

SR11000 システムへのログイン方法の変更について

システム運用係

1. 概要

2009年4月以降、これまでとは異なり、ログイン自体にはパスワードを使用せず「SSH鍵による認証」を行います。また、SSHはVersion2のみを有効とします。

そのため、初回ログイン時にのみ鍵の生成とシステムへの登録作業が必要となります。おおまかな流れは次のようになります。

- (1) Windows の場合はターミナルソフトを入手する
- (2) 認証に用いる鍵を生成する
- (3) Web ブラウザを用いて SR11000 に公開鍵を登録する
- (4) ログインする

手順は手元のマシンが Windows か UNIX 系オペレーティングシステム (MAC OS X を含む) かで異なりますので、OS ごとに分けて説明します。すでに公開鍵をお持ちの方は改めて鍵を生成する必要はありません。SR11000 システムへの鍵の登録のみで使用できます。

2. 接続情報

ログインに必要な情報は以下のとおりです。

ホスト名	sr11000-s.cc.u-tokyo.ac.jp
接続方法	SSH Protocol Version 2
認証方法	鍵による認証 (センター発行のパスワードはログインには使いません) 初回は Web による鍵登録が必要です。本章で説明します。

3. Windows システムからのログイン方法

Windows で使用できるターミナルソフトには PuTTY や Tera Term Pro などがあります。これらの中では PuTTY がもっとも鍵の扱いが容易なので、PuTTY を本センターの推奨ターミナルソフトとし接続方法を説明します。他のターミナルソフトについては解説しませんが、多くのソフトは鍵での認証に対応しているので SR11000 システムへのログインに使用することができます。また Cygwin を使用される方は UNIX 向けの解説をご覧ください。

① PuTTY の入手

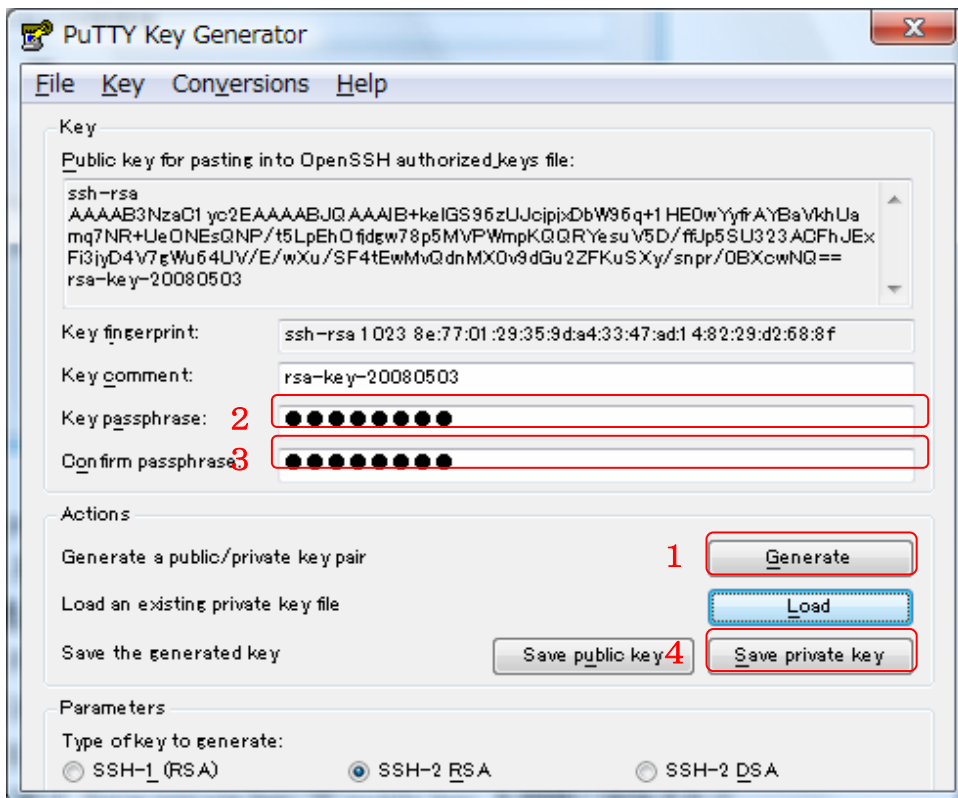
2009年3月現在 PuTTY は日本語化されたものが次のページより入手できます。

<http://hp.vector.co.jp/authors/VA024651/>

このページより日本語化 PuTTY をダウンロードし、適切なフォルダに展開してください。

② 鍵の生成

PuTTY の配布ファイルを展開すると puttygen.exe という実行可能ファイルがあるのでそれを実行します。PuTTY Key Generator の Window が開くので Generate ボタンをクリックします。すると画面の上の方にバーが出現するので、バーが右端に到達するまでバーの下あたりでマウスを動かします。



