東北学院大学
情報処理センターシステム 2019
リモートログインサービス
利用の手引き（教職員用）

2019 年３月４日（第１版）

東北学院大学　情報処理センター

目次

1. リモートログインサービスの概要

学内の研究室や、学外のサーバの利用やデータの転送を行うためのサービスである。

- 研究室の端末から学外のサーバにリモートログイン（SSH）、データ転送（SCP/SFTP）する。
- 学外の端末から研究室のサーバにリモートログイン（SSH）、データ転送（SCP/SFTP）する。

本サービスの利用には、情報処理センターへの利用申請が必要である。

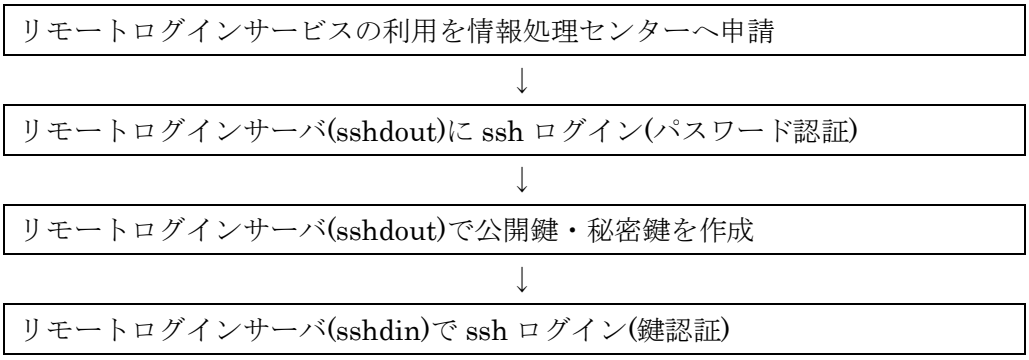
2. リモートログインサービスの構成

表 2-1 リモートログインサービス ログイン情報

利用形態	研究室から学外へアクセス	学外から研究室へアクセス
ホスト名	sshdout.ipc.tohoku-gakuin.ac.jp	sshdin.ipc.tohoku-gakuin.ac.jp
リモートログイン用 IP アドレス	157.118.206.22	157.118.206.23
可能な接続元ネットワーク	学内	学外
接続先可能なネットワーク	学外	学内
認証方式	パスワード認証	公開鍵認証

3. リモートログインサービスの利用概要

本サービスを利用する際の手順の概要は、次のとおりです。



4. 利用手順

4.1. リモートログインサーバ(sshdout)へのログイン

リモートログインサーバ(sshdout)への接続は、情報処理センター利用アカウントとパスワードでログインすることができます。

ご利用の端末で SSH ターミナルを起動し、リモートログインサーバ(sshdout)に ssh アクセスし、アカウントとパスワードを入力して、ログインします。

4.2. 公開鍵･秘密鍵の作成

リモートログインサーバ(sshdout) にログインしたら、リモートログインサーバ(sshdin)にログインするための必要な、ssh 用公開鍵・秘密鍵を作成します。

次の手順に従い、公開鍵・秘密鍵を作成します。

```
[XXXXXX@sshdout ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ipcmnt/.ssh/id_rsa):
    → そのままリターンを押します。
Enter passphrase (empty for no passphrase):
    → 鍵に設定するパスフレーズを入力します。
Enter same passphrase again:
    → もう一度パスフレーズを入力します。
Your identification has been saved in /home/ipcmnt/.ssh/id_rsa.
Your public key has been saved in /home/ipcmnt/.ssh/id_rsa.pub.
The key fingerprint is:
```

```
SHA256:bG0rcfpUy95NqYajkB02kFGd/CFEU7jUPYNhPac37r4
ipcmnt@sshdout.ipc.tohoku-gakuin.ac.jp
The key's randomart image is:
+---[RSA 2048]----+
(省略)
[XXXXXX @sshdout ~]$
```

作成が終わると、公開鍵・秘密鍵は、ホームディレクトリ直下の .ssh ディレクトリに格納されます。作成された公開鍵(id_rsa.pub)を、.ssh/authorized_keys ファイル名前を変更します。

```
[XXXXXX @sshdout ~]$ ls -l .ssh
合計 12
-rw------- 1 XXXXXX XXXXXX 1766　2 月 20 20:15 id_rsa
-rw-r--r-- 1 XXXXXX XXXXXX　420　2 月 20 20:15 id_rsa.pub
[XXXXXX @sshdout ~]$ mv .ssh/id_rsa.pub .ssh/authorized_keys
```

id_rsa： 秘密鍵ファイル。お使いの端末に格納し、SSH ターミナルで使用します。
id_rsa.pub： 公開鍵ファイル。リモートログインサーバに格納しておきます。

