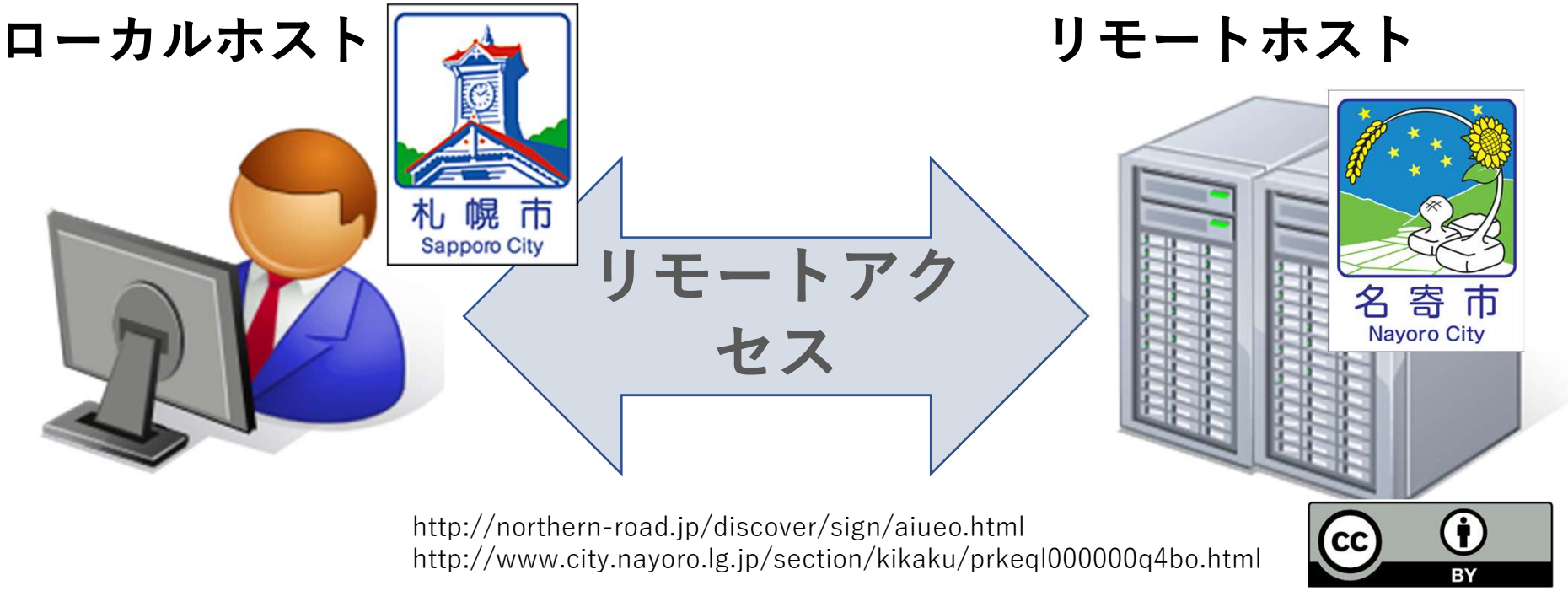
情報実験INEX 2020
第１回
SSH接続を行う準備

北海道大学理学院　修士課程２年
杉山　玄己

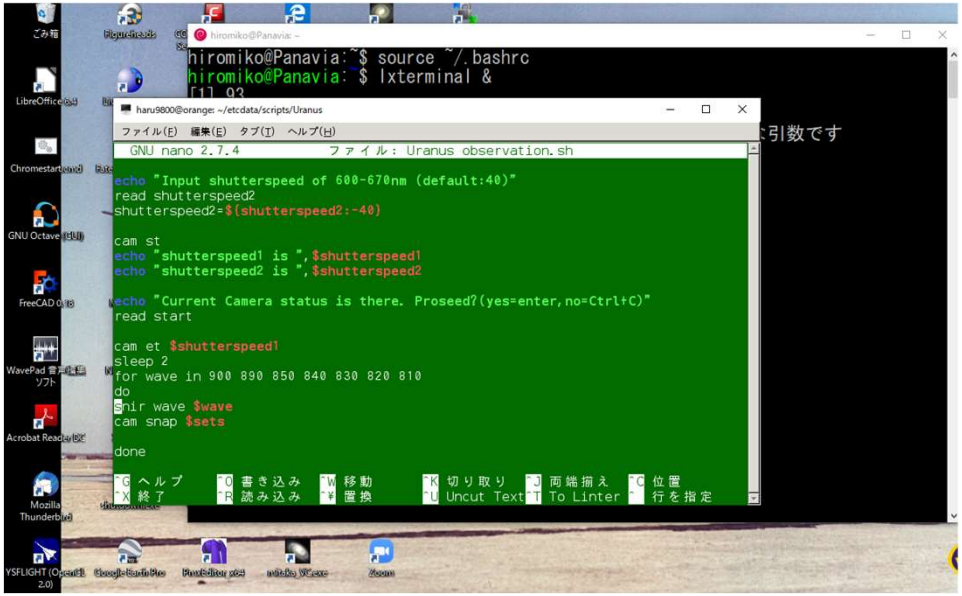
リモートアクセスとは

- 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



