

SSH を利用したセキュアな通信

専門技術班 中原 勝俊

1. はじめに

遠隔端末を利用して情報処理センターのサーバを利用する場合、telnet コマンドやTeraTerm Pro 等のターミナルエミュレータソフトを使ってログインします。この方法の場合、パスワードや通信内容が平文のまま通信路を流れてしまいますので、盗聴される危険性もあり危険です。特に現在では、外部からのアクセスに対してtelnet ポートが利用できる組織はまずないでしょう。現在は、通信路を暗号化して通信するSSH(Secure Shell)が標準となっています。また、SSH を利用することにより、ファイアーウォールを越えた通信が可能となります。そこで本稿では、学外から電子メールを送受信する方法を中心に、学外からのアクセスに利用するSSHによるセキュアな通信方法について説明します。

2. SSH でできること

SSH を利用することによりどのようなことができるのか説明します。まず、telnet の代わりとなる遠隔端末はもちろんのこと、ポートフォワーディングという機能を利用することによって以下のようなことが可能となります。

- (1) 学外から情報処理センターのメールサーバへのアクセス
- (2) 学外から情報処理センターのファイルサーバへのアクセス
- (3) 学内から外部のメールサーバへのアクセス

などです。(1)と(2)については、情報処理センターのサーバに接続元情報が登録してあれば、自宅のパソコンや出張先からアクセスできるようになります。もちろん情報処理センター内のサーバだけでなく、ご自分の教員室、研究室でサーバを立ち上げている方は、そのサーバとファイルのやり取りも可能になります。ポートフォワーディングとは、ゲートウェイのサーバにSSH 接続することにより、そのサーバを介してファイアーウォール内や外のサーバに直接アクセスすることができる機能です。SSH を使いますので、当然通信路は暗号化されてセキュアな通信となります。しかし、いかにSSH 接続といっても、すべての人やホストからの接続を許可するわけにはいきませんので、事前に情報処理センターに接続情報等を申請し、アカウントを発行してもらわなければなりません。

3. ポートフォワーディングの設定例

それでは実際に上記(1)～(3)を例として設定していきます。ですが、その前に必要となるソフトウェアをインストールしなければなりません。まずはSSH 接続のためのターミナルエミュレータソフトですが、Windows の場合、SSH 接続するためのコマンドは標準では用意されていません。そこで、以下のソフトウェアをダウンロードしてインストールしてください(Linux、MacOS X の場合、SSH は標準で利用できるのので不要です)。また、メールソフトについてはThunderbird、ファイル転送ソフトはWinSCP を利用します。もし、別のソフトを利用したい場合は、本稿で説明している設定を適宜読み替えてください。なお、ここでは、これらのソフトウェアのインストールについては説明しませんが、特に難しいことはありませんので、各自で対処してください。

[本稿で説明に利用するソフトウェア]

1 . UTF-8 TeraTerm Pro with TTSSH2 [<http://sourceforge.jp/projects/ttssh2/>]

2 . Thunderbird [<http://www.mozilla-japan.org/products/thunderbird/>]

3 . WinSCP [<http://winscp.net/jp/>]

