

SSH のポートフォワードを使ったメールサーバへのアクセス方法について

Windows XP+Portforwader 編

2010/8/6 改訂版

情報企画室ネットワークオフィス

Tel:2450

imr-net@imr.tohoku.ac.jp

金研では不正アクセスを防ぐ目的でネットワークにファイヤーウォールを導入しております。最近のインターネット事情を考えますと、安全を守るためには外部からの不正アクセスは可能な限り排除する必要があることはご理解いただけたと思います。

それでは、金研内部から外部へのアクセスについてはどうでしょうか？

「内部からのアクセスは厳しくなくてもいいのでは？」という感じは確かにするのですが、仮に金研内へ侵入を受けた場合、侵入者は第三者組織への不正アクセスの目的に金研を踏み台にすることが考えられ、この結果として金研外の組織の業務に支障が出た場合、その組織からは金研からの不正侵入に見えますので、損害賠償請求の対象に金研になることも考えられます。これはネットワーク経由の侵入のケースだけでなく、構内に立ち入られて情報コンセンタを使用されるケース、無線 LAN の設定不備で第三者に使用されてしまうケースも考慮しますと、それを防ぐためには内部から外部へのアクセスに対しても同様な制限を設けておく必要があります。

金研内外のコンピュータへ自由にアクセスできる環境が理想なのですが、ファイヤーウォールによってユーザーの皆様には不便を強めていることは否めないのが、大変申し訳なく感じています。しかし、最近のインターネット事情を考えますと、インターネットの一部を構成している組織では、ファイヤーウォールの導入が必要不可欠であることはご理解いただけたと思います。

このような事情で、金研の内部と外部の境界となる部分にファイヤーウォールが導入されているため、ファイヤーウォール内部に保護されているサーバ等へのアクセスは外部から直接行うことができません。同様に、ファイヤーウォールの内部に接続されているマシンから外部のサーバ等を利用する場合も直接行うこともできなくなっています。そのため、外部から金研内部へ、あるいは金研内部から外部への通信が必要な場合は、SSH(Secure Shell)の利用を申請していただいて

1.SSH サーバによる認証

2.通信経路上を流れるデータの暗号化による保護

を行っております。

このドキュメントでは金研のファイヤーウォールの外側にあるマシンから、SSH のポートフォワード機能を使ってファイヤーウォール内のメールサーバにアクセスする方法について説明しています。また、ファイヤーウォールの内側のマシンからファイヤーウォールの外側（インターネット上）にあるサーバ（メールサーバ以外でも可能です）へのアクセスも SSH の設定の変更だけで可能ですのでこのドキュメントを参考にしてください。

それでは、以下の流れに沿って SSH のポートフォワードを使ってファイヤーウォール内のメールサーバにアクセスする方法について説明いたします。

なお、ここでは Windows マシンを対象としておりますので、これ以外のマシン（Macintosh、UNIX）については別途お問い合わせください。

- ・必要なソフトウェア（TeraTerm、PortForwarder）の入手とインストール
- ・TeraTerm での SSH2 プロトコルと RSA/DSA 暗号による認証鍵ペアの作成と利用申請
- ・PortForwarder の設定ファイルの作成とメールソフトの設定変更
- ・SSH のポートフォワードの動作確認

1. Windows 上で SSH のポートフォワードを行うために必要なソフト

(1) 「TeraTerm」の入手とインストール

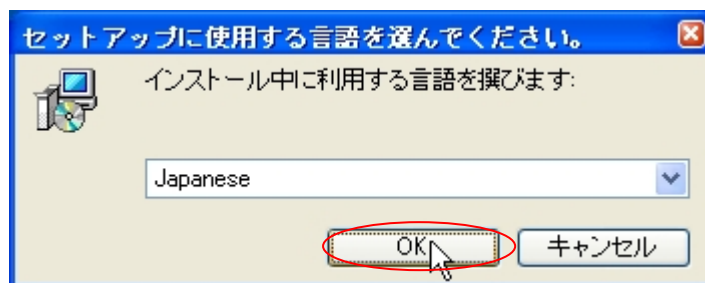
Windows 上で動作するターミナルエミュレータで、Telnet、SSH 接続ができます。

なお、TeraTerm 単体でも PortForwarding 機能がありますので、使いやすい方法を選択してください。

入手先 <http://tssh2.sourceforge.jp/>

最新版(2010/8/6 現在の最新版は 4.66)をダウンロードして、W クリック

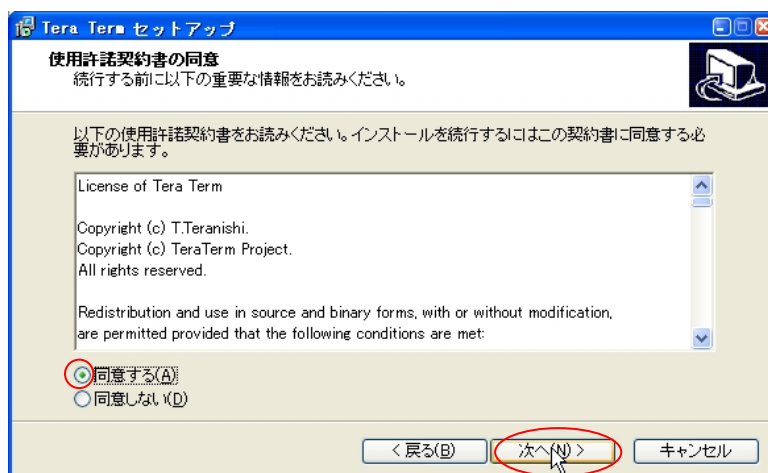
(a) インストーラーが起動するので Japanese/English のいずれかを選択



(b) インストール開始

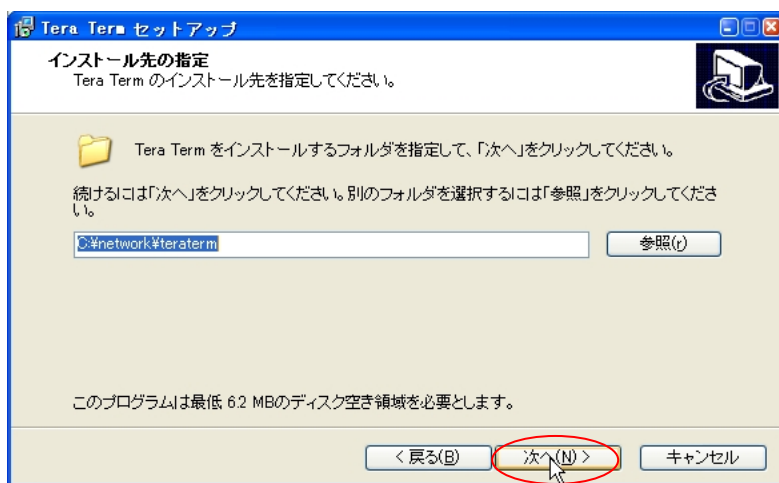


(c) 「同意する」を選択して「次へ」



(d) インストール先を選択

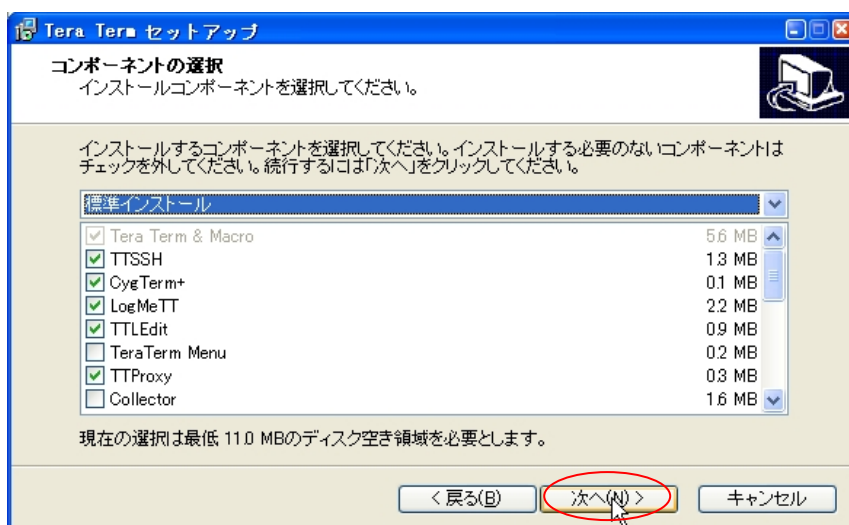
(図では標準の設定から意図的に替えています但し標準設定で問題ありません)



