National Institute of Informatics News ISSN 1883-1974 (Print) ISSN 1884-0787 (Online)

NII Today

61
Mar. 2017
National Institute of Informatics News

NII Interview

Wanted: Cyber-Security Talent

[With Cabinet Secretariat, Deputy Director-General of NISC]

Protecting Academic Freedom with Security

Goals of NII's Practical Training Program in Cybersecurity

[Information Initiative Center, Hokkaido University]

Information Security Measures Needed in Universities Today

Feature

Developing Cyber Security Human Resources

Safeguarding Academic Networks from Cyber Threats

This English language edition
NII Today corresponds to
No. 75 of the Japanese edition

Wanted: Cyber-Security Talent

Monitoring Services and Training to Boost Security of Academic Cyberspace

Masaru Kitsuregawa (Director General, National Institute of Informatics)
Interviewer: Masako Wakae (Senior Writer, Yomiuri Shimbun)

Research institutions face the daily threat of being targeted in cyber attacks that steal information and alter websites. Starting this summer, though, the National Institute of Informatics plans to systematically detect attacks carried out against the SINET5 academic network and then share this information with member universities and related institutions. Strategically the operation is aimed at killing two birds with one stone: to support interaction among institutions during an emergency and to utilize exchanges of data to train university cyber-security personnel. NII Director General Masaru Kitsuregawa tells us about the project.

Wakae Doesn't university cyber security seem naive when you think about the serious incidents that have happened recently, one after another?

Kitsuregawa It is troubling. We take seriously the climate at a university that encourages the freedom to conduct research. Strict information management, similar to what a company has, would be hard to get used to. It is necessary to accept researchers from various countries, then get each of the computers they bring in connected to a university network. In turn, maintaining intellectual property with security assurances has become urgent business.

Wakae It has also been pointed out that talented people are not being brought up to take on the burden of cyber security at universities.

Kitsuregawa Supercomputers used to symbolize what we now call IT. Access in the past to a university's computation services has been superseded by the importance of a network connection. Accordingly, the necessity for security has risen, but organizations haven't coped very well with the change in demand. At many organizations, it's often the case that the people in charge of computer and network operations take on security burdens outside their fields of specialization. Developing security talent is key. The situation is such that each one of the 1,000 research institutions we've counted in Japan has a hard time prepping a security specialist.

Wakae And that concern has led to the initiative for this project?

Kitsuregawa SINET5 connects universities and research organizations. NII will maintain systems that detect cyber attacks against the net, monitoring communications 24 hours a day, 365 days a year. Information about attacks and suspicious communi cations, and the results of analyses, will be sent to each organization in the network. If it is difficult for any group to deal with an incident, NII will offer interactive support as needed.

Wakae In short, NII appears set to establish a SOC (security operation center) and provide a monitoring service. Government-

Masaru Kitsuregawa

agency communications are already monitored by the National Information Security Center (NISC). And it was decided that the Information-Technology Promotion Agency (IPA) would monitor networks serving incorporated administrative agencies. Now, a similar service will finally help universities?

Kitsuregawa The university version of these services will resemble ISAC (Information Sharing and Analysis Center), the security information sharing organization that has begun working with some industries in Japan. Because cyber attackers tend to aim for similar industries at the same time, we know that other universities are probably being targeted when attacks on one university come to light. Even so, it has been pretty hard to assess damage from attacks. From now on, as soon as NII detects malware (malicious programs) or suspicious communications, we will notify the affected organization. In doing so, we want to glean beneficial defensive information from the affected organization to share with the others while keeping the name of the affected organization confidential.

Wakae So you expect a smoother distribution of helpful information if the damaged organization is kept anonymous. And other universities are more likely to take countermeasures if they have information describing how the malware behaves and where it is being sent.

Kitsuregawa Another one of our aims is to upgrade the skills of cyber-security people at each organization. First we'll have them trained in how to use analytical systems. After that, they'll receive observed data and analysis results daily from NII plus support in dealing with problems that occur. During this time, we'll also have them increase their competency by way of OJT (on-the-job training). In accepting university teachers and students as visiting researchers and interns, we are studying ways to check them out too.

Wakae Who are the beneficiaries of the monitoring service?

Kitsuregawa They are the national universities and the Inter-University Research Institute Corporations. A total of 102 of these organizations have joined SINET5—86 national universities and 16 research institute corporations. Currently around 80 percent have indicated they want to participate.

Wakae Yet, 844 organizations, including public universities, private universities, and technical colleges, are in SINET5. Will no more than 10 percent of them be involved in this project?

Kitsuregawa Coverage of operating expenses for the project depends on national university corporation grants that have left out private universities and technical colleges. Circumstances already stretch budgetary limits. Even this year's budget of 780 million yen will purchase just one-third of the equipment originally planned.

Wakae Really? Only that much to cover the SOC room, equipment costs, and personnel expenses?

Kitsuregawa It's not a lot. We will have to work wisely.

Wakae Do you presume that voluminous amounts of cyber-attack data will become available as a result of project monitoring?

Kitsuregawa That's the drawing card for the project. Data obtained from monitoring will be processed so as not to specify victims and then provided free of charge to academic institution researchers. Furthermore, our intention is to put it out within one hour of observation. Under the current framework, it takes at least a year for malware to make the rounds of the research community. In an age when tens of thousands of malware programs can be created in a day, cyber-attack patterns change significantly in a year. Security depends on speed. That makes supply of this data crucial.

Wakae The project also appears useful to those carrying out cyber-attack research on IoT equipment.