Key passphrase と Confirm passphrase に適当な他人に知られない文字列を入力します。センターから通知されたパスワードとは無関係なので、センターから発行されたパスワードを入力しないように注意してください。また、入力しなくても鍵としては使えますが、セキュリティ強化のため SR11000 システムに登録する鍵はパスフレーズで保護されていることを必須とします。パスフレーズはメモしたりファイルに書いたりしなくて済むよう、他人には推測されず、自分には覚えやすいものを設定してください。パスフレーズの入力が終了したら **Save private key** ボタンをクリックして鍵を保存します。この秘密鍵ファイルは絶対に他人に読まれることがないように、アクセス権には十分注意してください。この鍵が他人に読まれると SR11000 システムに不正侵入される危険性があります。**Save public key** は必要ありません (**Save private key** で **public key** も同時に保存されています)。以上で鍵の生成は完了ですが、次の登録作業のためにこの Window は開いたままにしておいてください。

③ 鍵の SR11000 システムへの登録

SR11000 システムには Window の上の方にある”Public key for pasting into OpenSSH authorized_keys file” と書かれた欄にある文字列を登録します。もし、前のステップの後 puttygen を終了してしまった場合は、再び puttygen を起動した後 ”Load”ボタンを押して前のステップで保存した鍵のファイルを読み込めば登録に必要な文字列が得られます。

鍵の登録のために、次の URL にアクセスしてください。

<https://regist.cc.u-tokyo.ac.jp/sr11000-key/>

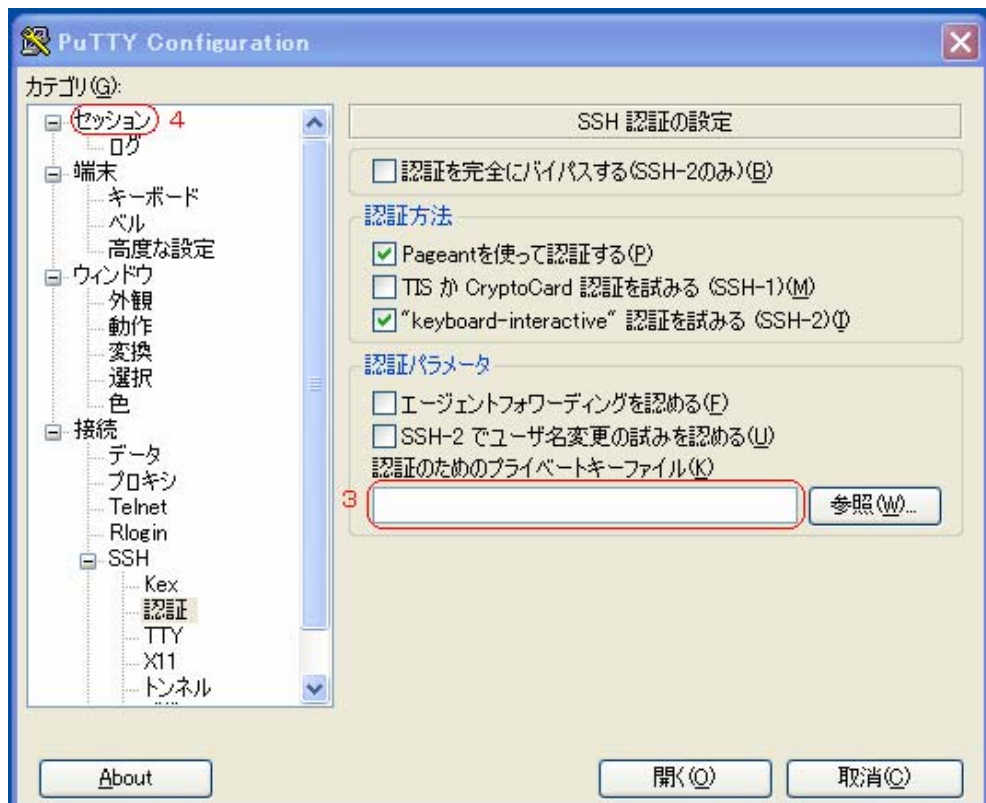
ユーザー名とパスワードを求められるので、センターから通知されたユーザー名とパスワードを入力してください。ここで入力するパスワードは鍵の保護のために入力したパスワードではなく、センター発行のパスワードです。認証に成功するとユーザーページが開きますので「公開鍵登録」のリンクをクリックしてください。開いたページの “Public Key” の欄に PuTTY Key Generator ウィンドウの ”Public key for pasting into OpenSSH authorized_keys file” に表示されている文字列をコピー&ペーストし、”Password” の欄に センター発行のパスワードを入力してください（すでに認証済みですが、セキュリティ上非常に重要な部分なので再度パスワード入力をお願いしております）。「登録」をクリックして完了画面が出れば登録完了です。登録まで少し時間がかかることがありますが、「登録」ボタンを何度もクリックしないようお願いします。

