

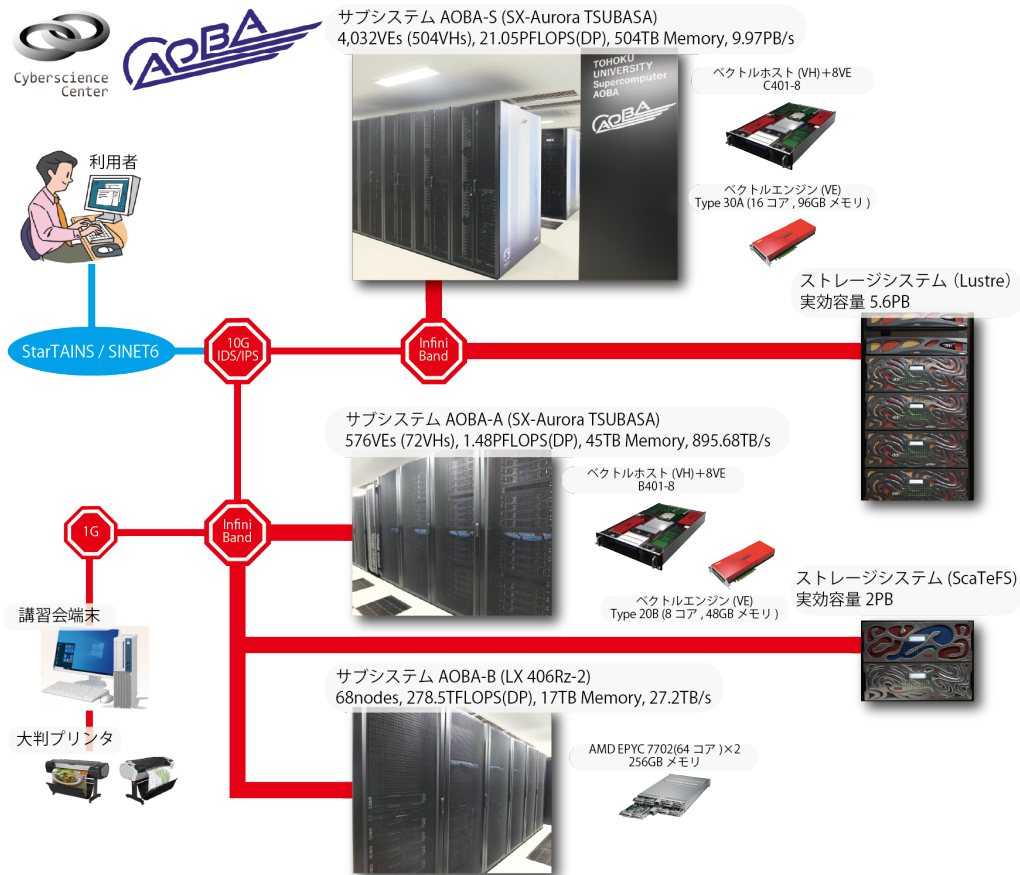
サイバーサイエンスセンター AOBAフロントエンドサーバ接続方法



2025.05

東北大学情報部 デジタルサービス支援課

AOBAシステムの概要



- 2つのフロントエンドサーバと、2つのストレージシステムがある
- AOBA-AおよびAOBA-Bを利用する場合
 - login.cc.tohoku.ac.jp経由でfrontにログインする
- AOBA-Sを利用する場合
 - sfront.cc.tohoku.ac.jpにログインする
- ログインはsshコマンドで秘密鍵を用いる方式

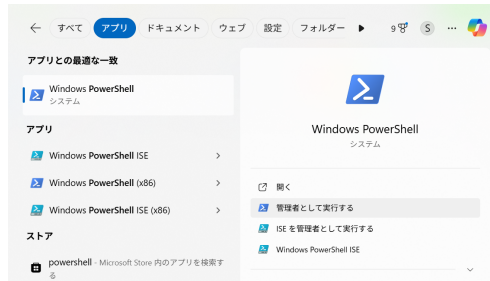
ssh接続の準備

Windows11の場合

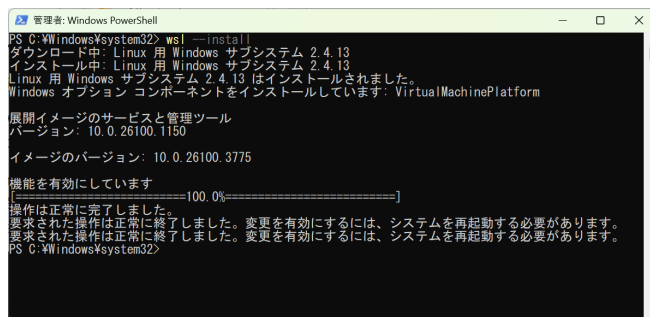
- WSL2 と Linux 環境 (Ubuntu) のインストール
- インストール方法については次ページとMicrosoftなどのページを参照
- <https://learn.microsoft.com/ja-jp/windows/wsl/install>
- https://qiita.com/SAITO_Keita/items/148f794a5b358e5cb87b

