Hokkaido University Information Initiative Center Guide for Proper Use of Interdisciplinary Large-Scale Computing Systems

April 1, 2025, Edition

Hokkaido University Information Initiative Center

Purpose of this Guide

Security incidents of unauthorized access, information leakage, and data falsification have been on the rise in information systems worldwide in recent years. To prevent such incidents, it is crucial to implement basic precautions, including proper management of user accounts and passwords, regular system management and monitoring, and application of the latest security updates.

This guide is designed for users of the Large-Scale Computing System (supercomputer system, research cloud system, cloud storage system, etc.) offered by the Hokkaido University Information Initiative Center (IIC). It summarizes important points to which IIC wants to draw attention of all users, including a comparison with public cloud services (commercial services offered for profit.) The research cloud system, in particular, must be operated with the utmost attention to security and privacy, as users have the authority to install and operate applications and share the same Kubernetes environment with other users. **We request that all users read this guide carefully BEFORE using the system and that they observe all the rules mentioned herein.** It is our hope that you will find the information in this guide helpful while using our system securely.

Notes

1. This guide may be revised without notice at any time. Please ensure to always refer to the latest version:

   URL
   https://www.hucc.hokudai.ac.jp/en/guide/guide-for-proper-use/

2. Please be aware that this guide is NOT comprehensive and focuses on points we believe to be the most essential. The service details and requirements illustrated in this guide are subject to change. As such, please refer to the latest information provided by IIC and other related departments to ensure the proper use of information systems.

Supercomputer System & Application Server

This page provides an overview of the Supercomputer System and Application Server offered by IIC and highlights key points that users should be aware of.

1. **Supercomputer System:** This system offers computation resources for large-scale scientific computing at a reasonable fee (approximately equivalent to the cost of electricity). When using the system, please ensure that suitable passwords and SSH private key settings are configured and strictly managed (see p. 6). Supercomputer system login nodes are shared resources used by system users to perform essential tasks such as logging in and compiling. Please do not perform tasks that occupy the CPU cores for extended periods, such as running long processes or production runs, as these can affect other users and disrupt system operations.

2. **Application Server:** The application server for conducting research on the Large-Scale Computing System is available solely to users who pay the Basic Service fee. When using the system, please ensure that suitable passwords and SSH private key settings are configured and strictly managed (see p. 6). As the system is a shared resource used by many users, please do not perform tasks that could affect other users or disrupt system operations.

3. Non-Japanese citizens who wish to use the Large-Scale Computing System (including the Supercomputer System) must undergo a security trade control evaluation. For details, please contact the User Support Desk in advance: hsay@iic.hokudai.ac.jp

4. Only faculty, employees, and students of Hokkaido University (HU) are permitted to run commercial software when using the Application Server (with few exceptions). When installing and using software licensed by a user on the supercomputer system or application server, the user is responsible for checking whether such use is permitted under the terms of the license agreement.

5. **Supercomputer System and Application Server Storage:** Users are permitted to store only research data related to the project described in their application, and in principle, only the data used on the supercomputer system and application server. **Please be aware that it is forbidden to use this service to store data of extremely high importance that would be seriously and severely affected if leaked or falsified (e.g., health records, sensitive personal information, My Number related information, drafts and information concerning exams, information related to grades and class rank) (see p. 7).**

Research Cloud System & Cloud Storage

Please ensure that you follow all the instructions outlined below when using the Research Cloud System or Cloud Storage.

1. **Research Cloud System:** Containerized service infrastructure based on Kubernetes technology is provided for research purposes. This so-called managed Kubernetes service and Kubernetes cluster construction and operation are managed by IIC. However, users are responsible for the installation and upgrades of individual applications (containers) running on the system, dealing with failures and vulnerabilities, and managing and backing up application data (persistent volumes).

2. When using the **research cloud system**, users will have strong authority equivalent to that of UNIX/Linux environment users and groups for the installation and operation of containerized applications. For technical reasons, IIC does not have authority over users and groups within the OS environment of individual containers. Therefore, **it is the user's responsibility to properly manage the installation and lifecycle of applications (containers) (see p.4). Even if the creation and management of applications are outsourced to external vendors, the ultimate responsibility lies with the users (see p.10).** Moreover, all registered accounts must be properly managed (p.4). Users are responsible for managing all data that is saved, processed, published, etc., through this service and should handle it appropriately (through encryption, duplication, monitoring, and backup, etc.) based on its importance (confidentiality, integrity, availability). Furthermore, please be aware that it is forbidden to use this service to store data of extremely high importance that would be seriously and severely affected if leaked or falsified (e.g., health records, sensitive personal information, My Number related information, drafts and information concerning exams, information related to grades and class rank) (p.7).

