X Windowの利用について
科学技術計算システムを利用するには?

目次

本パンフレットに関するお問い合わせ

X Windowの利用について (科学技術計算システムを利用するには?)

発行

農林水産研究情報総合センター
農林水産省 農林水産技術会議事務局 筑波産学連携支援センター 情報システム課
更新日: 2022年6月10日 Ver.0.6

問い合わせ

E-Mail: request @ affrc.go.jp

農林水産研究情報総合センター URL

URL https://itcweb.cc.affrc.go.jp/

1. MS Windows 用 SSH ターミナルソフト

1.1. PuTTY

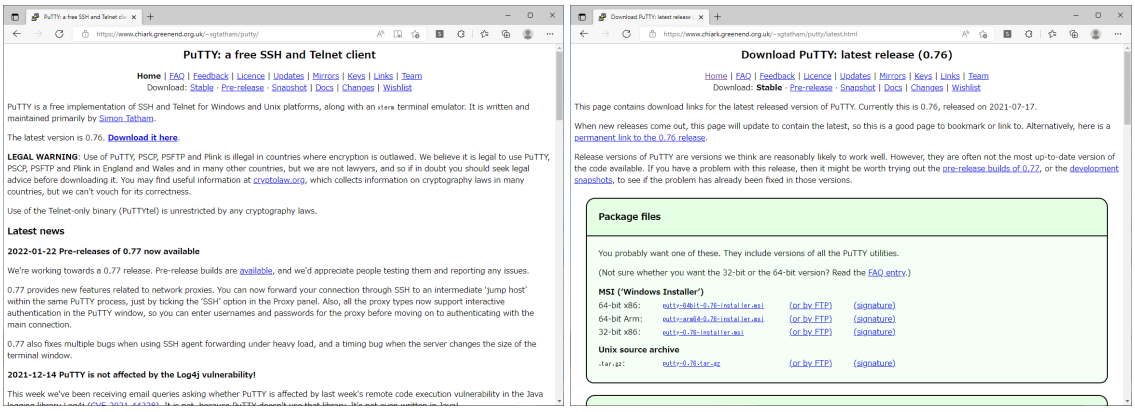
PuTTY(パティ)は、 Simon Tatham 氏が開発、公開(MIT License)している、Windows で動作する SSH クライアントプログラムを含むターミナルエミュレータ(端末ソフト)です。 標準で UTF-8 をサポートしていますので、UTF-8 環境であれば日本語の表示も可能です。

1.1.1. PuTTY の入手とインストール

ダウンロード

PuTTYの公式Webページからダウンロードします。

- 公式サイト: https://www.chiark.greenend.org.uk/~sgtatham/putty/index.html
- ダウンロード: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html



PuTTY の Web サイト

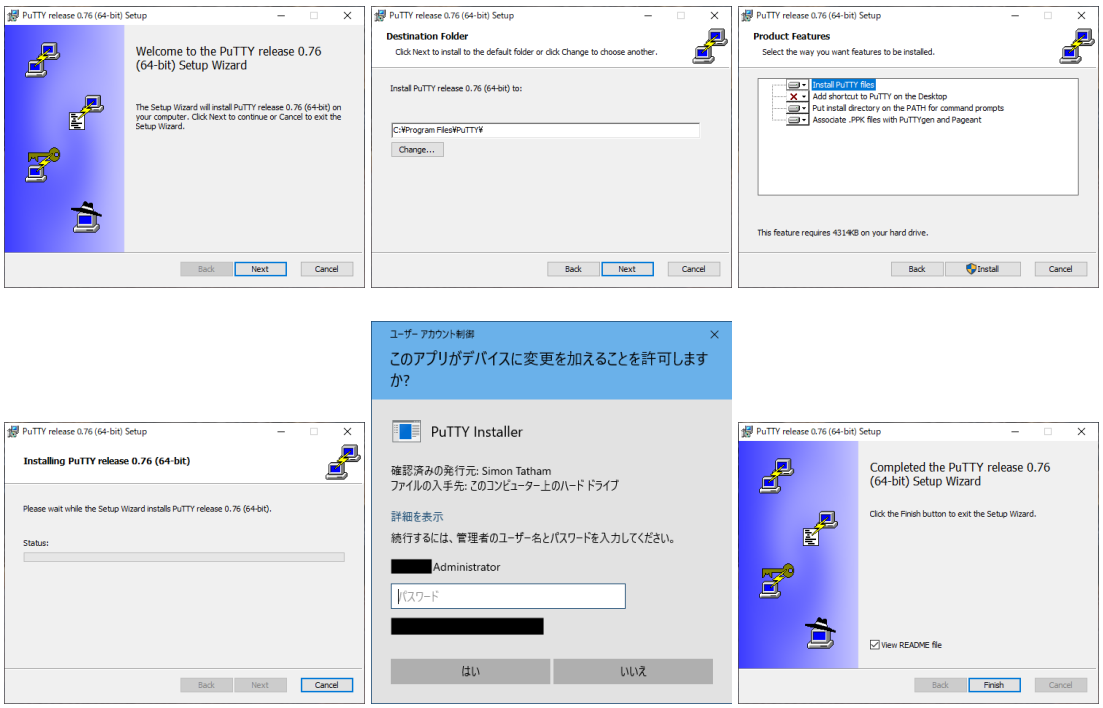
通常は、Windowsインストーラ版(64bit x86)をダウンロードします。

```
MSI ('Windows Installer')
64-bit x86: putty-64bit-0.76-installer.msi (or by FTP)  (signature)
```