3.1 学外から学内のメールサーバを使ってメールを送受信する設定

・TeraTerm Pro の設定

まず図1のようにTeraTerm Proを使って佐世保高専のゲートウェイサーバに接続します。

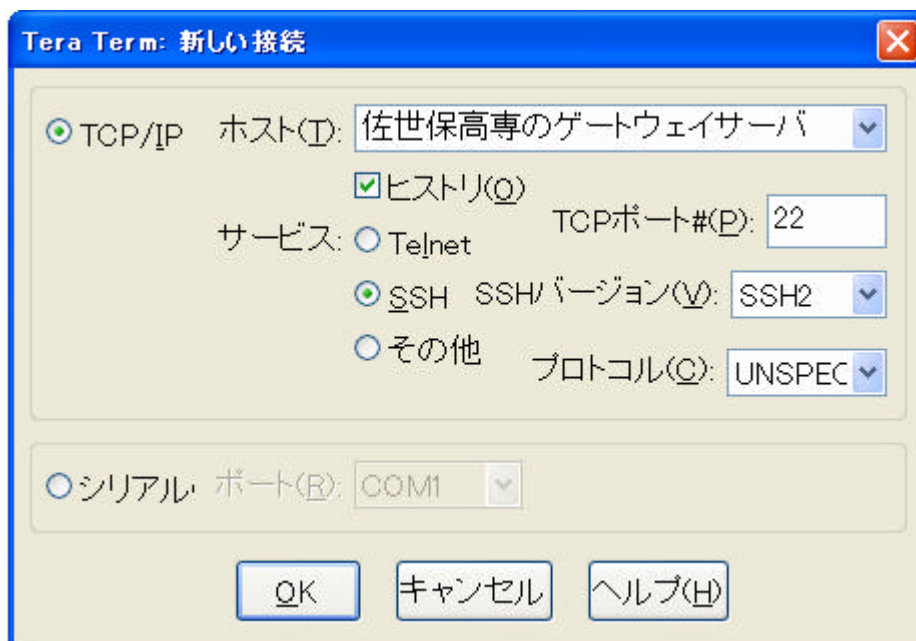


図1 . TeraTerm Pro の設定画面 1

ここでは明示していませんが、「ホスト(T)」のところには、実際には接続申請時にセンターから指定されるゲートウェイサーバ名か、IPアドレスを入力します。

続いて図2のような「SSH 認証」のウィンドウが開いたら、取得したアカウントとパスワードを「ユーザ名(N)」と「パスフレーズ(P)」の欄に入力してください。なお、最初に接続する場合、パスワードは申請時に情報処理センターから発行される仮のパスワードを使ってログインし、ログイン後直ちに passwd コマンドで必ず自分自身のパスワードに設定し直してください（アカウントが発行された後、一定期間が過ぎると仮パスワードではログインできなくなります）。

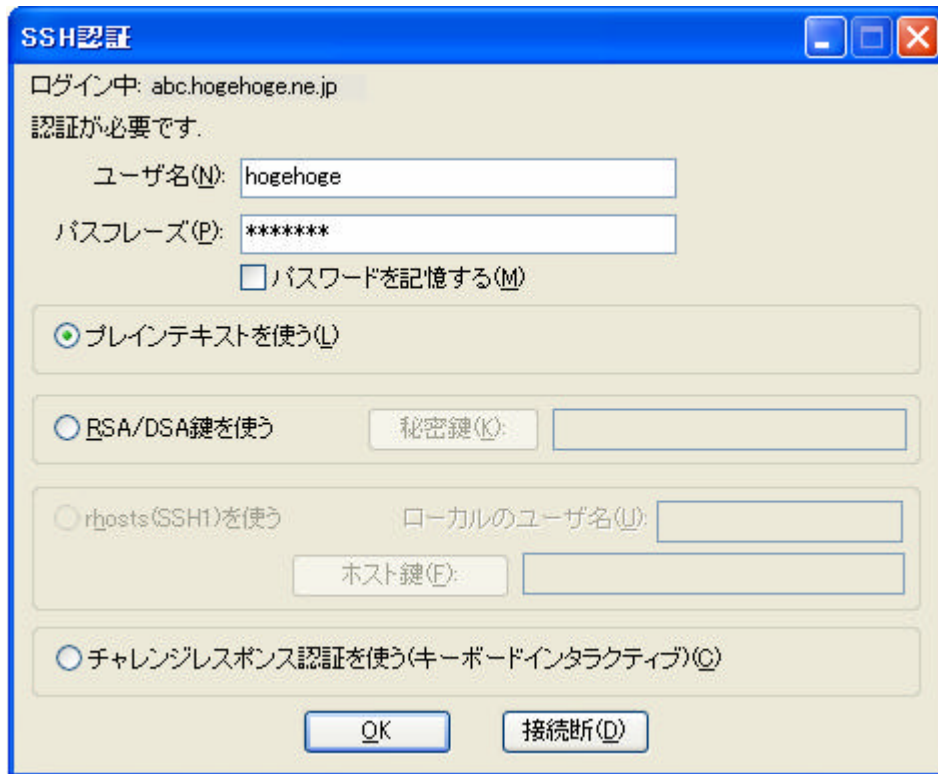


図 2 . TeraTerm Pro の設定画面 2

最初の接続の場合は、【OK】ボタンをクリックした後に図 3 のような「セキュリティ警告」が出ますが、【続行】ボタンをクリックして続行してください。なお、この処理によって SSH 接続の際に必要な暗号化通信のための鍵が作成されます。認証が完了したら図 4 のような端末のウィンドウが開くはずですが、くどいですが、先ほど説明したように最初に接続した直後には、必ず図 4 に示しているように passwd コマンドでご自身のパスワードに変更しておいてください。

