> 作成:平成19年5月8日 修正:平成29年3月1日

### SSH で公開鍵認証方式を使いログインする

#### 目 次

1.		はじめに1
2.		留意事項1
3.		公開鍵と秘密鍵の作成方法2
	3.1.	公開鍵と秘密鍵の作成2
	3.2.	公開鍵のサーバ登録5
4.		公開鍵認証によるログイン方法7

#### 1. はじめに

はじめに、このドキュメントは PKI (公開鍵認証基盤) についてある程度知識がある方を 対象に記述しています。従って「公開鍵認証」「秘密鍵」「公開鍵」「パスフレーズ」など、 以下の説明の中で出てくる用語がわからない方は各自で調べて、十分に用語を理解した上 でこのドキュメントを読み進めてください。

本学の遠隔端末接続サービスでは、学内ネットワークからの接続に限り、SSH のユーザ認 証方式の一つである「パスワード認証」を許可しています。この「パスワード認証」を使 用した場合、通信経路はホスト認証によって暗号化されますが、パスワードが通信経路に 流れます。また、何らかの理由でパスワードが第三者に知られてしまうと、不正アクセス の被害を受ける可能性があります。

これらの理由により、本学では自宅などのインターネット上から本学の遠隔端末接続サ ービスを利用する場合は「パスワード認証」によるユーザ認証を禁止しており、「公開鍵認 証」によるユーザ認証で接続する必要があります。

### 2. 留意事項

公開鍵認証を利用する場合、以下の事項に留意してください。

- 作成した秘密鍵は適切な場所に保管するようにしてください。
- パスフレーズを設定しないことができますが、その場合は秘密鍵が他人に入手される
   と、不正にログインされるなどの危険性が高くなります。必ずパスフレーズを適切に
   設定してください。
- 認証情報の暗号化の完全性を保証するものではありません。

Copyright(c) 2001-2021, Kyoto Sangyo University. All rights reserved.

# 3. 公開鍵と秘密鍵の作成方法

公開鍵と秘密鍵の作成方法にはいくつかありますが、ここでは本学の情報処理教室等で 利用できる Windows クライアントにインストールしている TeraTerm を利用します。公開鍵 と秘密鍵を作成する方法について「sandai」というユーザ ID を例に説明します。

# 3.1. 公開鍵と秘密鍵の作成

1. 共通アプリケーションにある「TeraTerm」を起動すると、下記のウインドウが表示され るのでキャンセルを押します。

Tera Term: 新しい接	統	×
● TCP/ <u>I</u> P	ホスト(T): bc2000.kyoto-su.ac.jp ロレストリ(Q) サービス: Telnet の <u>S</u> SH SSHバージョン(V): SSH2 の その他 プロトコル( <u>C</u> ): UNSPEC	•
◎ シリアル( <u>E</u> )	ボート(B): COM1: 通信ボート (COM1) OK キャンセル ヘルブ(出)	4

2. 「設定」から「SSH 鍵生成」を選択します。



Copyright(c) 2001-2021, Kyoto Sangyo University. All rights reserved.

SHI 🚺 🕑 KSH 🚺 💟 USA	A ビット数(B):	主5X(G)
CDSA-256 🔘 ECDSA	4- <u>3</u> 84 2048	閉じる( <u>C</u> )
CDSA- <u>5</u> 21 💿 <u>E</u> D255	19	
種のハスフレース: スフレーズの確認 コメント(Q):		
rypt KDF形式( <u>K</u> )	ラウンド数(N): 11	ô 🔤
スント(Q): コメント(Q): rypt KDF形式( <u>K</u> )	ラウンド数(N): [11	5

.....

3. 鍵の種類を「RSA」、ビット数を「2048」にして生成ボタンを押します。

4. 鍵のパスフレーズを入力して、公開鍵を保存します。公開鍵の保存は任意の場所で結構 ですが、このあと保存する秘密鍵とセットにしておくと良いでしょう。

建の種類	ピット業(B):	生成(G)
C RSA1 O RSA C DSA	2048	開じる(0)
© EUDSA-200 () EUDSA-384	2010	[ move (
○ COD3H- <u>9</u> 21 (○ ED20019)		
鍵を生成しました。		-
鍵のパスフレーズ: ●●●●●	*****	
バスフレーズの確認 ●●●●●		
コメント(0):		
□bervat KDE形式(K) ラ	ウンド数(N): 16	
■borypt KDF形式(K) ラ	ウンド数(N): 16	 a

5. 秘密鍵を保存します。秘密鍵は USB メモリ等に保存し、家に持ち帰ることができるよう にしておくとよいでしょう。**秘密鍵はむやみにコピーせず、オンラインストレージ等に** 保存したり、他人に渡したりしないよう、厳重に管理してください。

\_\_\_\_\_

鍵の種類 の RSA1 (④ <u>R</u> SA (⑦ の ECDSA- <u>2</u> 56 (⑥ EC の ECDSA-521 (◎ EC	) <u>D</u> SA )DSA- <u>3</u> 84 )25519	ビット数( <u>B</u> ) 2048	<u>生成(G)</u> 閉じる( <u>C</u>
鍵を生成しました。	•		
鍵のバスフレーズ:			
バスフレーズの確認			
⊐メント( <u>0</u> ):	-		- Ť
bcrypt KDF形式( <u>K</u> )	5	ウンド数(N): 16	
公開鍵の保存	7()	秘密鍵の保存(P)	