- 日本語化された「PuTTYjp」を公開されていた「hdk さん」は、バイナリ配布を終了しました。
  - 「バイナリ配布終了のお知らせ (2020-09-26)」
  - http://hp.vector.co.jp/authors/VA024651/PuTTYkj.html
- EUC や SJIS 環境を使う場合は、日本語化されたものを使うか、Tera Term を使ってください。

インストール手順

ダウンロードしたインストーラ(putty-64bit-0.76-installer.msi 2022/05/17 16:10)を
ダブルクリックして、インストーラを起動します。



起動したインストーラに従ってインストールします。途中で管理者権限を求められますので、管理者のパスワードを入力してください。
必要に応じて、ショートカットやタスクバーにピン留めしてください。

1.1.2. SSH 接続 (パスワード認証)

パスワード認証により、SSH 接続を行う手順を紹介します。 通信は暗号化されていますので、パスワードの送信も暗号化されています。

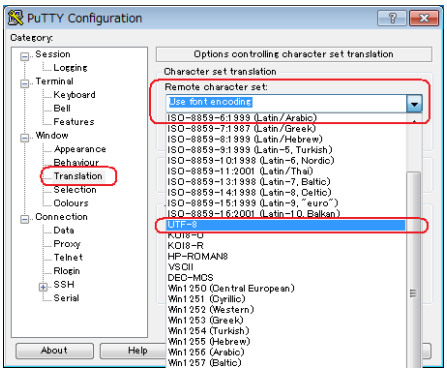
科学技術計算システムへのログインは、公開鍵認証(パスワード認証不可)になりました。

SSHの接続では、ホスト(サーバ)のホストキー(公開鍵)により、接続先の認証(なりすましチェックなど)を行っています。
初めて接続した場合、ホストキーを保存するよう求められますので、保存してください。 サーバの更新や再インストールなどによってホストキー(公開鍵)を作り直した場合、セキュリティの警告(保存されているホストキーと異なる)が出ますので、 ホスト(サーバ)の管理者に確認し、問題ない(サーバ更新などを行っている)ようでしたら「Accept」を選択して公開鍵を書き直して下さい。