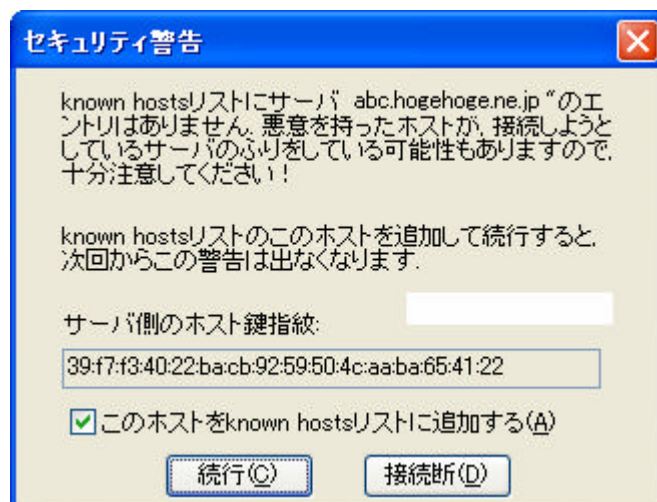


図 3 . TeraTerm Pro の設定画面 3

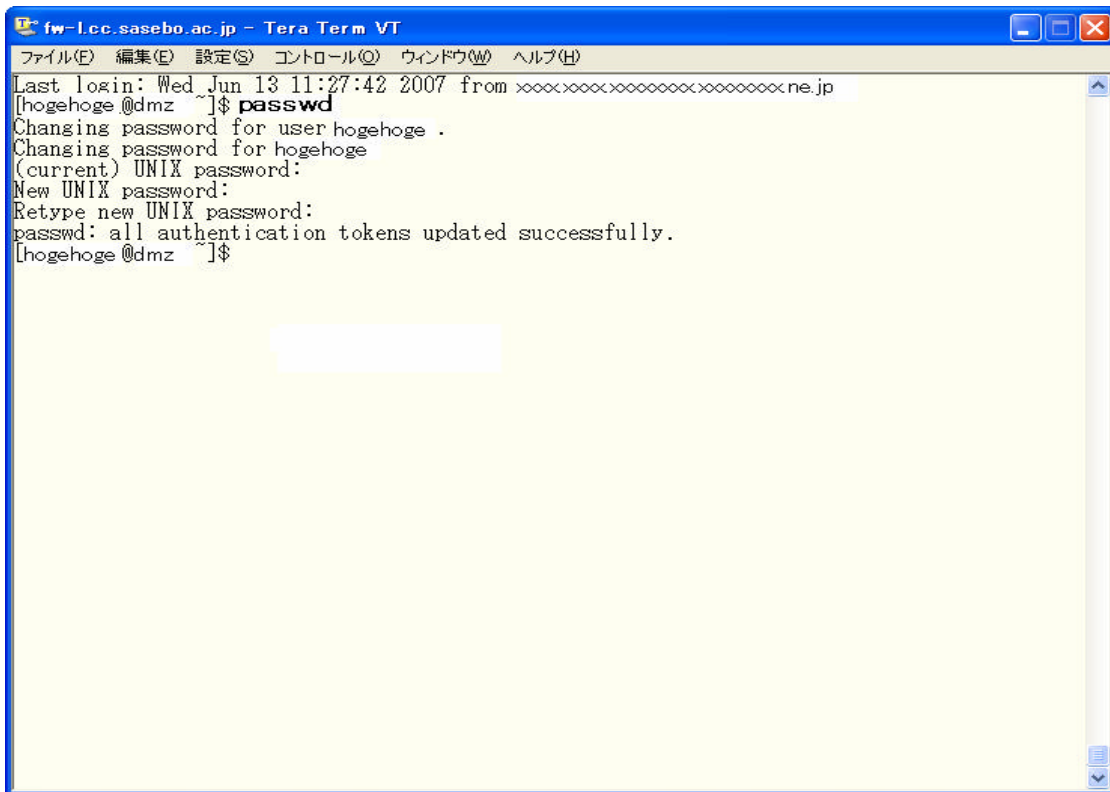


図 4 . passwd コマンド入力画面

続いてポートフォワーディングの設定をします。図 5 のように TeraTerm Pro のメニューの [設定] から [SSH 転送] を選択してください。

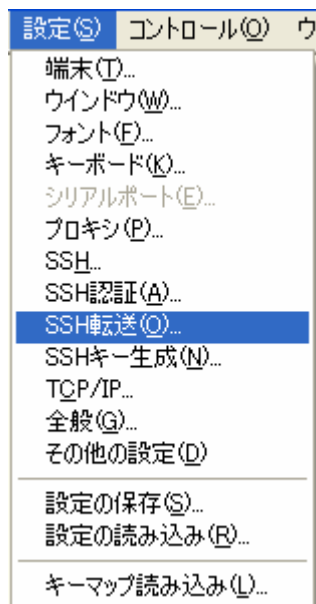
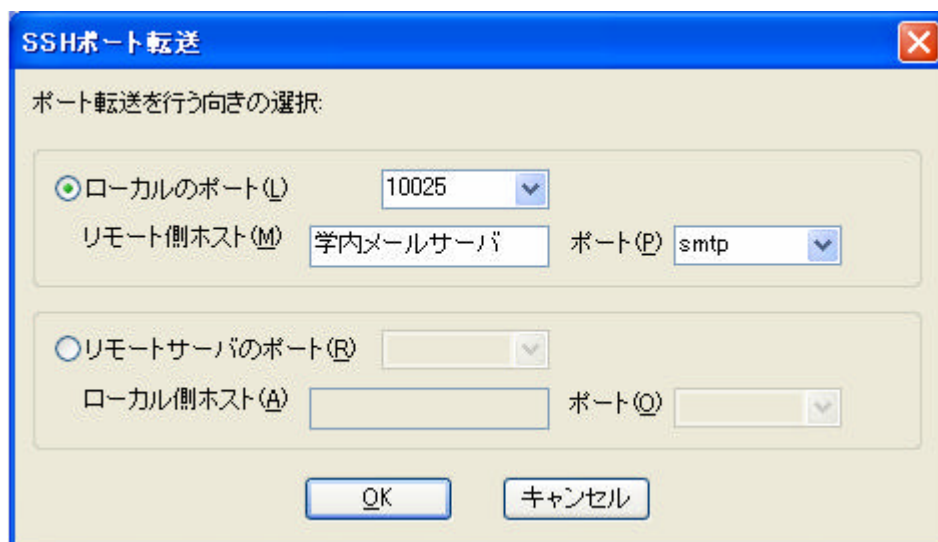


