[大規模科学計算システム]

SSH アクセス認証鍵生成サーバの利用方法

共同利用支援係 共同研究支援係

1. はじめに

大規模科学計算システムでは、セキュリティ強化のため、パスワード認証によるログインを廃止し、 公開鍵暗号方式によるログインのみ許可しています^{**1}。SSH アクセス認証鍵生成サーバ(以下、鍵サ ーバ)はセンターに SSH アクセスするために必要な公開鍵と秘密鍵のペアを生成し、ユーザのホー ムディレクトリに公開鍵を自動登録するサーバです。本稿では、その利用方法についてご紹介します。

ログインホスト名	認証方式 利用システム		
front.cc.tohoku.ac.jp	公開鍵	スーパーコンピュータ SX-ACE 並列コンピュータ LX 406Re-2	
file.cc.tohoku.ac.jp		データ転送サーバ	
_	パスワード ^{※2}	利用者端末 大判カラープリンタ 三次元可視化システム	

表 1 各ホストのログイン認証方式

※1: HPCI 課題、JHPCN-HPCI 課題で利用する場合は GSI 認証でのログインも可能です。詳し くは、以下のリンク先の「HPCI ログインマニュアル」をご覧ください。

http://www.hpci-office.jp/pages/hpci_manuals

※2:センター内施設(利用者端末・大判カラープリンタ・三次元可視化システム)は、ローカル ログインのため、パスワード認証でご利用いただけます。利用にあたり、秘密鍵を持参する 必要はありません。

2. 公開鍵暗号方式を使用する上での注意事項

以下のような行為は、不正アクセスのリスク(不正ログイン、クライアントのなりすまし、暗号化 された通信の暴露、他サーバへの攻撃等)が非常に高く、大変危険です。ご注意願います。

- ・ パスフレーズなしの秘密鍵を使用
- ・ 秘密鍵、パスフレーズの使い回し
- ・ 秘密鍵のメールへの添付、USBメモリやホームディレクトリへの保存
- ・ 公開鍵と秘密鍵のペアを同一ノード上に保存

3. SSH アクセス認証鍵の生成

鍵を生成すると、鍵サーバへのログインが自動的にロックされます。一度ログアウトすると、 以降は鍵サーバにはログインできなくなりますのでご注意ください。鍵の再登録が必要になっ た場合は共同利用支援係までご連絡下さい。本人確認の上、ロックを解除します。

(1) 鍵サーバに利用者番号と初期パスワード(変更している場合は変更後のパスワード)で SSH 接続します。

SSH アクセス認証鍵生成サーバ

key.cc.tohoku.ac.jp

リスト1 鍵サーバへの SSH 接続例

localhost\$ <u>ssh 利用者番号@key.cc.tohoku.ac.jp</u> 利用者番号@key.cc.tohoku.ac.jp's password: <u>パスワード</u>を入力 (初回接続時のメッセージ) : <u>yes</u> を入力

key\$(コマンド待ち状態)

(2) 以下のコマンド(cckey-gen)を実行し、メッセージに従って公開鍵と暗号鍵の鍵ペアを作成 します。必ずパスフレーズ(8文字以上)を設定して鍵を作成してください。

リスト2 公開鍵と暗号鍵の作成方法

key\$ <u>cckey-gen</u> Enter passphrase(8 or more characters) : <u>パスフレーズ</u> の入力(必ず設定) Enter same passphrase again: <u>同じパスフレーズ</u> を再度入力
(生成された秘密鍵の表示) '利用者番号'registration is completed. RSA private key is as follws.
8<8<
BEGIN RSA PRIVATE KEY Proc-Type: 4, ENCRYPTED DEK-Info: DES-EDE3-CBC, A3C27C703A6DF938
gp5U3M6wVIvuGLX80tYBAWC3WwNzX9TPu8e0CA9Pd/i6ijSNcVKp7lGJtuRzjfXV (中略)
FSwfyL63gRqxPZEmlcZzfDnhyX7ezdNNveZu37U/nq4TQj9+Q+RWHhjF9jwnuW6F END RSA PRIVATE KEY
8<8<

(3) 画面に表示された秘密鍵 (---BEGIN RSA PRIVATE KEY--- から ---END RSA PRIVATE KEY--- まで)をコピー&ペーストし、ローカル PC にテキストファイルとして保存します。 公開鍵は自動的にユーザのホームディレクトリに登録されます。秘密鍵はセキュリティを考慮 して消去されます。

4. 公開鍵暗号方式によるログイン方法

4.1 Linux/OS X のターミナルソフトから接続する方法

生成された秘密鍵をファイル名「id_rsa_cc」として「~/.ssh/」以下に保存した場合

(1) パーミッションを 600 に変更します。(初回のみ)

