How to Use AOBA (1st step)

スパコンAOBA利用の第一歩

Cyberscience Center, Tohoku Univ

Hiroyuki Takizawa
<takizawa@tohoku.ac.jp>

High Performance Computing

- **This course will provide an opportunity to use the AOBA supercomputer.**
  - Assuming that students already have the basic knowledge about ...
    - Use of basic Linux commands
    - C/C++ programming

These background knowledge topics will not be explained during the lecture and should be acquired beforehand through self-study.
It would also be better to be familiar with the software tools such as ...

Visual Studio Code with Remote Development extension

https://code.visualstudio.com/docs/remote/remote-overview

Login to Supercomputer

■ **Supercomputer = Shared Resource**

- Shared by many users
- Used remotely from your PC **via the Internet**

Communication data could be stolen?

System Configuration

■ Secure Way of Accessing AOBA

Accessible only from the login server

Job request

Login server
(login.cc.tohoku.ac.jp)

Front-end server

File Transfer

File server
(file.cc.tohoku.ac.jp)
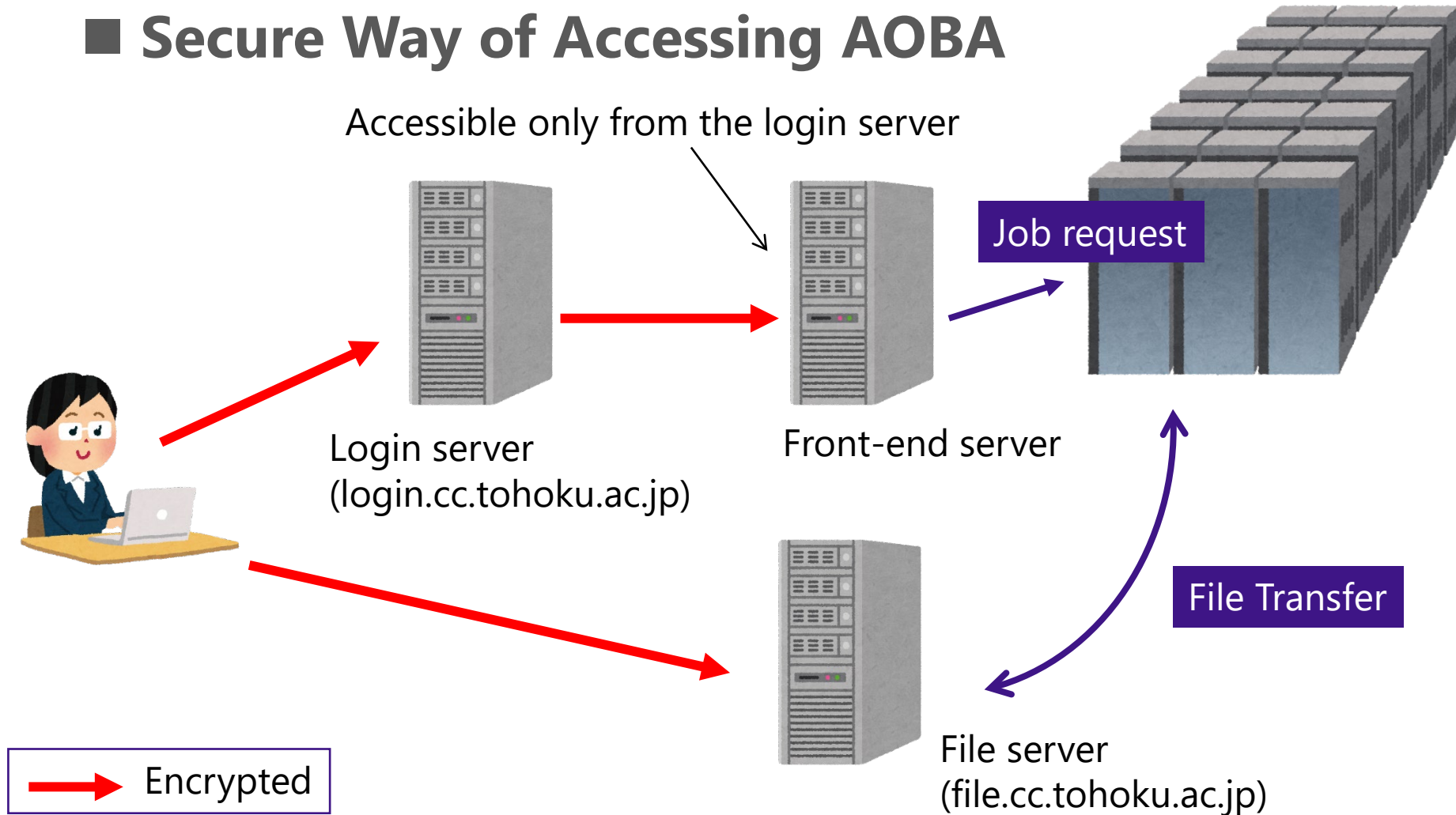
→ Encrypted

Secure Shell (SSH)

- **Communication Protcols for encrypted communication**
  - A number of **user authentication** mechanisms are available to check if a right person is going to access the remote computer.