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



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、電脳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

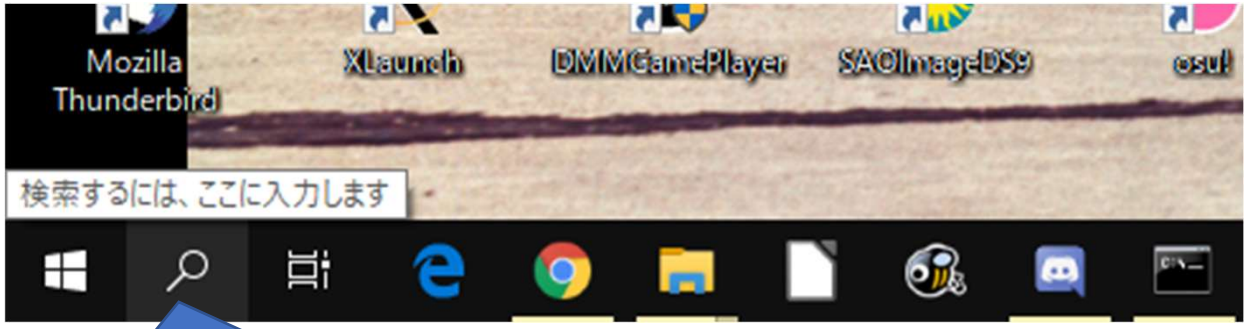
1. 鍵のペアを作成
2. 鍵を実験機に送る（suu経由）
   ↑今日やるのはここまで