Kitsuregawa For example, if a program were built in to detect specific scans at contact points of SINET5 and business-related networks, we might be able to understand a cyber attacker's intentions toward an IoT apparatus. These days, data controls the outcome of research. We want to contribute to cyber-security research in Japan by supplying massive amounts of fresh data.

(Photography: Yusuke Sato)

A Word from the Interviewer

Some years back I showed up at a study session on university cyber security. Even though many of the participants were shouldering the burden of running systems and networks at their respective universities, responsibility for security itself had been left, almost casually, to faculty members. And yet, without the opportunity for specialized training in cyber security, how could anyone budget for it? Furthermore, strict information management is anathema to the free research atmosphere at universities. Amid the increasing number of cyber attacks, managers at every level have grown impatient.

From having observed these troubles up close, I hold high hopes for the NII initiative. Most of all, it widens the road for sharing information as well as upgrading the skills of people in charge who have fought a lonely battle for cyber security at every university. It's unfortunate, though, that the subjects of this project are limited to the national universities. Why couldn't the project spread to the private universities and technical colleges?

I also expect utilization of the observed data for study purposes. Critics of cyber security in Japan like to point to the overwhelming lack of cyber-attack data on hand. As it is, researchers pay dearly for foreign-collected data because even the malware databases constructed overseas as a matter of course are insufficient. The NII endeavor should become a chance to review a number of "taboos" in Japan.

Masako Wakae

In 1988, she graduated from Aoyama Gakuin University and joined the Yomiuri Shimbun. Since 2014, she has been assigned to the city desk as a senior writer.

Protecting Academic Freedom with Security

Addressing the need to increase security after a series of cyber attacks

Ikuo Misumi

(Deputy Director-General, National center of Incident readiness and Strategy for Cybersecurity (NISC), Councilor, Cabinet Secretariat, Government of Japan / Visiting Professor, National Institute of Informatics (since April 2017))

"Maintaining cybersecurity is not an end unto itself. It is a means for protecting academic research and academic freedom." Ikuo Misumi, Councilor, Cabinet Secretariat, and Deputy Director-General of the National center of Incident readiness and Strategy for Cybersecurity (NISC) discusses the significance of cybersecurity for academic institutions. He explains that academic institutions first need to identify what needs to be protected and then invest resources such as funding and personnel accordingly.

Protecting research data from cyber attacks

—— In recent years, the Japanese government has allocated more of its budget to security measures after a series of cyber attacks on public institutions like the Japan Pension Service.

Misumi Greater awareness of cybersecurity is desirable. But I'm concerned about making security measures themselves the purpose of studies and neglecting to consider what should be protected in the first place. The means must be not confused with the end. For example, for universities and research institutions, the purpose of academic research is to be the first in the world to produce research results. If the achievements are beneficial to the world, that is a wonderful thing.

Data from research, especially from the natural sciences, are primarily stored in computers. If these data are stolen or falsified as a result of cyber attacks, research can be negatively affected. Cybersecurity is a critical means of protecting research and academic freedom, including the freedom of researchers to conduct research and the ability to present research results when they wish.

Research achievements are the fruit of the efforts of each and every researcher. Much of the research environments that make the achievements possible are supported by monies from citizens' taxes. If it is joint research, there is a contractual obligation to protect data. Each researcher must increase his or her consciousness of ensuring cybersecurity.

—— What is the role of NISC in improving security and fostering human resources?

Misumi NISC, where I serve as the Deputy Director-General, stands for the "National Center of Incident Readiness and Strategy for Cybersecurity." As its name suggests, the center prepares against security incidents like cyber attacks and is responsible for monitoring and auditing the networks of Japanese government ministries and agencies and planning cybersecurity strategies. The team consists of a mix of civil servants and private-sector workers. Initially consisting of 70 to 80 persons, the center has grown vastly in the past two years. It is expected to reach 180 staff members in 2016.

NISC is also dedicated to fostering human resources who are responsible for security in each government agency. Security managers with the rank of Deputy Director General were placed in each ministry from April 2016, and in the summer they created a human resources acquisition and development plan. Education and training of workers will be carried out based on this plan to increase security expertise.

In 2015, NISC detected suspicious communication to the outside world through the networks of the Ministry of Health, Labour and Welfare (MHLW), prompting the ministry to take action. This led to the discovery of targeted attacks against the Japan Pension Service. After this incident, the Basic Act on Cybersecurity was revised. NISC's purview for monitoring and auditing broadened from central ministries and agencies to include Incorporated Administrative Agencies and some Special Corporations.

—— After a series of cyber attacks, there is now greater understanding of the need for security. But we now face the issue of how to procure funds to cover the cost of concrete countermeasures.

Misumi Regardless of whether it is a public agency or private company, cybersecurity should be considered not as a cost but as investment to achieve the purpose of the organization.

For example, industries in the U.S. are aware of the question of how security is to be used to achieve the purpose of economic growth. Actually, when the economy is in a slump in the U.S., companies increase their IT investment. This is because for U.S. companies, IT is a business innovation tool for creating new business. It is considered an investment for producing profit. Expenditure on security can also be viewed as investment from the standpoint of creating trust in products and services and contributing to profit. Many Japanese companies, on the other hand, tend to view IT mainly as a tool for reducing costs, for example by automating work.

Developing human resources that act as "intermediary" between IT and management

Misumi Why is IT connected with business innovation in the U.S.? One reason may be that many company executive candidates have earned a master's degree in both management and IT. There is a system of

systematically nurturing personnel who serve as intermediary between IT and management. As a result, they can give appropriate advice to senior management about cybersecurity.