4.3. 秘密鍵の端末への格納

リモートログインサーバ(sshdout)で作成した秘密鍵を、ssh で利用する端末に格納します。

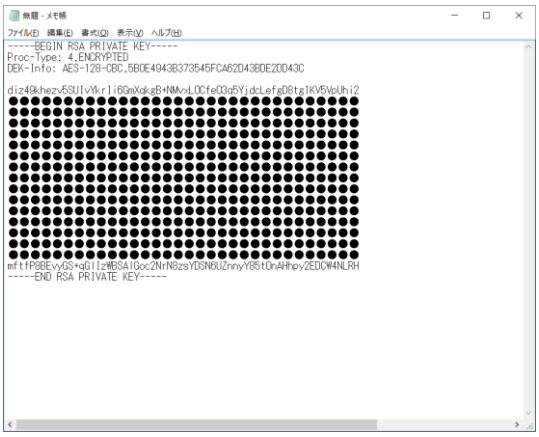
リモートログインサーバ(sshdout)で鍵を作成した後に、リモートログインサーバ(sshdout)上で、cat コマンドなどを用いて秘密鍵の内容を表示させます。

```
[XXXXXX @sshdout ~]$　cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,5B0E4943B373545FCA62D43BDE2DD43C

diz49khezv5SUIvYkrIi6GmXqkgB+NMvxLOCfeO3q5YjdcLefgD8tg1KV5VpUhi2
      :
（省略）
mftfP8BEvyGS+qGlIzWBSAlGoc2NrN8zsYDSN6UZnnyY85tOnAHhpy2EDCW4NL
RH
-----END RSA PRIVATE KEY-----
[XXXXXX @sshdout ~]$
```

