

情報実験INEX 2021 第1回 SSH接続を行う準備

北海道大学理学院 修士課程2年
山東 俊太



リモートアクセスとは

- 手元の計算機(**ローカルホスト**)から別の計算機 (**リモートホスト**)へのネットワークを経由して接続・操作すること
 - リモートログイン
 - リモートアクセスを用いたファイル転送

ローカルホスト



リモートアクセス

リモートホスト

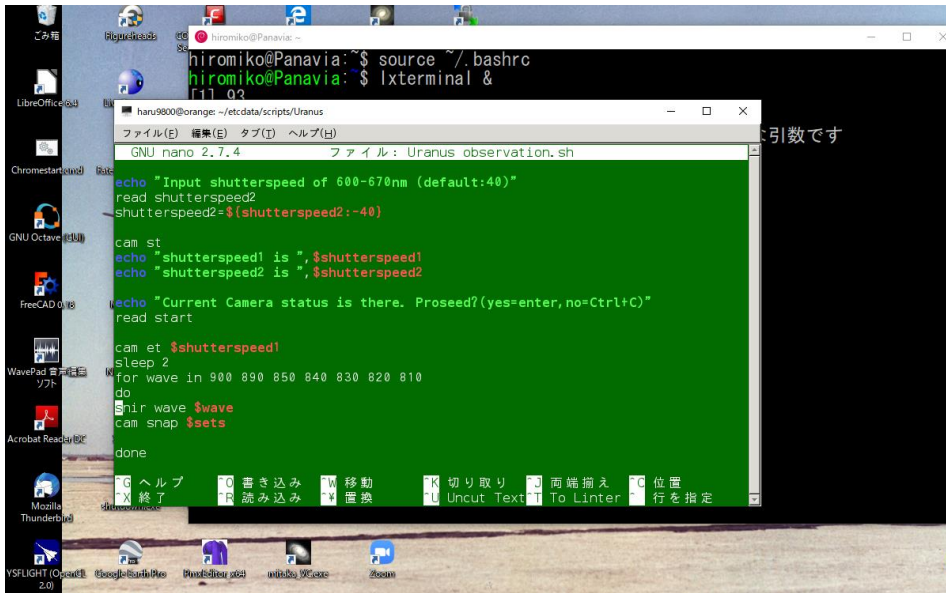


<http://northern-road.jp/discover/sign/aiueo.html>

<http://www.city.nayoro.lg.jp/section/kikaku/prkeql000000q4bo.html>



リモートアクセスを実現する手段： SSH



```
hiromiko@Panavia:~$ source ~/.bashrc
hiromiko@Panavia:~$ lterminal &
[1] 93
hanu9800@orange: ~/etc/data/scripts/Uranus
GNU nano 2.7.4   ファイル: Uranus observation.sh
echo "Input shutter speed of 600-670nm (default:40)"
read shutter speed2
shutterspeed2=${shutterspeed2:-40}
cam st
echo "shutterspeed1 is ", $shutterspeed1
echo "shutterspeed2 is ", $shutterspeed2
echo "Current Camera status is there. Proceed?(yes=enter, no=Ctrl+C)"
read start
cam et $shutterspeed1
sleep 2
for wave in 900 890 850 840 830 820 810
do
  hir wave $wave
  cam snap $sets
done
ヘルプ 終了 書き込み 読み込み 移動 置換 切り取り 両端挿入 位置 行を指定
```

図：SSHでEP Webサーバーに接続して作業している様子（緑色のウィンドウ）

- SSH(Secure Shell) : 暗号化技術により安全にネットワーク上の別の計算機に接続し、利用できる技術
- パスワードや公開鍵認証でユーザーを認証
- 例えば研究室の計算機に家の計算機から接続し、数値計算をさせたりすることができる

公開鍵認証方式

- 公開鍵認証方式：暗号化に使用する公開鍵と復号に使用する秘密鍵のペアを用いた認証方式
- インターネットを行き交う情報は比較的簡単に傍受、改ざんされてしまうため、情報を暗号化して重要な情報（パスワードなど）を守る必要がある
- 詳しくは別の回にて
- 今回の情報実習では公開鍵認証方式を用いて理学部8号館1階、電腦大飯店の情報実験機にssh接続を行う