Windows11に WSL2 と Linux 環境 (Ubuntu) をインストール

1. Windows PowerShellを管理者として実行する



2. コマンド `wsl --install` で WSL2をインストール後、Windowsを再起動

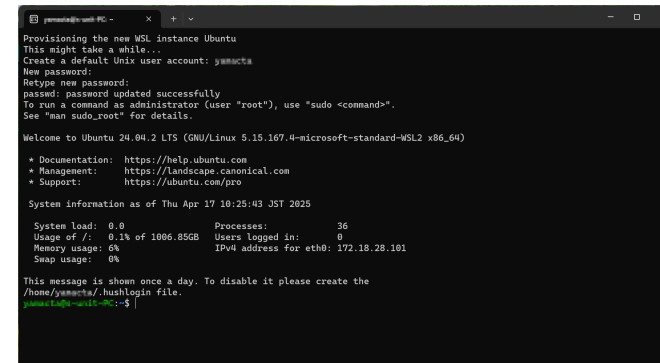


3. Windows PowerShellをユーザ権限で実行し、 コマンド `wsl --install -d Ubuntu` でUbuntuをインストール

4. Ubuntuを起動する



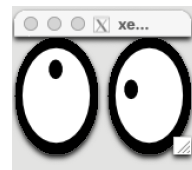
5. 初回起動時にユーザアカウントの作成と、パスワードの設定を必ず行う ユーザアカウント名は必ず英数字で作成



ssh接続の準備

Macの場合

- ・ XQuartzをインストール
- ・ 以下のページからインストーラーをダウンロード
- ・ <https://www.xquartz.org/>
- ・ インストール後、「ターミナル.app」を起動し、**xeyes** コマンドが実行されることを確認



秘密鍵ファイルの作成とダウンロード

- ・ 利用承認書に記載の（もしくは講習会参加用に提供された）利用者番号と初期パスワードで利用者ポータルにログインし、SSH暗号鍵ペアを作成する
- ・ サイバーHP -> 利用者ポータル -> 【鍵ペア作成・LDAPパスワード変更・AOBA-S 利用状況確認】 https://sportal.ss.cc.tohoku.ac.jp/thkportal/riyosha_login
- ・ 【SSH公開鍵登録】 をクリックし、任意のパスフレーズを設定した後 【鍵生成・登録】 をクリック
- ・ ローカルPCに秘密鍵ファイル「id_rsa_cc」がダウンロードされる

秘密鍵ファイルの移動とパーミッション変更

- Windows : Ubuntuを起動し、\$HOME/.sshディレクトリを作成した後、ダウンロードした「id_rsa_cc」ファイルを移動

```
mkdir $HOME/.ssh
```

```
mv /mnt/c/Users/ユーザアカウント名/Downloads/id_rsa_cc $HOME/.ssh/
```

- Mac/Linux : 端末（ターミナル）アプリを起動し、\$HOME/.ssh ディレクトリを作成した後、ダウンロードした「id_rsa_cc」ファイルを移動

```
mkdir $HOME/.ssh
```

```
mv $HOME/Downloads/id_rsa_cc $HOME/.ssh/
```

- Windows/Mac/Linux : ファイルのパーミッションを600に変更

```
chmod 600 $HOME/.ssh/id_rsa_cc
```

AOBA-A,B向けフロントエンドサーバへの接続設定ファイルの作成

- ・ .ssh フォルダ内にテキスト形式で、設定ファイル「config」を以下の内容で拡張子を付けずに作成する。「利用者番号」は発行された本人のものに書き換える。

Host login	# ログインサーバのニックネーム
HostName login.cc.tohoku.ac.jp	# ログインサーバ名
User 利用者番号	# 利用者番号は利用承認書に記載のものに書き換える
IdentityFile \$HOME/.ssh/id_rsa_cc	# ダウンロードした秘密鍵ファイルを指定
Host front	# フロントエンドサーバのニックネーム
HostName front	# フロントエンドサーバ名
User 利用者番号	# 利用者番号は利用承認書に記載のものに書き換える
IdentityFile \$HOME/.ssh/id_rsa_cc	# ダウンロードした秘密鍵ファイルを指定
ProxyJump login	# loginを経由した多段SSH接続を指定
ForwardX11 yes	# X11転送を有効にする
ForwardX11Trusted yes	# 信頼されたX11転送を有効にする