リスト3 パーミッションの変更

localhost\$ chmod 600 ~/.ssh/id_rsa_cc

(2) iオプションで使用する秘密鍵を指定してSSH 接続を行います。
 (iオプションを省略した場合は ~/.ssh/id_rsa あるいは ~/.ssh/id_dsa が利用されます)

リスト 4 ログインホストへの SSH 接続例

localhost\$ <u>ssh -i ~/. ssh/id_rsa_cc 利用者番号@front.cc.tohoku.ac.jp</u> Enter passphrase for key '/home/localname/.ssh/id_rsa_cc':<u>パスフレーズ</u>を入力 (初回接続時のメッセージ) : <u>yes</u> を入力 front\$ (コマンド待ち状態)

4.2 Windows の Tera Term から接続する方法

生成された秘密鍵をファイル名「id_rsa_cc」として「ドキュメント」以下に保存した場合

(1) 「ホスト名」を指定、「サービス」はSSH2 を選択し、[OK]を押下します。

Tera Term: 新しい接続
● TCP/IP ホスト(丁): front.cc.tohoku.ac.jp ・
● <u>S</u> SH SSHバージョン(⊻: <u>SSH2</u> ▼
◎その他 プロトコル(<u>C</u>): UNSPEC ▼
◎シリアル(E) ボート(B): COM1: 通信ボート (COM1)
OK キャンセル ヘルブ(H)

(2)「ユーザ名」に利用者番号、「パスフレーズ」に鍵ペアを作成した際に入力したものを入力、 「RSA/DSA 鍵を使う」を選択し、「秘密鍵」に保存した秘密鍵のファイルを指定します。 (秘密鍵ファイルの選択画面では、拡張子「すべてのファイル(*.*)」を選択します) [OK]を押下すると接続されます。

SSHIZII		RSA/DSA/ECDSA/ED25519秘密鍵ファイルの選択	R	— X —
ログイン中: front.cc.tohoku.ac.jp		C:¥Users¥localhost¥Documents	 マイドキュメン 	トの検索 👂
		整理 ▼ 新しいフォルダー	:==	• 🔳 🔞
		名前	日付時刻	サイズ
		id_rsa_cc	2015/03/05 18:05	2 KB
□ エージェント転送する(0)				
◎ ブレインパスワードを使う(」)				
BSA/DSA/ECDSA/ED25519鍵を使う 秘密鍵(L) id_rsa_cc	-			
○ rhosts(SSH1)を使う ローカルのユーザ名(山): ホスト錬(E):		4	11	•
 ● チャレンジレスボンス認証を使う(キーボードインタラクティブ)(©) ● Pageantが(使う) 		ファイル名(<u>N</u>): id_rsa_cc	 すべてのファイル 開<(Q) 	(*.*) キャンセル
OK 接続斯(D)				

4.3 Windows の WinSCP から接続する方法

WinSCP から接続する場合は、PuTTY 形式の秘密鍵を用意する必要があります。初回接続時は、 4.3.1 の手順に従い、鍵サーバで生成した秘密鍵を PuTTY 形式に変換してください。

4.3.1 秘密鍵を PuTTY 形式に変換

鍵サーバで生成した秘密鍵をファイル名「id_rsa_cc」として「ドキュメント」以下に保存した場合

WinSCP のログイン画面から WinSCP 付属の鍵生成プログラム 「PuTTYgen」を起動します。
 ([ツール] 押下→[PuTTYgen を実行] を押下)
 PuTTYgen がインストールされていない場合はインストールが必要です。

Dグイン		
■ 新しいサイト	セッション 転送プロトコルE SFTP ・ ホスト名他) ポート番号(8) 22 使 ユーザ名(0) パスワード(P) (保存(5) ▼ 試定(0) ▼	
<u>ツール(1)</u> サイトのインポート(I) 設定のインポート/復元(C) 設定のエクコポート/仮元(C)	 ログイン マ 閉じる ヘルプ(H) 	PUTTY Key Generator ? X File Key Conversions Help Key No key.
WinSCP データの消去(C) Pageant を実行(P) PuTTYgen を実行(G) WinSCP の更新を確認 環境設定(P) ノ「ージョン情報(A)		Actions Generate a public/private key pair Load an existing private key file Load Save the generated key Save public key Save private key Parameters Type of Key to senerate: ® RSA © DSA © EDDSA © ED25519 © SSH-1 (RSA) Number of bits in a generated key: 2048

(2) [Load]を押下し、鍵サーバで生成した秘密鍵ファイルを選択して[開く]を押下します。 (秘密鍵ファイルの選択画面では、拡張子「All Files(*.*)」を選択します)