3. 接続する（次回）

やってみよう
～Windows 10編

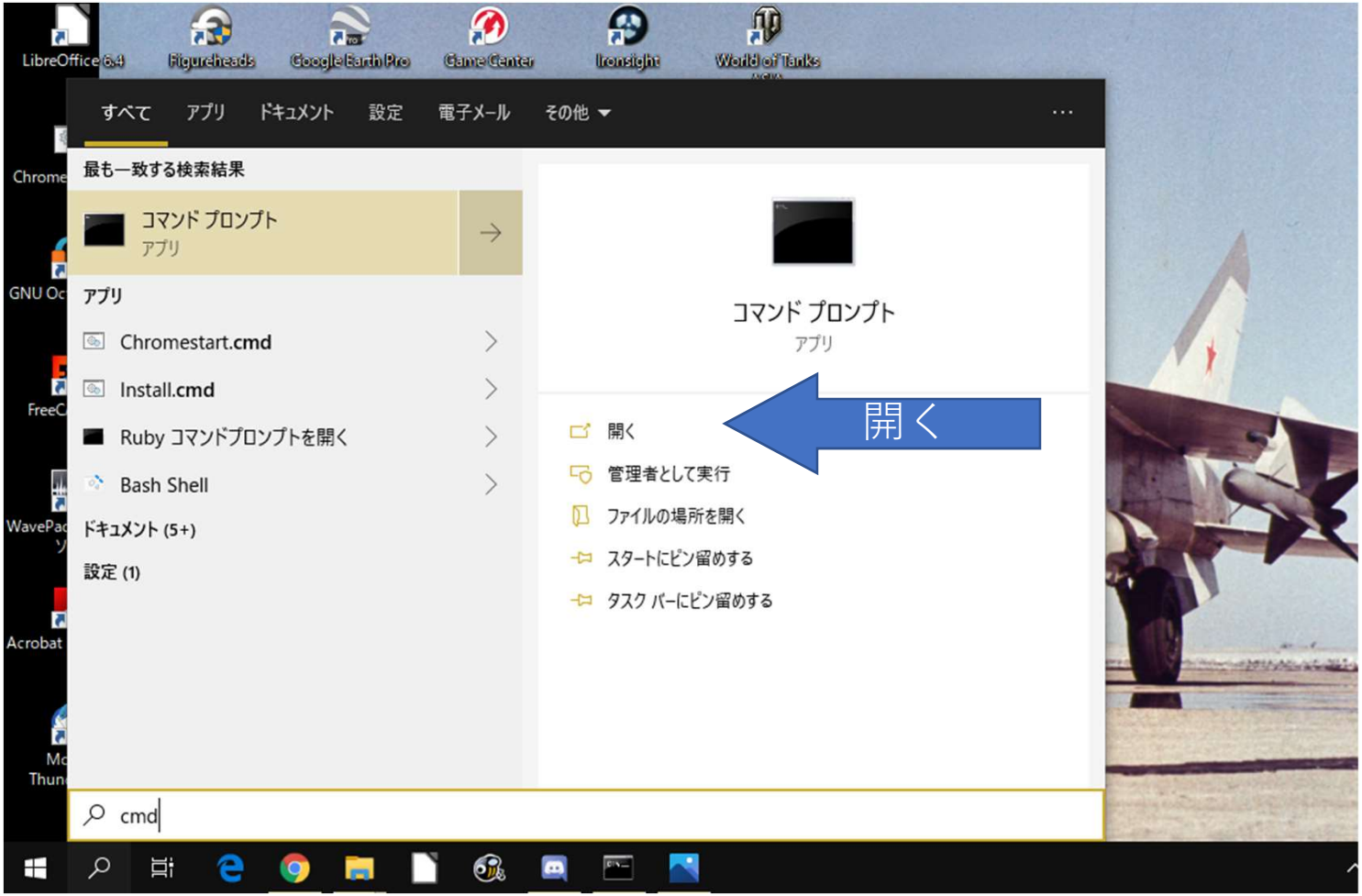
Macなどその他のOSの方は以下リンクから
http://www.ep.sci.hokudai.ac.jp/~inex/y2020/0522/lecture_ssh/ssh_keygen.html