There are not enough human resources who play such an intermediate role in Japan. We need to cultivate personnel who can advise senior management by proposing business strategies and laying cybersecurity on top of those foundations.

——In Japan, there is an outcry about the lack of security personnel. But the impression is that it is all about having more engineers.

Misumi I envision three types of security personnel: onsite engineers who manage IT, senior management who determine investment in security, and intermediary personnel who connect field IT engineers and senior management.

A new measure to increase the skills of engineers in the field is the new national certification for "Registered Information Security Specialist," established in October 2016. This qualification, renewable every three years, succeeds the previous Information Security Specialist Examination. For senior management, the Ministry of Economy, Trade and Industry (METI) has released revised "Cybersecurity Management Guidelines" in December 2016 with the goal of raising awareness of security in managers.

Meanwhile, it is difficult to cultivate intermediary personnel who connect senior management and cybersecurity implementers like engineers, and there is a chronic shortage of them. There are not a lot of places as there are in the U.S. to systematically develop human resources who are intimately familiar with both management and IT. How to foster intermediary personnel in companies and organizations will be a challenge.

—— What roles do NII and the academic information network SINET (Science Information NETwork) play in nurturing security personnel?

Misumi Besides being an academic research tool, SINET itself is a research subject for high-speed communication. Efforts are needed to protect frontline research like high-speed communication, while maintaining its ease-of-use for researchers.

NII is being counted on to play a role in the operation of SINET. Because real data constantly flows through SINET, it can be used for training university network administrators in practical cybersecurity.

Accelerating concrete studies in academia

Misumi Unfortunately, in the second half of 2016, a series of security incidents targeting academic institutions like the University of Toyama occurred one after another.*

To protect academic research from the threat of cyber attacks, it is necessary to determine where to allocate resources like personnel and funding, and how much. How will security personnel be developed? Academic institutions must first determine how much money to invest in security and then decide how to develop security personnel.

For example, in terms of facilities there is the need to have priority monitoring of connections between SINET and the Internet in Tokyo and Osaka.

In terms of human resources, what is needed are people with diverse skills. We need not only security experts but also network experts, legal experts, and leaders who determine policy by assembling these specialists into teams. A single person who is a "Top Gun" in security will not be able to maintain security. We need to advance such concrete considerations.

(Interview and text: Naoki Asakawa
Photo: Akiko Ikeda)

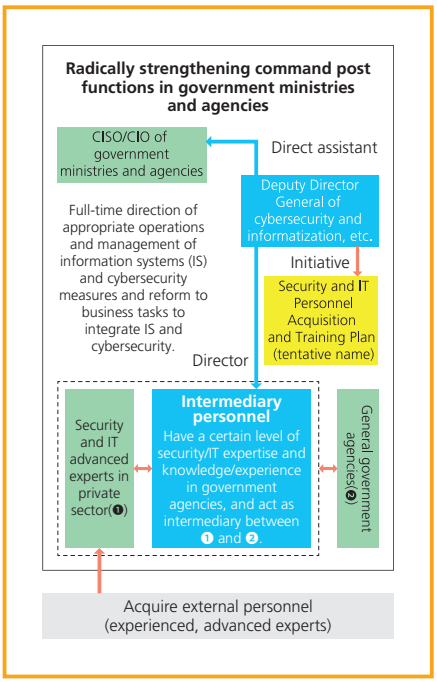

Figure Training of security and IT personnel in government agencies

* Personal computers in the University of Toyama's Hydrogen Isotope Research Center were infected by a virus as a result of targeted attacks, and research-related files were leaked. It was also reported that the PCs in the National Defense Medical College were illegally accessed through SINET.

Ikuo Misumi

Ph.D. (engineering), University of Tokyo. Assumed current position in June 2016 after serving as Director of the Information-technology SEcurity Center (ISEC), Information-technology Promotion Agency, Japan (IPA); Director of Information Security Policy Division, Commerce and Information Policy Bureau, METI; Director of Security Export Licensing Division, Trade Control Department, Trade and Economic Cooperation Bureau, METI; and Counsellor, Cabinet Secretariat, of NISC.

Goals of NII's Practical Training Program in Cybersecurity

A look at NII's Cybersecurity Human Resources Development Program

Hiroki Takakura

(Professor, Information Systems Architecture Science Research Division, NII/
Director of Cybersecurity Research and Development Center, NII/
Professor, School of Multidisciplinary Sciences, SOKENDAI (The Graduate University for Advanced Studies))

To be fully launched in July 2017, NII's Cybersecurity Human Resources Development Program has a flavor different from general human resources development programs. It does not have a curriculum, nor does it develop personnel in classrooms and with lectures. Instead, through a cooperative framework with NII, network administrators of universities use actual data and work situations to accumulate skills related to developing and implementing cybersecurity measures. Trained personnel are then assigned to Japan's national universities around the country. Professor Takakura discusses the purpose and features of this program.

Developing personnel who can comprehensively make decisions and take action

The genesis of the Cybersecurity Human Resources Development Program can be traced back to the data leak incident at the Japan Pension Service in June 2015 due to malware infection. At the time, NII had begun discussions on further strengthening the security of SINET. The data leak at the Japan Pension Service drew the concern of SINET-affiliated universities.

As a result of this incident, the Ministry of Education, Culture, Sports, Science and Technology (MEXT) requested the cooperation of all national universities to confirm the existence of malware infection in their systems. Several national universities shared suspicion that they were infected by the same malware that had attacked the Japan Pension Service.

