HYEC.ORG における
キーペアの作成方法

著：HYEC.ORG

1. 始めに

HYEC.ORG ではセキュリティポリシー上の理由から、FTP を許可していません。その代わりに、SCP を採用しています。しかし、標準の SCP はパーミッション（ファイルやディレクトリへのアクセス権）さえ許せば、サーバ上のどこにでもアクセスすることができてしまいます。そこで、HYEC.ORG では特別なバージョンの SCP を用いて、アクセスできるディレクトリを各ユーザのホームディレクトリに制限しています。また、パスワードによる認証を許可せず、SSH1/SSH2 のキーペア（対応する秘密鍵と公開鍵のこと）を用いた認証のみ許可しているため、より安全性が高くなります。

SCP は通信経路が暗号化されます。つまり、通信内容を盗聴されたり改変される可能性が低くなります。「通信内容を盗聴されたり改変されなくなる」わけではないことに注意してください。また、通信に使うポート（サーバとクライアントが通信するための窓口）がひとつだけであることから、接続する方もされる方もセキュリティ対策を立てやすいというメリットがあります。逆に、初心者や Unix 系の経験が乏しい人たちにとっては敷居が高く感じてしまいます。

でも、ちょっと待ってください。もし Windows を使用しているならば、普段使い慣れた FTP クライアントと同等の操作性で安全にファイルをやりとりできるようになるのです。覚えにくいコマンドをちまちまタイプする必要などありません。FTP クライアントを設定したことがある人ならば、SCP は難しくありません。それでは、最初の難関である「キーペアの作成方法」について説明しましょう。

2. ソフトウェアを入手する

先ほど、「SCP は難しくない」といいました。また、「コマンドをちまちまタイプする必要はない」とも言いました。これに関しては嘘偽りはありません。ただし、そのためには多少の手間が掛かります。ソフトウェアを入手しなければならないのです。

HYEC.ORG は「WinSCP」と「PuTTY」というソフトウェアを用いることを推奨します。ただし、これが唯一無二のものではないことに注意してください。他にお気に入りのソフトがあればそちらを用いて頂いて構いません。ただ、私たちはそのソフトウェアを知らないかもしれないので、何かあったとしても何もできないというだけです。

では、早速ソフトウェアを入手しましょう。まずは「WinSCP」から。こちらの方は日本語のページがありますので気が楽ですね。「http://www.tab2.jp/~winscp/」へアクセスしてみてください。下記のようなページが表示されるはずです。

図1：WinSCP の日本語版 Web ページ

うまく表示されましたか？表示されなければURLを再度確認してみてください。うまく表示されたなら、左側にあるメニューの上から5番目、「DOWNLOAD」をクリックしてください。下記のような画面が表示されるはずです。

