことができます。

ここでは、ファイル転送ウィンドウで隠しファイルを表示できるように、ファイル転送の設定を行ないます。**図 16**のように「**File Transfer**」をクリックしファイル転送設定に切り替え、「**Show Hidden Files**」のチェックボックスをマウスでチェックします。

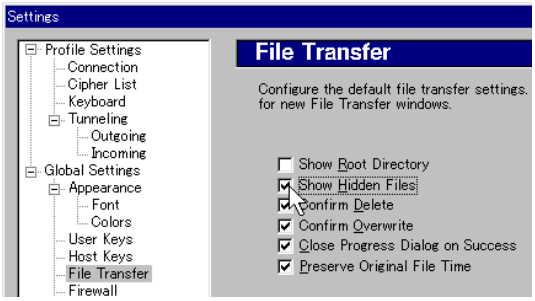

図 16. ファイル転送の設定

他のグローバル設定は、各自の好みで設定しましょう。なお、ユーザ鍵の管理については、「**3.4公開鍵認証で使う**」で説明します。

プロファイル設定では、接続するリモートホスト名やユーザ名、ポート番号、認証方法などの設定、接続で使用する暗号リスト、キーボードのマッピング、 X11 のトネンリング、受信用・送信用のトンネル (ポートフォワーディング) など設定を行なうことができます。

また、プロファイル設定は、接続するリモートホスト毎にプロファイルとして保存しておくことができますので、複数のリモートホストに接続する場合は、プロファイルとして保存して利用するのが便利です。

ここでは、既にリモートホスト (sakura) に接続した状態で、このリモートホストへの接続をプロファイルとして作成（追加）します。開いている「環境設定のダイアログボックス」は OK をクリックして閉じます。

プロファイルの作成（追加）は、**図 17**のようにメニューバーの「**File**」をクリックし、メニューから「**Profiles**」、さらに「**Add Profile...**」をクリックするか、**図 18**のようにツールバーの下のプロファイルバーをクリックし、メニューから「**Add Profile...**」をクリックします。

図 17. プロファイルの作成 (追加)1

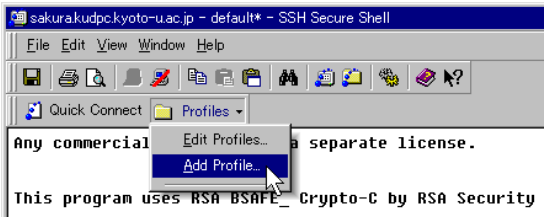

図 18. プロファイルの作成 (追加)2

図 19のようにプロファイル追加のダイアログボックスが表示されますので、プロファイルにつける名前 (この例では、sakura) を入力し、Add Current Connection to Profiles をクリックします。

図 19. プロファイル作成のダイアログボックス

接続しているリモートホスト (sakura) のプロファイルを作成 (追加) することができました。

3.4　公開鍵認証で使う

リモートホストへ公開鍵認証で接続するためには、PC 上にユーザ鍵を生成する必要があります。ユーザ鍵の生成は、環境設定のグローバル設定で行ないます。

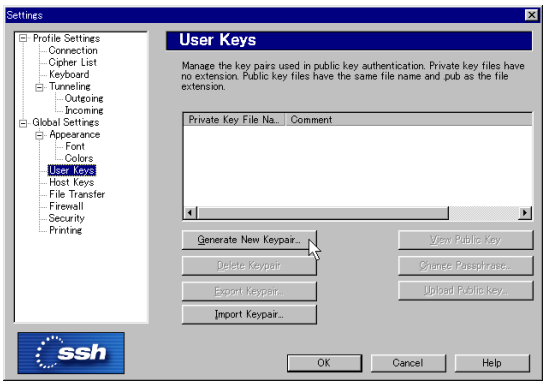

図 20. ユーザ鍵の設定

先ほど説明した手順で「環境設定のダイアログボックス」を起動し、**図 20**のように「**User Keys**」をクリックして、ユーザ鍵設定に切り替え、`Generate New Keypair...` をクリックして鍵生成ウィザードを開始します。

鍵生成ウィザードが開始すると、はじめに重要な情報が表示されますので、読み終えたら、**次へ** をクリックします。次の生成する鍵の長さもデフォルトの 1024 で構いませんので、**次へ** をクリックすると鍵の生成が開始されます。