However, the biggest problem in this episode was not the infection itself. What the universities suspected of being infected had in common were that they did not report the infection to university management.

Professor Takakura, Director of the NII Cybersecurity Research and Development Center, observes: "No matter the university, it will be infected by several malware a month. But in many cases, only the first malware is eliminated, and not the malware that it brings in afterwards. There have been many instances of universities not completely removing the malware, and not reporting the infections. They report an incident only after it has become serious."

The unavoidable conclusion is that network administrators and system administrator lack fundamental awareness of cybersecurity.

Another challenge is that few network and system administrators have the skills needed to appropriately communicate the dangers of malware infection and data leak to top university administrators.

Professor Takakura says: "Onsite engineers become absorbed by the features of malware and attacks themselves, especially if it is a new type of malware. However, what senior university administrators want to know is how the current state of a malware infection or attack will affect the management and operation of the university. Network and system administrators need the ability to report this accurately."

The priority and importance of measures to be taken differ depending on the cybersecurity incident, for example, the infection of a student's device by malware or an attack on a server containing important information. All universities need to create a system that can prioritize the incidents, determine what measures to take, clearly determine the extent of an attack's impact on the university, and report that to university administrators. The Cybersecurity Human Resources Development Program was created with the purpose of meeting this need, equipping personnel with understanding of cybersecurity, and placing them in universities.

Professor Takakura states: "What are needed are workers who can control traffic onsite. We want to foster 'intermediaries.'

Hiroki Takakura

These personnel not only have knowledge and work experience in network technology and security technology, but they can also comprehensively make decisions based on fragmentary information and carry out correct measures in response to changes in the situation. They are also knowledgeable about the law and can communicate with university administrators. We want to develop at least two such persons in each university."

What does NII offer?

NII is working on strengthening new security measures for SINET, which it built and operates. The Cybersecurity Human Resources Development Program is being advanced as part of this effort.

At present, NII is engaged in establishing the NII-SOC (Security Operation Center) (tentative name). This effort became full-fledged as a result of the Japan Pension Service data leak incident.

In the case of the Japan Pension Service incident, malware that caused the data leak was suspected to have also infiltrated NII for about half a year. The access logs of NII going back six months were reviewed. However, because the malware was repeatedly passed through servers with different IP addresses, and the access logs to popular sites were also included, it was necessary to analyze a vast amount of information. In NII's system environment, extracting just the log data took about a week. This episode revealed that there is a limit to access data analysis that can be performed by a single institution.

Meanwhile, as a result of the revision of the Basic Act on Cybersecurity, monitoring and auditing of Incorporated Administrative Agencies and Special Corporations in addition to central government ministries and agencies was added to the purview of the National center of Incident readiness and Strategy for Cybersecurity (NISC). Because National University Corporations were not included, legislation is being sought to enhance independent measures for protecting them.

With these conditions as the background, NII began conceiving new cybersecurity measures that cover SINET in 2015. In April 2016, the Cybersecurity Research and Development Center was inaugurated together with the launch of SINET5. The establishment of NII-SOC began in the center to realize the new concepts.

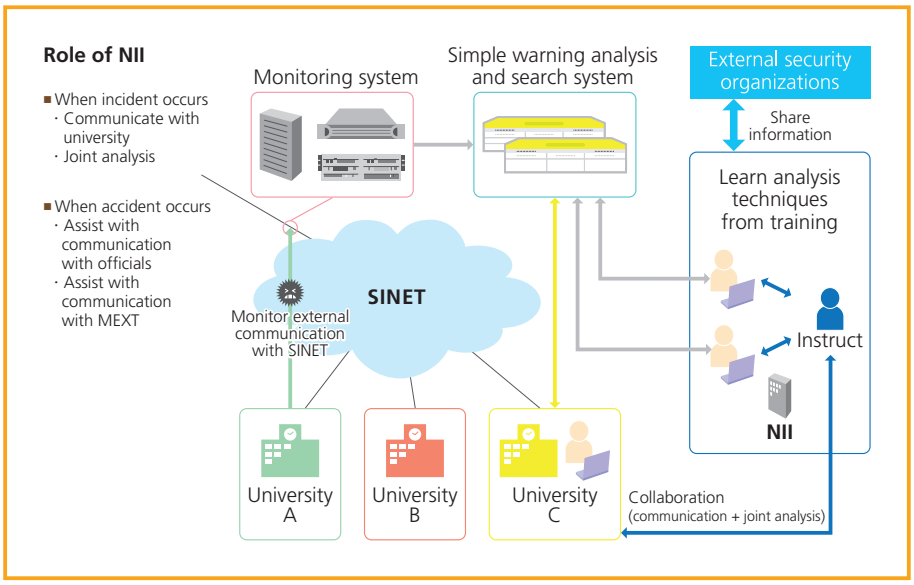

Figure **Role in NII in fostering cybersecurity human resources**

However, because the budget is limited, there are constraints to NII's efforts. NII-SOC's protection is limited to about 90 national universities. In addition, it will begin operations only during weekdays for a set number of hours. NII-SOC's responsibilities include the development of cybersecurity personnel with the cooperation of national universities without requiring them to hire new security personnel.

At NII-SOC, detection patterns are set based on the monitoring of communication outside the university firewalls. When suspicious communication is detected from the monitoring, the corresponding IP address is added to a database, and related suspicious communication data is organized and analyzed. The targeted university is then notified of the analysis results. Based on the results, the university studies, decides, and carry out countermeasures. The personnel who carry out these steps will be those trained by the Cybersecurity Human Resources Development Program.