3. **Cloud Storage:** A storage system like Dropbox is provided on campus, offering high capacity and fast uploads. The Basic Fee for the Large-Scale Computing System includes 1TB of storage (100GB for students) without incurring additional fees. Additional storage can be added in 1TB increments for an extra charge. Users are able to access files via the internet; as such, **please pay particular attention to the management of related passwords (see p.6). Furthermore, please be aware that it is forbidden to use this service to store data of extremely high importance that would be seriously and severely affected if leaked or falsified (e.g., health records, sensitive personal information, My Number related information, drafts and information concerning exams, information related to grades and class rank) (see p.7).**

Management of Servers, Networks, and Accounts

Because users manage applications (containers) made and installed on shared clusters, exclusive clusters, and related Kubernetes clusters on the research cloud system, they should handle all elements involved in that maintenance (OS, applications, accounts, passwords, data, etc.,) with the utmost attention, (refer to p. 11 on Responsibilities Related to the Service). Special attention should be given to the following points:

1. In order to address security vulnerabilities, **the research cloud uses containers originally prepared by trusted service providers. Please ensure that all containers are kept up-to-date with the latest security and software updates.** In addition to OS, it is essential to properly manage all software, libraries, middleware, etc. This includes web server programs like Apache, PHP libraries, CMSs like WordPress, and distributed computing environments like Hadoop, etc. Several software programs offer automatic updates. **If there are no particular issues, we strongly recommend enabling these automatic updates.** (In some cases, automatic updates may cause issues. In such instances, it is the responsibility of users to manage them appropriately.)

2. Examine and configure your firewall settings properly, such as closing all unnecessary TCP/UDP ports and limiting the number of senders to the minimum required. If you need to obtain an SSL server certificate, you can use the UPKI digital certification issuance service offered by the National Institute of Informatics at no extra charge. Please contact the User Support Desk for details: hsay@iic.hokudai.ac.jp

3. When accessing the server via SSH, which is the typical means of remote terminal operation, please configure the SSH server appropriately, including restricting the source IP. In particular, please disable Password Authentication (set PassworldAuthentication no in `/etc/ssh/sshd_config`) and use key-based authentication. In addition, please configure it so that the management account cannot log in directly (set PermitRootLogin no in `/etc/ssh/sshd_config`)。

4. By using a VPN (Virtual Private Network) with appropriate encryption you can enhance the security of the communication path. (Please do not use outdated methods with known vulnerabilities, such as PPTP.) However, if the source or destination is connected to other networks, such as in site-to-site VPNs, there may be unexpected ripple effects, such as propagation of unauthorized communications or computer viruses. As such, please exercise caution when choosing, setting up, and operating a VPN.

5. For research and development test systems and other systems that contain **highly confidential information and carry considerable risk if leaked, please ensure that access permissions are minimized.** Furthermore, when accessing

from those limited terminals, be sure to use a VPN with proper encryption and SSH with key authentication.

6. When registering a new account, ensure that the user sets a suitable password and properly manages their SSH key authentication (see p.6). In the event that a user **graduates or is transferred, please promptly delete their account** and appropriately handle any linked data. Furthermore, if an account will be inactive for some time, please lock it and take other necessary precautions until it is intended to be accessed again.

7. If a non-Japanese citizen wishes to make a server account, they must first undergo a security trade control evaluation. For details, please contact the User Support Desk in advance: hsay@iic.hokudai.ac.jp

8. In addition to managing OS accounts, users must properly control all applications and middleware. This includes web server programs like Apache, content management systems such as WordPress, and distributed computing environments like Hadoop. **Please ensure that you check all default passwords, as some software may have simple default passwords.**

9. If a user possesses a license for software they intend to install on the Cloud System server, it is their responsibility to verify whether the license agreement permits such use.

10. Due to the importance of identifying cases of unauthorized access as soon as possible, access and network logs should be checked regularly. **If you come across a suspicious login or communication, please contact the IIC Computer Security Incident Response Team (CSIRT) immediately: hpc-security@iic.hokudai.ac.jp. Prompt detection and reporting are crucial to preventing further damage.**

Password and Key Management

For authentication information, such as passwords, that are required for using services offered by the Large-Scale Computing System, make sure you have taken necessary measures as described in the following.