図 5 . TeraTerm Pro 設定画面 3

メニューを選択して開いたウィンドウの【追加】ボタンをクリックしてください。図 5 のような「SSH ポート転送」というウィンドウが開きます。ここでは、メールの設定を行いますので、送信と受信の

2つの設定を行わなければなりません。まず送信の設定ですが、メールの送信にはSMTPというプロトコルを使い、そのポート番号には25番が割り当てられています。このポート番号は、サーバ(リモート)側では重要な意味を持ちますが、クライアント(ローカル)側には何番を指定しても構いません。そこで、「ローカルのポート」の設定欄には、慣例的に「10025」という値を指定します。続いて「リモート側のホスト」欄には、申請時に指定されたサーバ名を指定してください(図6の中に記述されている”学内メールサーバ”という名前ではありません)。「ポート」欄には「25」という値を指定するか、欄右の選択タグから「smtp」を選択します。続いて受信側の設定ですが、受信には通常POP3というプロトコルを使い、そのポート番号には110番が割り当てられています(図7)。送信の場合と同様に「ローカルのポート」の設定欄には「10110」という値、リモート側の「ポート」欄には「110」という値を設定するか、「pop3」を選択します。IMAPを利用している人は、同じようにローカルポートに「10143」、リモートポートに「143」か「imap」を指定してください。



SSHポート転送

ポート転送を行う向きを選択:

ローカルのポート(L) 10025

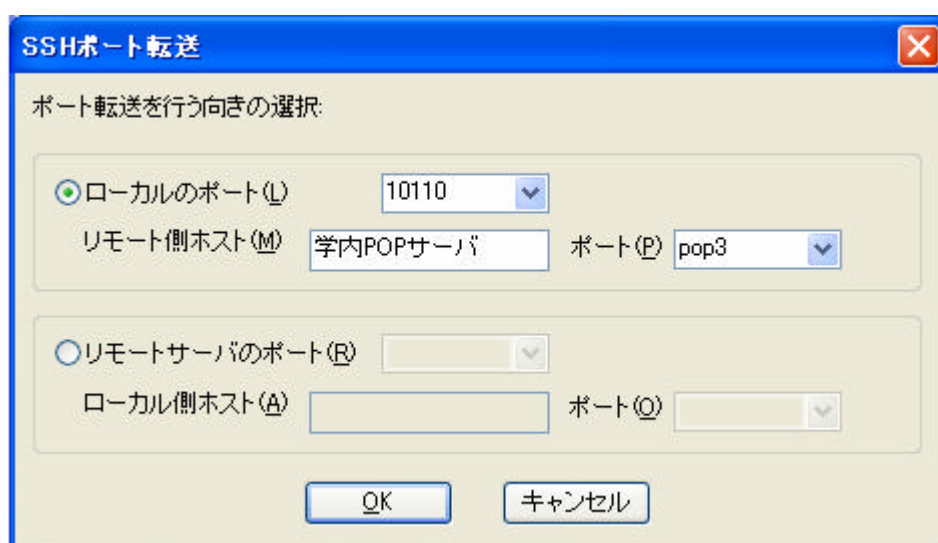
リモート側ホスト(M) 学内メールサーバ ポート(P) smtp

リモートサーバのポート(R)

ローカル側ホスト(A) ポート(Q)

OK キャンセル

図6 . TeraTerm Pro 設定画面 4



SSHポート転送

ポート転送を行う向きを選択:

ローカルのポート(L) 10110

リモート側ホスト(M) 学内POPサーバ ポート(P) pop3

リモートサーバのポート(R)

ローカル側ホスト(A) ポート(Q)