The formal launch of the Cybersecurity Human Resources Development Program is scheduled for July 2017. Since March 2017, a trial run has begun with the participation of 15 universities, ranging from large to small. Tools developed by NII-SOC are being fine-tuned for ease-of-use and optimization. The program is being observed over three weeks to examine how smoothly the human resources development program can be implemented. From April, the program will be expanded to about 60 national universities, with all energy devoted to preparations for the program's formal launch.

Raising the overall level of cybersecurity

Related to the Cybersecurity Human Resources Development Program, Professor Takakura is attempting to start several new initiatives through NII-SOC. One of them is offering malware samples to universities.

Until now, it has been difficult for Japanese universities to procure the latest samples within the country. As a result, compared with the ability of overseas security-related organizations and security vendors to obtain malware samples quickly and research and develop countermeasures, in Japan research by universities is greatly limited. Professor Takakura says, "Even though NII-SOC has restrictions on where it can send samples, a new security event can be researched by creating a system whereby researchers can get fresh and real data. I want to accelerate cybersecurity research in Japan through this program."

Another effort is creating internships for undergraduate and graduate school students. NII can provide universities with logistics support for the development of future cybersecurity personnel by providing a variety of information.

The practical training-based Cybersecurity Human Resources Development Program is drawing attention not only for developing human resources, but also for its promise to raise the level of cybersecurity in Japan.

(Interview and text: Katsuyuki Okawara
Photo: Yusuke Sato)

Information Security Measures Needed in Universities Today

Raising the level of human resources with program using practical data

Hiroyuki Minami

(Professor, Information Initiative Center/Director of Cybersecurity Center, Research Division of Cybersecurity, Hokkaido University / CIO Aide, Information ICT Promotion Office/Chief Officer of Information Security Management Section, Hokkaido University/ Visiting Professor, National Institute of Informatics)

NII's Cybersecurity Human Resources Development Program, which utilizes SINET, has been in its trial run in March 2017. The participation of 60 of Japan's 86 National University Corporations is expected for this pilot program. Representing the participating national universities, Professor Hiroyuki Minami of Hokkaido University discusses the current state and challenges of universities' information security, and the promise of the human resources development program to address them.

Challenges faced by universities

In recent years, research institutions such as universities have been besieged by cyber attacks, and reports of incidents including suspicions of information leak have increased. Hokkaido University is no exception. In late December 2015, illegal access of the university's network and leak of personal information was suspected. The results of an investigation by a third-party committee afterwards concluded that information leak could not be confirmed. However, this incident caused many to question why it occurred despite the existence of a cybersecurity department.

Serving as Director of Hokkaido University's Cybersecurity Center, Professor Hiroyuki Minami discusses the circumstances specific to universities, which are different from general companies.

"Companies have departments dedicated to information technology, and it is possible to implement a comprehensive top-down compliance policy. However, in universities with many researchers, there is the need to respect their own independence to a certain extent. Thus, it is difficult to carry out uniform management of IT."

Because Hokkaido University applied a rigid, top-down system after the aforementioned incident, the number of illegal accesses and attacks has decreased. However, the attacks have become more sophisticated, and defenses against them are engaged in a game of cat and mouse. This challenge is the same at every university and research lab.

"Universities also face other particular issues due to their nature." Professor Minami says, "First, they have many visitors, both from other parts of Japan and from abroad. An Internet environment should be provided to researchers from abroad who reside for several weeks to conduct research. But we can't confirm that their own devices are clean."

Another issue is that the level of awareness about information security and compliance varies among individual members of a university. In many cases, actual information leaks occurred due to carelessness. For example, "I stored personal information on a USB stick and lost it after I took it outside the university" and "I carelessly opened an attachment file in a suspicious email."

To increase the level of information literacy at Hokkaido University, training of faculty members on information security through e-learning is currently being carried out. Even though the attendance rate is almost 100 percent every year, security incidents still occur.

Sharing case studies across the entire network

Recently, viruses that act like malware in leaking internal information to the outside have been increasing. As a result, monitoring of data sent externally must also be carried out in addition to guarding against these attacks. Although illegal access is often

Hiroyuki Minami

B.A in Letters, M.S and Ph.D. in Engineering, Hokkaido University. Current position since October 2015 after positions in the Department of Information and Management Science, Otaru University of Commerce and the Center for Information and Multimedia Studies, Hokkaido University.

