ISSUES 2

Cybersecurity for the IoT Era

Joint Research by Keio University and Hitachi Targeting both People and Technology

Hideki Sunahara, Ph.D.
Professor, Keio University Graduate School of Media Design

×

Hiroshi Saito
President of Security Businesses Division, Services & Platforms Business Unit, Hitachi, Ltd.

Cybersecurity is growing in importance along with the progress of digitalization. It is against this background that Keio University and Hitachi have embarked on joint research into cybersecurity as part of work towards the creation of a super smart society in which systems of many different types are linked together. The research includes the training of personnel as well as the development of technology for information-sharing platforms. In this article, Professor Hideki Sunahara of Keio University, who is a prime mover of this joint research, and Hiroshi Saito, who is involved in the management of Hitachi's security business, discuss subjects that include the issues surrounding cybersecurity in the era of the IoT and collaborative initiatives by industry and academia.

Expansion of Cyberspace and Growing Diversity of Threats

Saito: As the era of the Internet of Things (IoT) brings greater openness and connectivity, cybersecurity is becoming increasingly important. Professor Sunahara, you have participated in establishing the Internet in Japan and in the associated research since the very beginning through your involvement in the Japan University Network (JUNET) and Widely Integrated & Distributed Environment (WIDE) project. What are your views on the progress of cybersecurity?

Sunahara: The history of the Internet in Japan can be said to date back three decades from this year (2018). In July 1988, the University of Tokyo, Keio University, and Tokyo Institute of Technology linked together in what we would now call an internet. Subsequently, just before the connection to the USA was added in January 1989, a computer virus called the Morris worm was unleashed. Although, fortunately, it did not result in any damage in Japan, it helped us realize that maintaining security was an issue to be taken seriously. I remember the discussion we had at the time about the extent and value of disclosure, and the need to investigate things like the associated effects on the community.

Saito: While the Internet can now be thought of as part of the fabric of society, was the presumption present from the outset that some people have malicious intentions?

Sunahara: No, that wasn't part of our thinking to begin with. However, having started with pranks, there have been many cases in which things have escalated from there. The hack on the NEM virtual currency that featured in the news recently is one such example, and malicious intentions tend to enter the picture wherever there is value at stake. This is why my colleagues and I have been talking since the early days about the likely need for organizations such as the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) that deal with security incidents.

Hideki Sunahara, Ph.D.

Graduated from the doctoral program at the Faculty of Science and Technology, Keio University, in 1988. After working first as an assistant professor at the University of Electro-Communications, then as an associate professor at the Information Technology Center of the Nara Institute of Science and Technology in 1994, he was appointed a professor in 2001. He was appointed professor at the Graduate School of Information Science in 2005 and to his current position in April 2008. His activities have included involvement in establishing and conducting research into the Internet in Japan through his work with Jun Murai (a professor at the Faculty of Environment and Information Studies, Keio University) and his team on JUNET (from 1984) and on the WIDE project (from 1988). In 2005, he embarked on the Live E!Project for sharing environmental information over the Internet together with Professor Hiroshi Esaki of the University of Tokyo.

He is currently involved in the Information Bank project that is working on a framework for providing safe and secure access to personal information.

Saito: Hitachi, too, started out with faith in the goodness of human nature. Although we first established a capacity for dealing with external attacks about 15 years ago, this was based on the concept that, so long as we effectively blocked intrusions from outside, there would be no problem with allowing free access internally. Since then we have tried to keep things as open as possible within the company so as to free up the flow of information.

Unfortunately, the ransomware-based cyber-attack that caused damage around the world in 2017 shattered this illusion. The source of the infection was a device at an overseas group company, and unlike old-style worms that are slow to propagate and against which we can take action once the threat is identified, this time around the worm rapidly spread through networks throughout the world. While the need to protect against external threats goes without saying, this was a painful reminder that internal countermeasures are also important. Along with system vulnerabilities, we now live in a time when we need to take seriously threats that are potentially present within the company.

Collaboration between Industry, Academia, and Government Key to Building Security Expertise

Sunahara: I always emphasize that it is people who are the greatest vulnerability. Regardless of their age, universities contain a mix of grown-ups and those whose attitudes are less mature. Having received an education is no basis for complacency, as exemplified by those students with few qualms about illegally uploading copyrighted material. In cases like that, my duty of care includes making them properly aware of the illegality of their activities.

