SSH鍵作成とログイン PuTTY 版

自然科学研究機構 岡崎共通研究施設 計算科学研究センター(RCCS)

(PuTTY 0.80 で動作確認)

更新履歴

- •2019/5/28 初稿作成
- 2019/7/9 PuTTYgenについての記述を追加
- 2021/2/1 推奨鍵種を Ed25519 に変更。他微調整
- 2021/5/24 PuTTY 0.75 向けに更新
- 2022/1/5 PuTTY 0.76 で動作確認
- 2022/12/20 PuTTY 0.78 で動作確認。新システム向けに改訂
- •2023/6/2 用語の修正
- 2024/1/18 PuTTY 0.80 で動作確認



この資料ではPuTTYと付属ツールを用いてSSH鍵を作成し、 ログインサーバへログインする手順を説明します。



- PuTTYのインストール
- •SSH鍵の生成
- ・ 公開鍵の登録
- ・ログイン

<u>PuTTYのインストール</u>

PuTTY は以下のサイトよりダウンロードができます。

https://www.chiark.greenend.org.uk/~sgtatham/putty/

以下のアドレスから最新版のダウンロードページができます。 <u>https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html</u>

MSI(Windows Installer)版を指示に従ってインストールしてください。 以下では PuTTY および PuTTYgen を利用します。

PuTTYを既にインストール済で PuTTYgen が見つからない場合は、 ダウンロードサイトの Alternative binary files の中から PuTTYgen (puttygen.exe) を選んでダウンロードしてください。



PuTTYgen を起動します。 Windows 10 の場合は例えば以下の場所から起動できます。



<u>SSH鍵の作成(2)</u>

RCCS では以下の種類の鍵を推奨しています。

- Ed25519 (EdDSA 指定、Ed25519 (255 bits) 選択; Ed448 は不可)
- ECDSA (ビット数 256, 384, 521)
- RSA 4096 ビット (RSA 選択、右下数字を 4096; 要 PuTTY 0.75 以降)
- 良くわからない、こだわりの無い場合は Ed25519 でお試しください

PuTTY Key Generator	? ×	
File Key Conversions Help		
Key		
No key.		
	鍵種類指定後	クリックして生成
	(クリック後、	マウスカーソルを
	移動させると	_進みます)
Actions	3	
Generate a public/private key pair	Generate	
Load an existing private key file	Load	
Save the generated key	Save public key Save private key	
Parameters Type of key to generate:		鍵の種類を指定します
Curve to use for generating this key:	2 Ed25519 (255 bits)	

鍵の長さ指定 (RSA, ECDSA, EdDSA 時)

SSH鍵の作成(3)

鍵の生成が終わると以下のような表示になります。

	😴 PuTTY Key Gene	rator			? ×
	File Key Conversio	ons Help			
RCCS では秘密鍵の 《スフレーズには 英小文字	Key Public key for pastir ssh-ed25519 20210524	ng into OpenSSH authorized keve	: file: 1		eddsa-key-
	Key fingerprint:	ssh-ed25519 255 SHA256:			
天八又于	Key comment:	eddsa-key-20210524			
数字	Key pa sphrase:	•••••	•	<u></u>	
記号	Confirm passphrase	••••••	•	2	
	Actions				
74悝を召む10又子	Generate a public/p	rivate key pair			Generate
人上のものを指定する	Load an existing priv	vate key file			Load
こうお願いしています	Save the generated	key		Save public key	Save private key
	Parameters				3
	Type of key to gene ○ RSA	rate: O DSA — O) ECDSA	● EdDSA	

ログイン用の公開鍵は こちらを使います。 一日メモ帳などに書き 出し、保存することを お勧めします。 (ssh-やecdsa-から始まる 全てをきちんとコピー してください。)

パスフレーズを設定後、 ここをクリックして 秘密鍵を保存 rccs.ppk や ccfep.ppk の ようにわかりやすい名前 をつけましょう

- 秘密鍵については他人の触れない場所に保存してください。
- OpenSSH 用の秘密鍵が必要な場合は、Conversions メニューから作成できます - 公開鍵の保存を忘れた場合も Conversions メニュー等から鍵を読み込めば復元 できます。秘密鍵を無くした場合は作り直しです。