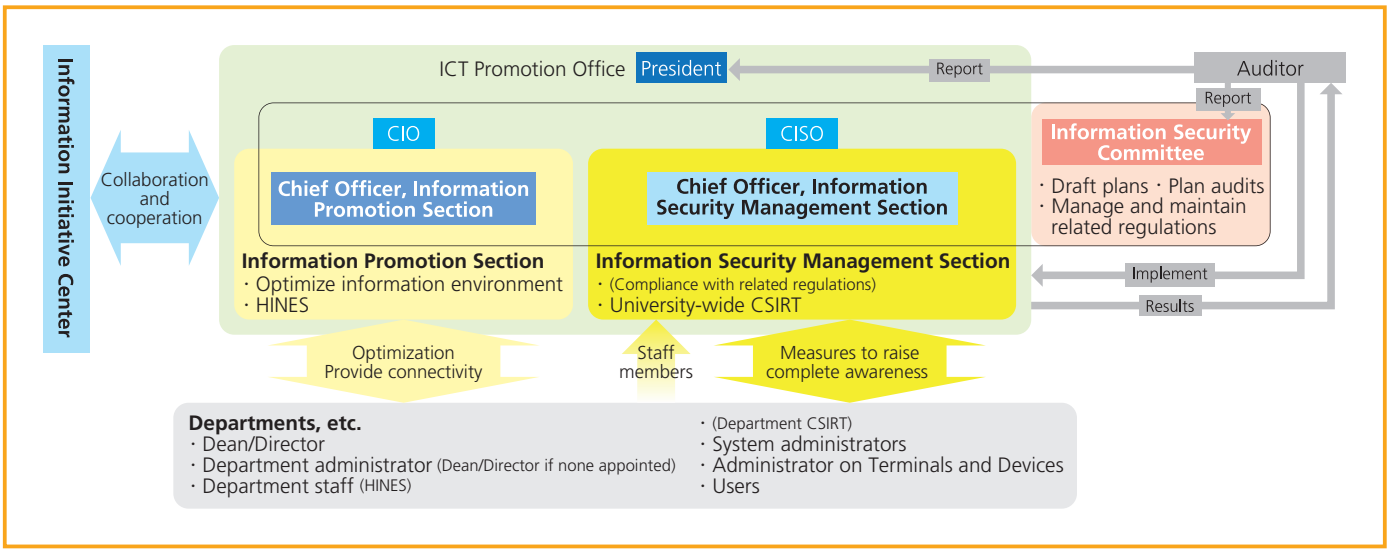

Figure **Hokkaido University's security framework (excerpt of related areas)**

detected from external indicators, we have established our own measures to discover them autonomously. Anomalies must be quickly discovered so they do not spread to other institutions.

"As the lack of security personnel in universities continues, increasing the skill level of internal personnel has become an urgent issue," says Professor Minami.

NII's Cybersecurity Human Resources Development Program, targeting the technical staff in charge of information security at Japan's national universities, is being offered precisely to address this issue. Using the tools developed by NII, this program seeks to improve the ability of security personnel to handle actual situations by using live data, including case studies of actual attacks on the SINET network. It seeks to arm them with practical skills such cybersecurity techniques and the ability to respond to accidents and incidents and explain them to university management.

Professor Minami says, "University faculty members usually only have the chance to access their own sites. But if we can utilize the data of the entire network, practical cases of incidents like information leaks can be shared. Faculty members will realize a sense of urgency and seek to improve their security skills."

Cultivating university technical experts with proper knowledge is critical

To improve information security measures, universities can use private-sector training programs or outsource to security vendors. What advantages are there, then, to nurturing personnel internally with NII's human resources development program?

"Private-sector programs are mainly geared toward companies, and the fact that they do not take university-specific background information into account is an issue," says Professor Minami. "Of course, they provide generic knowledge. But some parts do not necessarily conform to the actual workings of universities."

For example, Hokkaido University has campuses that are geographically distant from one another. It has a set of special situations, such as having a network with the Faculty of Fisheries Sciences' training ship. The university also handles data that are generally not accepted by companies, such as unencrypted data sent by specialist institutions abroad. Highly confidential data unique to research institutions flow through the university, and image and video data have also been growing in recent years. In short, for universities the quality and quantity of data clearly differ from those of general companies.

Professor Minami says, "Even if private specialists were to be sent to universities, by the time they realize a university's special circumstances, they would return to their companies. Also, in many cases daily network operations and security are integrated in a university. Even if a certain measure might be significant in terms of security, it couldn't be applied because it might conflict with daily operations. Therefore it is necessary to brush up the technical skills of internal personnel who understand these situations with an academic program that focuses on information security in universities. Ultimately, such a program is also beneficial in terms of costs."

Toward developing "intermediary personnel" with total knowledge and technical skills

The final bastions of security are individual websites connected to network terminals. Onsite administrators who operate and protect these websites will become conscientious of the security of the entire network by learning how to use information on the actual network. They will also come to understand the state of information communications in similar-sized universities, forming a network of onsite fellow onsite administrators, and gain the ability to exchange information. New local communities can develop as a result. These communities will play an extremely useful role in strengthening security.

Professor Minami says, "In an era in which the overall level of information security personnel must be raised, I'm very thankful of the opportunities created by NII to improve their skills. What's more, what is needed right now are personnel who not only have specialized knowledge, but can handle the whole range of security issues, acting as intermediaries between onsite administrators and university managers or external parties. I have high hopes that with its practical nature, NII's Cybersecurity Human Resources Development Program will foster such personnel."

(Interview and text: Yuko Sakurai
Photo: Yusuke Sato)

News 1 Presentation of research achievements from graduate students

On January 4, NII hosted a presentation of research results by students belonging to SOKENDAI (the Graduate University for Advanced Studies) and cooperating graduate schools. Twenty-five students each gave five-minute presentations on achievements from their diverse daily research activities. Their findings were passionately received by attending students and faculty members.

After the presentations, eight NII faculty members announced the results of judging and awarded prizes to the two presenters below for their research achievements.

- **Fumiki Sekiya**
  「Discrete curve fitting in the presence of noise」
- **Ning Zheng**
  「Numerical Solution of Nonnegative Constrained Least Squares Problem and Its Applications」

At the award ceremony after the beginning-of-the-year speech on January 13 by NII Director General Masaru Kitsuregawa, the recipients received from him a memorial plaque and certificate.

News 2 "Cloud Utilization Seminars" held

The 7th and 8th "Cloud Utilization Seminars" were held on December 21, 2016 (Wednesday) and January 17, 2017 (Tuesday), respectively. The purpose of the seminars is to provide faculty members and researchers from universities and research institutions with the experience of how to use the cloud in research and educational activities.