In technical terms, the practice of using firewalls and other such countermeasures has been in place for about 20 years now. At my own university, there have been considerable changes made with the firewall split into parts that have the same as the normal security level, parts that have been slightly secured, and parts that have been highly secured.

Saito: Keio University and Hitachi have been working on joint research into security since 2016 and I imagine that the differences between

Hiroshi Saito

Joined Hitachi, Ltd. in 1985 where he spent many years working on the development of public-sector systems. After being appointed information supervisor at Hitachi China and Chairman of Hitachi Beijing Tech Information Systems Co., Ltd. in 2013, and deputy manager of the public-sector systems business in 2015, he was appointed to his current position in 2016.

He is currently engaged in work on Hitachi's security strategy in his role as President of Security Businesses Division, Service Platform Business Division Group.

a university and a company are considerable (see Figure 1). One of these is the effort made to ensure that threats (such as malware) from inside the university do not have an impact outside the university (so that the university does not become a perpetrator).

Companies, on the other hand, focus on keeping external threats out (to avoid becoming a victim). Another difference is that, whereas staff at a company remain at the organization for longer than students at a university, there is a rapid turnover of people at universities, including the students. How to train young staff in the future is currently a cause for concern at those departments within Hitachi that deal with security. What is the state of security education at universities?

Sunahara: The training of security staff is certainly an issue of concern (see Figure 2). I have been involved in information security education for about the last 10 years and the students who have studied the subject are not just out there working in companies; a cycle has also begun to establish itself whereby some of them are returning to university to upgrade their skills. Examples of this can be found among staff from organizations like JPCERT/CC.

Figure 1 | **Framework for Joint Research by Keio University and Hitachi**

The two organizations are working together on the development of technologies such as those for keeping people's personal information safe and for managing security in the face of cyber-attacks that are growing in scale and sophistication.

Hitachi, Ltd.	Quality, technical capabilities, real-world experience
Keio University	Leader in Internet research, research and development (including the IoT), experience with research that includes societal mechanisms as well as technology

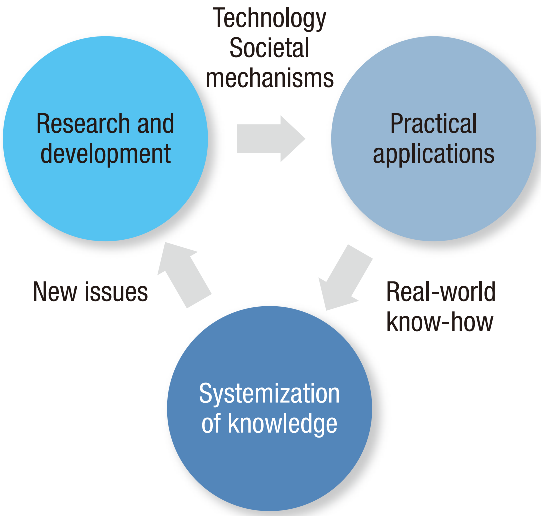
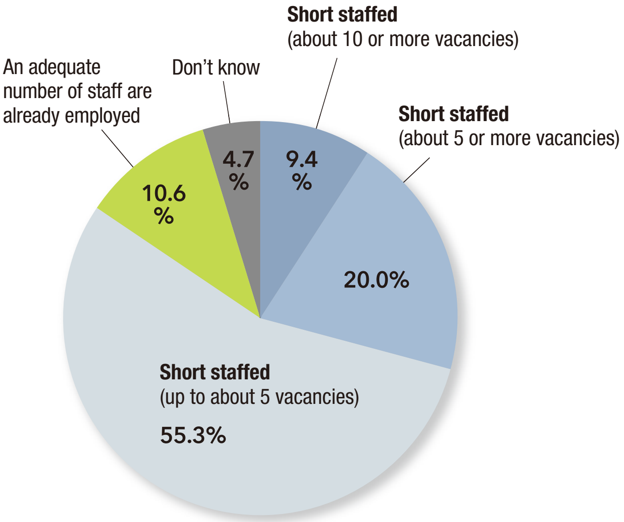


Figure 2 | **Shortage of Cybersecurity Expertise at Information Systems Departments**

Information systems departments at approximately 85% of the companies surveyed reported a shortage of staff with cybersecurity expertise.



Source: FY2016 Survey of Corporate Cybersecurity Measures (Summary), National Center of Incident Readiness and Strategy for Cybersecurity

This human resource development process goes beyond just turning out qualified staff, with a certain type of quality assurance also being needed. We call it branding, the recognition of students as security experts being a form of brand, and I believe it is vital not only to demonstrate to the wider world that these people have upgraded their skills, but also to make this apparent within the companies involved.