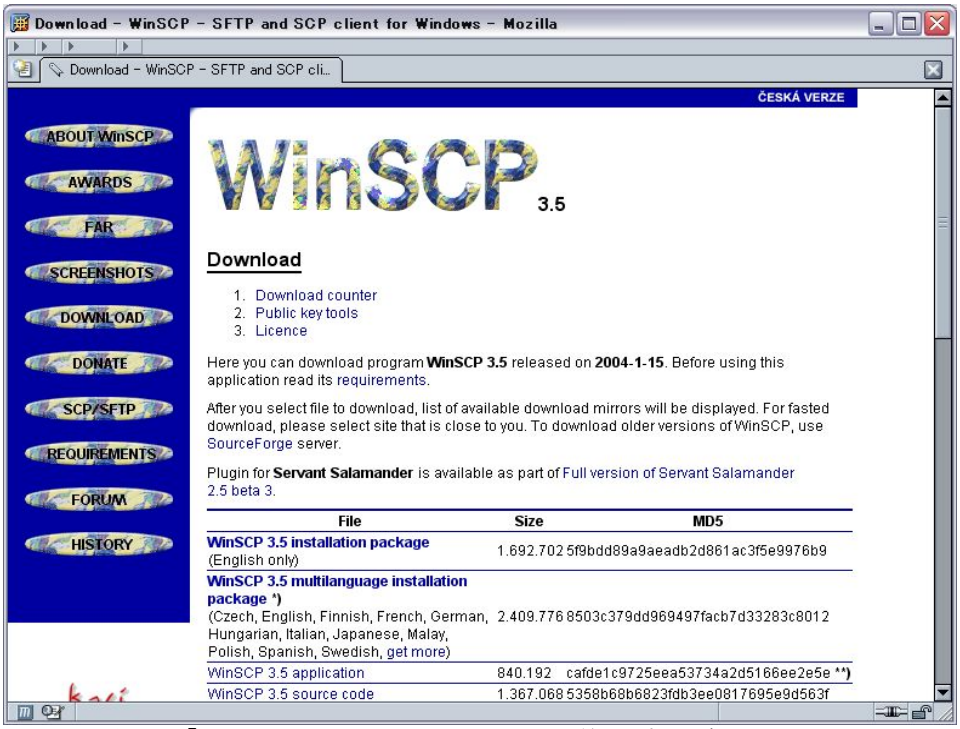

図2：「DOWNLOAD」をクリックした後に表示される画面

このドキュメントを執筆している時点では、WinSCP3.5が最新版のようです。上記画面をよくご覧ください。下の方に「WinSCP 3.5 multilanguage installation package」というリンクがあるのが分かりますか？これをダウンロードしてください。これを使うと日本語で表示されるようになります（正確に言えば日本語でも表示されるようになります）。これはインストーラが付いていますから、ダウンロードしたものをダブルクリックし、画面の指示に従っていけばインストールすることができます。

では続いて「PuTTY」をダウンロードしましょう。こちらの方は最初から英語ですが、さほど難しくはありませんし、迷うこともないはずです。

では、「http://www.chiark.greenend.org.uk/~sgtatham/putty/」にアクセスしてみてください。下記のような画面が表示されるはずです。