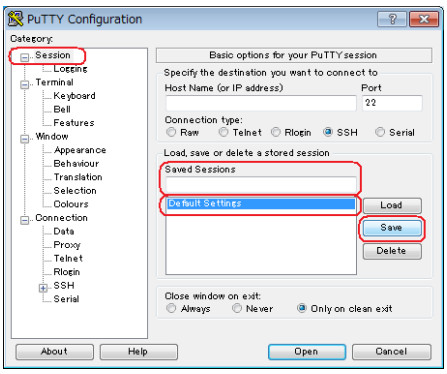
初期設定

PuTTY を起動すると、「PuTTY Configuration」ウィンドウが開きます。

文字コードの設定は、デフォルトで「UTF-8」になっており、その他の項目も標準設定で問題ないと思います。
必要に応じて、設定項目を確認し変更してください。

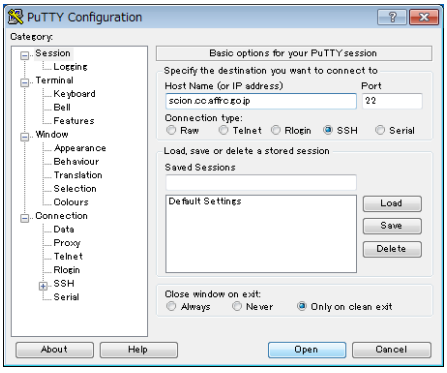


よく利用する設定を保存することができます。
Category:「Session」を選択し、「Saved Session」欄に名前を付けて「Save」を押して登録します。 登録されたセッション名を選択して読み込む事で接続先毎の設定を一括して変更することができます。 共通する設定は「Default Settings」を選択して保存すると良いでしょう。



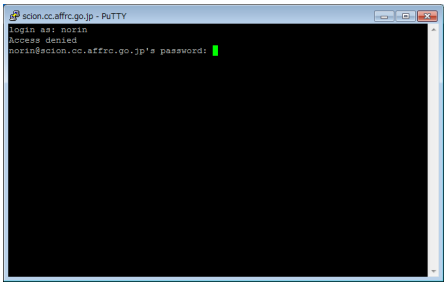
接続

Category:「Session」を選択し、「Host name (or IP address)」欄に接続先のホスト名を入力して、「Open」 をクリックします。

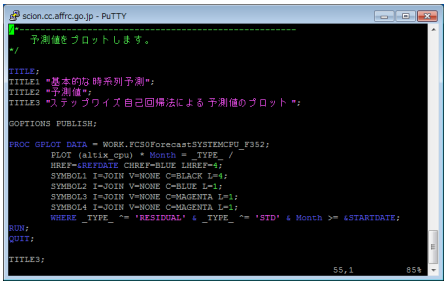


初めて接続するホストの場合、ホストの公開鍵を登録するかどうかの確認ダイアログが表示されます。
通常は「Accept」を選択して登録します。
もし、接続先ホストの公開鍵が変更された場合は、「WARNING-POTENTIAL SECURITY BREACH!」の様なダイアログが表示されます。 この場合、別のホストが接続先になりすましていることが考えられますので、ホストの管理者に確認してください。

ターミナルのウィンドウが開きますので、「login as:」に続いてログイン名を、「passwd:」に続いてパスワードを入力してください。



文字コードの設定を UTF-8 にしていれば、日本語 (UTF-8 環境) の表示も問題ありません。



1.1.3. SSH 公開鍵認証による接続

パスワード認証と比較して、よりセキュアな公開鍵認証を利用する手順を紹介します。

- 自分の認証キー (秘密鍵と公開鍵のペア) を生成します。
- 接続するホストに公開鍵を登録します。
- PuTTY に秘密鍵の場所 (PATH) を登録します。
- 接続先ホストのユーザ環境に公開鍵が登録されている場合、秘密鍵と照合されます。 秘密鍵を参照するには、パスフレーズの入力が必要です。