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

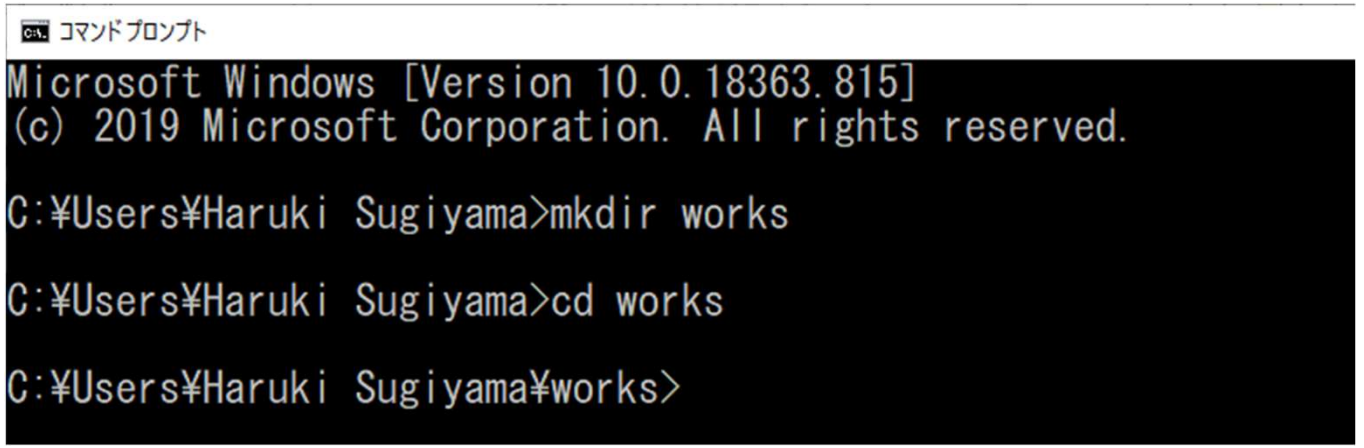
- コマンドプロンプトに以下のコマンドを入力

※“>”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

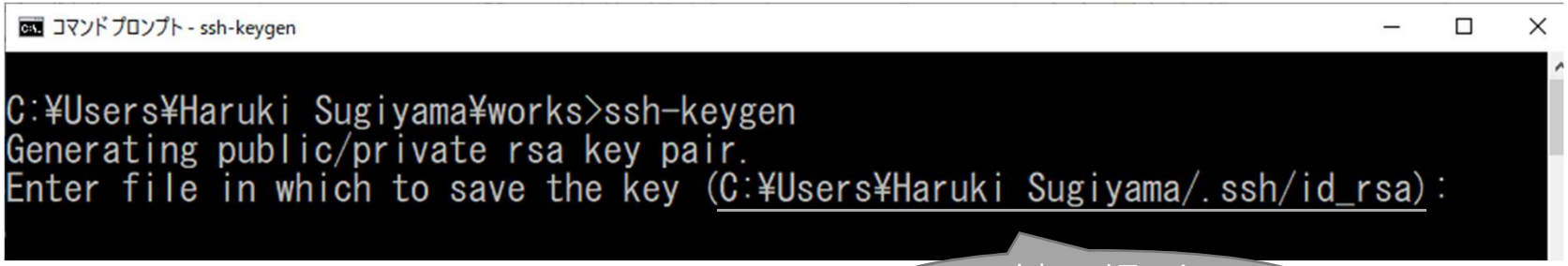