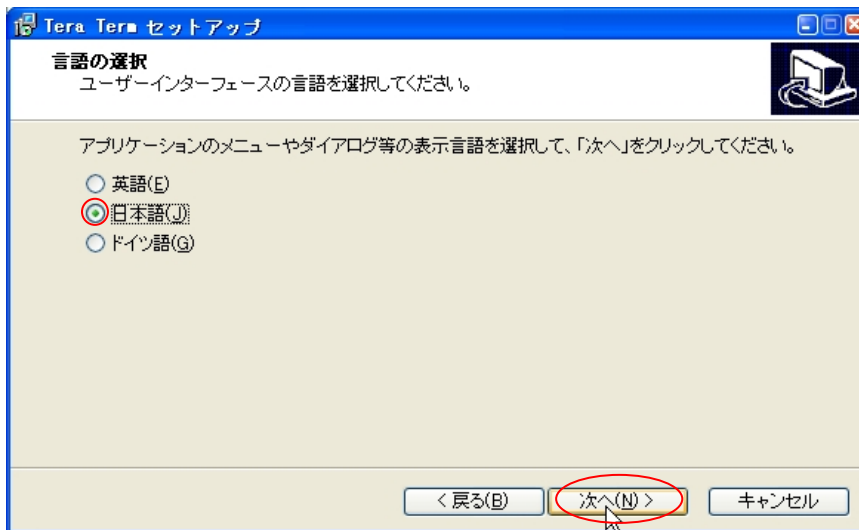
(e) インストール内容を選択

標準設定で問題ありませんが、鍵の作成では「TTSSH」だけで可能です。

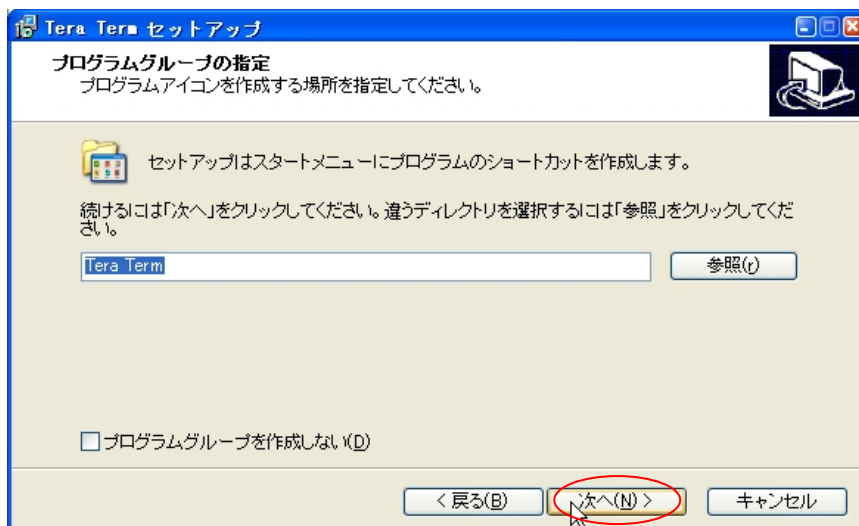
(k)の記述も参考にしてください。



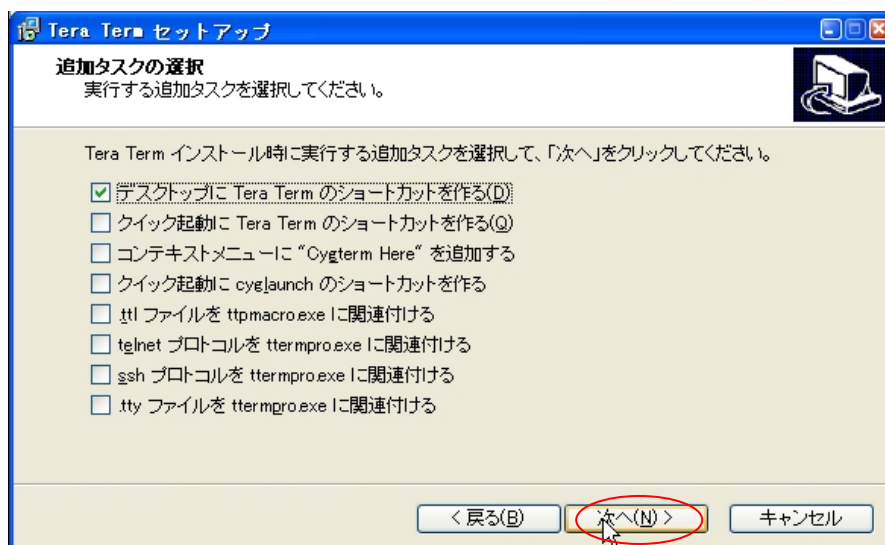
(f) 言語の選択(英語/日本語/ドイツ語の選択が可能です)



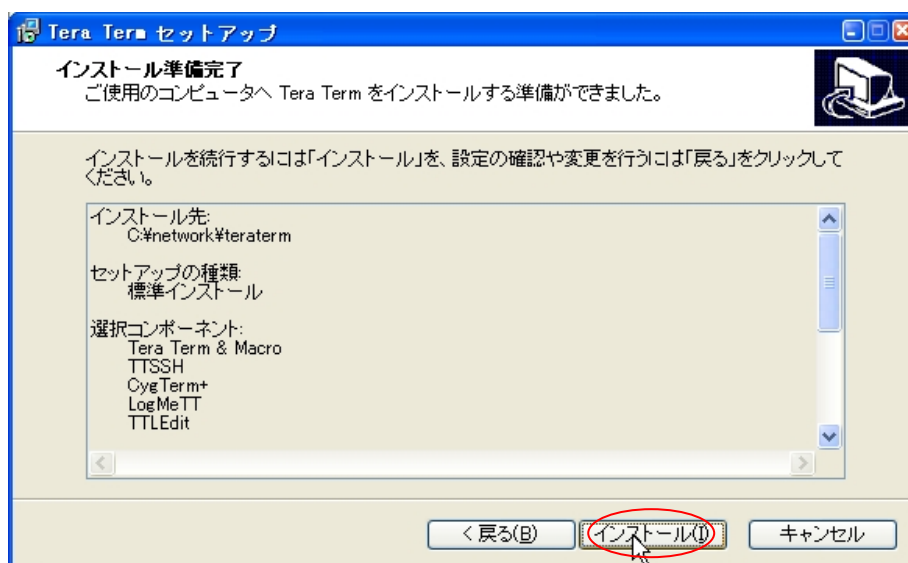
(g) プログラムグループの指定(標準設定で問題ありません)



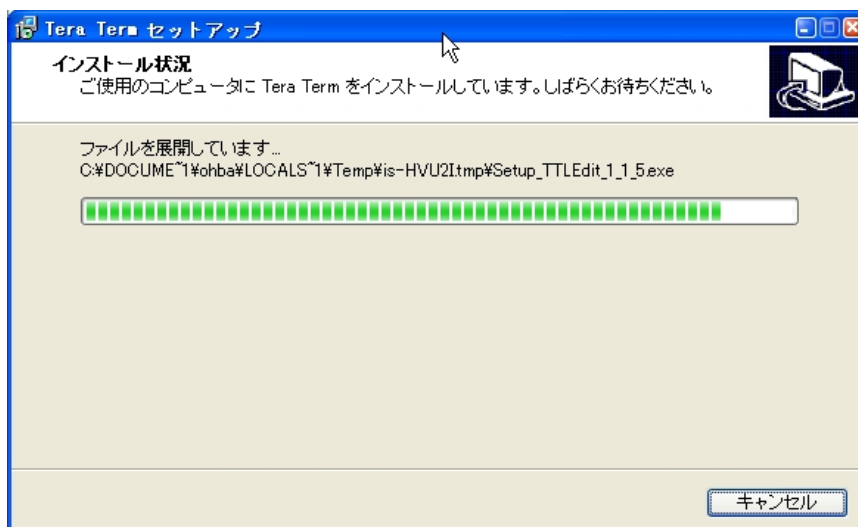
- (h) ショートカットの作成など
標準設定で問題ありませんが、必要があれば追加してください