For the 7th seminar, entitled "Legal Issues and Measures Surrounding Deployment and Use of the Cloud: Reducing Legal Risks," the law firm of Atsumi & Sakai gave a lecture on cloud deployment and utilization issues such as software licenses, personal information protection laws, trade secrets, intellectual property, and legal precautions when using foreign data centers. The lecturers also discussed legal issues and measures to reduce legal risks when moving forward with cloud deployment and use. Topics included terms of agreement and data handling when using the cloud, modification and termination of cloud services, and the occurrence of security incidents. The seminar drew the participation of many members of universities and research institutions due to its extensive content, and was highly praised.

For the 8th seminar, entitled "How to Use Amazon Web Services (AWS) for SINET Cloud Connection Services," NII's Academic Infrastructure Division gave an introduction of SINET cloud connection services. Amazon Web Services Japan representatives then gave a lecture outlining AWS and specific methods for using AWS via SINET cloud connection services. The seminar provided participants with the know-how to use the cloud by connecting it to the high-speed and secure SINET5 network.

NII plans to continue holding Cloud Utilization Seminars in FY2017.

News 3 CiNii Books gain new functions

CiNii Books is an information search service that archives academic materials (total of more than 100 million volumes of books, journals, etc.) from Japanese universities. It includes over 10 million volumes accumulated in NACSIS-CAT (union catalog database), which is operated by NII with the participation and cooperation of university libraries and research institutions throughout all of Japan. Besides bibliographic information (volume title, authors, publishing information, table of contents, introduction of contents, etc.), users can also search archival information, such as in which library a material is located.

While NACSIS-CAT covers almost all library collections of paper books nationwide, there is growing demand for functions to search and browse digital materials and digital archives (digitized library materials released on networks) using CiNii Books.

Thus, to enhance the usefulness of CiNii Books, functions linking the service to the Comprehensive Database of Archaeological Site Reports in Japan were added in March 2016, and to the U.S. HathiTrust Digital Library and the National Diet Library Digital Collections in November of the same year. With these new functions, links to digitized archives of books and magazines are displayed on CiNii Books' search screen. These digital archives include survey reports of exhumed cultural assets (Comprehensive Database of Archaeological Site Reports in Japan), book collections of U.S. universities digitized by the Google Books Library Project and other efforts (HathiTrust Digital Library), and ancient books and documents and pre- and post-World War II books and magazines (National Diet Library Digital Collections). Their text can be accessed with just a single click.

In the five years since CiNii Books began in November 2011, the service has been upgraded numerous times. Added features include new search items, provision of APIs, updated user interfaces, and support for mobile devices. NII will continue to enhance and expand CiNii Books' functions and data partnerships to further improve the service's convenience in searching and browsing academic materials, enabling users to continue to rely on it as their information search service of choice.

—— What do you do in an "administrative" role? (Ikezawa)

Sakai Usually, an administrative job in a research lab means supporting researchers. But as an Inter-University Research Institute, NII has the role of advancing projects. Besides networks, the cloud, and security, it also offers a variety of academic content services like CiNii (NII journal articles database service) and KAKEN (database of Grants-in-Aid for Scientific Research). We in the Cyber Science Infrastructure Development Department are responsible for maintaining these services. The department is composed of two divisions: the Academic Infrastructure Division and the Scholarly and Academic Information Division. In both divisions we maintain hardware and software and procure operational budget to provide these services. A wide range of tasks are split among 27 full-time employees and a similar number of support staff. As the head of administration my job is to see that our tasks as a whole are moving forward without delay.

—— I used CiNii to search for journal articles when I was a college student!

Kamei Is that right? We're responsible for maintaining and updating the systems involved in the services provided NII. The Kumamoto earthquakes last year collapsed a bridge spanning highways, and communication cables between Kumamoto and Oita were cut. However, because an alternate route was secured automatically, there was no interruption in communication.

Sakai Cyber attacks against networks have become more intense recently. How to respond is a major challenge for NII as a whole. Actual security-related work is carried out by a specialist department, so our job is to support them.

—— What's attractive about your job ?

Sakai Actually, there are very few staff members who have worked in NII administration their entire career. Before arriving at NII I worked at libraries. Many other staff members work at NII through personnel exchanges with university libraries and information centers. We gain experience from a variety of workplaces, and feel a sense of excitement in trying new things for our job of supporting NII researchers.

Kamei Our mission as administrators is to support researchers so what they wish to do can be realized. As an Inter-University Research Institute, NII also has the grand mission of "supporting the enrichment and improvement of Japanese universities' educational environment nationwide." I myself feel the reward of being part of this pursuit.

—— I'm sure work at NII keeps you busy. What do you do to relax?

Sakai If anything happens at NII, we're contacted right away. But my hobby is playing the drums on my days off. It began as a way to stay mentally sharp, but I'd like to play sessions with friends in the future.

Kamei I'm usually busy with work, but I like to collect old things. So on my days off, I've browsed used book stores in the Jimbocho district, which is near NII. Until now, I've worked in the countryside, so I've been away from home for many years. Now that I'm transferred to Tokyo, I try to spend as much time with my family as possible.

(Written by: Akiko Ikeda Photography by: Yusuke Sato)

NII People Vol.4

What is the mission of the NII administrative department in providing services to researchers?

Kiyohiko Sakai

(Deputy Director of Cyber Science Infrastructure Development Department)

Studied history in college. After graduation, worked in libraries. Was employed at NII's predecessor organization, the National Center for Science Information Systems, and as a result, joined NII. Afterwards, performed administrative roles at the libraries of Saitama University, the University of Tokyo, Yamaguchi University, and Nagoya University. Intimately familiar with the specifics of university libraries. Assumed current position in 2015.