OK キャンセル

図7 . TeraTerm Pro 設定画面 5

以上の設定が完了したら、メニューの[設定]から[設定の保存]を選択して、「TERATERM.INI」というファイルに設定した内容を上書き保存してください。以上で学外からメールを送受信するためのポートフォワーディングの設定は完了です。続いてメールソフト側の設定を行います。

・メールソフトの設定

Thunderbird の設定をします。まず送信用(SMTP)の設定ですが、図 8 のように「サーバ名」の欄に「localhost」と指定するところが注意点です。「ポート番号」欄には、TeraTerm Pro の SSH 転送の設定の際に指定した「10025」番を指定します。「ユーザ名」欄には、学内のメールサーバに登録しているユーザ名を指定します。つまり、自分自身のメールアドレスの「x x x@post.cc.sasebo.ac.jp」の x x xの部分になります。

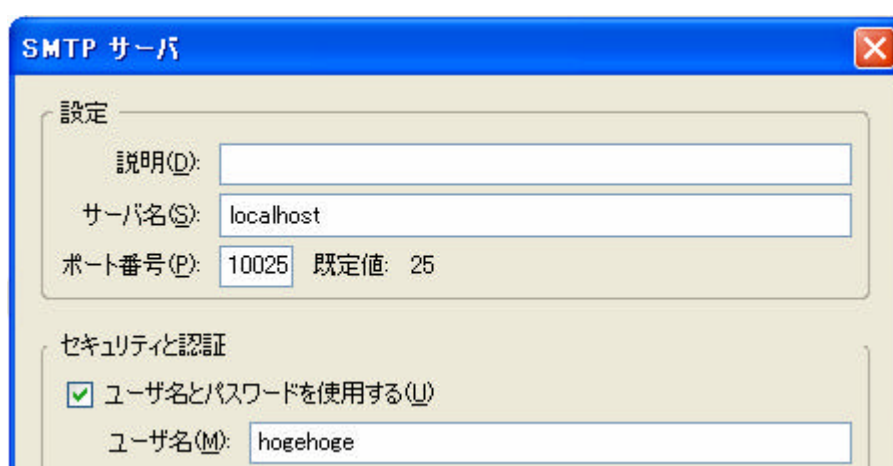


図 8 . Thunderbird の設定画面 1

続いて受信用(POP3)の設定も同じように、「サーバ名」の欄に「localhost」、「ポート」欄に「10110」番を指定します(図 9)。

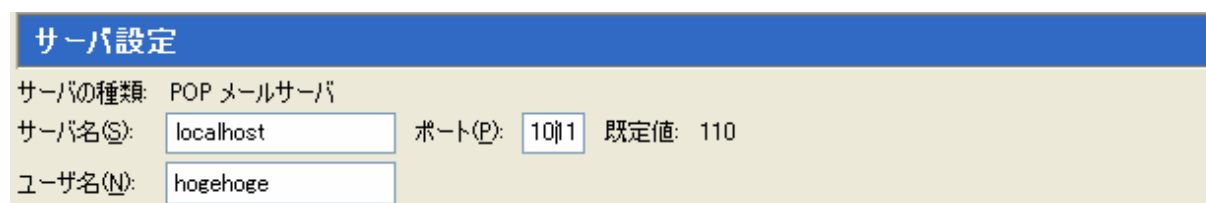


図 9 . Thunderbird の設定画面 2

以上でメールの設定は完了です。IMAP を利用している人は、受信設定を IMAP 用に読み替えてください。設定が完了したらメールを送受信してみてください。学内にいるときと同じように学外でもメールが送受信できるようになるはずですが、メールの送受信は、常にTeraTerm Pro を起動した状態で行ってください。TeraTerm Pro が起動していないとポートフォワーディングは行われず、メールの送受信はできませんので注意してください。