さっそくやってみよう

- 手順

1. 鍵のペアを作成

2. 鍵を実験機に送る (moodle 経由)

↑ 今日やるのはここまで

3. 接続する (次回)

やってみよう ～Windows 10編

Macなどその他のOSの方は以下リンクから

http://www.ep.sci.hokudai.ac.jp/~inex/y2021/0416/lecture_ssh/ssh_keygen.html

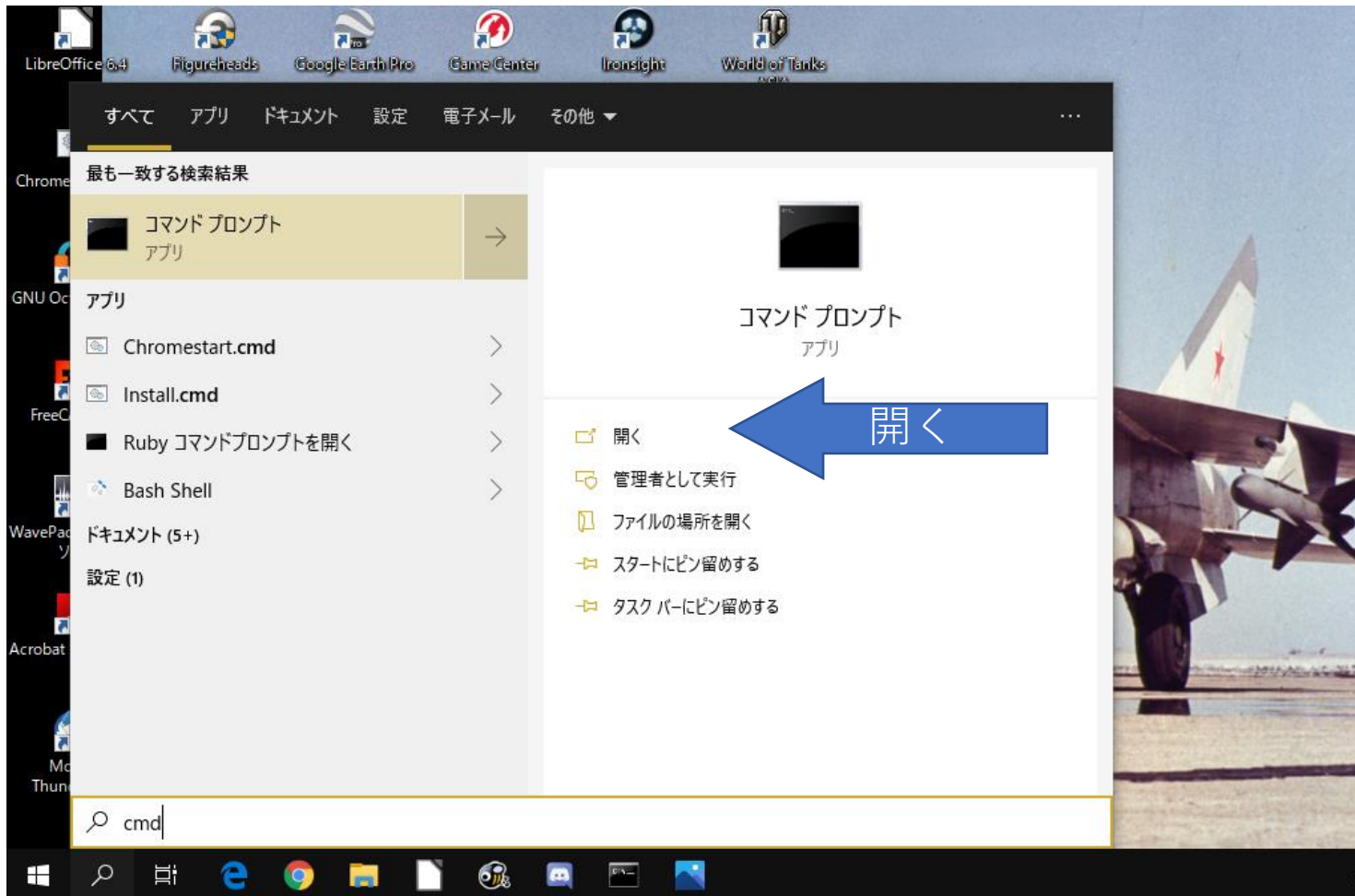
Windows のユーザ名が日本語の方はユーザ名が半角英数のみのユーザを作成してください