- **Public Key Infrastructure (PKI)**
  - A pair of a **public key** and a **private key** is used for user authentication.

- **There are many SSH clients**
  - Windows Subsystem for Linux (WSL)
  - Windows Powershell
  - MacOS

Cyberscience Center

AOBA User Portal

■ **Create a pair of one private key and its correspongind public key**

🔑 **A private key is used to prove your identity.** You must always **keep it secret**, and never put it on the Internet. You must store it only on your own PC.

🔒 **A public key is actually something like a key hole.** In the case of AOBA, it is **automatically put** onto login, front, and file servers.

AOBA User Portal

https://www.ss.cc.tohoku.ac.jp/thkportal/riyosha_login/

login   front   file
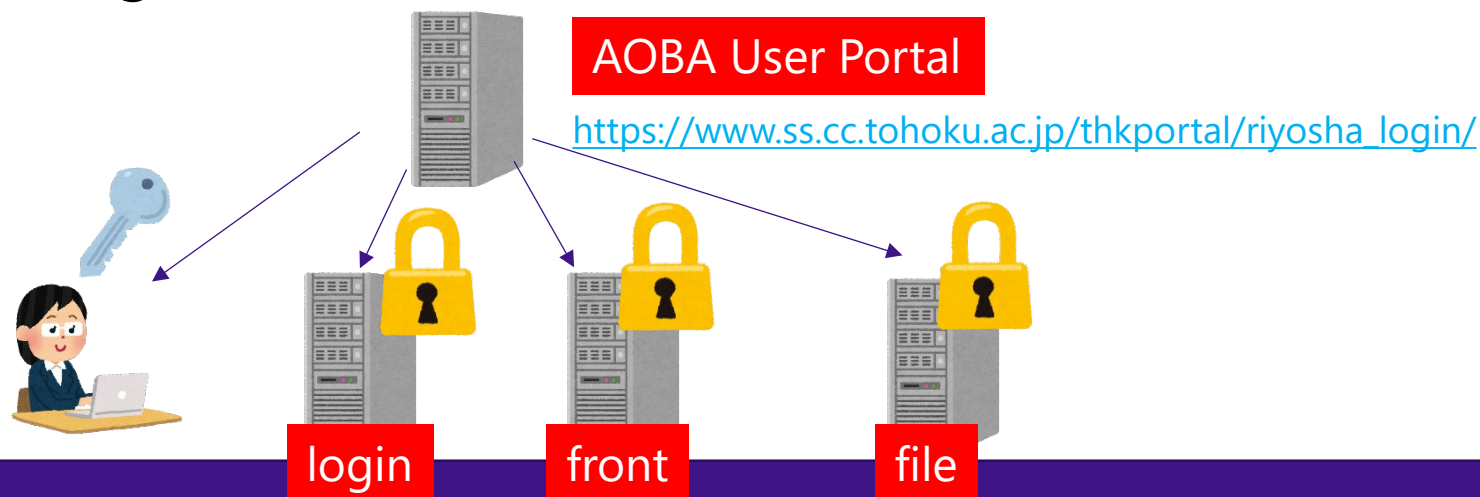
Login to AOBA Portal

■ You need **User Id** and Initial **Password**

- The initial password is used to login to the portal site and to create keys.

Login to the portal page

Logout

Create a key pair

Create a Key Pair

■ **Set a Passphrase** for your private key

- Even if your private key is stolen, it still needs the passphrase for user authentication.

Enter Your Secret Pass Phrase Twice

Private key is downloaded onto your PC
Public key is registered in remote servers.

Set up your Windows PC

■ **Move the private key (Don't copy) to …**
- Create a folder **C:¥Users¥[Name]¥.ssh**
- Here, [Name] is probably your name on your PC.

■ **Create a text file "config" in the same folder (be sure no file extention)**

```
# For login server
Host login
HostName login.cc.tohoku.ac.jp    # host name
User [User Id]                     # User Id at portal
IdentityFile ~/.ssh/id_rsa         # private key file
# For front server
Host front
HostName front.cc.tohoku.ac.jp    # host name
User [User Id]                     # User Id at portal
ProxyCommand ssh -CW %h:%p login  # access front via login
IdentityFile ~/.ssh/id_rsa
# For file server
Host file
HostName file.cc.tohoku.ac.jp     # host name
User [User Id]                     # User Id at portal
IdentityFile ~/.ssh/id_rsa         # private key file
```