1. Instruct ALL Users of the accounts for the servers and services you are using to keep their passwords strong and secure. A strong password is long, uses a combination of numbers, letters, and special characters, and does not contain simple keywords which can be easily guessed. **Administrator passwords, in particular, must be very strong and must be managed in a way that ensures they do not risk being leaked.** Additionally, please ensure that the same password is never used on other systems or services.

2. Users are responsible for the proper and strict management of SSH private key in the SSH public key authentication. Please ensure that the private key is stored in a location accessible only to the user and managed with utmost care to prevent leakage. Set a passphrase for the private key, similar to the password mentioned in item 1 above, and **do not use a key without a passphrase under any circumstances.** Furthermore, **do not store the private key on the Large-Scale Computing System.**

Management of Information and Data

1. The handling of information should be determined in accordance with the level of its importance. For example, **highly confidential information must be encrypted and never taken out of your department.** Make sure you are familiar with the rules and regulations specified in the department or organization that owns such information in advance. All HU staff and related personnel must be familiar with the National University Corporation Hokkaido University Internal Standards Concerning Grading and Handling of Information Assets. Furthermore, **do not save information such as** entrance exam problems, exam-related information, health records, sensitive personal information, or other highly confidential data on the supercomputer storage system which are available on the supercomputer system and application server, or research cloud system in the Large-Scale Computing System provided by IIC. (For such information, please use a dedicated system or terminal isolated from the internet, or the on-campus online storage system authenticated by HU's SSO system.)

2. Private and personal data must be managed with the utmost care. **If there are guidelines established by departments (e.g., a department related to medicine), you must abide by these guidelines. The same applies to information related to export control. Such information should not be taken out of the country without prior approval.**

3. To prevent research misconduct, research data is **required to be kept for 10 years from the date of the publication of results.** Data preservation is primarily the responsibility of the researchers themselves, but, if necessary, they are welcome to use the Cloud Storage (WebDAV storage) offered by IIC. If using a public (commercial) cloud service, each researcher must ensure their data does not contain confidential information or is appropriately encrypted before using such services.

4. Do not rely solely on one system when saving to the Research Cloud System and the applications running on it. Instead, we strongly encourage that you backup your data across several different systems. This approach will help ensure that you still have access to your data if one system is compromised by unauthorized access or infected with ransomware (malicious software that forcibly encrypts data or otherwise makes it inaccessible.)

5. Properly set access rights and public availability settings of your information and data. **A mistake in the settings may lead to unintentional distribution or leakage of confidential information.**

6. We ask that you exercise caution as an internet IT system when using the Large-Scale Computing System and please do not deal with illegal or otherwise harmful content while using the system.

Reference Information

- Standards for Information Classification and Handling Restrictions at National University Corporation Hokkaido University

  https://www.hokudai.ac.jp/jimuk/reiki/reiki_honbun/u010RG00000949.html
  (in Japanese)

- Information Classification for Handling Data in the Storage of Large-Scale Computing Systems Provided by the Information Initiative Center at Hokkaido University

Service	Information Classification Category	Usage Purposes
Information Initiative Center Supercomputer Storage System	Confidentiality Level 2 Information	Storing research data related to the project registered at the time of application
Information Initiative Center Research Cloud System Cloud Storage	Confidentiality Level 3 Information	Storing research results related to the project registered at the time of application. Safe storage of research data

Removal of Access Restrictions

As part of the comprehensive security measures that IIC has been taking, all communications from outside HU are blocked. If you need to access on-campus servers from outside HU, you must file an application to remove restrictions to the Information Security Management Section, ICT Promotion Office. All applications and inquiries relating to applications should be sent to: exception-apply@security.hokudai.ac.jp

1. When applying, specify the minimum required application names, TCP/UDP port numbers, and transmission sources. Please refrain from using unspecified transmission sources (0.0.0.0.0/0 in CIDR notation) as much as possible.

   (Since this will expose the port to a theoretical maximum of 4.3 billion devices worldwide, please limit such cases to those that are absolutely necessary, such as port 443 for HTTPS.)