1. コマンドプロンプトを起動する
 1. Windowsボタンの隣の検索バーに”cmd”と入力
 2. “コマンドプロンプト”を実行



ここに”cmd”と入力

コマンドプロンプトを起動する

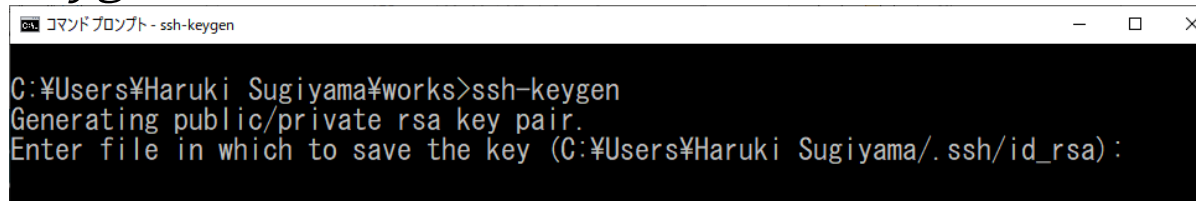


鍵ペアの作成

- コマンドプロンプトに以下のコマンドを入力

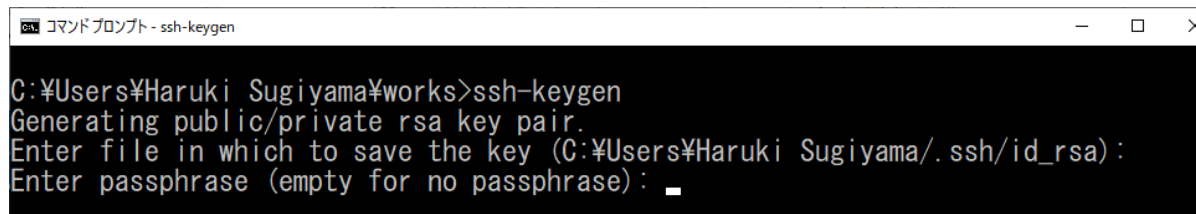
※“>”はプロンプトと呼ばれる文字で、入力待ちであることを示すため、入力しなくてよい

> *ssh-keygen*



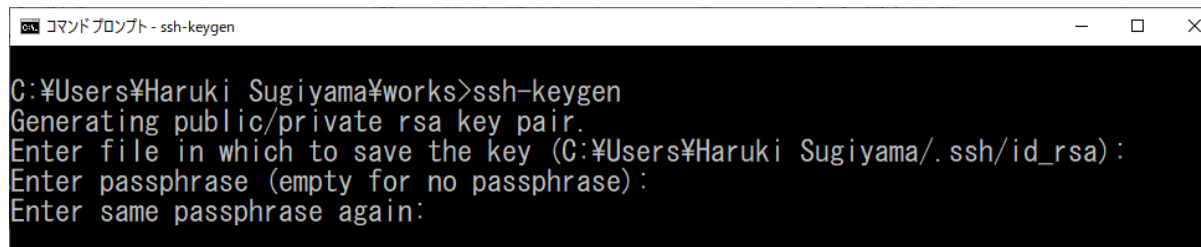
```
コマンドプロンプト - ssh-keygen
C:¥Users¥Haruki Sugiyama¥works>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:¥Users¥Haruki Sugiyama/.ssh/id_rsa):
```

Enterキーを押す



```
コマンドプロンプト - ssh-keygen
C:¥Users¥Haruki Sugiyama¥works>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:¥Users¥Haruki Sugiyama/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
```