Saito: While it is rare in Japan for someone who has taken a job at a company to go back to university study, I understand that in the USA there is a steady flow of people between universities and both the private sector and government. The absolute number of people involved may be different, but I think that maintaining the cycle you talked about into the future is extremely important.

Sunahara: Yes. With people, quality matters more than quantity. Whether or not they ultimately become a chief information officer or chief information security officer, because universities and companies on their own are not able to foster personnel who have been through this process, I want us to coordinate effectively, including the government.

Saito: If such a cycle is to be maintained, it is essential that companies themselves establish career-paths for these people.

Sunahara: That is another area I would like to see considered in our joint research with Hitachi. If universities provide security training in which there is an assurance of quality, and companies go on to hire such people, it will likely result in a lifting of student motivation. This is because it will mean that companies value what the students are learning at university.

Saito: That is one of the aims of the joint research. The series of interviews that form part of the conventional recruitment process are not well suited to identifying students capable of taking up high-level specialist roles such as in information security. Accordingly, along with reviewing the students' character and skills, we are very grateful that we are able to utilize references from teaching staff in the selection process, as with this program.

Detailed Exercises that Foster Practical Skills

Saito: I understand you are putting a lot of effort into information security education at Keio University. While security does not form part of university entrance exams, what measures are you taking to lift undergraduates' knowledge of security to the level of master's programs?

Sunahara: The Faculty of Policy Management and Faculty of Environment and Information Studies at our Shonan Fujisawa Campus (SFC) have an exam in "information" available as an elective option. There are also some other private universities that include "information" among the subjects for their entrance exams, and we are beginning to see students arriving with a certain level of knowledge in the subject.

One example from my university is a course in basic security knowledge offered to third-year students from the Faculty of Science and Technology and SFC faculties that also includes practical lessons. These equip the students with practical skills through exercises that include participation in on-campus penetration testing, virus analysis, and a security software vendor card game. The course also incorporates facets that form part of ethics education, with the students having to sign a mock confidentiality agreement when exercises are conducted at partner companies. The joint research with Hitachi has taught me much about things like what companies need and how to boost performance, and I have taken away many pointers that help us train the sort of students that companies are looking for.

Saito: I expect that we would see greater progress at university if students were able to get a basic grounding in information processing at the high school level rather than only beginning their study of information security at university. In that regard, how do you feel about the policies of the Ministry of Education, Culture, Sports, Science and Technology (MEXT)?

Sunahara: MEXT has a good understanding of the importance of information security education and is undertaking a variety of measures. Along with the SecCap program with which I am currently involved, examples of this include supporting information security education for people in the workforce. There are now more than 20 security teams in the group of universities that make up SecCap, with the ultimate intention being to involve around 40 universities. As we have trained around 100 people a year in each of the last four years, this means around 400 to 500 people have entered the workforce. This should create a virtuous circle as qualified students go on to become the teachers of the future.

Saito: Companies like us are working with the Ministry of Economy, Trade and Industry (METI) on strengthening cybersecurity to protect critical infrastructure in the lead up to 2020, and this represents a successful handing over from MEXT to METI.

Acceleration in Establishment of Security Infrastructure Based on Information Sharing and International Cooperation

Saito: Meanwhile, when thinking in terms of supply chains and trading partners, cooperation with other organizations and a global outlook are essential. While it is necessary to maintain an extensive flow of global information that includes security intelligence, people tend to assume the profit motive is at work when it is companies that are taking the lead, whereas an academic approach is expected when it comes to network-building. What are you doing in relation to these issues?