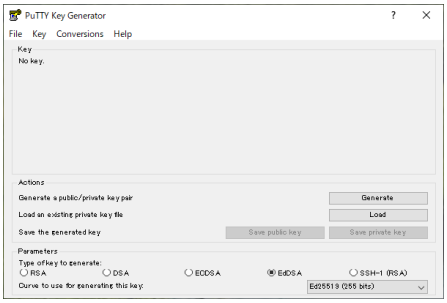
自分の認証キーを生成

PuTTY と同時にインストールされた PuTTYgen を使います。 Windows のスタートメニューから、「PuTTY」「PuTTYgen」を起動します。

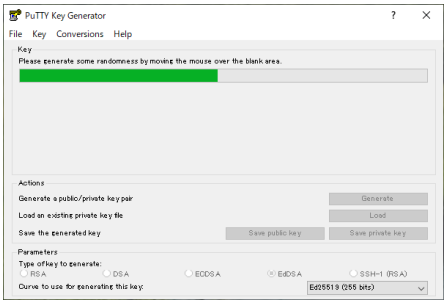
生成するキーのタイプを指定します。

- 「EdDSA」を選択し、「Ed25519 (255 bits)」を指定します。

Ed25519 か RSA 2048 bit以上を作成してください。

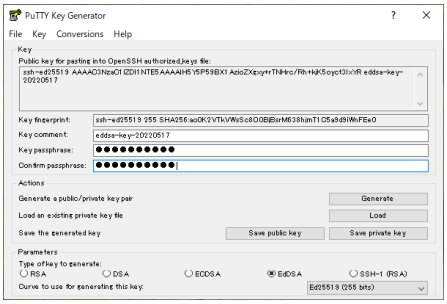


キーを生成します。



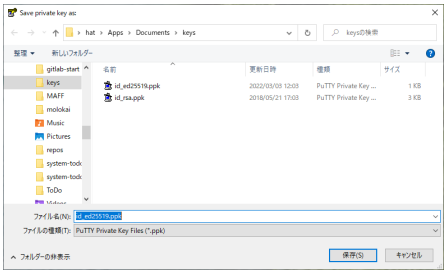
- 「Generate」ボタンをクリックします。
- ボタンをクリックした後に、ウィンドウ内でマウスカーソルを適当に動かす(ランダムな値を与える)と、キーが生成されます。

生成したキーのパスフレーズを入力します。



- 生成したキーはパスフレーズを知っている者(自分)だけが使えるようにするため、必ずパスフレーズを入力してください。
- パスフレーズを入力しないと、秘密鍵(パソコン)を盗まれた場合、誰でもなりすましてログイン可能です。

生成したキーを保存します。



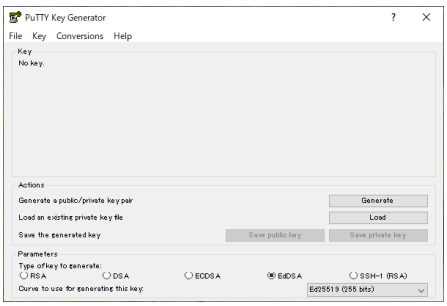
- パスフレーズを入力したら、「Save private key」ボタンを押して秘密鍵を保存します。 ここでは、ファイル名「id_ed25519.PPK」とします。
- ユーザのディレクトリ配下に「_ssh」などのフォルダを作成し、その配下に保存します。(C:\Users\ユーザ名_ssh)
- 同様に、公開鍵を「Save public key」ボタンを押して、ファイル名「id_ed25519.pub」などとして保存します。

接続するホストに公開鍵を登録

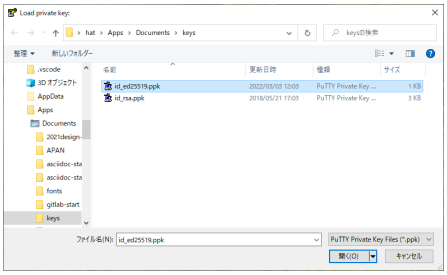
科学技術計算システムでは、公開鍵登録用の専用Webサイトで登録を行います。
登録する公開鍵は、OpenSSH形式となりますので、生成した秘密鍵を「PuTTYgen」に読み込むことで、OpenSSH形式の公開鍵を表示し、コピー&ペーストして登録することができます。

パスワード認証を禁止しているサーバについては、それぞれのシステムで公開鍵登録の方法が異なりますので、管理者に確認してください。 (公開鍵をメールやファイルなどで管理者あてに送り、管理者が登録するといった方法もあります)

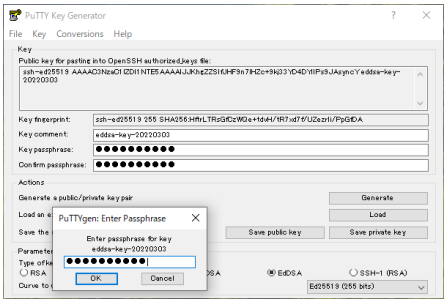
PuTTYgenを起動して、「Load」ボタンをクリックし、秘密鍵を読み込みます。