Enterキーを押す



```
コマンドプロンプト - ssh-keygen
C:¥Users¥Haruki Sugiyama¥works>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:¥Users¥Haruki Sugiyama/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

Enterキーを押す




```
コマンドプロンプト
C:\Users\Haruki Sugiyama\works>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\Haruki Sugiyama\.ssh\id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\Haruki Sugiyama\.ssh\id_rsa.
Your public key has been saved in C:\Users\Haruki Sugiyama\.ssh\id_rsa.pub.
The key fingerprint is:
SHA256:3pLzHKJ3sI2wx93+j3oYXL9kqvWZHxwUnwFbB0Mr+R4 haruki sugiyama@Panavia
The key's randomart image is:
+---[RSA 2048]---+
|                 |
|                o==|
|               .oo*|
|              o..o.|
|               oo   |
|             S    .Eo|
|            ...o  o..+o|
|           +**o.  +=o.|
|          ..**+.  +.oo+|
|         .o .oo++o=+|
+-----[SHA256]-----+
C:\Users\Haruki Sugiyama\works>_
```

うまくいくとこのような画面が出ます

鍵の作成が完了したので、右上の閉じるボタンをおしてください



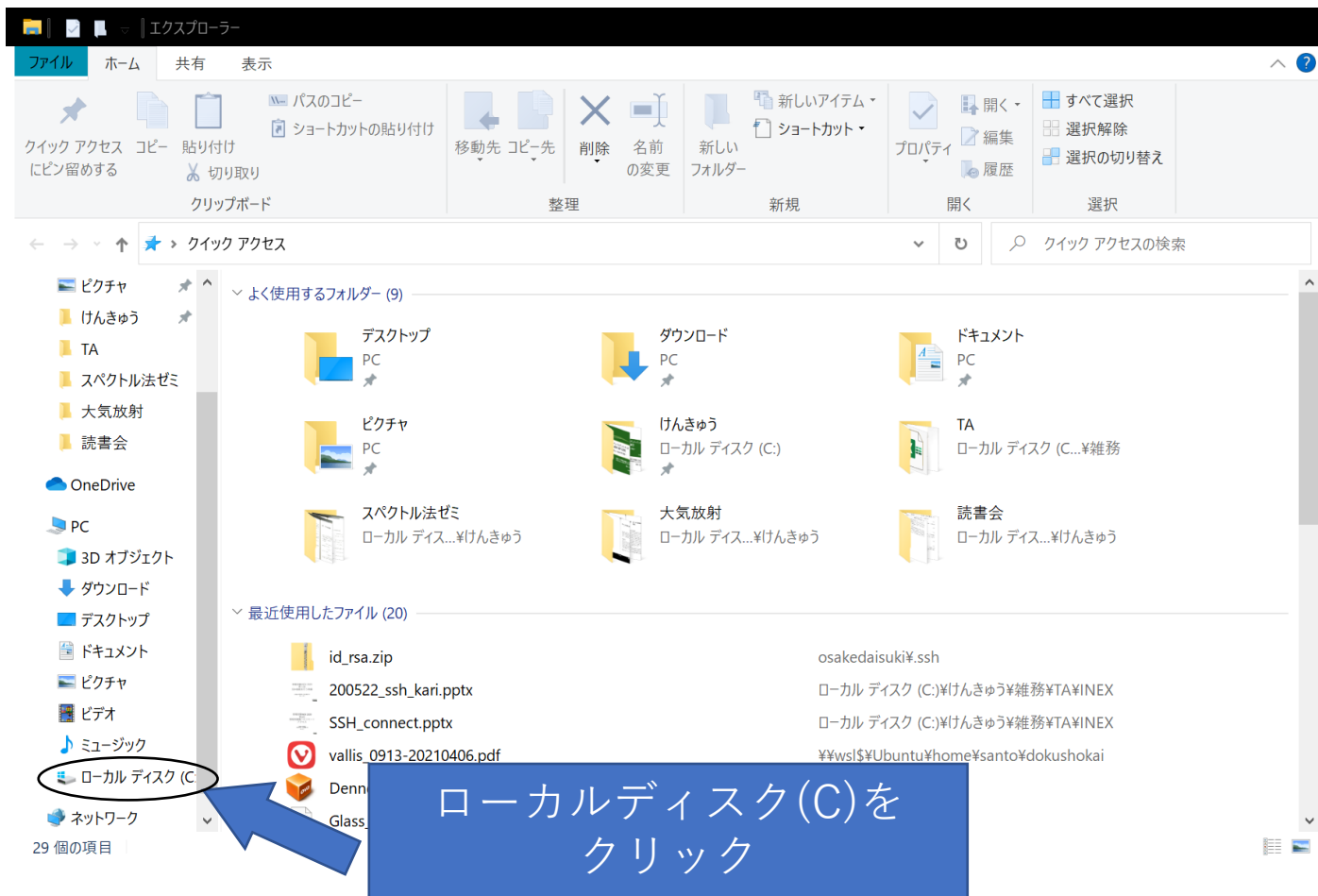
本日の課題その2