Koji Kamei

(Director of Academic Infrastructure Division, Cyber Science Infrastructure Development Department)

Studied social sciences in college. After being employed by Chiba University, transferred to the Ministry of Education, Culture, Sports, Science and Technology (MEXT). Assumed current position in 2016 after working in various MEXT agencies. Has experience of working together with Deputy Director Sakai when both members were at Yamaguchi University.

From left: Koji Kamei, Ayaka Ikezawa, and Kiyohiko Sakai. Thank you for giving us access to the workplace of all those who support NII's services!

Face-to-face with "NII People"

Interviewing people who handle the administration of NII?! I wondered what in the world they do. It turned out that they vigorously support the services provided by NII. I was surprised by the wealth of local experiences Messrs. Sakai and Kamei had. That enabled them to have an abundance of knowledge and intuition needed to provide NII services.

Ayaka Ikezawa

Celebrity/Engineer. Known as "The Ruby Goddess", she is especially active in IT fields. The author of *Programming Wo Hajime Yo Idea Wo Jitsugen Saseru Saiko No Tool* (Let's Start Programming: The Best Way to Realize your Ideas) (Daiwashobo). Won the Special Jury Award at the 6th Toho Cinderella Audition.

Essay

Utilization and Distribution of Data

Ryoji Mori
Attorney at law/
Visiting Professor,
National Institute of Informatics

Until now, the utilization and distribution of data—most notably, personal data—has been described as essentially dual in nature. For example, as a basic theme of the Cabinet-approved IT strategy "Declaration to be the World's Most Advanced IT Nation," the government advocates "smooth distribution and utilization of data."

But, so far, no one has come up with a viable way of monetizing personal data through its distribution. Among big league GAFA global platforms—Google, Apple, Facebook, and Amazon—Google and Facebook derive the core of their earnings from advertising, and exploit the personal data they have collected not by selling it but rather by keeping the data and utilizing it in-house. As the Forth Industrial Revolution emerges, there is a lesson to be learned here if Japan seeks to develop its own GAFA type operation: that the retention of data is not necessarily a bad thing. Nor should we forget that the distribution of personal data constitutes a potential threat to privacy and involves security costs. An overemphasis on distribution and openness is thus clearly not the optimum approach. Perhaps a combined open and closed system design might offer a better approach that provides selective access to medical and financial concerns while strictly protecting individuals and primary acquisition companies in all other areas.

In fact, a remarkably similar concept has been proposed in a different context. In steering the direction of copyright law revision in Japan, the Council for Cultural Affairs recently released a "Draft report on the future direction of rights restrictions that accurately meet the needs of the new era." Addressing a long-standing debate over whether to adopt U.S.-style general fair-use provisions, this report will have enormous significance in determining the success or failure of the *Forth Industrial Revolution.*

Rather than embrace American-style general fair-use doctrine, the report advocates a dual approach imposing broad restraints on rights having little or no adverse impact on copyright holders while imposing much narrower restraints on rights in areas requiring high use for public purposes. With this open and closed approach, only after confirming necessity of use, would those areas be opened up.

Yet this leaves us with a rather unpleasant feeling. I suppose the worst that could happen would be that personal data would be increasingly distributed and utilized, and copyrighted works would be distributed and utilized without serious reflection or without seriously considering how the copyright holder might be disadvantaged.

Even if the *Fourth Industrial Revolution* is accompanied by a painful learning process, it should nevertheless represent a step forward in terms of individual human rights. The cost of the revolution will be borne by businesses that are unable to adapt and remain mired in traditional business models.

Awards

- Dr. Junichi Yamagishi, Associate Professor, Digital Content and Media Sciences Research Division, National Institute of Informatics, recipient of the 13th (FY2016) JSPS PRIZE.
- Dr. Daichi Kitamura, SOKENDAI, Department of Informatics, Ono Laboratory, recipient of the 7th (FY2017) JSPS IKUSHI PRIZE.
- Dr. Shinji Takaki, Yamagishi Laboratory, Digital Content and Media Sciences Research Division, National Institute of Informatics, recipient of the Information Processing Society of Japan's FY2016 IPSJ Yamashita SIG Research Award.

Future Schedule

June 7-9 | NII OPEN FORUM 2017.

June 9-10 | NII OPEN HOUSE 2017. Research presentations are open to the public in the Hitotsubashi Hall and other venues.

For details and to preregister to participate in events, please refer to the the following NII website:
http://www.nii.ac.jp/openhouse/

Notes on cover illustration The illustration represents cyber security where an intruder kept out of the castle by vigilant gatekeepers. The cartoonish intruder and gatekeepers represent the abstract notion of cyber space.

Weaving Information into Knowledge
NII

National Institute of Informatics News [NII Today]
No. 61 March 2017
[This English language edition NII Today corresponds to No. 75 of the Japanese edition.]
Published by National Institute of Informatics, Research Organization of Information and Systems
Address | National Center of Sciences 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430
Publisher | Masaru Kitsuregawa **Editorial Supervisor** | Ichiro Satoh
Cover illustration | Toshiya Shirotani **Copy Editor** | Madoka Tainaka
Production | MATZDA OFFICE CO., LTD., Sci-Tech Communications Inc.
Contact | Publicity Team, Planning Division, General Affairs Department
TEL | +81-3-4212-2164 **FAX** | +81-3-4212-2150 **E-mail** | kouhou@nii.ac.jp

Bit (NII Character)

http://www.nii.ac.jp/en/about/publications/today/