) 上記のようにメールの受信には、通常 POP と IMAP というプロトコルが利用されます。一般的にメールが利用され始めた初期の頃は、IMAP をサポートしているメールソフトが少なかったことから、現在でも IMAP の利用者が少ないのですが、最近のメールソフトでは、ほとんど IMAP もサポートされています。POP と IMAP の違いは、メールボックスの取り扱い方が違うという点です。メールの受信は、一見同じように見えますが、POP はローカルのコンピュータ、つまり、利用者のパソコンにメールをダウンロードして、そこにメールボックスが作成されるのに対し、IMAP はサーバ上にメールボックスが作成されます。このことから、職場と自宅といった複数の場所からメールを送受信する場合は、IMAP の方が便利です。IMAP に対応するメールソフトがあれば、Linux、Windows、MacOS X、Solaris 等、どのような OS であってもまったく同じようにメールが読み書きできます。例えば、休日に自宅の Windows マシンでメールを見て、不要なメールを削除し、メールボックスを整理していたとします。次の日出勤して職場の Linux マシンでメールソフトを起動したとき、メールボックスの内容は、整理した後の状態になっているのです。また、パソコンを新しく変えた場合とか、人事異動で使っていたパソコンが変わった場合、それまで利用していたパソコンに保存しているメールの移行に苦慮しているという話をよく聞きます。その場合でも IMAP でしたら何の問題もありません。古いパソコンでは設定を削除して、新しいパソコンでは新たに接続の設定をするだけです。ただし、IMAP も良い点ばかりというわけではありません。メールを読む際にネットワークを介するため、処理に時間がかかります。また、サーバにメールを残すため、セキュリティや容量の面でサーバに負荷をかけてしまう等、運用で気をつけなければならない点もあります。ただし、POP の場合でもサーバにメールを残すという設定をしている場合は、サーバへの負荷という点では同じになりますし、重要なものはローカルマシンのメールボックスにダウンロードしてしまえば問題はありません。と言っても、勘違いしないで欲しいのですが、私は POP よりも IMAP を推奨しているわけではありません。設定の容易さや使いやすさ、スピードといった点では、POP の方が勝っていると思います。いずれにせよ、どちらにも一長一短がありますので、各自でご判断ください。なお、google 等で「POP IMAP」などというキーワードで検索すると、ページが多数ヒットしてきますので、それらを参考にしてみるのもよいかと思います。

3.1 学外から学内のサーバにファイルを送受信する設定

ポートフォワーディングを利用することによって、学外から学内のファイルサーバにアクセスして、ファイルをダウンロード、アップロードすることも可能です。メールの送受信の場合と同じように、最初に TeraTerm Pro でポートフォワーディングの設定をします。図 10 のように、「ローカルのポート」の設定欄には「10022」という値、リモート側の「ポート」欄には「22」という値を設定します。「SSH ポート転送」のウィンドウで【追加】ボタンをクリックして「SSH ポート転送」ウィンドウを開いてください。

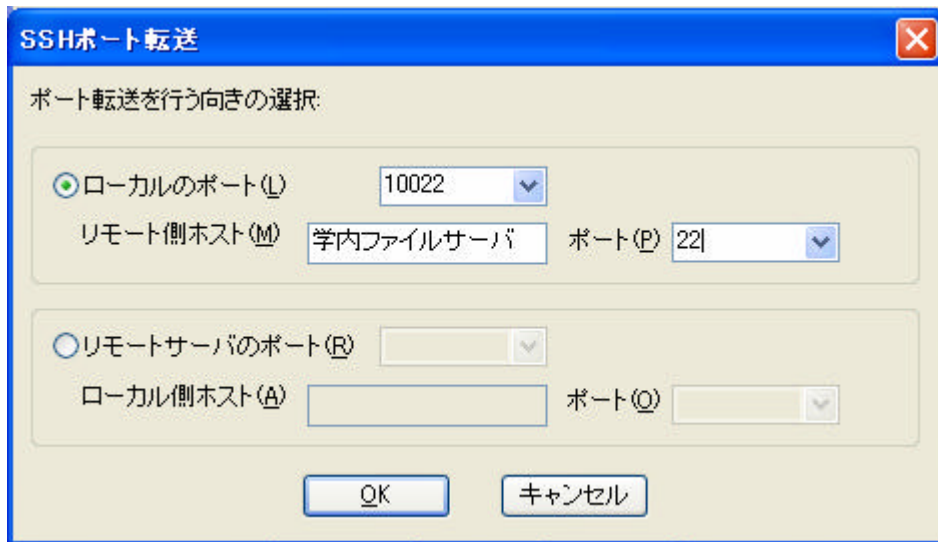


図 10 . TeraTerm Pro の設定画面 6

以上の設定が完了したら、「TERATERM.INI」ファイルに設定した内容を上書き保存してください。続いてファイル転送ソフト側の設定を行います。

・ファイル転送ソフトの設定

WinSCP の設定を行います。WinSCP を起動したら開く「WinSCP ログイン」ウィンドウで [新規] ボタンをクリックしてください。図 11 のようにホスト名等の設定を行うウィンドウが開きます。そこにメールの場合と同じように「ホスト名」欄に「localhost」、「ポート番号」欄に「10022」番を指定してください。ユーザ名まで記述したら [保存] ボタンをクリックしてください。続く「セッションの保存名」にはわかりやすい名称を指定して、[OK] ボタンをクリックしてください。以上で接続のための設定は完了です。