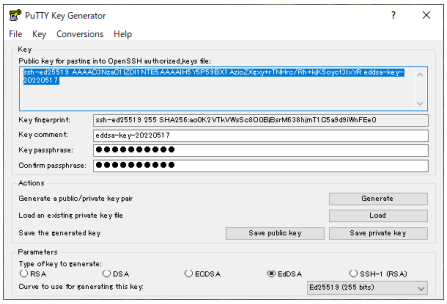
保存した秘密鍵を選択します。



秘密鍵を開くため、パスフレーズを入力します。



Public key for pasting in to OpenSSH authorized_keys file: に、表示されている公開鍵をコピーして、公開鍵登録します。

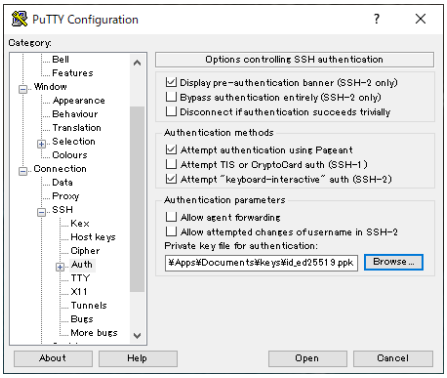


- サーバのホームディレクトリ配下の .ssh/authorized_keys ファイルにペーストします。
- 科学技術計算システムでは、専用Webインターフェースでこの作業を行います。

PuTTY に認証キー (秘密鍵) を登録

再度、PuTTY を起動し、初期設定で保存したセッション名を選択し「Load」(「読込」) をクリックします。

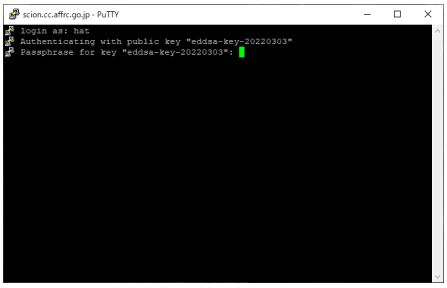
Category:から「SSH」を選択し、「Auth」をクリックします。
「Private key file for authentication:」の欄に秘密鍵のファイルを指定します。「Browse…」ボタンでファイ ルを指定できます。



秘密鍵の設定を保存するため、Category:「Session」をクリックし、セッション名を指定して保存しておきます。

公開鍵認証での接続

接続先ホスト名を指定し、「Open」をクリックしてターミナルを開きます。
公開鍵が登録されているホストであれば、
「Pathphrase for key "eddsa-key-20220517“」の様に表示されますので、 パスフレーズを入力してログインします。



システムログイン端末による公開鍵の登録(パスワード認証が許可されている場合)

パスワード認証が許可されているシステムの場合は、次の方法で公開鍵を登録することが可能です。

- PuTTYを起動して、パスワード認証でホストにログインします。
- 上記「接続するホストに公開鍵を登録」で説明した PuTTYgen を使用し表示した OpenSSH 公開鍵をコピーして、 `.ssh/authorized_keys` に追加します。
- 端末上のコマンドは、以下のようにします。(一行で入力します)

```
[norin@fe01 ~]$ echo "ssh-ed25519
AAAAxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx eddsa-key-
20220517" >> ~/.ssh/authorized_keys
```

  - `echo "` まで入力し、コピーした公開鍵をペーストします。
  - 続けて `" >> ~/.ssh/authorized_keys` と入力して、エンターキーを押す。

- `cat` コマンドで、登録された `authorized_keys` を確認します。

```
[norin@fe01 ~]$ cat ~/.ssh/authorized_keys
ssh-ed25519 AAAAxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
eddsa-key-20220517
```

- ファイルパーミッション (アクセス権限) に注意してください。

```
[norin@fe01 ~]$ ls -l .ssh
合計 30
-rw------- 1 norin research  100  4月 13 11:04 authorized_keys
```

  - `authorized_keys` のアクセス権限が `-rw-------` の様になっていない場合は、 `chmod 600 .ssh/authorized_keys` としてください。

- 設定を確認したらログアウトしてください。