秘密鍵が保存できたら、閉じるボタンを押してウインドウを終了します。

次項では、作成した公開鍵を接続先のサーバに登録する方法を説明します。

## 3.2. 公開鍵のサーバ登録

公開鍵認証を行うには、接続するサーバの自身のユーザホームディレクトリ以下の所定 ファイル(.ssh/authorized\_keys)に公開鍵を登録する必要があります。下記の手順に沿 って進めてください。登録は学内ネットワークに接続した端末で実施します。

1. TeraTermを起動し、接続先サーバを確認して OK を押します。

Tera Term: 新しい接	続	x
® TCP∕ <u>I</u> P	ホスト(T): cc2000.kyoto-su.ac.jp ・ ビストリ(O) サービス: TCPボート#(P): 22 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	
◎シリアル(E)	ボート(R): COM1: 通信ボート (COM1) OK キャンセル ヘルプ(H)	*

2. 「ユーザ名 (本学ユーザ ID)」、「パスフレーズ (**POST にログインする際のパスフレーズ**)」 を入力します。

ユーザ名( <u>N</u> ): sanda	ii		
パスフレーズ(P): 🔸			
	スワートをメモリ上に記) ージェント転送する( <u>0</u> )	思する( <u>M</u> )	
・ プレインパスワードを	吏う(上)		
© <u>R</u> SA/DSA/ECDSA/E	D25519鍵を使う [	秘密鍵( <u>K</u> ):	
● rhosts(SSH1)を使う [	ローカルのユ ホスト鍵(E): ] [	-fa(y)	
◎ チャレンジレスボンス	認証を使う(キーボード-	(ンタラクティブ)( <u>C</u> )	
Pageantを使う			

Copyright(c) 2001-2021, Kyoto Sangyo University. All rights reserved.

ログインができたら先ほど作成した公開鍵を cc2000 に設置します。まずは設置するための場所を作成します。下記の通りにコマンドを実行してください。
 ※「<sup>~</sup>/.ssh」が既に存在している場合は、このステップは不要です。

\$ mkdir ~/.ssh	
\$ chmod 700 ~/.ssh	

4. 公開鍵の「id\_rsa.<u>pub</u>」をTeraTermにドラッグ&ドロップします。

		ーター 🕨 リムーバブル ディスク (F:)
Cc2000.kyoto-su.ac.jp - sandai@cc2002: ~ VT ファイル(F) 編集(E) 設定(S) コントロール(O) ウン (H) sanda i@cc2002: * \$	<ul> <li>         登理         <ul> <li></li></ul></li></ul>	印刷 書き込む 新しいフォル 名前 id_rsa id_rsa,pub

5. コピー先を指定するダイアログが表示されますので「<sup>~</sup><u>/.ssh</u>」と入力し、「SCP」を押します。(sshの前にある「.」をつけ忘れないようお願いします。)

ファイル転送を行	いますか?
SCP	
送信先(T):	~/.ssh/
	 空のときはホームディレクトリに送信されます

#### ■■ コンピュータ環境の使い方 ■■

6. 公開鍵を登録します。下記のコマンドを実行してください。

\$ cd ~/.ssh
\$ cat id\_rsa.pub >> authorized\_keys
\$ chmod 600 authorized\_keys
\$ rm id\_rsa.pub
\$ exit

※exit を入力すると TeraTerm が終了します。

# 4. 公開鍵認証によるログイン方法

この項では、3の項で作成・保存した公開鍵と秘密鍵を用いた、公開鍵認証によるログ イン方法について説明します。ここではTeraTermを使用し、cc2000に「sandai」というユ ーザ ID で、公開鍵認証でログインする方法を説明します。

1. TeraTermを起動し、接続先サーバを確認して OK を押します。

Tera Term:新しい	<u>接続</u>	x
● TCP/IP	ホスト(T): cc2000.kyoto-sulac.jp ロビストリ(Q) サービス: TCPポート#(P): 22 の SSH SSHバージョン(V): SSH2 の その他 プロトコル(Q): UNSPEC	•
◎ シリアル( <u>E</u> )	ボート(B): COM1: 通信ボート (COM1)	•
	○K キャンセル ヘルプ(H)	

■■ コンピュータ環境の使い方 ■■

 「ユーザ名(本学ユーザ ID)」、「パスフレーズ(鍵作成時に設定したパスフレーズ)」を 入力します。次に「RSA/DSA/ECDSA/ED25519 鍵を使う」にチェックを入れ「秘密鍵」ボ タンをクリックし、作成した秘密鍵を選択し、OK を押します。

.....

SSH認証	
ログイン中: cc2000kyoto-su.ac.jp 認証が必要です.	
ユーザ名( <u>N</u> ): sandai	
パスフレーズ(B): ●●●●●●●●●	
パスワードをメモリ上に記憶する(M)	
□ エージェント転送する(0)	
◎ プレインパスワードを使う(1)	-
◎ <u>R</u> SA/DSA/ECDSA/ED25519鍵を使う 秘密鍵( <u>K)</u> F:¥id_rsa	
◎ rhosts(SSH1)を使う ローカルのユーザ名(山)	2
- ホスト鍵(E)	
◎ チャレンジレスポンス認証を使う(キーボードインタラクティブ)(○)	
◎ Pageantを使う	
OK 接続断( <u>D</u> )	

3. 以上で公開鍵認証が行われ、ログインが完了します。