終了すると**図 21**のように、**次へ** が現れますので、クリックして次に進みます。

図 21. ユーザ鍵の生成

次に、生成した鍵のファイル名とコメント、パスフレーズの入力を行ないます。コメントは省略できますが、ファイル名とパスフレーズは入力の必要があります。この例では、「File Name」に `my-PC`、「Comment」に `PC user Keys`、パスフレーズには適当なフレーズを入力しています。パスフレーズは確認のために、二度入力します。

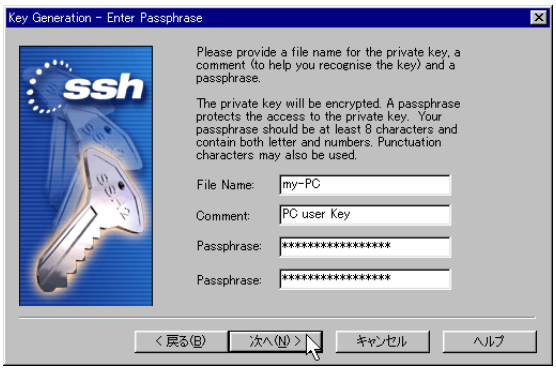

図 22. ユーザ鍵のファイル名とパスフレーズ

図 22のように入力し、**次へ** をクリックするとユーザ鍵の生成は完了です。

公開鍵認証で使うためには、生成したユーザ鍵 (公開鍵) を接続するリモートホストへ転送しておく必要がありますので、このまま続けて、**図 23**のように `Upload Public key` をクリックして公開鍵の転送を行ないます。

図 23. 公開鍵の転送

図 24のように公開鍵を転送するためのダイアログボックスが表示されます。公開鍵を保存するリモートホストのフォルダ (ディレクトリ)、リモートホスト上の認証ファイルを指定することができますが、デフォルトのままで構いません。

`Upload` をクリックすると、リモートホストに公開鍵を転送し、終了すると自動的にダイアログボックスが閉じますので、鍵生成ウィザードの **完了** をクリックして終了します。

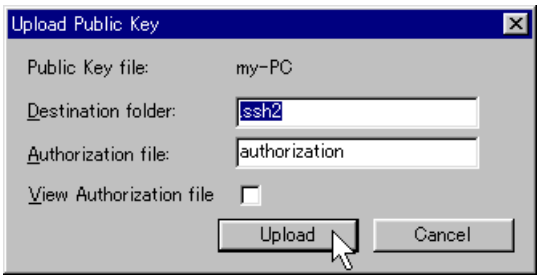

図 24. 公開鍵転送のダイアログボックス

環境設定のダイアログボックスも OK をクリックして閉じます。

【注意点】

接続するリモートホストの SSH サーバが、SSH Communications Security 社のバージョン 2 の SSH(SSH Protocol Version 2) の場合、ここまでの作業で公開鍵認証による接続が可能ですが、本センターの UNIX 系システムのように、OpenSSH のサーバに接続する場合は、以下のように鍵ファイルのフォーマット変換を行なわなければなりません。

鍵ファイルのフォーマット変換は、リモートホスト (sakura) で行ないます。ターミナルウィンドウでリモートホスト (sakura) に接続し、`ssh-keygen` コマンドにオプション (`-X`) を指定して、フォーマット変換し、これを`~/.ssh/authorized_keys2` ファイルに追記します。

`~/.ssh` というディレクトリが無い場合は、あらかじめ作成しておきましょう。

```
sakura%  mkdir ~/.ssh
sakura%  ssh-keygen -X -f s2clnt.pub →
           >> ~/.ssh/authorized_keys2
```

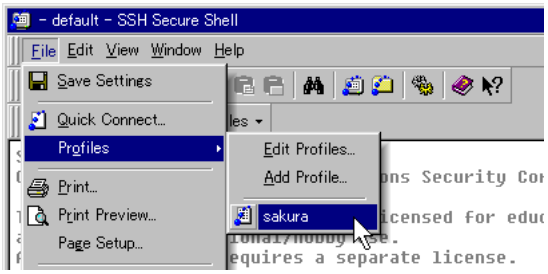

図 25. プロファイル (sakura) を指定して接続

以後、**図 25**のように、作成したプロファイル (sakura) を指定して、リモートホストに接続する場合は、**図 26**のようにパスフレーズを入力するダイアログボックスが表示され、正しいパスフレーズを入力することで公開鍵認証で接続します。