>mkdir works

>cd works

>ssh-keygen

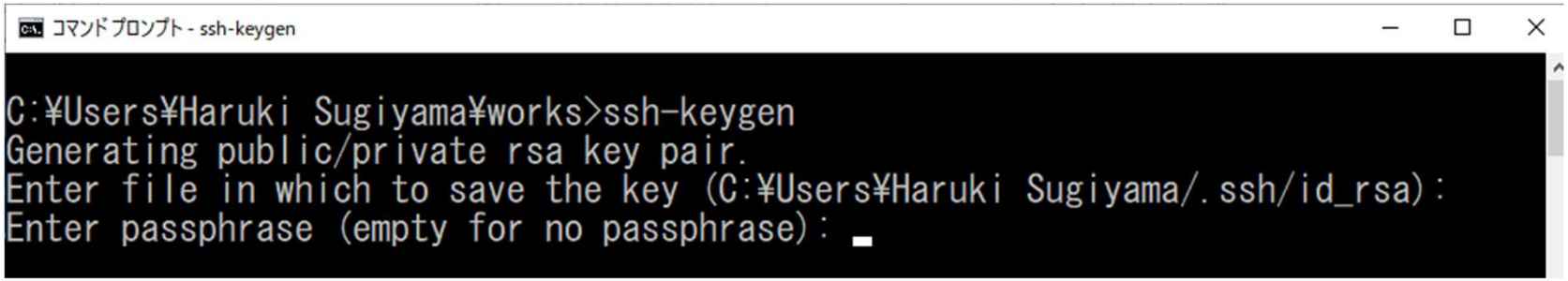


>ssh-keygen

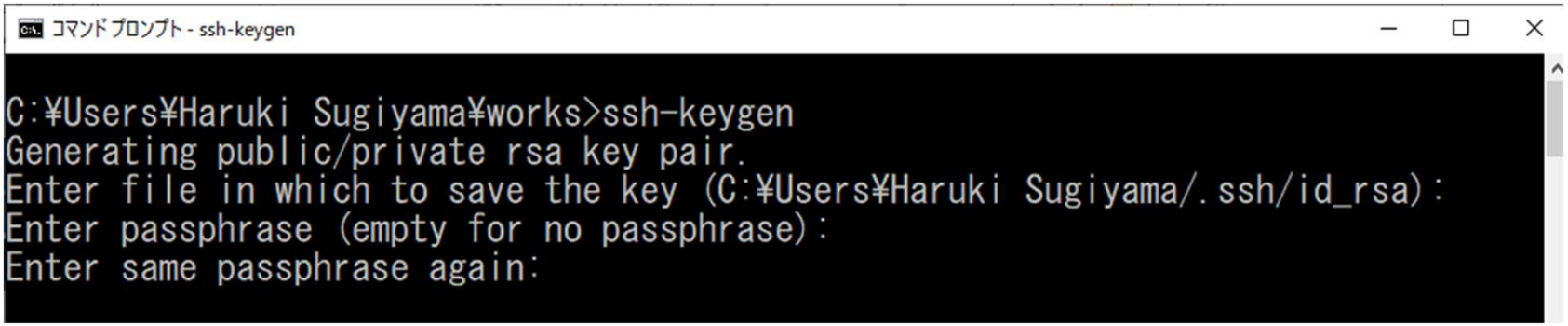


Enterキーを押す

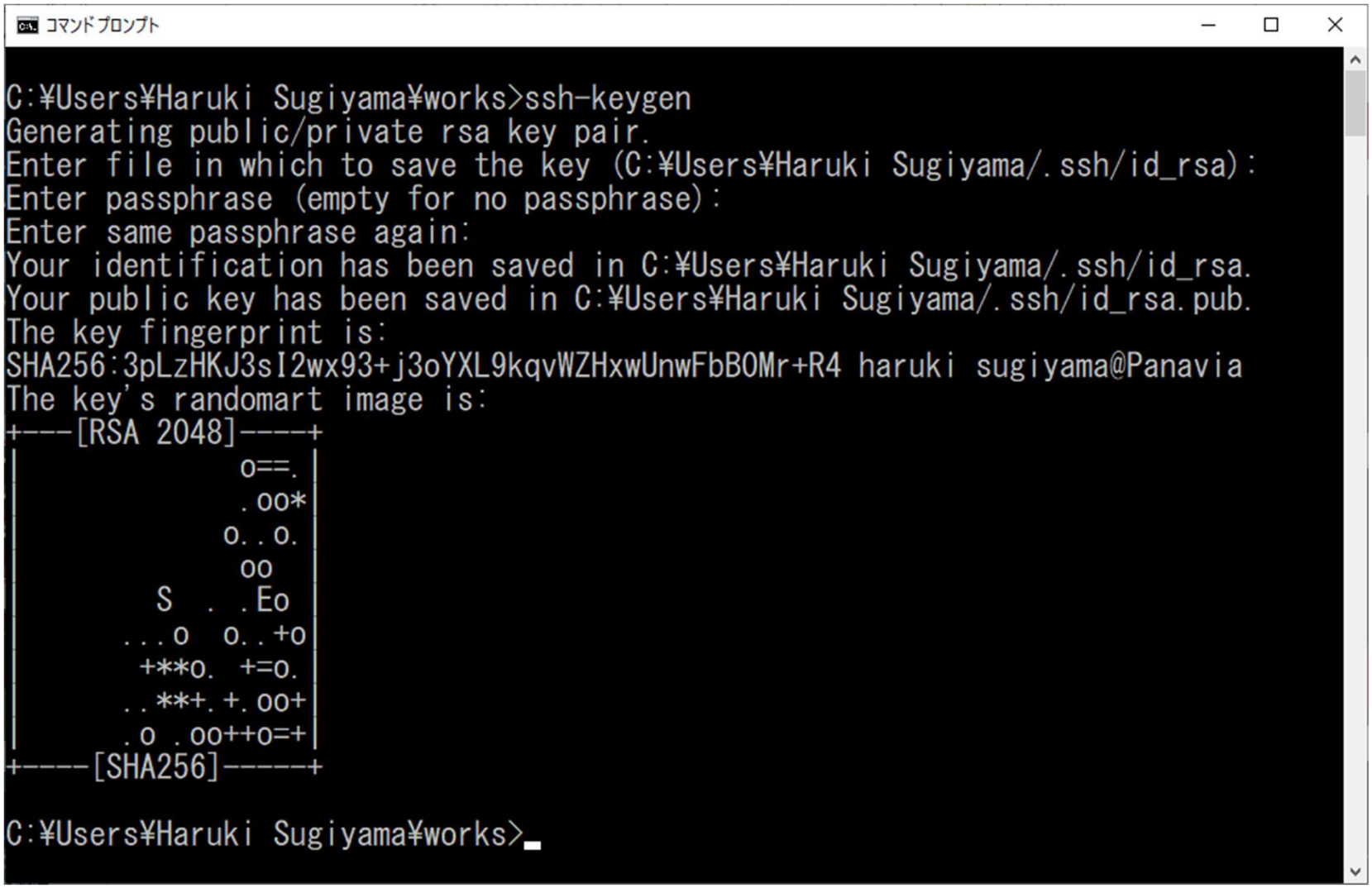
鍵の場所



Enterキーを押す

