7. Information Systems and Cyber Security Center (ISCSC)

Information network, systems and security

At NIFS, research activities generate a large amount of experimental and computational data. Some results are produced from the data by an information system that is organically connected by an information network.

From FY2023, the structure of the information systems and the information networks was reorganized from the "Division of Information and Communication Systems" to the "Information Systems and Security Center", which consists of three groups as described below. Each group operates under the direction of a group leader. Since there is naturally some overlap in the areas for which each group is responsible, some of the members serve on more than one group at the same time.

The Information Network Group provides a stable information network environment. Information networks can be regarded as the foundation of research activities, but they are still in their infancy and cannot be a reliable foundation simply by connecting devices. It is important to examine the functions of network devices and consider security.

To ensure the stable operation of information networks, we conducted maintenance work on the necessary equipment. In FY2013, the NTP server, which receives time information from GPS satellites and distributes it to network devices, and the security system that prevents unregistered terminals from connecting to the LHD experimental LAN was updated.

In addition, in FY2023, we conducted a review of our information security equipment and installed a new DNS firewall, also known as the DNS Reputation Service. Most of the current communication uses web services, and the communication channel is encrypted with HTTPS. Previously, a targeted attack detection system installed in the communication channel detected malware and other suspicious communications, but the encryption made it difficult to verify the contents. In contrast, many communications use DNS, a service that converts host names to IP addresses, to initiate a connection, and DNS firewalls, a type of cloud service, can block malicious communications before they take place by returning invalid IP addresses when queried by known malicious hosts.

The Information Systems Group develops, operates, and maintains the various information systems that form the foundation of the Institute, as well as those related to public relations, evaluation, and research support. The efficiency of an information system depends on data design and programming methods. User comfort also depends on the quality of the user interface (UI). Therefore, 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.

In FY2023, the NIFS Article Information System (NAIS), which is responsible for managing the Institute's research activities, was renovated to support the latest versions of the basic software (Operating System) and the framework, Play Framework. In addition, some parts of the UI have been revised. We have reduced the number of accounts that users must manage by switching from NAIS's own user authentication system to COLiD, a collaborative researcher authentication system. In the future, we plan to further integrate user authentication mechanisms to provide secure and convenient services.

The Cyber Security Group works with the Information Network Group and the Information Systems Group to create a strong security structure. This includes user education. In addition, members of the Information Security

Group also serve as the Computer Security Incident Response Team (NIFS-CSIRT), and in the event of a security incident, they will investigate the cause and respond to minimize the damage. Additionally, they collaborate with the institutional CISO and the Information Security Manager to address the incident. The NIFS-CSIRT is also a member of the CSIRT of the National Institutes of Natural Sciences (NINS-CSIRT), and shares information with them in regular operations.

In the 2023 fiscal year, information security training for new staff and for all offices was conducted via video on demand. Fortunately, no significant incidents occurred, and several events were responded to. In collaboration with NINS, information incident response training and targeted email training were conducted. Internal audits of information security were conducted with each other and with NINS.

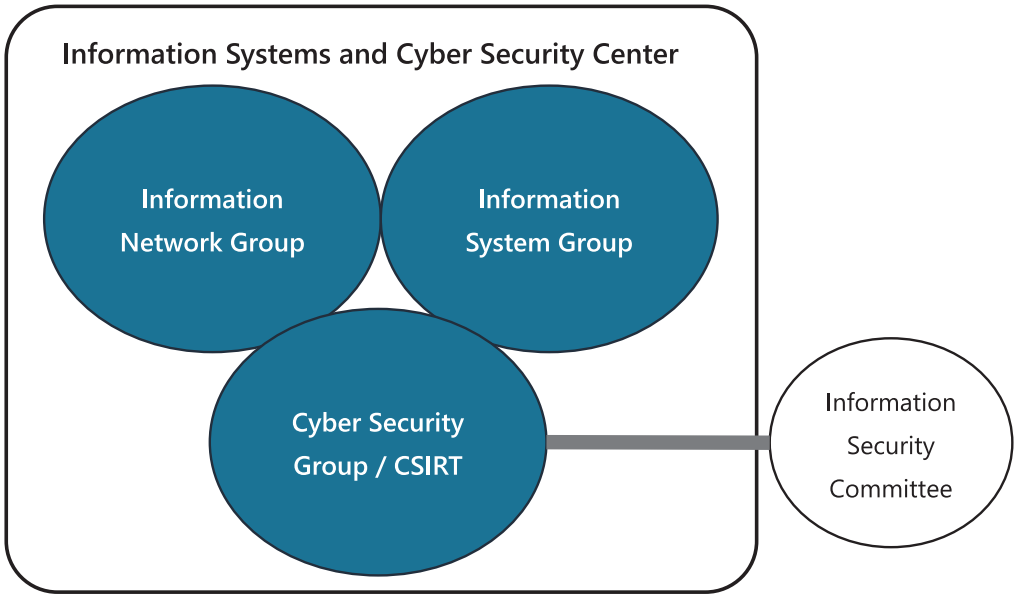

Fig. 1 Structure of Information Systems and Cyber Security Center.

(T. Yamamoto)