図 26. パスフレーズ入力のダイアログボックス

3.5 X11 のトンネリングについて

ローカルの PC で X サーバが動作している場合、X11 のトンネリングを有効にしてリモートホストに接続すると、リモートホストの X クライアントを安全な通信経路で PC 上で利用することができます。

X11 のトネンリングの設定は、接続するリモートホスト毎にプロファイル設定で行ないます。デフォルトでは、X11 のトンネリングは無効となっていますので、有効とする場合は、プロファイルを編集します。

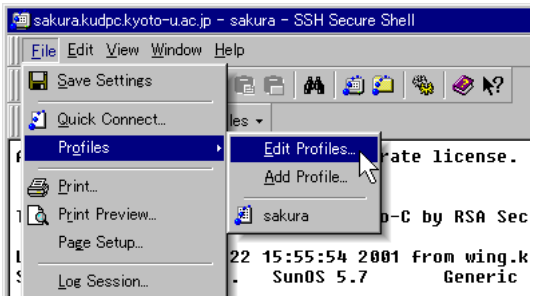

図 27. プロファイルの編集 1

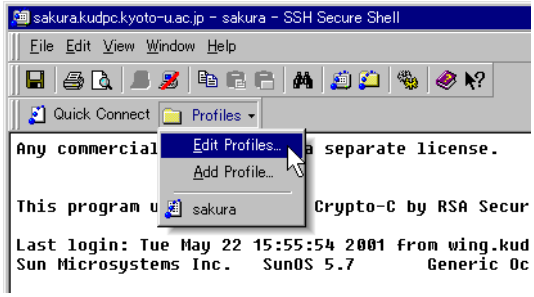

図 28. プロファイルの編集 2

プロファイルの編集は、**図 27**のようにメニューバーの「**File**」をクリックし、メニューから「**Profile**」、さらに「**Edit Profiles...**」をクリックするか、**図 28**のようにツールバーの下のプロファイルバーをクリックし、メニューから「**Edit Profiles..**」をクリックします。

X11 のトンネリングを有効するリモートホストのプロファイルを選択し、「**X11 Tunneling**」のタブをクリックし、**図 29**のように「**Tunnel X11 connections**」のチェックボックスをチェックし、`OK` をクリックします。

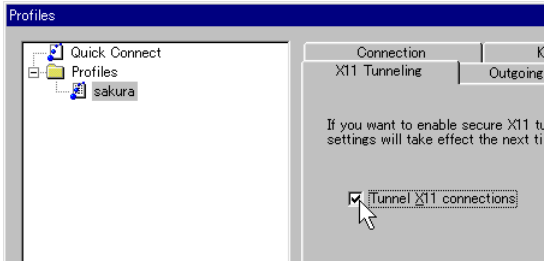

図 29. X11 のトンネリング設定

これで、 X11 のトンネリングが有効となり、リモートホストの X クライアントを安全な通信経路で利用できます。

3.6 ポートフォワーディングについて

SSH には、任意のポートを安全な通信経路に仕立てる機能 (ポート転送、ポートフォワーディング) が用意されています。

一般的に PC のメーラーは、リモートホストの POP(Post Office Protocol) サーバに接続してメールを受信し、 SMTP サーバに接続してメールを送信しています。特に POP サーバへの接続には、リモートホストのユーザ名とパスワードが必要となり、ネットワーク上にそのまま文字列が流れることになり、非常に危険です。

このポートフォワーディングを活用することで、PC のメーラーを安全な通信経路で利用することが可能となります。

SSHWin では、このポートフォワーディングを「**送信用トンネル**」と「**受信用トンネル**」という形態でサポートしています。「送信用トンネル」は PC からリモートホストへ送るデータを保護し、「受信用トンネル」はリモートホストから PC が受けるデータを保護します。通常、 PC がクライアントとなる場合は、「**送信用トンネル**」の設定を行なえば良いでしょう。

送信用トンネルの設定は、接続するリモートホスト毎にプロファイル設定で行ないますので、**図 27**または**図 28**のようにして、プロファイルのダイアログボックスを表示します。

送信用トンネルの設定を行なうリモートホストのプロファイルを選択し、「**Outgoing Tunneling**」のタブをクリックし、**図 30**のように `Add...` をクリックします。