	😴 Load private key:
PUTTY Key Generator File Key Conversions Help	G () マ () C:¥Users¥localhost¥Dournents マ ・ 新しいフォルダーの検索 P
Key No key	整理 ▼ 新しいフォルダー 🔠 ▼ 🗍 🔞
	名前 更新日時 サイズ
	id_rsa_cc 2016/12/19 11:50 2 KB
Actions	
Generate a public/private key pair Generate	
Load an existing private key file	▶
Save the generated key Save public key Save private key	
Parameters Type ofkey to generate:	ファイル名(N):
● RSA ○ DSA ○ ECDSA ○ EC25519 ○ SSH-1 (RSA) Number of bits in a generated kay: 2048	開く(0) ▼ キャンセル

(3) 鍵サーバで生成した秘密鍵のパスフレーズを入力し、[OK]を押下します。



(4) [Save private key]を押下すると、PuTTY 形式に変換された秘密鍵が保存されます。
 (保存先/ファイル名は任意。拡張子は.ppk を推奨)

😴 PuTTY Key Genera	tor		? <mark>×</mark>
File Key Conversion	ons Help		
Key Public key for pasting in	to OpenSSH authorized	ljke ys file:	
ssh-rsa ************************************	**************************************	kalalailailailailailailailailailailailail	******
Key fingerprint:	ssh-rsa 2048 ******		
Key comment:	imported-openssh-key	(
Key passphrase:	•••••		
Confirm passphrase:	•••••		
Actions			
Generate a public/privat	te keypair	(Generate
Load an existing private	key file	(Load
Save the generated key	r	Save public key	Save private key
Parameters			
Type of key to generate	: SA © ECDS	A 🔘 ED25519	🗇 SSH-1 (RSA)
Number of bits in a gene	rated key:		2048

4.3.2 ログイン方法

PuTTY 形式の秘密鍵をファイル名「id_rsa_cc.ppk」として「ドキュメント」以下に保存した場合

(1) 「ホスト名」を指定、「ユーザ名」に利用者番号を入力し、【設定】を押下する。

🔁 ログイン	
■ 新しいサイト	セッション 転送プロトコル(E) SFTP ▼ ホスト名(E) front.cc.tohoku.ac.jp 22 ● 2-ザ名(U) 利用者番号 (保存(s) ▼ 設定(D) ▼
ツール(T) ▼ 管理(M) ▼	ヨロダイン 閉じる ヘルプ(H)

(2) 「SSH」→「認証」を選択し、「秘密鍵」に PuTTY 形式の秘密鍵のファイルを指定して[OK] を押下します。

度なサイトの設定	· · · · · · · · · · · · · · · · · · ·
環境 - ディレクトリ - ごみ箱 - SFTP - ジェル 接続 - プロキシ - トンネル SSH - 建空正 - バグ対策 メモ	常に SSH2 の認証をパイパスする(5): 認証オブション 『Pagent での認証を読みる(P) SSH2 でキーボードによる認証を許可する(1) 『パスワードを自動送信する(P) SSH1 で TIS または CryptoCard 認証を許可する(1) 認証条件 「エージェントの転送を許可する(F) 秘密鍵(K) C:¥Users¥localhost¥Documents¥id_rsa_cc.ppk GSSAPI 「GSSAPI/SSPI 認証を許可する (SSH-2)(G) 「GSSAPI/SSPI 証明書の権利委譲を許可する(C)
色(C) ▼	OK キャンセル ヘルプ(H)

(3) [ログイン]ボタンを押下します。

🔒 ログイン		_ _ ×
🚅 新しいサイト	セッション 転送プロトコル(E) SFTP ▼ ホスト名(E) front.cc.tohoku.ac.jp ユーザ名(U) パスワード(E) 利川用者番号 (保存(S) ▼	ポート番号 (R) 22 ▲ 設定(D) ▼
ツール(T) ▼ 管理(M) ▼	🔁 ログイン 🔻 閉じる	<u>ヘルプ(H)</u>

(4) パスフレーズを入力し、[OK]押下すると接続されます。

パスフレ	νーズの入力 - ***** @front.cc.tohoku.ac.jp 🛛 🚬
	サーバを探索中・・・
	サーバに接続しています・・・
	認証しています・・・
	ユーザ名" 利用者番号" を使用中
	公開鍵 "imported-openssh-key" で認証中
秘密鍵	"mported-openssh-key" のパスフレーズ:
•••••	
E 20)セッションのパスワードを記憶する(R)
	ок (++>>tz// ////н)

4.4 その他の 0S/アプリケーションから接続する場合

各アプリケーションのヘルプを参照ください。

5. おわりに

本稿では、SSH アクセス認証鍵生成サーバの利用方法を紹介しました。ご不明な点、ご質問等ございましたら、お気軽にセンターまでお問い合わせください。