- (i) インストールの準備が完了したので「インストール」



(j) インストール中



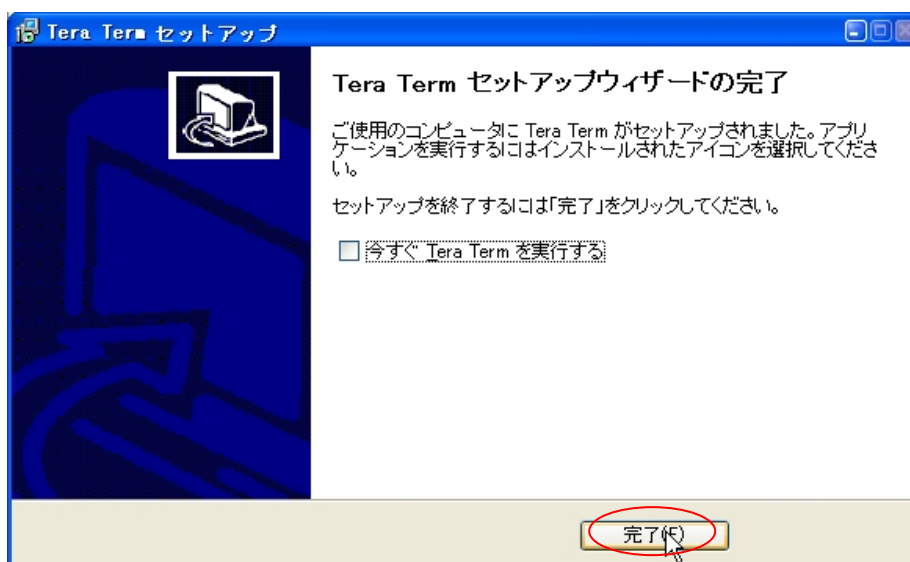
(k) 追加のソフトのインストール

※TeraTerm だけを使う場合は、キャンセルを選択しても問題ありません。

(e)で TTSSH 以外のチェックを外すとキャンセルされます。

必要な場合はインストールしてください

いずれの場合も、このダイアログがでるまでインストール作業を進めます。



これで TeraTerm のインストールが終了です。

(2) 「PortForwarder (ポートフォワーダー)」の入手とインストール

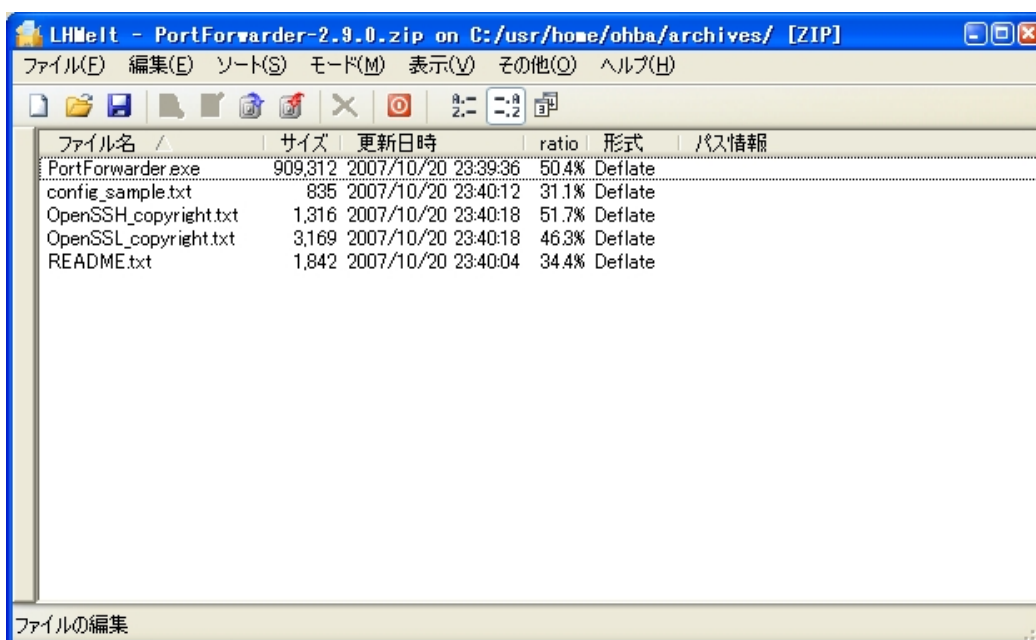
Windows 上で SSH のポートフォワードを行うために良く使われている「PortForwarder (ポートフォワーダー)」というフリーソフトがありますので、ここでは、このソフトを利用することにします。PortForwarder は SSH のポートフォワード機能を Windows 上で利用可能に実装したソフトウェアです。

入手先 <http://toh.fuji-climb.org/pf/JP/>

最新版(2010/8/6 現在の最新版は 2.9.0)をダウンロード

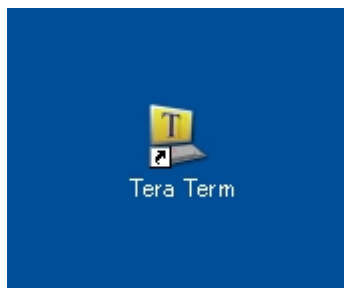
「PortForwarder-2.9.0.zip」を <http://toh.fuji-climb.org/pf/JP/download.htmlp.html> から入手し、解凍ツール(図は LHMelt を使用しています)を使って、適当なフォルダに展開します。

LHMelt で「PortForwarder-2.9.0.zip」の中を見るとこうなっています。

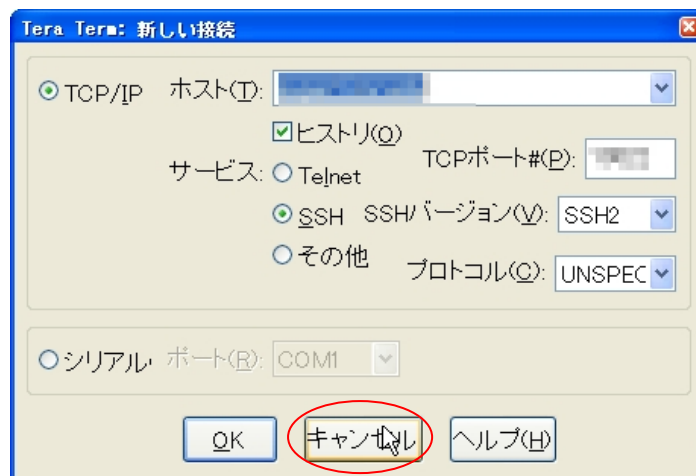


2. SSH2 プロトコルと DSA 暗号による認証鍵ペアの作成と利用申請
認証鍵ペア（公開鍵、秘密鍵の2種類）の作成には TeraTerm Pro を利用します。

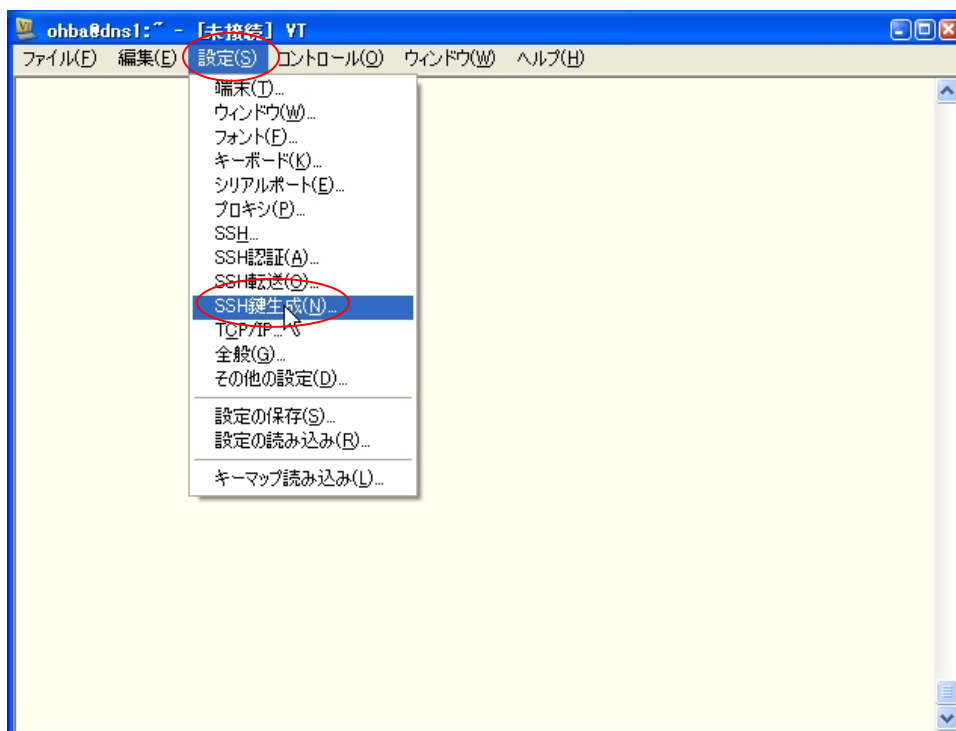
(1) デスクトップのショートカットを W クリック



(2) 初期設定(使用中の設定でも)では、このようなダイアログが出るので「キャンセル」



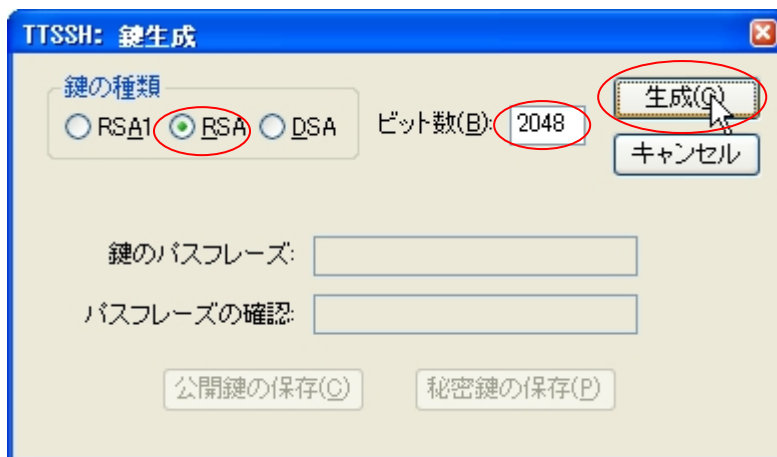
- (3) 「設定」 → 「SSH キー生成」 を選択



- (4) 「RSA」あるいは「DSA」を選択し「生成」

※この時、RSA の場合はビット数は「2048」でも問題ないようですが「DSA」の場合は「1024」としないと、後でサーバと SSH 接続でエラーが出るようです。