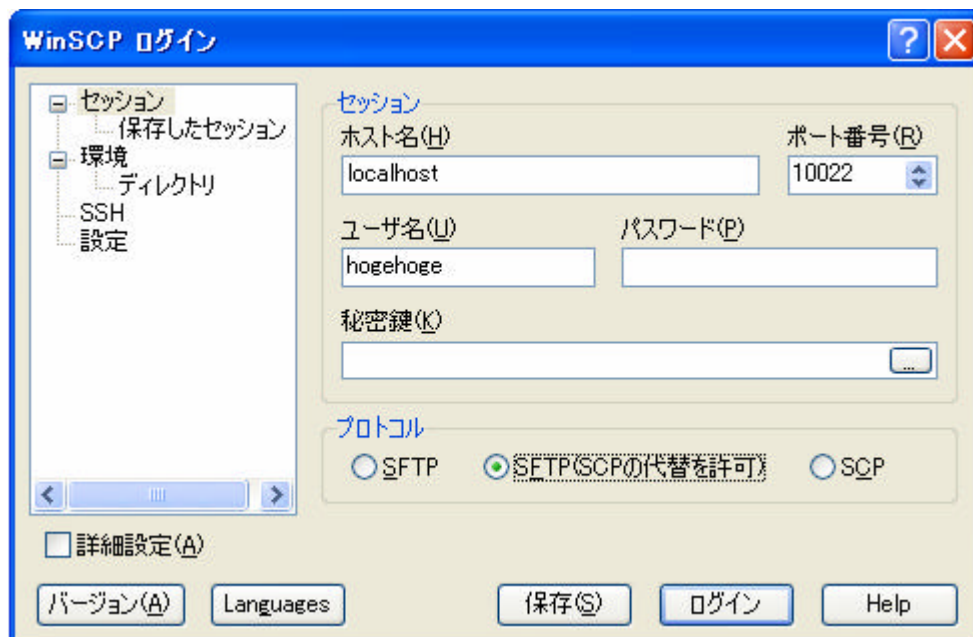


図 11 . WinSCP の設定画面 1

設定が完了したら、「WinSCP ログイン」のウィンドウに先ほどの保存時に指定した名称が表示されますので、そこを選択して [ログイン] ボタンをクリックします。WinSCP を利用する場合、ゲートウェイと接続先のサーバが SSH で接続されるため、初めて接続するサーバでは、図 12 のような警告が出ます（最初だけ）が、ここでは [はい] ボタンをクリックして次へ進んでください。

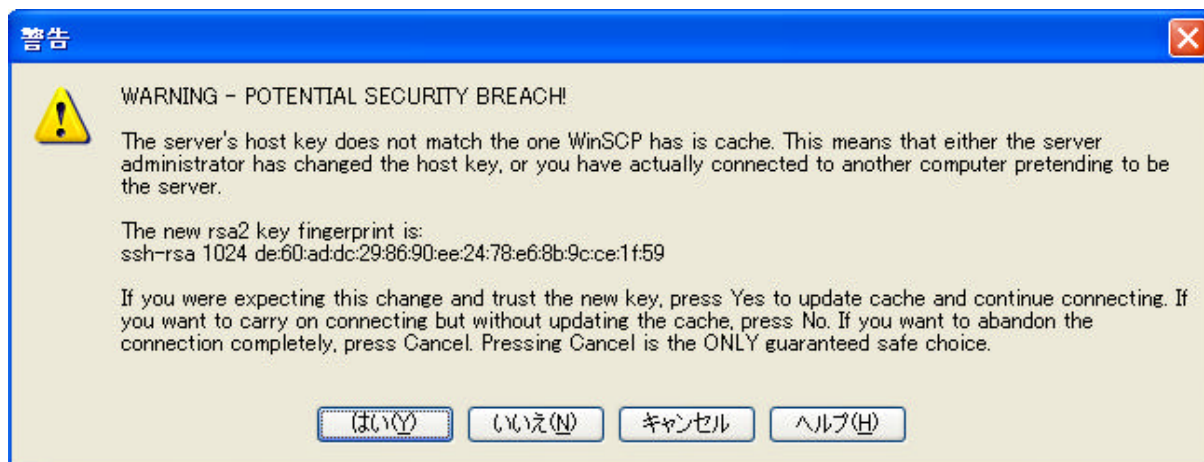


図 12 . WinSCP の設定画面 2

その後、学内ファイルサーバのパスワードを入力すれば、図 13 のような FTP ソフト等で見慣れたウィンドウが表示されます。このウィンドウの左側がローカルのパソコン側、右側がサーバ側となり、学外からファイルのダウンロード、アップロードが可能となります。