When Outsourcing the System Construction

When outsourcing all or part of system construction or operation on the Cloud System to an external contractor, **the overall responsibility remains with the user and NOT the contractor.** Contractors are only responsible for the duties assigned to them in their contracts. Please pay attention to the following points before signing an agreement with a contractor.

1. **Clearly indicate which parts of business are to be handled by external contractors and which parts will be handled by you (as the user).** For example, when asking a contractor to create a website, if the contract specifies that the contractor will only handle website content creation, then the server management and security measures must be managed by the user.

2. Selecting the right contractor is also the responsibility of the user. Do not select a contractor based solely on cost; instead, carefully consider their business performance and check if they have third-party certification (e.g., PrivacyMark). When outlining specifications in an outsourcing contract, make sure to include important security requirements such as compliance with the security policy and the handling of information according to its level of importance.

3. When HU faculty and employees place an order relating to information systems including the conclusion of an agreement with a contractor, an application for the optimization of the information system may be required (application is mandatory in the case of procurement relating to external cloud systems). For details, please refer to the link below.

   https://www.oicte.hokudai.ac.jp/ict/optimisation.html (in Japanese)

Scope of Responsibilities (Between Service Provider and Users)

The following table shows the service requirements for the Large-Scale Computing System offered by IIC, along with the general requirements for public cloud services (commercial services offered for profit) for comparison. The responsibilities of the service provider and of the user are specified for each service so as to clarify the separation of duties. **Keep in mind that the final responsibility for ensuring the security of items listed under "Service User Responsibilities" lie solely with the user.** Make sure you take all necessary measures to ensure the security of items under your supervision.

Service	Service Provider Responsibilities	Service User Responsibilities
Information Initiative Center Supercomputer System Application Server	Hardware, operating system, job scheduler, application software (excluding those introduced by the users themselves)	Appropriate management of accounts, passwords, SSH private keys, data, resources, and applications introduced by users themselves, etc.
Information Initiative Center Supercomputer Storage System	Hardware (storage, network), storage management software	Appropriate management of accounts, passwords, data, encryption of confidential information, access authorization settings, etc.
Information Initiative Center Research Cloud System (Shared Clusters)	Hardware (server, network, storage), host OS, deployment and operational management of Kubernetes clusters shared among service users	Proper installation and operational management of containers (guest OS, library, application), management of container persistent data, accounts, passwords, SSH private keys, and containers monitoring, etc.
Information Initiative Center Research Cloud System (Exclusive Clusters)	Hardware, host OS, deployment of Kubernetes clusters occupied by service users (management and operation of Kubernetes clusters are the responsibility of the users)	Operational management of occupied Kubernetes clusters, proper installation and management of containers (OS, libraries, applications), management of container persistent data, accounts, passwords, SSH private keys, and monitoring of containers and Kubernetes clusters, etc.
Information Initiative Center Cloud Storage	Hardware (storage network), storage	Proper management of accounts, passwords, and data; encryption of confidential information,

	management software	access authorization settings, etc.
Public Cloud (when renting a server/storage system or platform)	Service provider's requirements (normally up to hypervisor and cloud management software)	Everything else (management of operating system, software, data, account and password, and server monitoring)
Public Cloud (when using a web service)	Service provider's requirements	Everything else

Reference Information (URLs and E-mail Addresses)

Hokkaido University Information Initiative Center: https://www.iic.hokudai.ac.jp/

・Large-Scale Computing System Portal: https://www.hucc.hokudai.ac.jp/

(Interdisciplinary Large-Scale Computing System)

・Large-Scale Computing System User Support Desk: hsay@iic.hokudai.ac.jp

・Large-Scale Computing System CSIRT: hpc-security@iic.hokudai.ac.jp

(Contact for Security Incidents Related to Large-Scale Computing Systems)

Hokkaido University ICT Promotion Office https://www.oicte.hokudai.ac.jp/ (internal use only)

・ICT Security Office exception-apply@security.hokudai.ac.jp

(Inquiries and submission address for communication restriction removal requests)

・Hokkaido University CSIRT security@oicte.hokudai.ac.jp

(Contact for security incidents related to Hokkaido University, excluding Large-Scale Computing Systems)

Hokkaido University Information Initiative Center

Guide for Proper Use of

Interdisciplinary Large-Scale Computing Systems

As of April 1, 2025

https://www.hucc.hokudai.ac.jp/guide/guidance/

Inquiries about this guide:

hsay@iic.hokudai.ac.jp