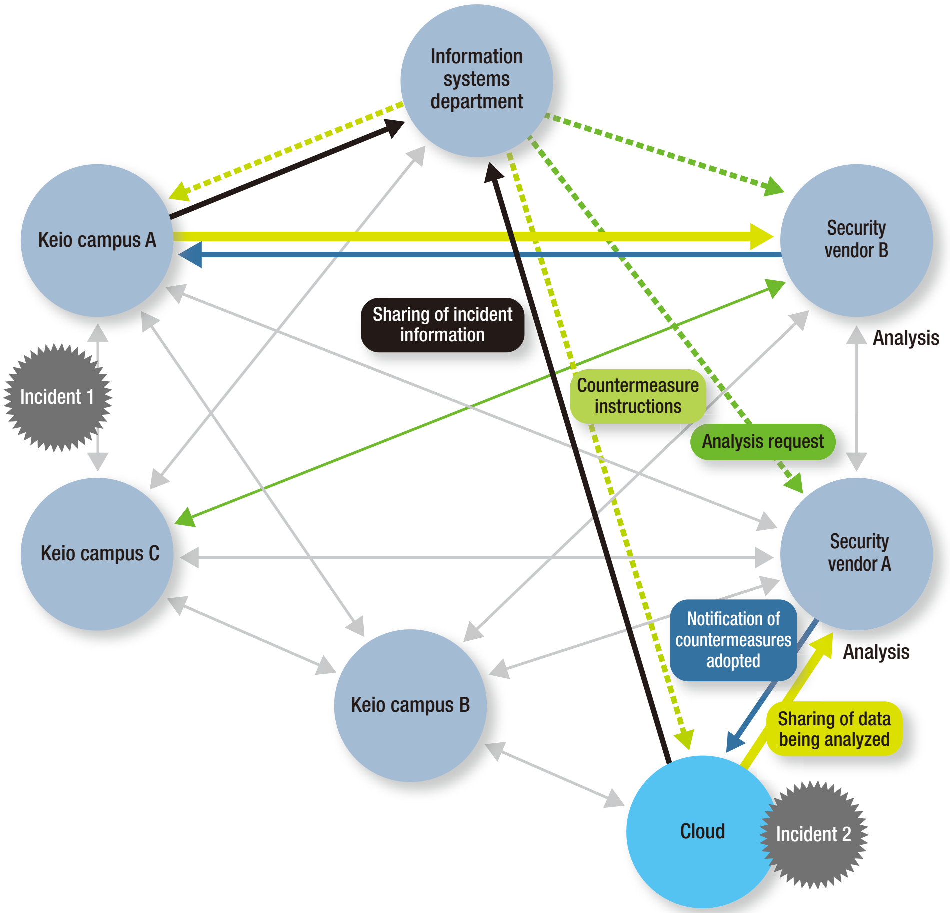
Sunahara: Talking about information sharing to begin with, the borderless nature of cyberspace means that those engaged in defense need to work together in ways that transcend the barriers between them. Unfortunately, the sharing of security information is made difficult by the risks that come with it, information leaks among them. Accordingly, Keio University and Hitachi are developing the core technologies for sharing information about security incidents, something we call “distributed security operation” (see Figure 3). The results of this joint research are starting to appear, including trials that demonstrate the automation of incident response and the completion of requested analyses in less than one second.

Saito: It might well have been possible to gain advance warning of the activities of that ransomware that attacked Hitachi.

Sunahara: The warning signs should have been visible. With the idea of expanding the scope of the joint research by Hitachi and Keio University, Chubu Electric Power Co., Inc. joined in the work from 2017. Our aim is to implement security operations for protecting critical infrastructure and other sites from cyber-attack, using intrusion detection systems (IDSs) and other forms of information technology (IT).

Figure 3| **Distributed Security Operation**

An autonomous-distributed structure in which organizations deal with incidents themselves while also working together when necessary.


Information systems department
Keio campus A
Security vendor B
Sharing of incident information
Analysis
Incident 1
Countermeasure instructions
Analysis request
Keio campus C
Security vendor A
Notification of countermeasures adopted
Analysis
Keio campus B
Sharing of data being analyzed
Cloud
Incident 2

Regarding the second matter of international cooperation, in 2016 we established the InterNational Cyber Security Center of Excellence (INCS-CoE), bringing together universities from the USA, UK, and Japan at the invitation of Keio University. The center serves as a forum for the sharing of information and research, including the holding of international symposiums. Discussions about cybersecurity are also taking place within academia in the grouping of China, South Korea, and Japan, where the question of what role universities should play is, I believe, serving as the point of connection between universities, and also between companies.

Saito: The joint research is expanding what Hitachi is capable of and providing us with a broader view. To go back to our initial discussion, this more open and interconnected world we live in is also one in which more interconnection is needed between the information held by those engaged in providing protection. In this respect, I hope to see this collaboration between industry and academia deepen further, beyond just people and technology.

Sunahara: I also hope to see the joint research deliver on its promise and serve as a driving force in society.

Saito: I look forward to working together in the future. Thank you for taking the time to share your valuable knowledge with us today.