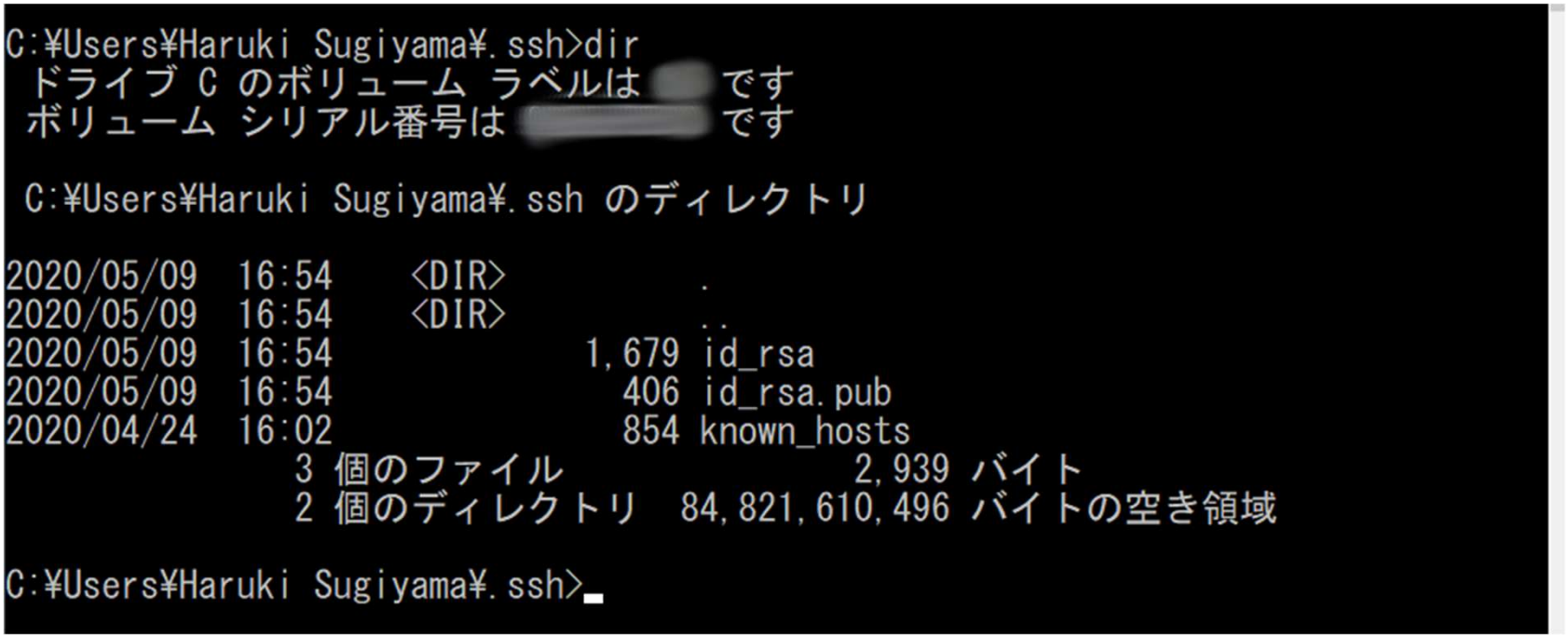


Enterキーを押す



うまくいくとこのような画面が出ます

鍵ができているか確認
>cd ../.ssh
>dir



図のように***id_rsa***と***id_rsa.pub***が存在すれば成功です。***id_rsa***のファイルが**秘密鍵**、***id_rsa.pub***が**公開鍵**です。ここで作成した公開鍵をzip圧縮しsuuにアップロードするのが今回の課題です。