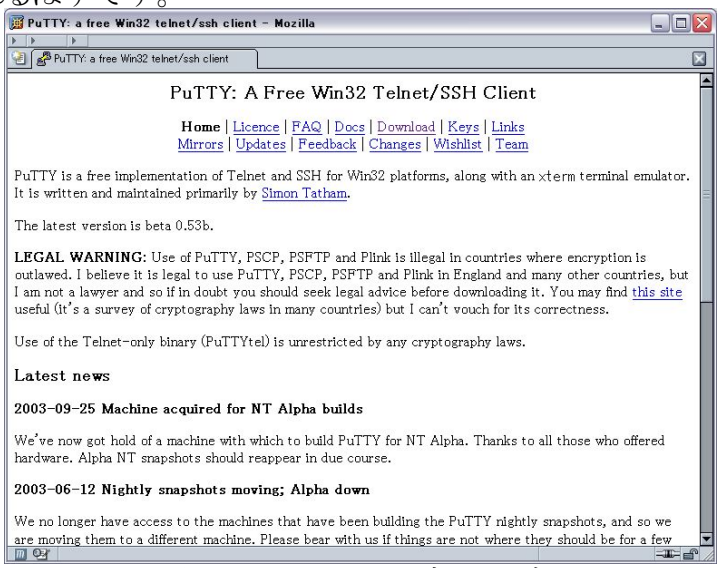

図3：PuTTYの公式ページ

表示されましたね？それではこのページの上部にある「Download」というリンクをクリックしてください。下記のような画面が表示されるはずです。

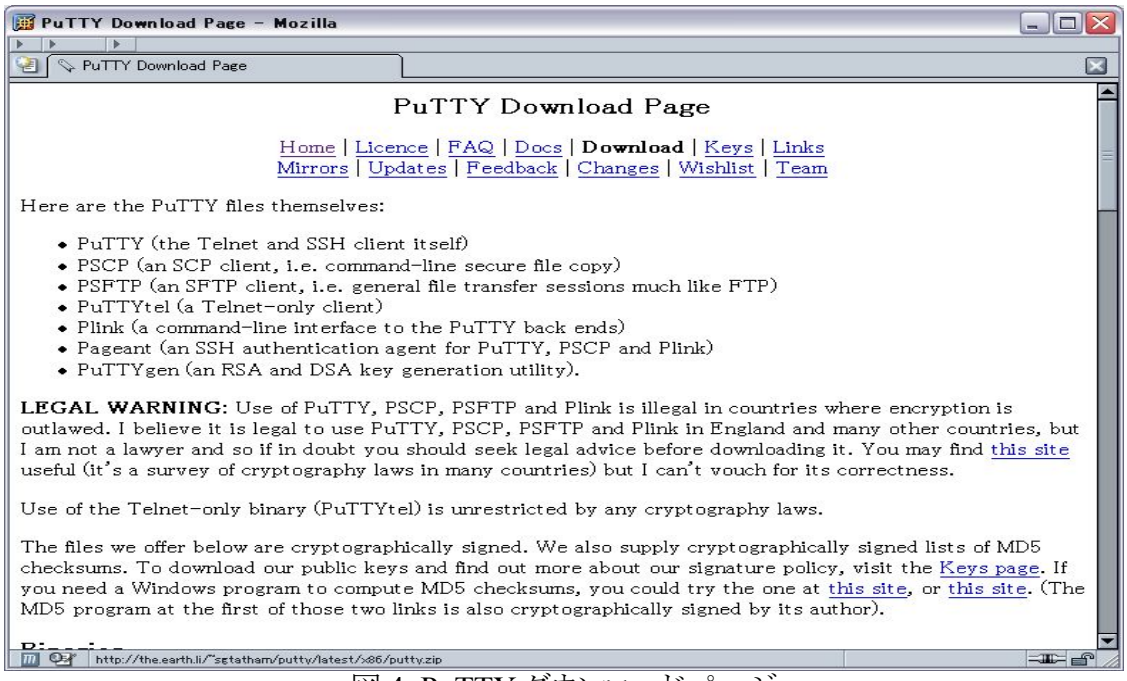

図 4：PuTTY ダウンロードページ

このページに切り替わったら、下の方にスクロールしてみてください。「**For Windows 95, 98, ME, NT, 2000 and XP on Intel x86** 」という文字が太字で表示されているはずです。