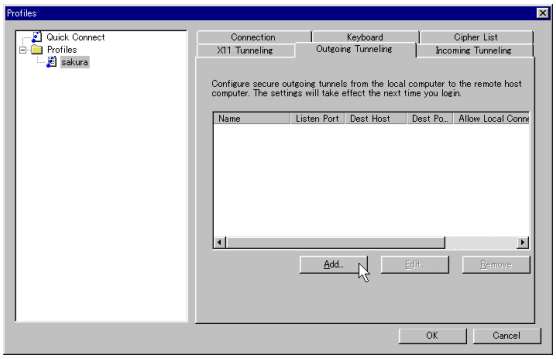

図 30. 送信用トンネルの設定

送信用トンネル設定のダイアログボックスでは、**名前**と**受信ポート**、**接続先ポート**を入力します。

この例では、リモートホスト (sakura) を POP サーバと SMTP サーバとしてメールを利用する場合の送信用トンネルの設定を行ないます。

まず、 POP サーバへの接続を保護する場合の設定を行ないます。「Display Name」には、後ですぐ連想できるような名前として pop 、「Listen Port」には、リモートホストのデータを受け取る PC 側の任意のポート番号として 9110 、「Destination Port」には、リモートホスト側の POP サーバのポート番号、 110 を入力します。

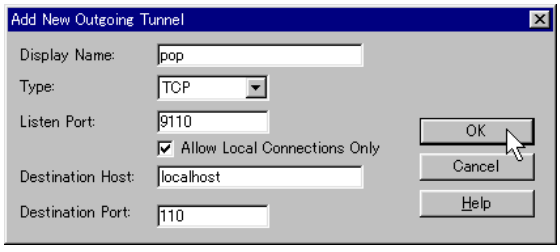

図 31. POP サーバ用の設定

図 31のように入力し、OKをクリックするとPOP サーバ用の設定が完了します。

次に、同じようにSMTP サーバへの接続を保護する設定を行ないます。**図 32**のように入力し、OKをクリックするとSMTP サーバ用の設定が完了します。

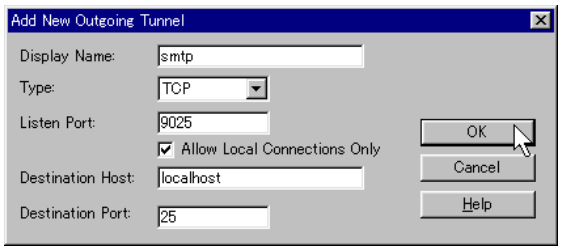

図 32. SMTP サーバ用の設定

なお、この設定は次回のリモートホスト (sakura) への接続から有効となります。

PC のメーラーの設定を紹介します。ここで例としているメーラーは、**AL-Mail32** ですが、POP と SMTP のポート番号が設定できるメーラーであれば、どのようなメーラーでも構いません。

POP と SMTP のサービスをポート・フォワーディング機能により、お使いの PC のポートに設定していますので、**図 33**のように、「サーバ情報」の「**POP3 サーバ名**」と「**SMTP サーバ名**」の欄に、localhostと記入し、**高度な設定** をクリックして、**図 34**のように、「**POP3 ポート番号**」の欄に、9110と「**SMTP ポート番号**」の欄に、9025を記入します。

これで、メーラーの設定は完了です。OK をクリックして、画面を閉じます。

図 33. AL-Mail32 のオプション画面

図 34. Al-Mail32 の高度な設定画面

実際にポートフォワーディングを利用してメーラーを使うためには、あらかじめリモートホスト (sakura) に接続しておかなければなりませんが、あまりターミナルウィンドウを使わない場合は、メール用にトンネルのみを許可するプロファイルを新しく用意しておくこともできます。

図 27または**図 28**のようにして、プロファイルのダイアログボックスを表示し、既に作成しているプロファイル (sakura) を**マウスの右ボタン**でクリックし、メニューから「**Copy**」を選択し、プロファイルをコピーします。