図は SSH2+RSA でビット数 2048 の鍵ペアを作成する場合の例です。

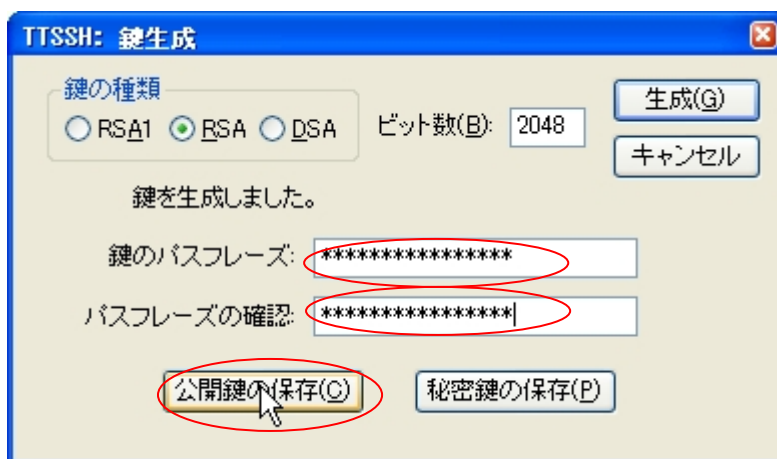


(5) パスフレーズの入力が有効になるので「同じ内容」を2箇所に入力

「公開鍵の保存」でファイルを保存します。

アルファベット以外に数字、記号も使用して、ある程度長い方が他人に見破られる確率が下がりますので、大文字、小文字、数字、記号の混在使用を推奨します。なお、入力内容は「*」となり、文字列は表示されませんので、パスフレーズは正確に入力してください、また、パスフレーズは公開鍵、暗号鍵から復元できず、当然、サーバ管理者も分かりませんので、パスフレーズは正確に記憶するようにお願いします。

(パスフレーズを忘れた場合は鍵ペアの再作成以外の方法はありません)

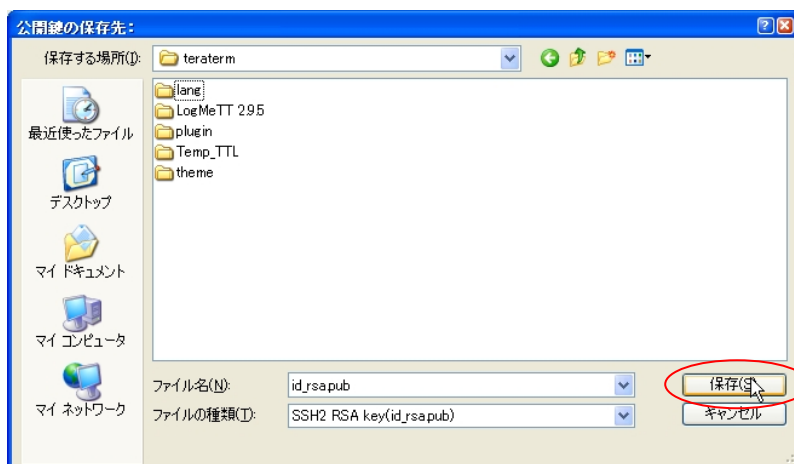


(6) 公開鍵をを保存します。

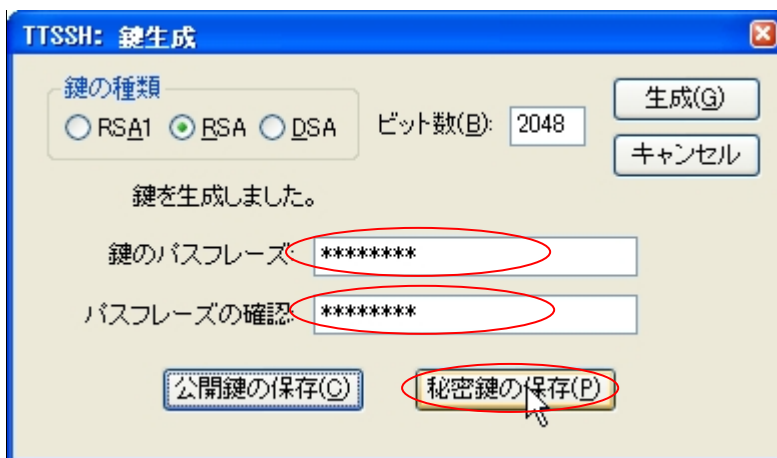
ファイル名は RSA の場合は「id_rsa.pub」

DSA の場合は「id_dsa.pub」となります

利用申請時に公開鍵のファイルをメールに添付して提出していただく必要がありますので、保存先を覚えてください。なお、Windows の設定によっては「.pub」の部分の表示がされない可能性もありますので、拡張子まで表示する設定にしてください。

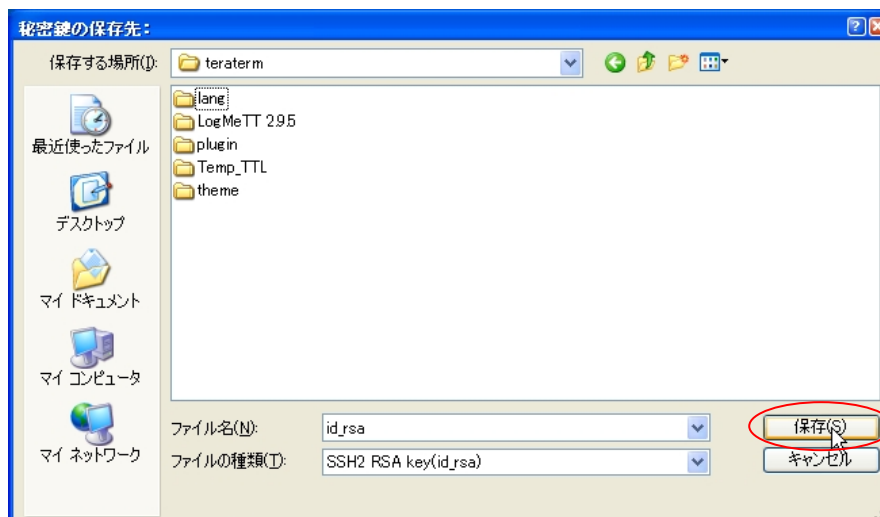


- (7) パスフレーズ、ビット数の内容は書き換えず、秘密鍵の保存



- (8) 秘密鍵を保存します。
ファイル名は RSA の場合は「id_rsa」
DSA の場合は「id_dsa」となります

秘密鍵は Portforwader で利用するためにパソコン内でコピーすることになりますので、保存先を忘れないようにしてください。



以上の様にして、認証鍵ペア（公開鍵(id_***.pub)、秘密鍵(id_***)) が生成できましたら、公開鍵のファイル「id_dsa.pub」をメールに添付して情報企画室情報班ネットワーク担当宛（担当：大場 ohba@imr.tohoku.ac.jp あるいは imr-net@imr.tohoku.ac.jp）にお送りください。

メールで公開鍵をお送りいただくことで、SSH 利用申請とさせていただきます。担当者が、SSH サーバ(ssh.imr.tohoku.ac.jp)上に申請者のユーザーアカウントを作成し、

お送りいただいた公開鍵を登録する作業を行い、完了後に初めて SSH の利用が可能になります。必要な手続きが終了しましたら、担当者の方からその旨連絡をいたします。

なお、公開鍵、秘密鍵、パスフレーズは、SSH 接続でユーザーを特定するために非常に重要な物になりますので、紛失や漏洩等が起きないように、厳重な取り扱いをお願いいたします。