- 先ほど作成した公開鍵をmoodleにアップロードしてください
- 提出方法や鍵の作成方法など、分からないことがあれば4限の質問時間をお願いします

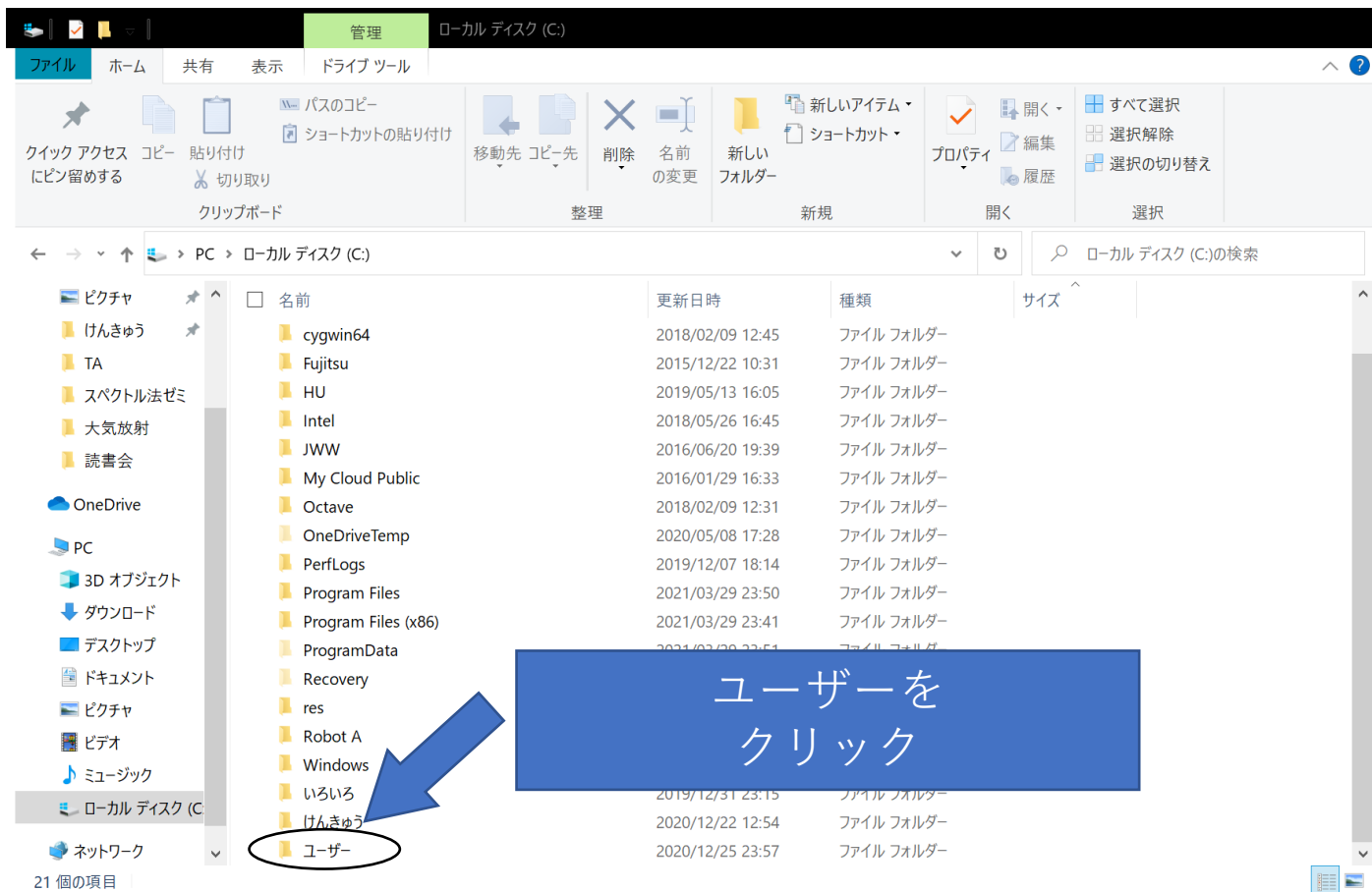
この課題が未達成の場合、今後の実技課題を一切受けられなくなります！！

確実に提出してください！！

公開鍵の場所 (標準の場合)



公開鍵の場所 (標準の場合)

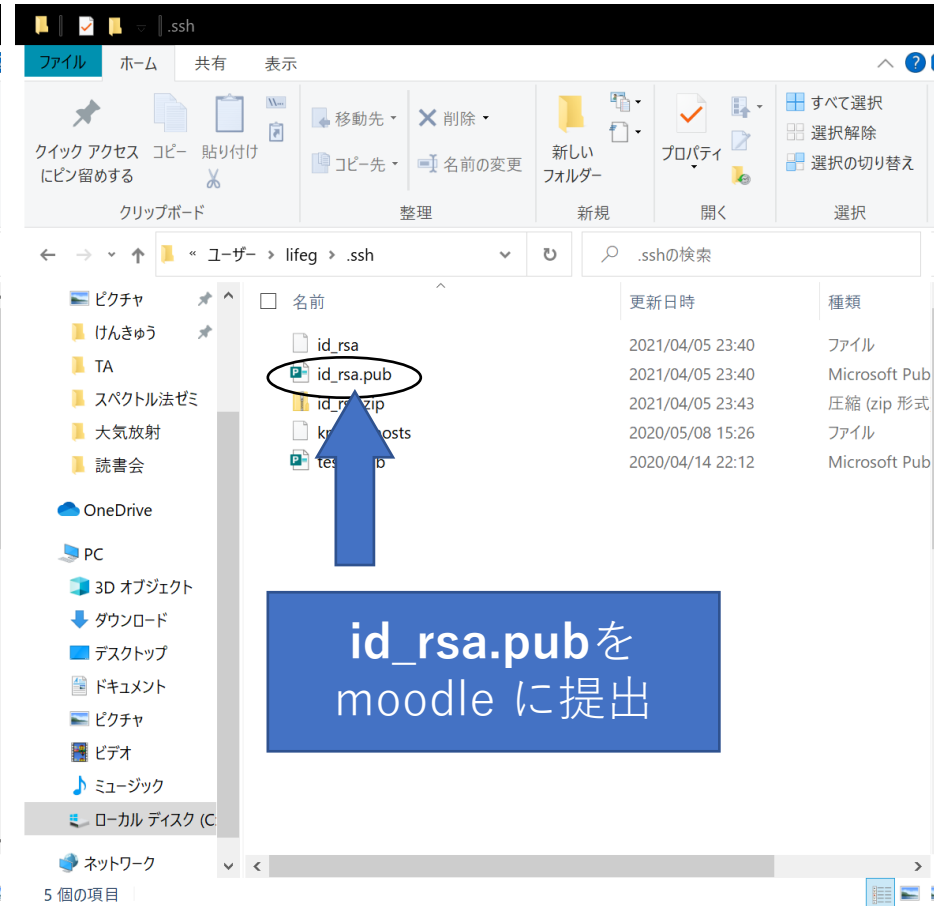
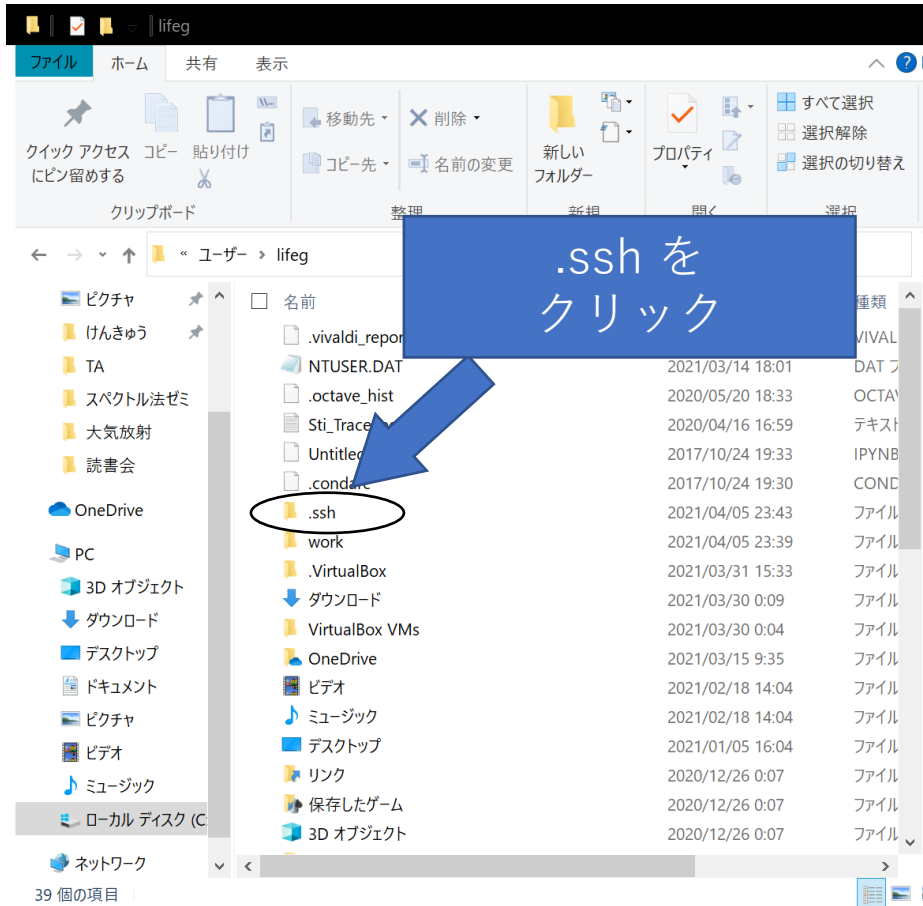


公開鍵の場所（標準の場合）

先ほどコマンドプロンプト
上に表示されていたユーザ
名のフォルダをクリック

```
Microsoft Windows [Version 10.0.19041.867]  
(c) 2020 Microsoft Corporation. All rights reserved.  
  
C:\Users\lifeg>
```

公開鍵の場所



秘密鍵(pubがついていないid_rsa)は絶対にmoodleに送信したり、他人に渡したりしないでください!!!

参考資料

- 入門OpenSSH 新山 祐介
<https://www.unixuser.org/~euske/doc/openssh/book/index.html>

- Windows10標準機能でSSH認証用の公開鍵と秘密鍵を作成する方法 株式会社スリースターソフトウェア

<https://www.threestarsoftware.co.jp/gitlab/windows10%E6%A8%99%E6%BA%96%E6%A9%9F%E8%83%BD%E3%81%A7ssh%E8%AA%8D%E8%A8%BC%E7%94%A8%E3%81%AE%E5%85%AC%E9%96%8B%E9%8D%B5%E3%81%A8%E7%A7%98%E5%AF%86%E9%8D%B5%E3%82%92%E4%BD%9C%E6%88%90%E3%81%99/>

情報実験INEX 2020 第1回 SSH接続を行う準備 杉山 玄己

http://www.ep.sci.hokudai.ac.jp/~inex/y2020/0522/lecture_ssh/pub/200522_ssh.pdf