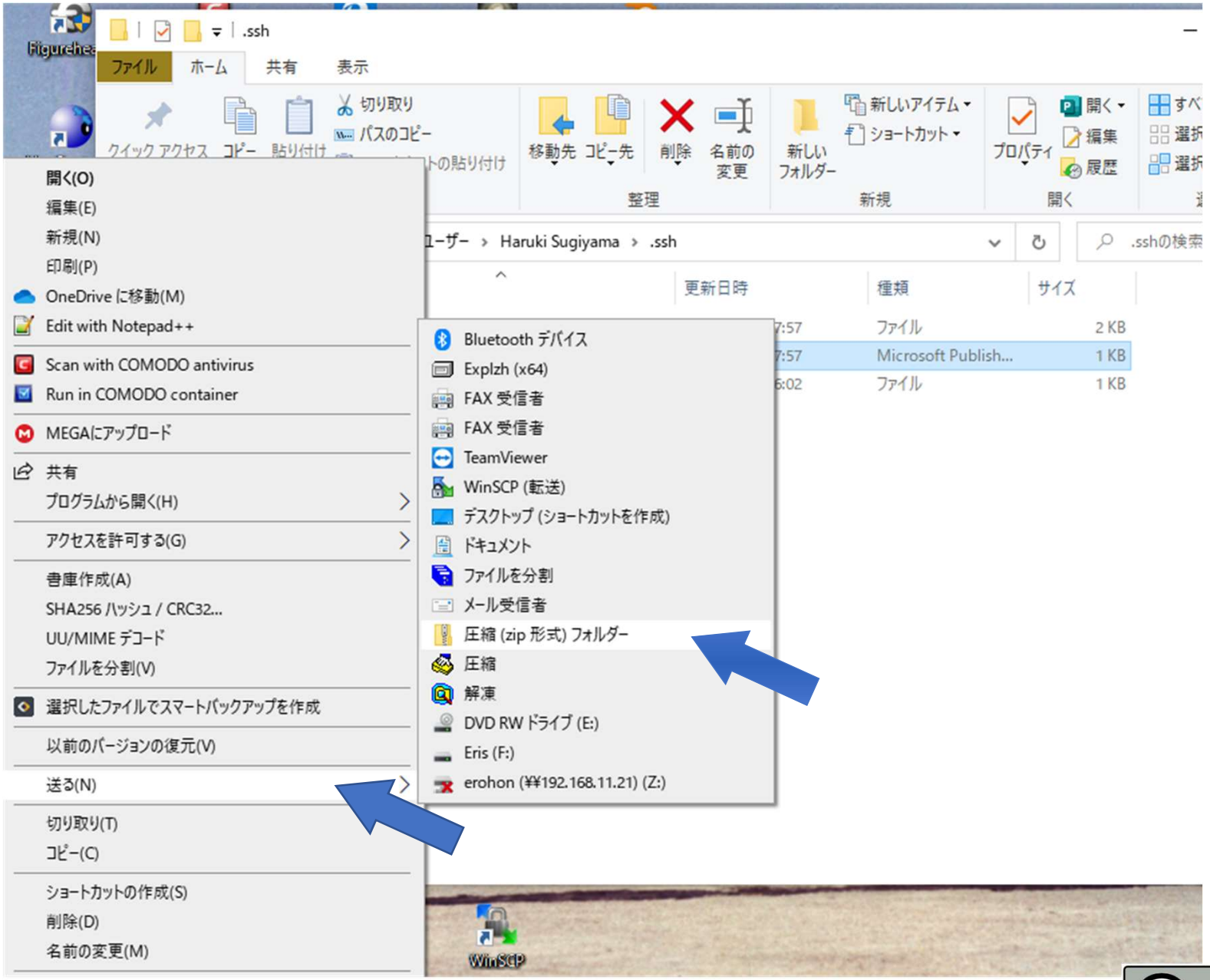
秘密鍵は絶対にsuuに送信したり、他人に渡したりしないでください！！！

本日の課題その2

- 先ほど作成した公開鍵をzip形式に圧縮し、suuにアップロードし、ファイルへのURLを参考URL欄に添付したレポートを提出してください。
- レポートタグは”[2020]1, SSH公開鍵”です。
- タイトルは[SSH公開鍵の作成]としてください。
- 本文には空欄でも構いませんが、もし作業中に苦労した点、分からなかった点があればそれについて書いてください。

公開鍵をzip圧縮する方法

- エクスプローラでC:¥Users¥＜ユーザー名＞¥.sshを開く
- 「Cドライブ」→「Users（もしくはユーザー）」→「ユーザー名」→「.ssh」
- Id_rsa.pubを右クリック
- 「送る」→「圧縮（ZIP形式）フォルダー」
- ファイル名は”id_rsa.zip”に
- “id_rsa.zip”が完成


.ssh
ファイル
ホーム
共有
表示
クイック アクセス
コピー
貼り付け
切り取り
パスのコピー
移動先
コピー先
削除
名前の変更
新しいフォルダー
新しいアイテム
ショートカット
プロパティ
開く
編集
履歴
整理
新規
開く
ユーザー › Haruki Sugiyama › .ssh
.sshの検索
更新日時
種類
サイズ
ファイル 2 KB
Microsoft Publish... 1 KB
ファイル 1 KB
開く(O)
編集(E)
新規(N)
印刷(P)
OneDrive に移動(M)
Edit with Notepad++
Scan with COMODO antivirus
Run in COMODO container
MEGAにアップロード
共有
プログラムから開く(H)
アクセスを許可する(G)
書庫作成(A)