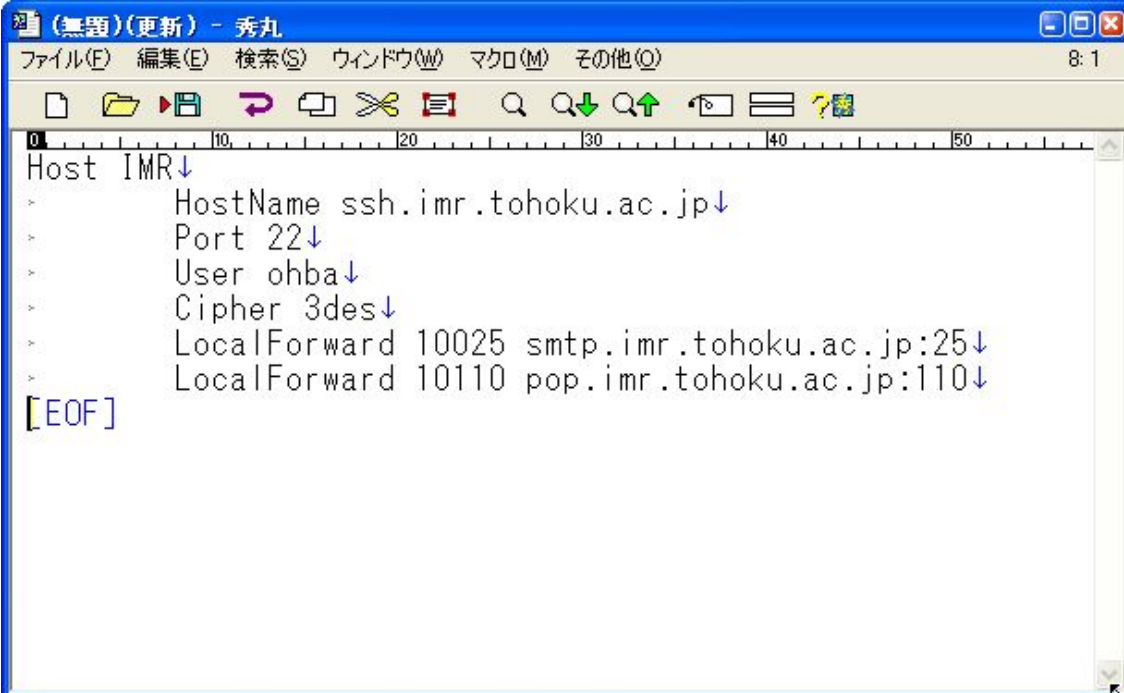
3. 設定ファイルの作成例

2.までに SSH の利用申請・登録が終了したものと、次は SSH のポートフォワード機能を使うための各種の準備に入ります。

この文書の例では、必要なすべてのファイルは、PortForwarder を展開したフォルダに置くようにして説明しています。

まず、「メモ帳」などのテキストエディタを使って、以下のようなポートフォワード設定ファイル(config.txt)を作成し、秘密鍵(id_***)と同一フォルダに保存します。

(config.txt の例：メールの送受信をするための設定)



```
Host IMR
  HostName ssh.imr.tohoku.ac.jp
  Port 22
  User ohba
  Cipher 3des
  LocalForward 10025 smtp.imr.tohoku.ac.jp:25
  LocalForward 10110 pop.imr.tohoku.ac.jp:110
[EOF]
```

上の記述例は新ネットワーク側の SSH 認証サーバ用の記述で、所内のメールサーバへ接続する設定例です。それぞれの設定内容を簡単に説明すると

1 行目：Host IMR

これは設定名であり、任意で構いません。

複数の設定を 1 つの設定ファイルに書く場合は、それぞれ別にします。

2行目 : **HostName ssh.imr.tohoku.ac.jp**

これは、使用する SSH サーバ名に関する記述ですので
この通りに書いてください。

3行目 : **Port 22**

これは SSH サーバへの接続ポート番号を書くところですので、
この通りに書いてください。

4行目 : **User ohba**

ここには SSH サーバに登録してあるユーザー名を書きます。
例では ohba になっていますが、ここには各自のユーザー名を書いてください。

5行目 : **Cipher 3des**

ここは暗号化に関するところですので、この通りに書いてください。

6行目 : **LocalForward 10025 smtp.imr.tohoku.ac.jp:25**

ここは自分の PC の 10025 番ポートと、目的とする SMTP サーバ
(smtp.imr.tohoku.ac.jp)の 25 番ポート(SMTP ポート=送信サーバポート)を
関係付けることを表しています。
10025 のところは任意で構いませんが、1025 以上にしてください。
(1024 以下は使用目的が決まった予約ポートのため、通常は使用しません)

7行目 : **LocalForward 10110 cmsspop.imr.tohoku.ac.jp:110**

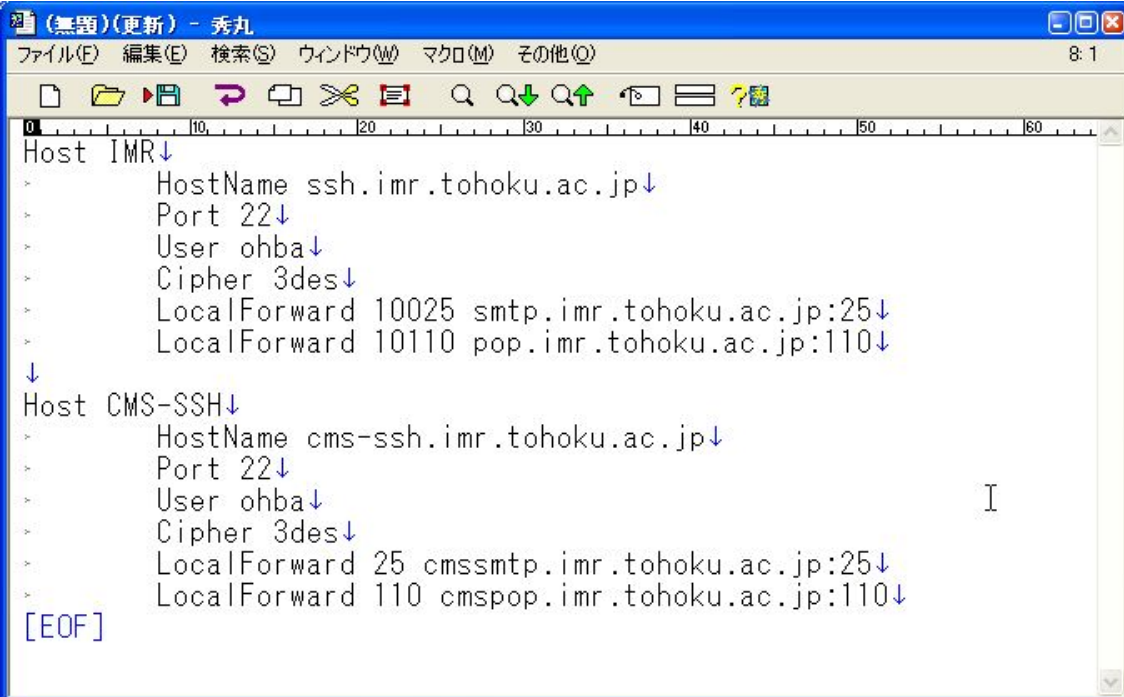
ここは自分の PC の 10110 番ポートと、目的とする POP サーバ
(pop.imr.tohoku.ac.jp)の 110 番ポート(POP3 ポート=受信サーバポート)を
係付けることを表しています。
10110 のところは任意で構いませんが、1025 以上にしてください。
(1024 以下は使用目的が決まった予約ポートのため、通常は使用しません)

目的とするサーバが外部の場合、所外の組織から接続許可を受けているならば
8行目以降に

LocalForward 10xxx aaa.example.co.jp:xxx

のような記述を順次追加していくことで、外部への接続も可能になります。

また、スーパーコンピュータの SSH 認証サーバ(cms-ssh.imr.tohoku.ac.jp)も併用する必要
がある場合、公開鍵と秘密鍵が共通ならば



```
(無題)(更新) - 秀丸
ファイル(F) 編集(E) 検索(S) ウィンドウ(W) マクロ(M) その他(O) 8:1
Host IMR↓
>   HostName ssh.imr.tohoku.ac.jp↓
>   Port 22↓
>   User ohba↓
>   Cipher 3des↓
>   LocalForward 10025 smtp.imr.tohoku.ac.jp:25↓
>   LocalForward 10110 pop.imr.tohoku.ac.jp:110↓
↓
Host CMS-SSH↓
>   HostName cms-ssh.imr.tohoku.ac.jp↓
>   Port 22↓
>   User ohba↓
>   Cipher 3des↓
>   LocalForward 25 cmssmtp.imr.tohoku.ac.jp:25↓
>   LocalForward 110 cmspop.imr.tohoku.ac.jp:110↓
[EOF]
```