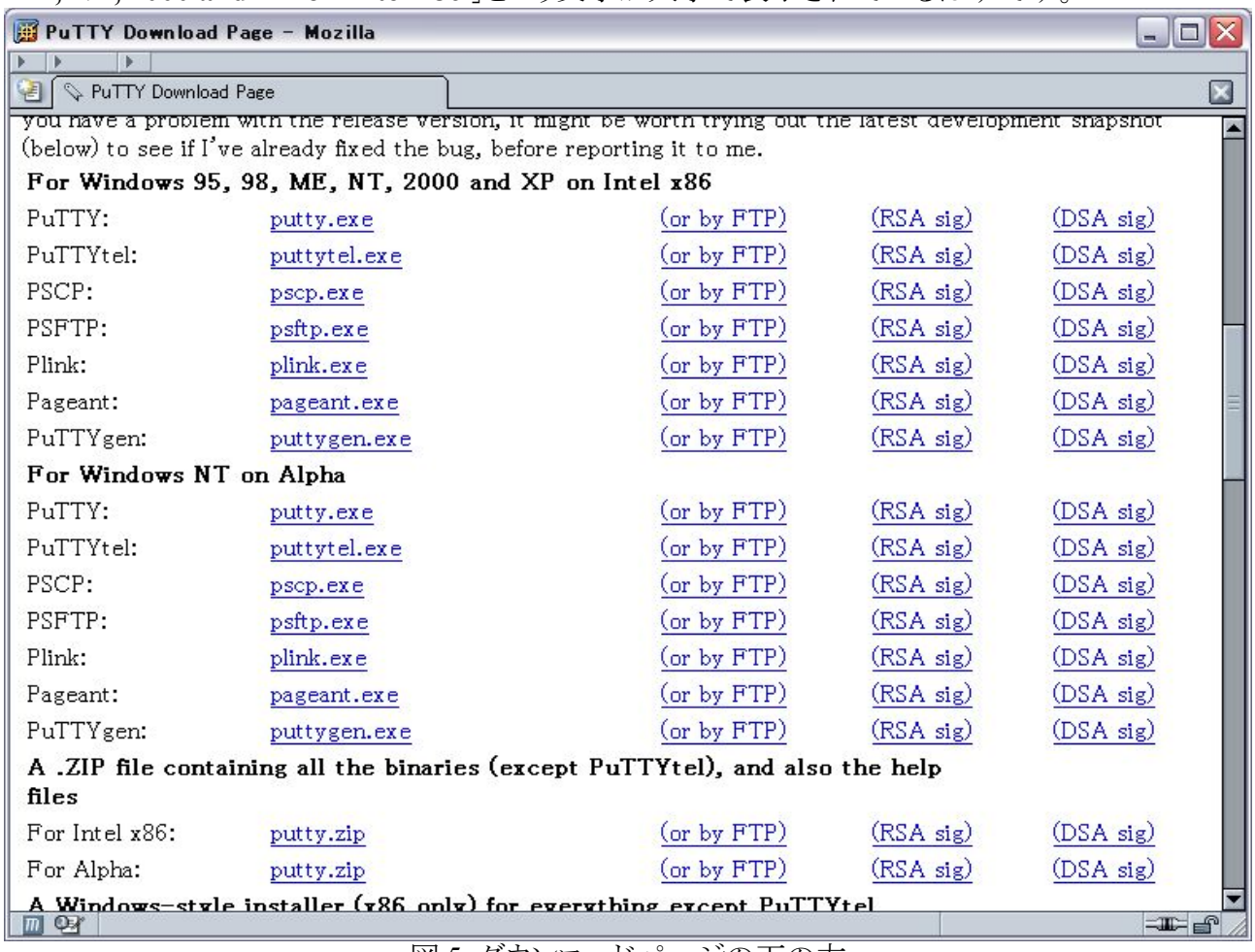

図 5：ダウンロードページの下の方

ここで必要となるのは「PuTTYgen」のみです。「puttygen.exe 」と青色の下線が引いてあるリンクをクリックしてください。保存場所を聞かれると思いますので、お好きなところに保存してくださいね。ここでひとつ注意です。「**For Windows NT on Alpha** 」の下にある「puttygen.exe」をダウンロードしないでください。 もし、貴方が SCP だけでなく SSH も使いたいのなら、「putty.exe 」と「pageant.exe 」もダウンロードしておいてください。

もしインストーラが必要なら、「**A Windows-style installer (x86 only) for everything except PuTTYtel** 」の下にある、「putty-0.53b-installer.exe 」をクリックしてダウンロードしてください。こちらをダウンロードしてダブルクリックするとインストーラが起動し、おなじみの手順でインストールすることができます（ただし、英語で表示されますし、使わないソフトウェアもインストールされます）。ちなみに、「**A .ZIP file containing all the binaries (except PuTTYtel), and also the help files** 」の下の「For Intel x86: 」という文字の右側にある「putty.zip 」というリンクをクリックすると、インストーラなしのバージョンをダウンロードすることができます（こちらを使用するときは *ZIP* 形式の圧縮ファイルを解凍できるソフトウェアが必要です）。

まあ、インストーラ有りのバージョンをダウンロードしてインストールしておけば間違いないでしょう。

3. キーペアを作る

それでは早速キーペアを作りましょう。と、その前に、作成したキーペアを保存しておくフォルダを作成しておいてください。このフォルダは自分以外の誰にも見られない場所に作成してください。これから作成するキーペアはとても重要なものです。厳重に管理してください。

それでは先ほどダウンロードした「puttygen.exe」をダブルクリックしてください。インストーラからインストールした場合はスタートメニューの中にあるかもしれません（*HYEC.ORG* としては未確認です）。すると下記のようなウィンドウが表示されるはずです。

図6：PuTTYgen 起動直後

まず、SSH1 と SSH2 のどちらを作成するか決めてください。HYEC.ORG サーバではどちらも使用できるようになっていますが、SSH2 だと接続できないという報告を受けています（*HYEC.ORG* のテスト環境では *LAN* の内外を問わず接続できています）。ちなみにセキュリティ的には SSH2 を用いた方がよいとされています。

どちらを作成するか決めたら、「Parameters」という部分の「Type of key to generate」という部分を見てください。ここに「SSH1（RSA）」、「SSH2 RSA」、「SSH2 DSA」の3つが並んでいるのが確認できるかと思います。この中から好きなものを選択してください。ちなみにその下にある「1024」という数字ですが、これは気にしなくて構いません（鍵のビット長を指定するものですが、そのままでも十分だと思われます）。