AOBA-S向けフロントエンドサーバへの接続設定ファイルの作成

- ・ .ssh フォルダ内にテキスト形式で、設定ファイル「config」を以下の内容で拡張子を付けずに作成する。「利用者番号」は発行された本人のものに書き換える。
- ・ AOBA-A,B向けに作成した設定ファイル「config」に追記してもよい。

Host sfront	# フロントエンドサーバのニックネーム
HostName sfront.cc.tohoku.ac.jp	# フロントエンドサーバ名
User 利用者番号	# 利用者番号は利用承認書に記載のものに書き換える
IdentityFile \$HOME/.ssh/id_rsa_cc	# ダウンロードした秘密鍵ファイルを指定
ForwardX11 yes	# X11転送を有効にする
ForwardX11Trusted yes	# 信頼されたX11転送を有効にする

SSH接続テスト

AOBA-A,B 向けフロントエンドサーバの場合

- Windowsの場合はUbuntuを起動
- Mac/Linuxの場合は、端末（ターミナル）アプリを開く
- 以下のコマンドでAOBA-A,B向けフロントエンドサーバにSSH接続ができるかを確認

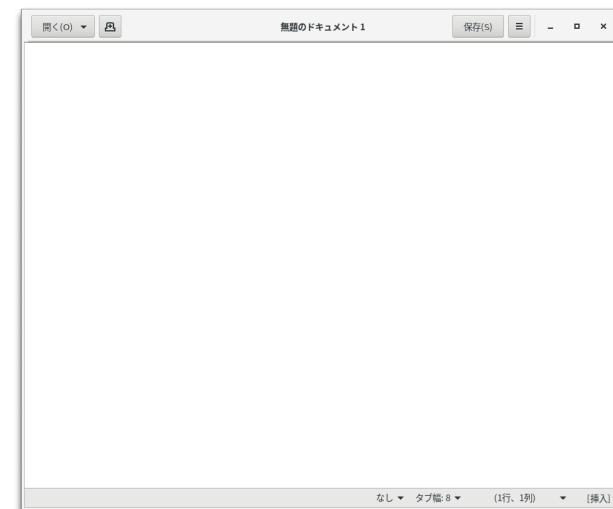
ssh front

秘密鍵作成時に自身で設定したパスフレーズを入力（2回必要）

（初回接続時のメッセージが出たら、**yes** で進む）

接続に成功するとプロンプトのホスト名が front1 または front2 になる

- **gedit** & コマンドでGUIのテキストエディタが開くことを確認



SSH接続テスト

AOBA-S 向けフロントエンドサーバの場合

- Windowsの場合はUbuntuを起動
- Mac/Linuxの場合は、端末（ターミナル）アプリを開く
- 以下のコマンドでAOBA-S向けフロントエンドサーバにSSH接続ができるかを確認

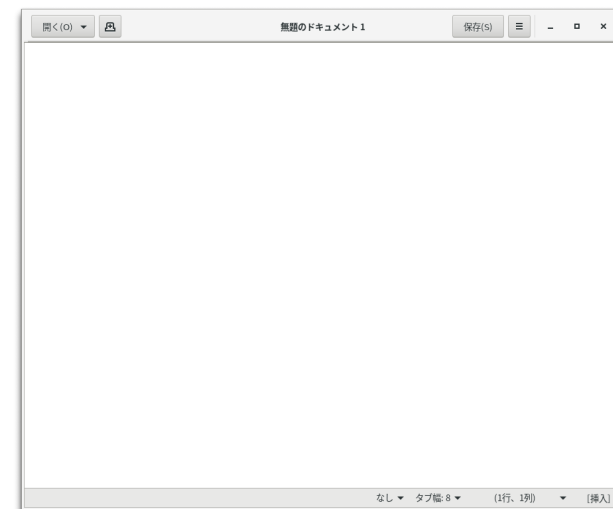
ssh sfront

秘密鍵作成時に自身で設定したパスフレーズを入力（1回必要）

（初回接続時のメッセージが出たら、**yes** で進む）

接続に成功するとプロンプトのホスト名が sfront1 または sfront2 になる

- **gedit** & コマンドでGUIのテキストエディタが開くことを確認





東北大学 サイバーサイエンスセンター
東北大学情報部 デジタルサービス支援課