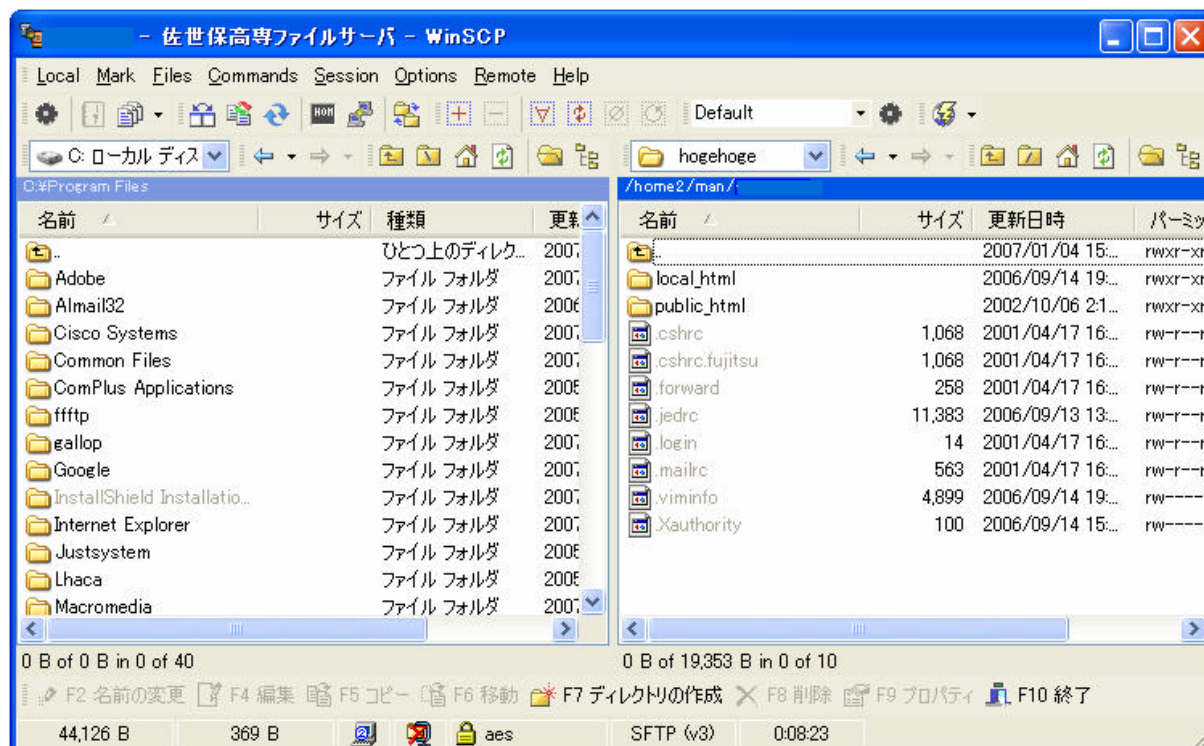


図 13 . WinSCP の画面

) ファイル転送には通常FTP というプロトコルが利用されます。FTP プロトコルをポートフォワード
ィングする場合、ユーザ名、パスワードなどの認証の部分は暗号化されますが、転送されるデータの
部分は暗号化されません。学外から接続する場合、当然その間はインターネットが介在します。学内
で利用する場合は、途中でデータが改ざんされるとか、盗聴されるといった危険性はほとんど考えな
くてもいいのですが、様々な人がつながっているインターネットを介した通信を行う場合は、できる
限り安全な通信方法で通信することをお勧めします。ファイル転送でも現在ではFTP よりも SSH を
利用した SFTP が標準になっています。そこで、学外からのファイル転送には WinSCP 等の SSH に対応
したファイル転送ソフトを利用してください。WinSCP は、FFFTP 等の FTP クライアントソフトと使い
方などの点でほとんど差がなく、使いやすいソフトウェアです。

3.3 学内から学外のメールサーバを使ってメールを送受信する設定

学内から学外のメールサーバに対して直接メールを送受信する方法を説明します。ポートフォワ
ィング機能を利用することにより、このような接続も可能となります。ただし、その場合、当然学
外に自分のメールアドレスがあるサーバが存在しており、かつそのサーバがインターネットを介し
て smtp と pop3 等の接続を受け付けるということが前提になります。設定に関しては、3.1 項をそのま
ま参考にすることができます。TeraTerm Pro のポートフォワードィングの設定では、図 6、7 を参考に
「リモート側ホスト」に学外の smtp サーバと pop3 サーバを指定します。メールソフトの設定では、
図 8、9 をそのまま参考にしてください。以上の設定で学内から学外のメールサーバに対して直接メ
ールの送受信が可能になります。

4. おわりに

1990 年代以降インターネットは飛躍的に発展し、電話に代わる情報通信のインフラとして、今後ま
すます定着していくことが予想されます。しかし、一方で不正アクセスや個人情報漏洩問題等、情報
セキュリティの脆弱さに対しては、まだまだ不十分な面が多いのも現実です。情報セキュリティを確
保するための究極の対策は、インターネットにつながらないことです。しかし、それは本末転倒であり、
もはやインターネットから得られる情報は、教育・研究に限らず、あらゆる面で社会生活には欠かせ
ないものとなっています。そのため、組織、個人に関わらず、ファイアウォールやウィルス対策など、
対応すべき情報セキュリティ対策をしっかりと行った上で、上手にインターネットを利用していくこ
とが重要であると思います。