指定しましたか？指定したなら、真ん中のあたりにある「Generate」というボタンをクリックしてください。すると下記のような画面に変わるかと思います。

図7：「Generate」ボタンをクリックした直後

この画面になったら、「Key」と書いてある枠の中でおもむろにマウスを動かしてください。少しずつバーが右側に向かっていくはずです。バーが一杯になると鍵が生成され、下記のような画面になるはずです。

なお、「Key Passphrase」と「Comfirm Passphrase」という部分が空白になっているかと思いますので、必ずパスワードを指定してください。ここに指定するパスワードはサーバへの接続とは一切関係ありませんので好きなものを指定して構いません（鍵を使用するときに使用します。これを指定することによって、鍵が盗難にあってもこの鍵を使用した接続を難しくすることができます）。

図 8：鍵が作成された

ここで、「Generate」ボタンの下にある、「Save public key」と「Save private key」をそれぞれ一回ずつクリックし、先ほど作成したフォルダの中に保存してください。「Save public key」で保存した方が公開鍵、「Save private key」で保存した方が秘密鍵となります。どちらも厳重に保管してください。

これで終わり・・・ではありません。ここでこのソフトウェアを終了させないでください。続いて「Public key for pasting into authorized_keys file:」という部分の下にある長い数字（又は英数字）の羅列をコピーしてください。これがサーバに登録する公開鍵になります。これをコピーしたら、一切改変せずに HYEC.ORG に送付してください。そのときは、メールの本文に添付して頂いてもテキストファイルとして添付して頂いても構いません。

さて、これが SSH1 のキーペアを作成し、HYEC.ORG へ公開鍵を送付するまでの流れになります。では、SSH2 の方も見てみましょう。全体の流れとしては SSH1 のときと対して代わりありません。まったく同じ手順で作成できます。

唯一違うのは「HYEC.ORG に送付する公開鍵」の取得場所だけです。先ほど SSH1 の公開鍵を送付するときは、『「Public key for pasting into authorized_keys file:」という部分の下にある長い数字（又は英数字）の羅列をコピーして HYEC.ORG へ送付してください。』といいましたが、実は「Save public key」で保存したものを送付して頂いても構わないのです。SSH1 の場合はどちらも同じものが出力されるためです。

ただし、SSH2 の場合は事情が違います。下記の画面を見てください。SSH1 の場合と違って、「Public key for pasting into authorized_keys file:」となっていた部分が「Public key for pasting into OpenSSH authorized_keys2 file:」となっているのに気付きましたか？

画面9：SSH2 のキーペアを生成した場合

実は SSH2 の場合は「Save public key」で保存した内容と「Public key for pasting into OpenSSH authorized_keys2 file:」に表示される内容が異なるのです。これは、SSH2 の鍵の形式が統一されていないために起こる問題です。HYEC.ORG サーバは「OpenSSH」というソフトウェアを採用しています。よって、「Public key for pasting into OpenSSH authorized_keys2 file:」に表示される内容が公開鍵となります。この内容をコピーしてメールの本文に貼り付けるかテキストファイルとして添付して頂ければ HYEC.ORG 側でサーバに登録致します。

上記の例では「SSH RSA」の鍵を生成する方法を紹介しましたが、「SSH2 DSA」でもまったく同じです。

4. 鍵ができたら後は終わったも同然

これでキーペアの作成は終了です。いかがですか？思っていたよりも簡単にできたのではないかと思います。HYEC.ORG をご利用になる皆さんも上記手順でキーペアを作成してみてください。

さて、最大の難関である鍵の作成が終了しましたので、続いて WinSCP の設定を行いましょう。ところで皆さんは FTP クライアントの設定をしたことがありますか？もし、この質問に「はい」と答えられるのであれば、WinSCP の設定など赤子の手をひねるようなものです。

では、早速 WinSCP の設定を行いましょう・・・といいたいところですが、長くなってしまいましたので今回はこの辺で終わりにしたいと思います。WinSCP や PuTTY（Pageant）の設定については別なドキュメントでご紹介したいと思いますので、そちらの方を参照してください。

もし、このドキュメントの内容で間違いを見つけたり、うまくいかなかったり、分からないことがあったのなら、webmaster@hyec.org までご連絡ください（当然のことですが、*HYEC.ORG* サーバをご利用の方に限ります）。