表示された内容（「-----BEGIN RSA PRIVATE KEY-----」から「-----END RSA PRIVATE KEY-

----」まで）をコピーし、端末上のメモ帳などのテキストエディタにペーストします。



端末上の任意のフォルダに、任意の名前を付けて保存します。また、学外からリモートログインサーバ(sshdin)に ssh 接続する端末に、本ファイルを格納します。

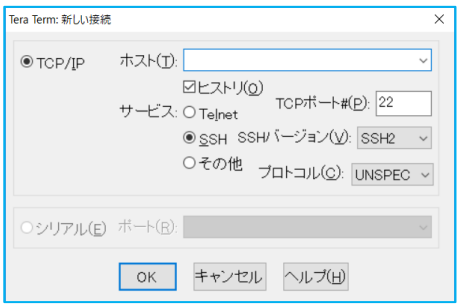
4.4. リモートログインサーバ(sshdin)へのログイン

リモートログインサーバ(sshdin)に SSH ターミナルソフト、SCP/SFTP ソフトを使って接続します。

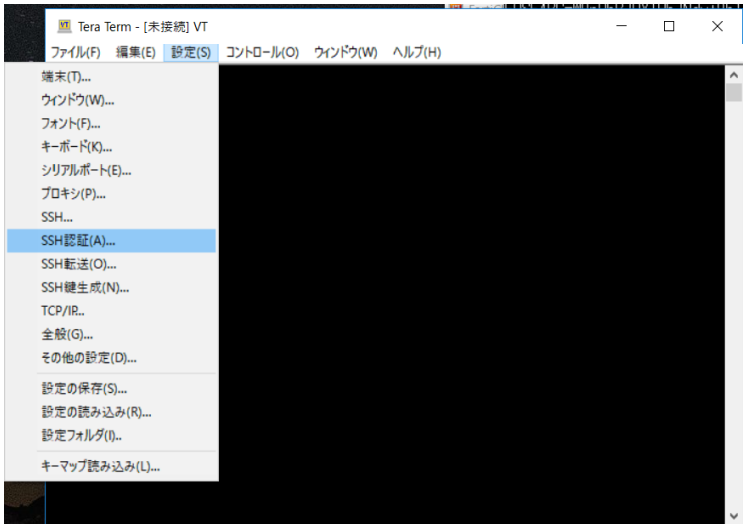
以下は、TeraTerm の例です。

お使いの SSH ターミナルソフトの使い方を確認の上、鍵の取り扱い、設定などを適宜行ってください。

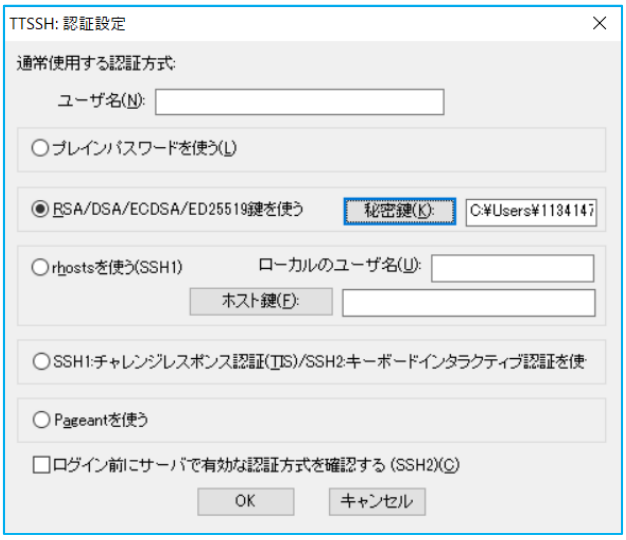
1) TeraTerm を起動します。「新しい接続」ウィンドウが表示されますが、「×」でウィンドウを閉じます。



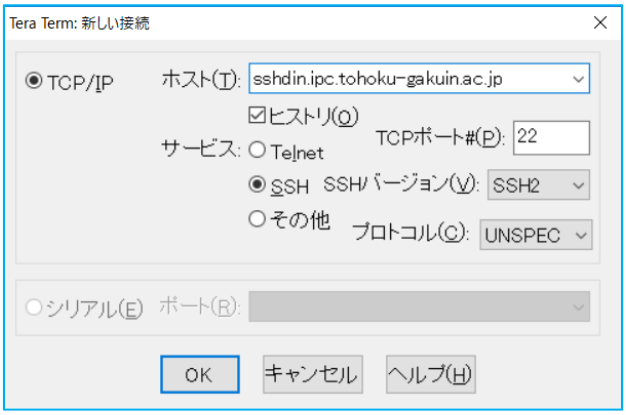
2) TeraTerm メニューの「設定」メニュー → 「SSH 認証」を選択します。



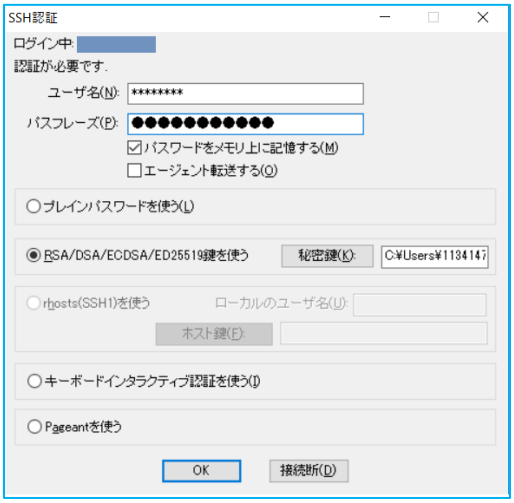
3) 「RSA/DSA/ECDSA/ED25519 鍵を使う」を選択し、「秘密鍵」ボタンをクリックし、保存した秘密鍵ファイルを選択したら、「OK」をクリックします。



4) 「ファイル」メニュー →「新しい接続」を選択し、接続先にリモートログインサーバ(sshdin)を指定し、「OK」をクリックします。



5) 「ユーザ名」と鍵を作成した際に入力した「パスフレーズ」を入力し、「OK」をクリックし、リモートログインサーバ(sshdin)にログインします。



4.5. ファイル利用

リモートログインサーバにログインすると、利用者のホームディレクトリが利用できます。

ファイル転送を行う場合には、ホームディレクトリ配下をファイルの保存場所として一時利用して行ってください。

4.6. ログアウト

遠隔端末の操作を終了する場合は、リモートログインサーバからログアウトします。ログアウト方法は、アクセスサーバへの接続方法によって異なりますので、利用するソフトの利用方法に従ってください。

（例）

・ SSH ターミナルソフトでアクセスサーバに接続している場合：
“logout”若しくは、“exit”コマンドを実行する。

5. 留意事項

なし