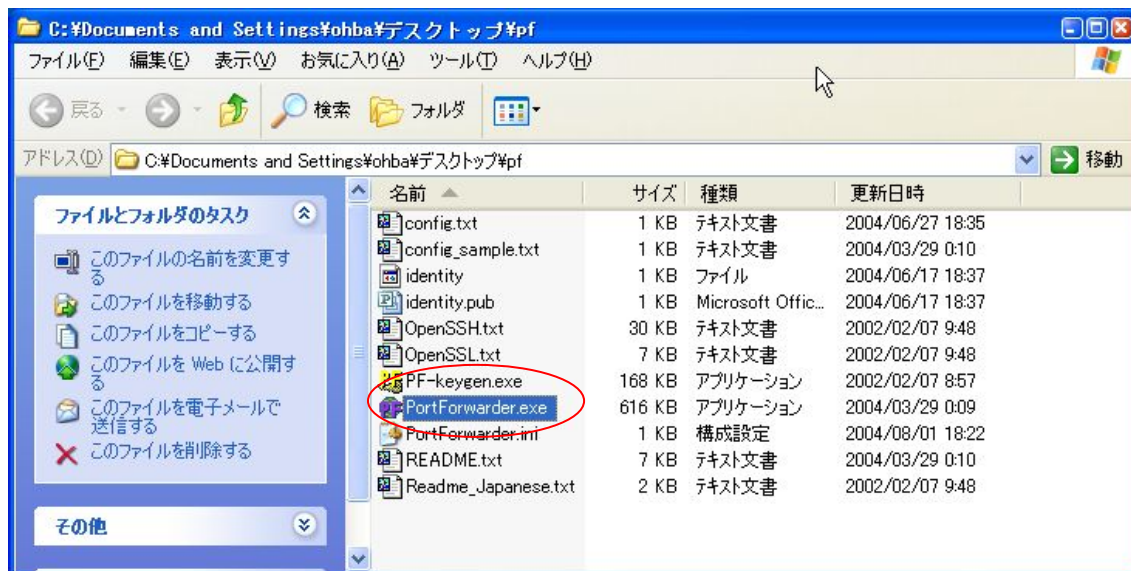
のように、複数のサーバを1つの設定ファイルに記述して、**Portforwader** の起動時に
認証を受けるサーバを選択することで、切り替えることもできます。

また、公開鍵と秘密鍵が別のものを使っている場合は、それぞれの設定ファイルと鍵を
別フォルダへ置き読み込む **config.txt** を切り替えることでも認証を受けるサーバを変更す
ることが可能になるなど、柔軟な設定が可能なようです。

4. Portforwarder の起動

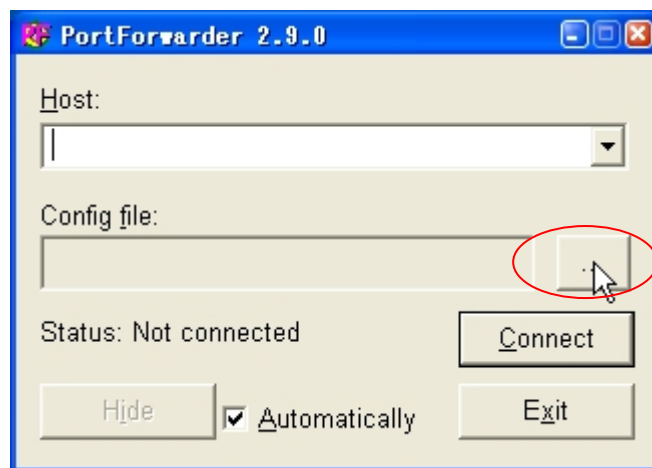
- (1) インストールした、PortForwarder.exe を起動します。