公開鍵の登録

実際にログインをする前に生成した公開鍵を 登録する必要があります。

以下のリンクに手順がありますので、 こちらに従って登録して下さい。 <u>https://ccportal.ims.ac.jp/account/</u>

PuTTYgen の「Save public key」の鍵ではダメです。 画面上部に表示される Public key for pasting into... と 表示されているテキストをコピー & ペースト(もしくは保存 したファイルからコピー)してください。

秘密鍵は他人の触れない場所に保存してください。



それではPuTTYを起動します。

PuTTY Configuration	2	X
Putty Configuration Category: Category: Category: Category: Congging Terminal Category: Compared Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy SSH Serial Telnet Rlogin SUPDUP	Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Port 22 Connection type: O SSH O Serial O Other: Telnet Load, save or delete a stored session Saved Sessions Default Settings Load Save Delete Close window on exit: Always O Never O Only on clean exit	
About	Open Cancel	

(左画面のメニューの表示順序は PuTTY のバージョンによって少し違う場合があります)



「Session」で Host Name に ccfep.ims.ac.jp と入力します

PuTTY Configuration		×
Category: Session - Logging Terminal - Keyboard - Bell - Features Window - Appearance - Behaviour - Translation - Selection - Colours Connection - Data - Proxy SSH - Serial - Telnet - Rlogin - SUPDUP	Basic options for your PuTTY ses Specify the destination you want to connect Host Name (or IP address) ccfep.ims.ac.jp Connection type: Image: SSH SSH SSH Serial Other: Telnet Load, save or delete a stored session Saved Sessions Default Settings Close window on exit: Always Never Image: Only on clear	sion to Port 22 ✓ Load Save Delete
About	Open	Cancel

<u>ログイン(3)</u>

Connection -> Data で Auto-login username にユーザ ID 入力

B PuTTY Configuration	×	
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy SSH Serial Telnet Rlogin SUPDUP	Data to send to the server Login details Auto-login username uid When username is not specified: • Prompt • Use system username (Motoshi Kamive) • Terminal details Terminal-type string xterm Terminal speeds 38400,38400 Environment variables Variable Add Value Remove	を入力 り指定 うの)
About	Open Cancel	

(このステップは省略できます。省略した場合、接続時に入力することになります。)



Connection -> Data -> SSH-> Credentials で秘密鍵(.ppkファイル)を指定

PuTTY Configuration	งท	×	
Category: Logging 	▲ Credentials to authentic Public-key authentication Private key file for authentication: Certificate to use with the private key Plugin to provide authentication respon Plugin command to run	TYgenで作成、保存し 建ファイルを指定しま ************************************	った ます
About	Open	Cancel	

Credentials メニューが無い場合は、Connection -> Data -> SSH に秘密鍵を 入力するフィールドがあるはずです



このまま接続できますが、Session で一旦設定を保存します。

PuTTY Configuratio	n X
Category: Session 	Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Connection type: Onnection type: SSH SSH Load, save or delete a stored session RCCS Default Settings Load RCCS Default Settings Close window on exit: Always Never Only on clean exit
About	

3. 保存できたら接続しましょう



初回接続時にはまず以下のようなダイアログが表示されます。



- ad:de:79:30:81:b0:b1:6a:17:f5:6f:ea:f4:b4:3b:de (MD5)
- e3:a9:bb:6f:e4:a9:37:fd:98:14:54:16:3c:81:2d:aa (MD5)
- 07:7e:df:7b:16:47:a8:f5:7c:48:b0:a3:d3:86:71:6a (MD5)

fingerprint

有効な鍵の

- wnEM30z4AxyDJ9XI/DdGr2PINeoivFRR8v5krXHEmdU (SHA256)
- 0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZElolfVqXvbI (SHA256)
- Nhg+9Lgj3XeuW//A/j7jqgUJIIxWehryCtStIp1Dirs (SHA256)



接続すると秘密鍵のパスフレーズを聞かれるので入力します。





正しいパスフレーズを入力できれば、以下のようにログインできます。



ヒント: Pageant を起動し、鍵を登録しておけばログインのたびにパスフレーズを 聞かれることが無くなります。(Pageant への登録時だけは入力が必要です)