登録作業を 2 回以上行くと、最初に登録した鍵は削除されます。また、一度でもログインすると Web 経由での公開鍵登録はできなくなります。複数のコンピュータからログインするために公開鍵を 2 個以上登録する方法や、ログインした後の鍵の変更方法は後の「鍵について」の節で説明します。

④ ログイン

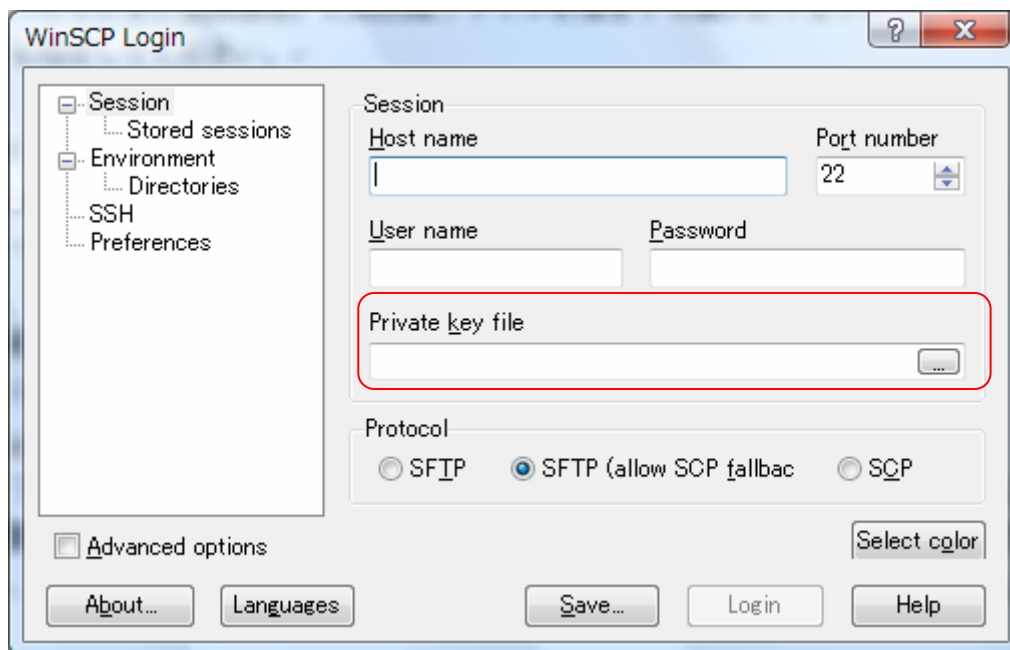
PuTTY を起動すると次ページ上のような画面が出ます。図に示した順番で以下のように情報を設定します

1. ホスト名を入力
2. 「SSH」の「認証」画面に移動して秘密鍵ファイルを設定する
3. 「セッション」画面に戻ってセッション名を入力し、保存する
4. 「開く」ボタンで接続する。ユーザー名を入力すると鍵のパスワードを聞かれるので、鍵作成の時に設定したパスワードを入力する。



⑤ ファイルコピー

ファイルコピーには WinSCP というソフトが使用できます。WinSCP は PuTTY Key Generator で生成して保存した秘密鍵がそのまま使えます。ホスト名やユーザー名を登録する「セッション登録画面」に秘密鍵ファイルを指定する欄がありますので、秘密鍵ファイルを指定してください。



4. UNIX システムからのログイン方法

Linux や MacOS X , Windows 上の Cygwin からのログインには OS にデフォルトでインストールされている OpenSSH が使用できます。

① 鍵の生成

次のコマンドを入力してください

```
$ ssh-keygen -t rsa
```

最初に鍵の保存場所を聞かれます。これはそのままリターンで大丈夫です。次にパスフレーズを求められるので入力して下さい。センターから通知されたパスワードとは無関係なので、センターから発行されたパスワードを入力しないように注意してください。また、入力しなくても鍵としては使えますが、セキュリティ強化のため SR11000 システムに登録する鍵はパスフレーズで保護されていることを必須とします。パスフレーズはメモしたりファイルに書いたりしなくて済むよう、他人には推測されず、自分には覚えやすいものを設定してください。確認のためもう一度パスフレーズを入力したら鍵生成は完了です。