デスクトップにショートカットを作っておくと以降の操作が楽になります

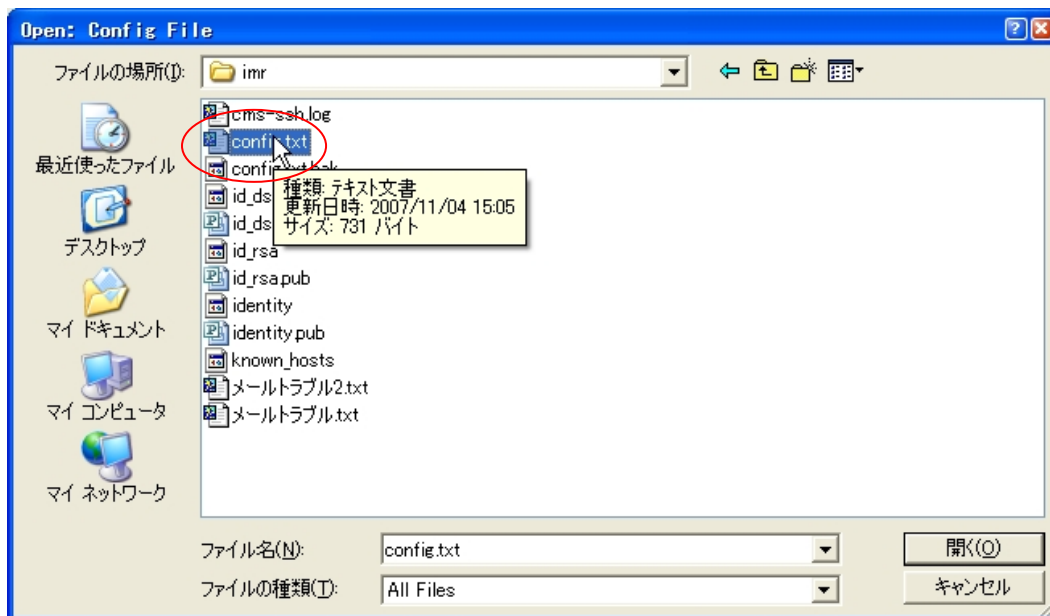


- (2) 「Config file:」のある場所を指定します。

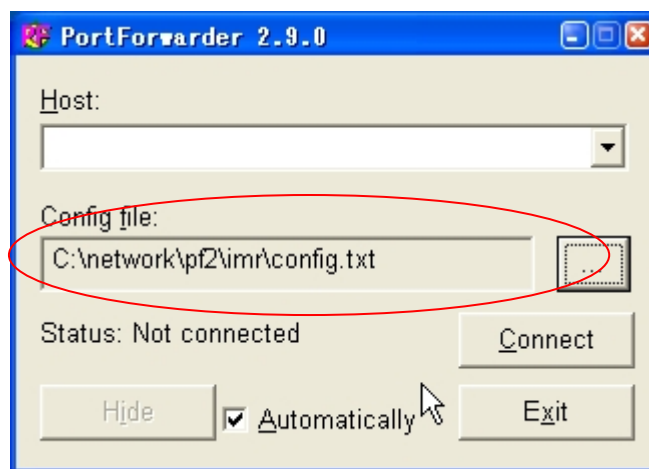
ここをクリック



(3) config.txt を指定

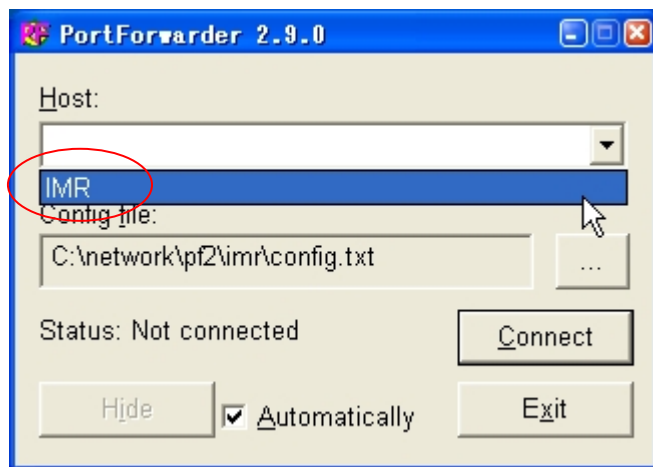


(4) 設定ファイルの指定が完了



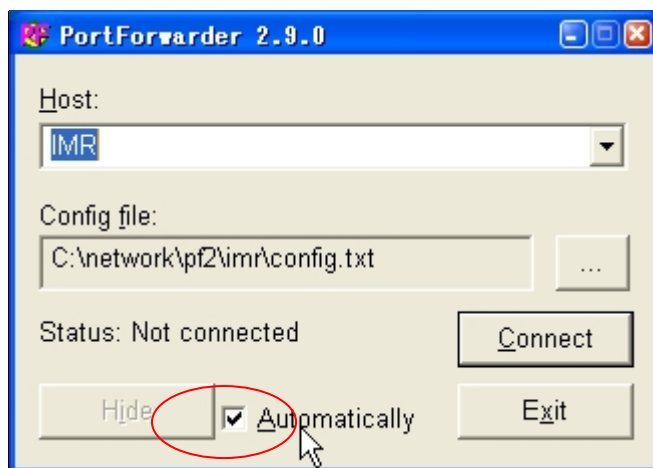
(5) SSH 認証サーバの指定

設定ファイルに複数の Host を記述してあると、それぞれ選択可能になります。



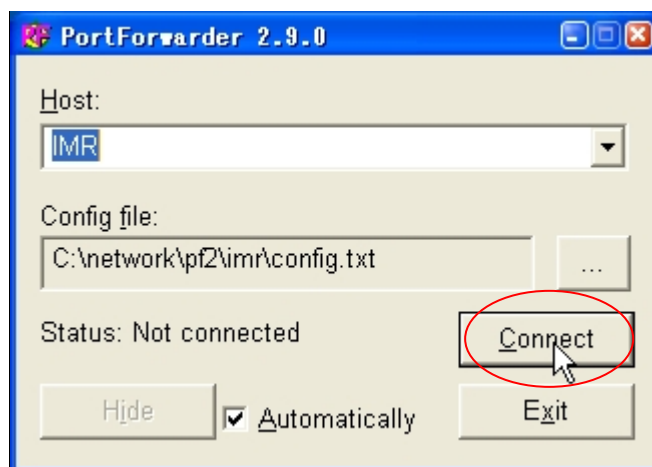
(6) 選択完了

Automatically のチェックを入れると、接続後に自動的にタスクトレイに収容されます。



(7) 接続

「Connect」を押す。

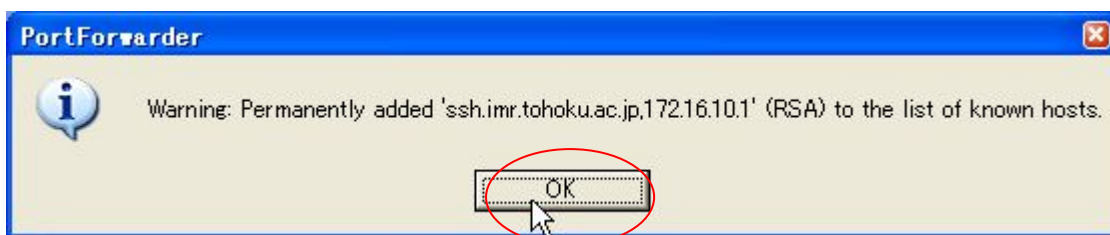


(8) サーバ情報の保存(一度目のみ)

SSH サーバ（ここでは `ssh.imr.tohoku.ac.jp`）に初めて接続する時のみ、以下のメッセージが表示されますので「はい」をクリックしてください。



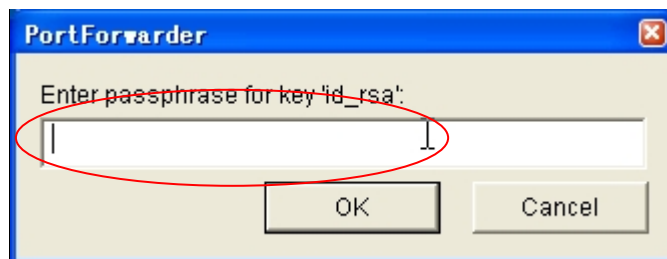
「はい」を押すと、以下のメッセージが表示されますので「OK」をクリックします。



これで、一度接続した SSH サーバの情報は暗号鍵と同じフォルダ内に `known_hosts` というファイルとして保存され、2回目以降はこのメッセージは出なくなります。

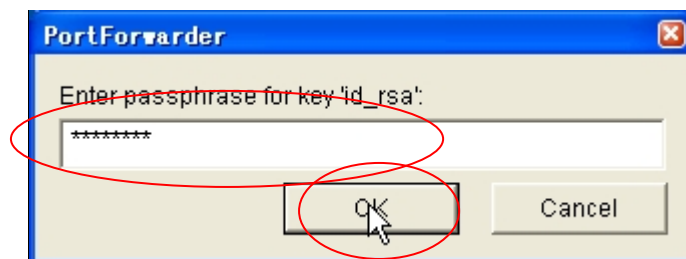
(9) パスフレーズの入力

入力する画面が出ますので、認証鍵ペアを作成したときに設定したものを正しく入力してください。



入力内容途中はこのようになり、内容は読めません。

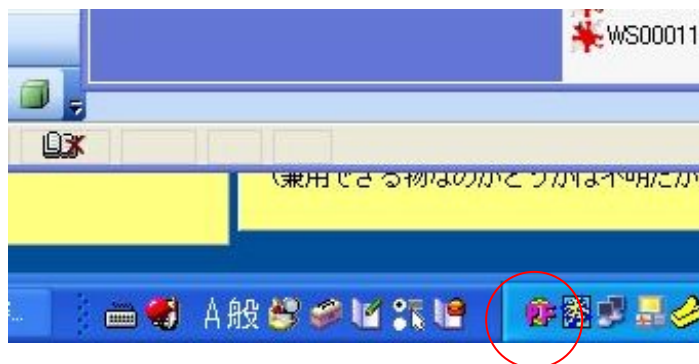
また大文字小文字は区別されますし、パスフレーズはサーバ管理者にも一切分かりませんので、忘れないようにご注意ください。