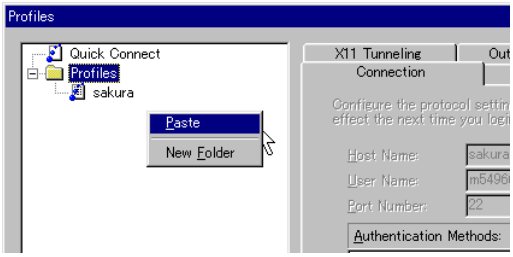

図 35. メール用のプロファイル作成

次に、**図 35**のように、適当な位置で**マウスの右ボタン**をクリックし、メニューから「**Paste**」を選択し、先ほどコピーしたプロファイルを貼り付けます。名前が重なるため名前の変更が指示されますので、適当なプロファイル名を入力します。

新しく作成したプロファイル (mail sakura) を選択し、「**Connection**」のタブをクリックし、**図 36**のように、「**Request Tunnels only (Disable Terminal)**」のチェックボックスをチェックし、OKをクリックします。

新たに作成したプロファイルを使用して、リモートホスト (sakura) に接続する場合、ターミナルウィンドウは表示されません。

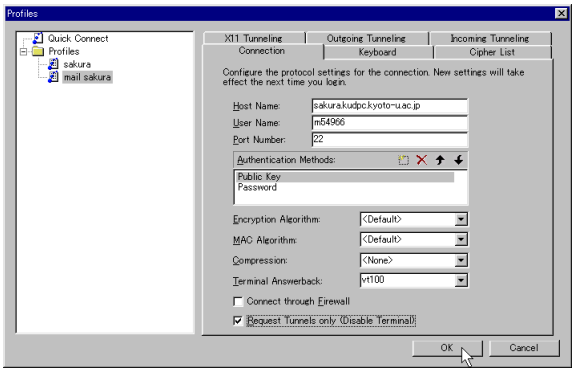

図 36. メール用のプロファイル編集

4　おわりに

今回、本センターの UNIX 系システムに導入した、より強度の高い暗号方式を用いるバージョン 2 の SSH(SSH Protocol Version 2) を PC からの利用方法について簡単に紹介しました。

今回、紹介した英語版の SSHWin は、バージョン 2 の SSH をサポートしているクライアントですが、英語版と言うことでメニューやメッセージ、ヘルプも英語であり、また、端末エミュレータであるターミナルウィンドウも残念ながら日本語が扱えません。

日本語の端末エミュレータを利用したい方は、ポートフォワーディングを活用するのが、現状ではもっとも有効な手段だと思います。

平成 13 年 3 月末に発表された日本語版 SSHWin では、メニューやメッセージなど、全て日本語化されており、非常に使いやすくなっています。

残念ながら現時点では、大学関連向けのライセンスが用意されていませんが、今後、期待したいと思います。なお、評価版は SSH Communications Security 社のホームページから入手できますので、日本語版 SSHWin も使ってみてください。

英語版から日本語版へ切り替える場合、一旦、英語版をアンインストールする必要がありますが、インストール先を変更しなければユーザ鍵ファイルや各種設定はそのまま利用することができます。なお、日本語版をインストールしてもメニューバーの表示が英語のままとなりますが、こちらは、メニューバーの「**View**」をクリックし、メニューから「**Reset Toolbars**」をクリックするとリセットされ、日本語で表示されるようになります。

日本語版 SSHWin の扱える漢字コードは、現バージョンでは SJIS に固定されているのが少し残念です。新しいバージョンでは、各種漢字コードを扱えるようになることを期待しています。

なお、最新情報は下記の URL で提供を考えていますので、本稿と合わせてご覧ください。

`http://www.kudpc.kyoto-u.ac.jp/Services/SSH/`

この記事に関して、ご意見・ご質問などございましたら、プログラム相談室までご連絡ください。

【補足】

前回の解説記事、本センター広報「SSH の使い方 (2) –OpenSSH への移行について –」 (Vol.34 No.2) の中で、「**3 SSH2 からの利用方法**」の部分について補足しておきます。

SSH2 では、公開鍵認証を行なう場合、他のホストの公開鍵を`~/.ssh2` 配下に適当な名前で置き、`authorization` と言う名前のファイルを作成し、他ホストの公開鍵を指定しますが、この他に、自分自身 (ローカルマシン) のユーザ秘密鍵ファイルを指定するために、`~/.ssh2` 配下に、 `identification` と言う名前のファイルを作成し、その中に次のような形式で秘密鍵ファイルを指定する必要があります。

```
IdKey id_dsa_1024_a
```

この場合、 `id_dsa_1024_a` が、自分自身の秘密鍵ファイルです。

この部分の説明が不足していましたので、今回補足しておきます。