

# 7. Information Systems and Cyber Security Center (ISCSC)

## Information network, systems and security

NIFS research activities generate vast amounts of experimental and computational data. An information system linked to an information network analyzes these data, and the results are published externally.

The Information Systems Security Center is an organization that coordinates information systems and information networks. The center is divided into three groups: Information Networks, Information Systems, and Cyber Security (Information Security) and each operate under the direction of a group leader. There is some overlap in the areas of responsibility, so some members belong to multiple groups.

The Information Network Group is committed to providing a stable information network environment. Information networks are the foundation of research activities, but simply connecting devices is insufficient to create a reliable infrastructure. Therefore, it is imperative to thoroughly verify the functionality of network devices and to consider security.

We have performed necessary maintenance on equipment to ensure a stable operation of the information network. In the 2024 fiscal year, we installed wireless access points (APs) in some buildings of NIFS. This enabled Wi-Fi access in the usual usage areas within the target buildings. As before, we use eduroam for authentication, and institutions that are members of eduroam can use it without prior setup. This wireless AP installation is planned to be implemented over multiple years, and we will continue to proceed with it in the 2025 fiscal year and beyond.

An information network requires multiple servers to operate. Our group has been building a private cloud using VMware vSphere from VMware, but with Broadcom's acquisition of VMware, the licensing system has changed significantly. This has led to a significant increase in licensing costs. The servers and storage components of the private cloud are nearing the end of their maintenance period. We have therefore decided to transition away from VMware vSphere in conjunction with hardware updates and are currently conducting research for procurement in the 2025 fiscal year.

A firewall and an access gateway that performed security checks on terminals connected to the firewall in advance had been installed between the LHD experimental network (LHD-LAN) and the research infrastructure network (NIFS-LAN). We discontinued the operation of the access gateway and updated it to a firewall compatible with Active Directory authentication. This change shifted the authentication method from device-based to user-based authentication. We also expanded the connection bandwidth and installed optical fiber between buildings.

The Information Systems Group develops, operates, and maintains various information systems that form the foundation of the institute, as well as those related to public relations, evaluation, and research support. At the stage of developing information systems, we conduct appropriate system development, such as clarifying requirements through interviews with relevant parties, to facilitate and improve the efficiency of research activities. On the other hand, in order to improve the operational efficiency of the entire institute, it is not necessarily appropriate to have a system in which only the Information System Group conducts system development, and we believe that it is necessary for the field staff, who are familiar with the business, to create their own tools. For supporting this concept in the near future, we are working to build up knowledge and technology.

In FY2024, the NIFS Research Activity Database (NRAD), a database of the Institute’s research activities, was established. NRAD also references multiple external databases, allowing for the inclusion of achievements that were previously missing from the NIFS Article Information System (NAIS), as well as improving the accuracy of the data for each achievement itself. We have shut down a research-related-event support system “Workshop”, which we had developed and operated independently. Instead, we have introduced the open-source software “Indico”, which is also used by many other institutions. The “Workshop” system required users to create a user account for each workshop, but by linking with a Google account, users can now participate in multiple workshops by creating an account only once. This has improved convenience for users.

The Cyber Security Group works with the Information Network Group and Information Systems Group to build a robust security system that includes user education. The group’s members serve as the Computer Security Incident Response Team (NIFS-CSIRT). They respond to security incidents by investigating their causes and minimizing damage. The group works directly with the institution’s Chief of Information Security Officer (CISO) and information security managers to respond to incidents. NIFS-CSIRT is a member of the National Institute of Natural Sciences CSIRT (NINS-CSIRT) and regularly shares information with them.

In fiscal 2024, we introduced SPC Leak Detection, an account leakage management service provided by SourcePod. Leaked account information is traded on the dark web, which cannot be accessed with a normal web browser. The newly introduced service investigates whether information using the institute’s email address, such as the account name, has been leaked onto the internet or dark web. If a leak is detected, the service notifies the individual via email and records the incident on the management site.

As in previous years, we also conducted information security training via video on demand. Fortunately, there were no serious incidents in fiscal 2024. We also collaborated with NINS to conduct information incident response training, targeted email training, and internal audits related to information security.

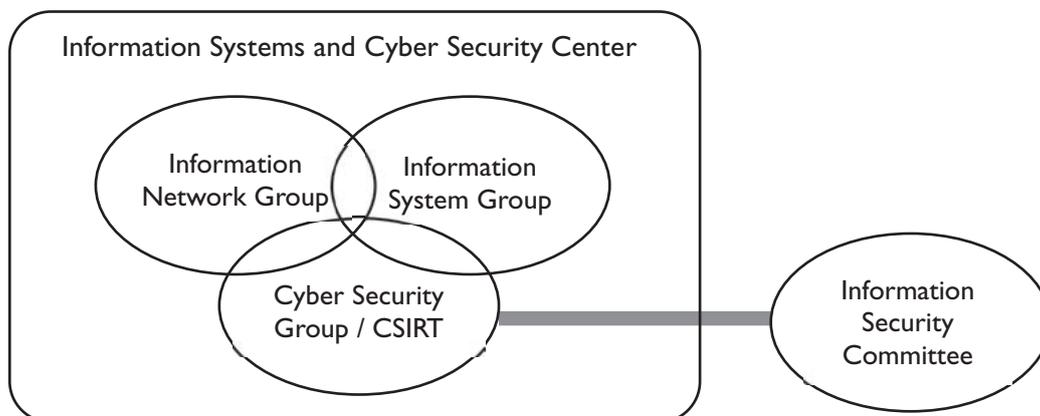


Fig. 1 Structure of Information Systems and Cyber Security Center.

(T. Yamamoto)