Cyberscience Center

Windows PowerShell

Windows PowerShell
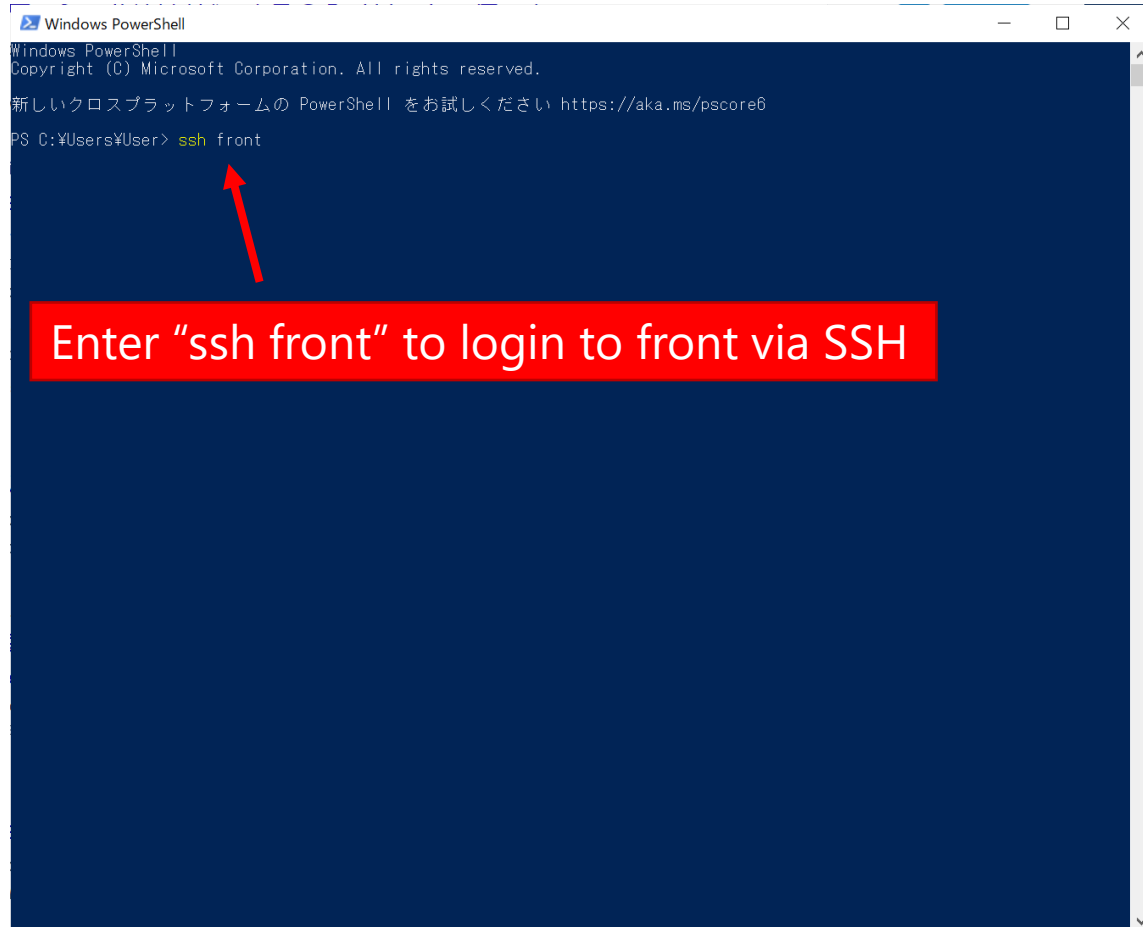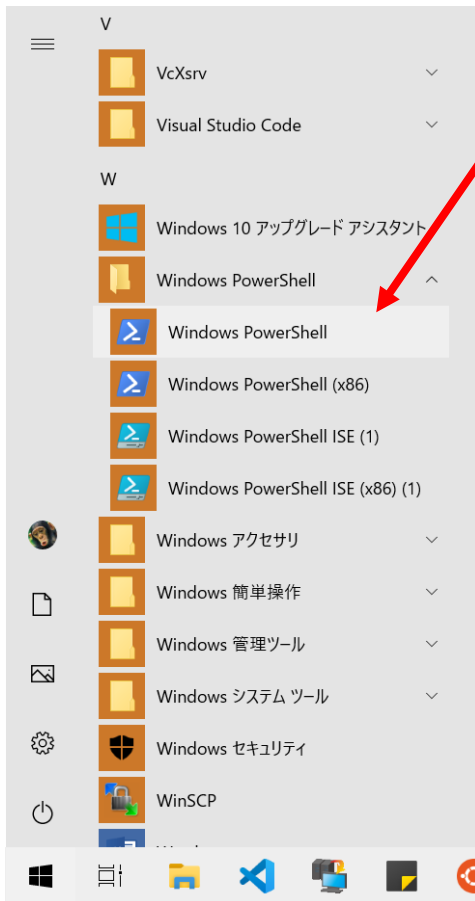
Enter "ssh front" to login to front via SSH

FAQ

■ **If you got the following message,**

```
CreateProcessW failed error:2
posix_spawn: No such file or directory
```

then, first find the ssh.exe on your system.

```
PS C:¥Users¥User> gcm ssh

CommandType     Name                                    Version    Source
-----------     ----                                    -------    ------
Application     ssh.exe                                 7.7.2.1    C:¥WINDOWS¥SYSTEM32¥OPENSSH¥ssh.exe
```

```
# For front server
Host front
HostName front.cc.tohoku.ac.jp
User [User Id]
ProxyCommand C:¥WINDOWS¥SYSTEM32¥OPENSSH¥ssh.exe -CW %h:%p login
IdentityFile ~/.ssh/id_rsa
```

Use it in your "config" file