② 鍵の SR11000 システムへの登録

鍵の登録のために、次の URL にアクセスしてください。

<https://regist.cc.u-tokyo.ac.jp/sr11000-key/>

ユーザー名とパスワードを求められるので、センターから通知されたユーザー名とパスワードを入力してください。ここで入力するパスワードは鍵の保護のために入力したパスワードではなく、センター発行のパスワードです。認証に成功するとユーザーページが開きますので「公開鍵登録」のリンクをクリックしてください。開いたページの“Public Key”の欄に `~/.ssh/id_rsa.pub` の内容をコピー&ペーストし、“Password”の欄にセンター発行のパスワードを入力してください（すでに認証済みですが、セキュリティ上非常に重要な部分なので再度パスワード入力をお願いしております）。「登録」をクリックして完了画面が出れば登録完了です。登録まで少し時間がかかることがあります。「登録」ボタンを何度もクリックしないようお願いします。

登録作業を 2 回以上行くと、最初に登録した鍵は削除されます。また、一度でもログインすると Web 経由での公開鍵登録はできなくなります。複数のコンピュータからログインするために公開鍵を 2 個以上登録する方法や、ログインした後の鍵の変更方法は次節「鍵について」で説明します。

③ ログイン

```
$ ssh sr11000-s.cc.u-tokyo.ac.jp -l xxxxxx
```

でパスワードを入力すればログインできます。自動的に公開鍵認証が行われます。

④ ファイルコピー

```
$ scp file xxxxxx@sr11000-s.cc.u-tokyo.ac.jp:
```

でパスワードを入力すればコピーできます。自動的に公開鍵認証が行われます。

5. 鍵について (Windows, UNIX 共通)

① Web 登録システムの有効期間

Web による鍵登録が可能なのは最初にログインに成功するまでです。常に登録システムを開いておくと、悪意を持った第三者にパスワードが漏れた場合に登録システムを通じて攻撃者が生成した鍵が登録されてしまい、鍵認証にしている意味がなくなってしまうためです。鍵が未登録なはずなのに登録システムに登録を拒否された場合は、何者かによって鍵を登録されてしまったことになるので、至急センターまでご連絡下さい。

② Web 登録システムに入力できる鍵

Web 登録システムは OpenSSH 形式の鍵を受け付けます。Windows では推奨ソフトである PuTTY の他、Tera Term Pro もこの形式の鍵を生成します。

③ 鍵の追加と変更

ログインした後に、他のマシン用の鍵を追加したり、登録済みの鍵を変更する場合は SR11000 システムにログインし、`~/.ssh/authorized_keys` に書かれている公開鍵をエディタで直接編集してください。一行に一個の公開鍵を書きます。鍵の文字列は長いため、多くの場合は複数行にわたって表示されることとなりますが、データ上は一個の鍵は一行でなくてはなりません。鍵の途中で改行を入れないようご注意ください。このファイルを削除したり、書かれている公開鍵を壊してしまうとログインできなくなります。

④ 秘密鍵の管理

鍵の生成方法で説明したとおり、秘密鍵を守ることは SR11000 システムのセキュリティを守る上で非常に重要なので、パスワードや秘密鍵が他人に漏れることのないよう十分ご注意ください。万が一秘密鍵が他人に漏れた場合は必ずセンターに連絡し、適切な処置についてご相談下さい。複数のマシンから SR11000 システムにログインする場合は、それぞれのマシンで鍵を生成して、上で説明した方法で SR11000 システムの方に鍵を追加します。秘密鍵をコピーして他のマシンで使用してはいけません。

⑤ 別システムへのログインに使用している鍵の流用

一台のクライアントマシンから SR11000 システムと他の公開鍵認証を用いるシステム両方にログインする場合、他のシステムに登録した鍵を SR11000 システムにも登録することは差し支えありません。ただし、他のシステム用に登録していた鍵がパスワードで保護されていない場合は SR11000 システムには登録できません。一般的に、パスワードのない鍵の使用は非常に危険なので、その場合は、別のシステムに登録していた鍵の方をパスワード付きに変更し、それを SR11000 システムにも登録することをお勧めします。

UNIX システムで複数の鍵を使い分けたいときは `~/.ssh/config` に次のように書きます。

```
(例) sr11000-s.cc.u-tokyo.ac.jp には秘密鍵 ~/.ssh/id_rsa_sr11000 を使用するとき
Host sr11000-s.cc.u-tokyo.ac.jp
    User z00000
    IdentityFile ~/.ssh/id_rsa_sr11000
```