SHA256 ハッシュ / CRC32...
UU/MIME デコード
ファイルを分割(V)
選択したファイルでスマートバックアップを作成
以前のバージョンの復元(V)
送る(N)
切り取り(T)
コピー(C)
ショートカットの作成(S)
削除(D)
名前の変更(M)
Bluetooth デバイス
Explzh (x64)
FAX 受信者
FAX 受信者
TeamViewer
WinSCP (転送)
デスクトップ (ショートカットを作成)
ドキュメント
ファイルを分割
メール受信者
圧縮 (zip 形式) フォルダー
圧縮
解凍
DVD RW ドライブ (E:)
Eris (F:)
erohon (¥¥192.168.11.21) (Z:)
WinSCP

suuへのアップロードと ファイルへのURLの張り方

- suuにログイン
- 上のメニューから「アップロード」を押す
- 「ファイルを選択」ボタンを押し、先ほど作成した「**id_rsa.zip**」を選択
- ファイルを選択できると、ボタンの隣にファイル名が表示される
- 説明に記入し、アップロードボタンを押す
- 「アップロードしたもの」ページが表示されるのでサムネイルを右クリック→「リンクのアドレスをコピー（Google Chrome）」
- コピーしたアドレスをレポートの参考URL欄に張り付け

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　ー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/

INEX2019リモートアクセス/ ネットワークセキュリティ 情報実験 第8回 (2019/06/21)吉田 辰哉
http://www.ep.sci.hokudai.ac.jp/~inex/y2019/0621/lecture/pub/inex20190621.pdf