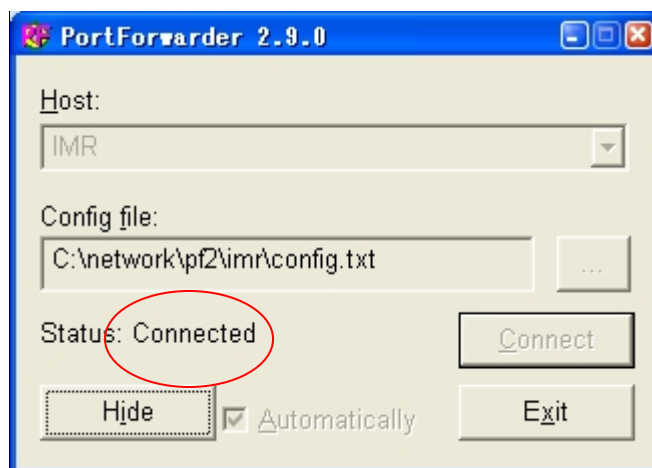
入力が終わったら「OK」をクリックします。

(10) 認証完了

パスワードが正しく入力され、認証が成功すると、SSH サーバに接続されます。自動で、タスクトレイへ移動する設定にしておけば、タスクトレイへ移動します。



その設定をしていない場合は、



と、「Status: Connected」となります。

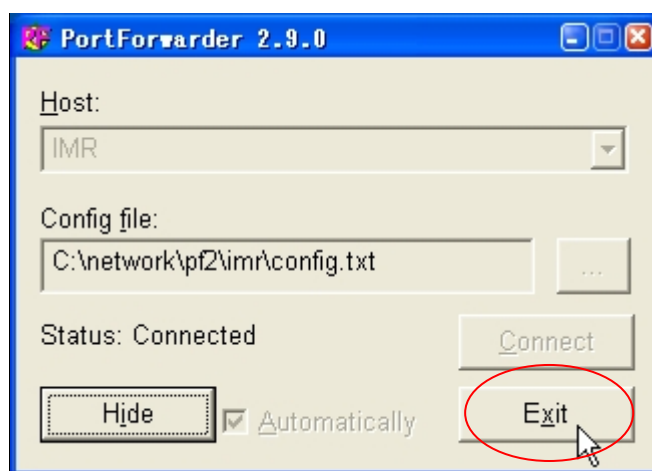
これで SSH サーバへのログインが完了です。

接続終了

タスクトレイへ移動した場合は
「右クリック」して「exit」します。



その設定をしていない場合は、

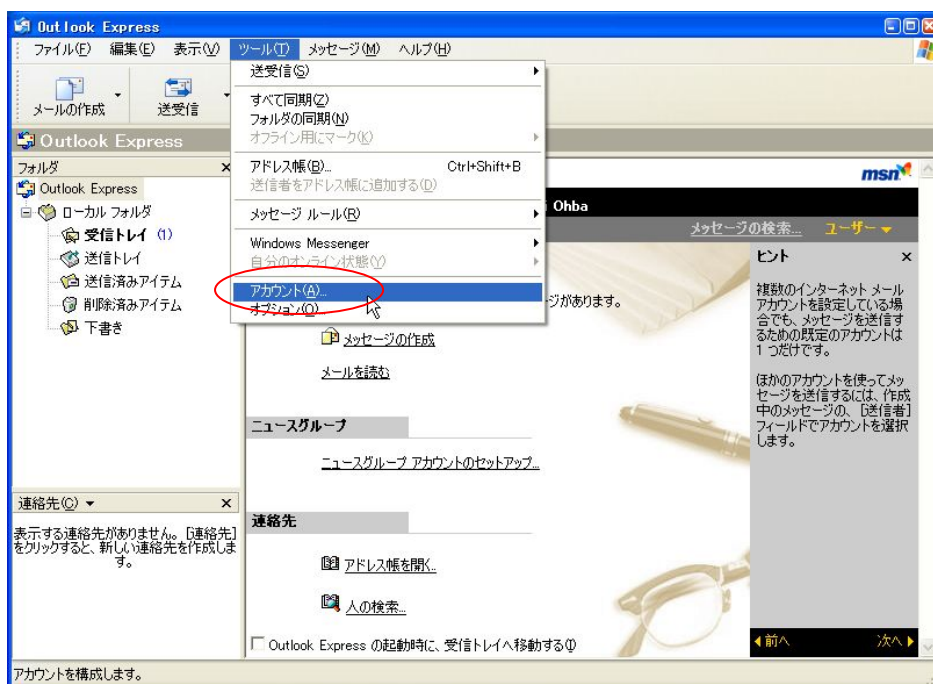


と、「Exit」をクリックします。

5. メールソフトの設定

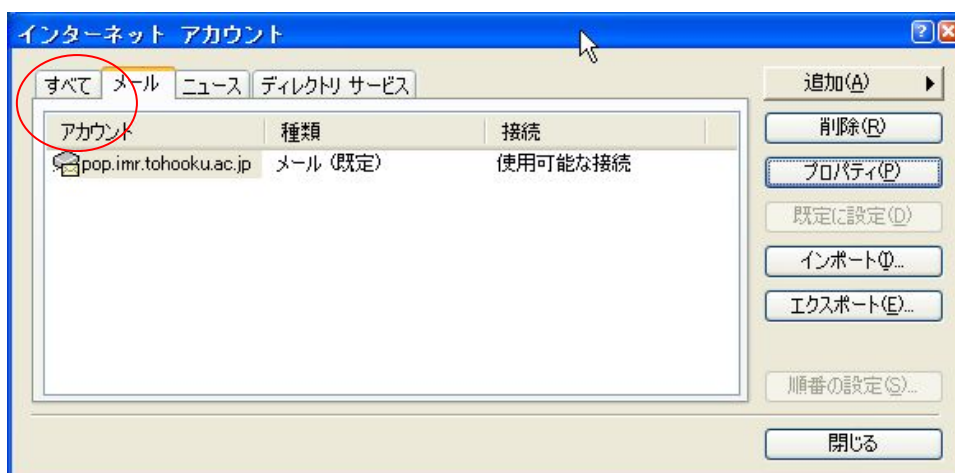
ここでは、Outlook Express での設定を例として示しますが、「サーバ名」と「利用する port 番号」を変更することが基本となります。

(1) 「ツール」 → 「アカウント」を開きます。

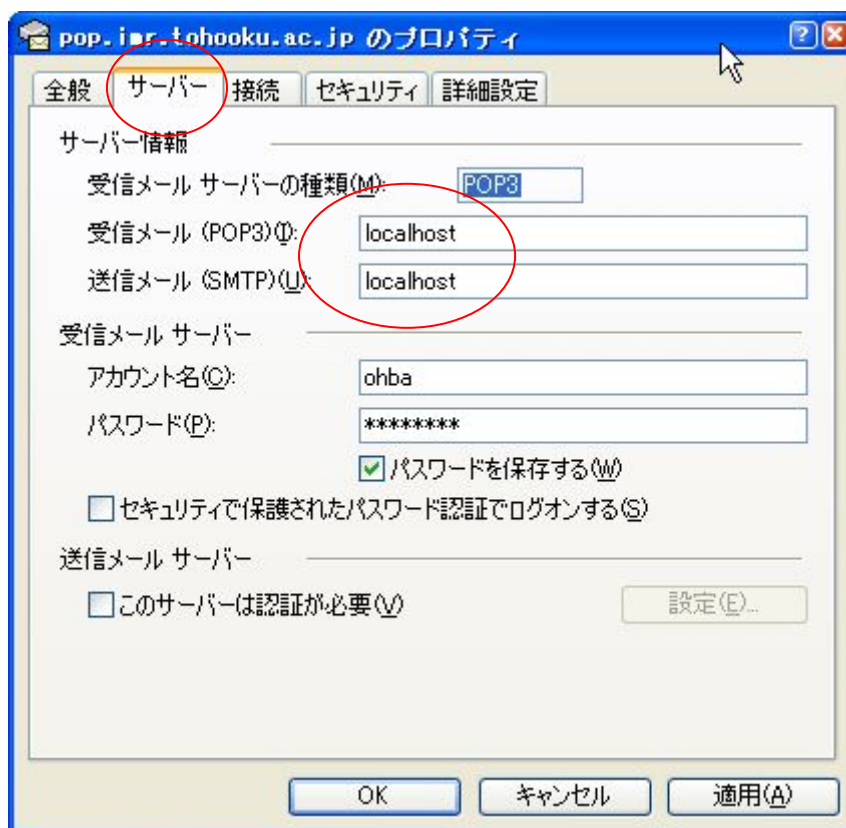


(2) 「メール」タブを選択

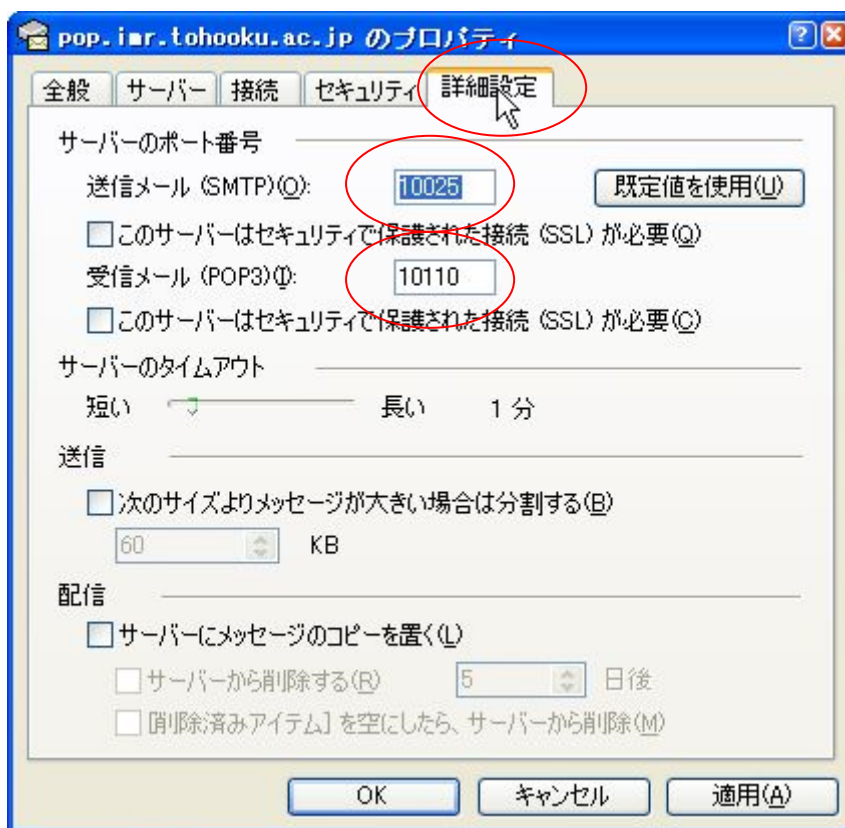
SSH を利用したいアカウントを選択(この例では 1 つしかありません)



- (3) 「サーバ」タブを選択
サーバ名を「localhost」へ修正



- (4) 「詳細設定」タブを選択
サーバのポート番号を config.txt に設定した数字に修正



設定修正後に「適用」をクリックで設定が反映されます。

ここでは、**Outlook Express** を例にしましたが、「サーバの接続 port」が自由に設定できるメールソフトならば、同様の設定で接続できるものと思われます。

設定の基本は、ポートフォワード設定ファイル(config.txt)に記載した

```
LocalForward 10025 smtp.imr.tohoku.ac.jp:25
```

```
LocalForward 10110 pop.imr.tohoku.ac.jp:110
```

の Localhost と、local 側の数字にメールソフトの設定をあわせ、各メールソフトの設定を

```
サーバ名      「localhost」
```

```
port          「10xxx」
```

```
SMTP サーバでは 10025、POP サーバでは 10110
```

のように、修正することになります。**Outlook Express** 以外にも、**Netscape** メール、**Winbiff**、**AI-Mail** 等での接続を確認していますので、各自でお試してください。

6. 環境の持ち歩き

PortForwarder は必要なすべてのファイルがフロッピーディスク 1 枚以下の容量で収まります。**SSH** のポートフォワード機能のみを使うのであれば、これらをフロッピーディスクや **USB** メモリなどにコピーしておけば、パソコンが変わってもメールクライアントソフトの **SMTP** サーバと **POP** サーバの記述を「localhost:****」のように書くだけで良いことになりますので大変便利です。

また、**PortForwarder** のコピーを持って移動するということは、鍵ファイルを持って移動することになります。以前に比べて **USB** メモリなどが大容量化されてきていますので、**PortForwarder** 以外の **SSH** クライアント、例えば、**TeraTerm Pro** や **putty** のアーカイブや実行環境を一緒に持って移動していれば、移動先で端末が変わっても **SSH** によるパスワード認証でのログインができる環境を持った状態で移動できるメリットもあります。

ただし、移動先の **PC** に持っているファイルのコピーやソフトのインストールが可能かどうかは、移動先の組織の許可を受けてからにしてください。また、鍵ファイルを持っての移動の際は、記録メディアの紛失には注意をしてください。