



The ICSCoE Report is a public relations newsletter on ICSCoE's activities

Program alumni association “Kanae-kai” holds the first general assembly

The “Kanae-kai”, launched in July 2018, is an alumni community of people who have completed the Core Human Resource Development Program. The first cohort of 76 graduates is actively involved in forming personal networks across different years, collaborating in cyber security measures across various industries, updating their knowledge and contributing back to society. The first general assembly was held on November 9, 2018.

From the General Assembly

Keynote Speech

Deputy Director-General for Cybersecurity and Information Technology, METI

Dr. Ikuo Misumi

In the keynote speech entitled “Cyber Security Policy of the Ministry of Economy, Trade and Industry - Collaboration and Leadership -”, Dr Misumi pointed out that new technologies such as artificial intelligence (AI) and IoT etc. may enrich the lives of people in a society that successfully achieves Society 5.0, but they will also increase the risk of economic and social losses. Therefore, personnel with new perspectives that are different from conventional ones will be needed. All alumni of the program will be core personnel who are expected to support Japan's critical infrastructure and work on common issues by crossing industry boundaries.

A photo of the battleship “Mikasa” which played an active part in the Russo-Japanese War was projected, and the graduates responsible for the new era were compared to the protagonist Saneyuki Akiyama in the novel “Clouds above the Hill”.



Status update from alumni

Vice-Chairperson of Kanae-kai, Daiwa House Industry Co., Ltd.

Mr. Takashi Okabe

Mr. Okabe, kept us entertained talking about his activities as a captain and a staff officer steering his company's ship through the vast ocean, or cyber security. He reported that “initiatives are being taken and implemented to improve the security of the entire Daiwa House Group”. With his inherently outstanding sense of balance, he is taking on 2 difficult challenges - managing the security of the group and improving services for users of the information system.

Next, 5 alumni presented a status report and talked about their activities at each company, referring to the wide-ranging knowledge that they obtained from the Core Human Resource Development Program.

All attendees at the venue gave a big round of applause to their associates facing the same security issues in different industries.





Alumni interview with Mr. Naoaki Kimura from the chemical industry

Before the Interview

I, interviewer, was told that he was a very relaxed person despite holding such an important position so I looked forward to the interview as an opportunity for me to get to know his personality and to find out what he has been doing since returning to work.



Mr. Naoaki Kimura (46)

- Manager, IT Strategy & Planning Tosoh Corporation
- Current duties: Study of in-house security measures in the medium-term plan

Q1 | Did your company assign any tasks to you when you participated in the program?

I didn't receive any detailed instructions from the company in particular, but due to my age and job title, I attended the program thinking that I would be expected to play an important role in leading my company's security measures after returning to work.

Q2 | What are the good points after actually attending the program?

All the trainings were very refreshing. Instead of just classroom lectures, the programs which consisted mainly of exercises were especially excellent. In addition, the trainees came from a variety of industries, so it was very useful to hear their ideas and thoughts in discussions during the lectures and at other times. As I communicated with a variety of people from different industries and with different ages and career backgrounds, I also managed to resolve issues in detail.

Q3 | What duties will you have when you return to work? Have the contents of the trainings been helpful?

I'm considering our company's own security measures. Since I had a long career in the information system department, I used to consider things from the perspective of that department only, but after attending the program, I can now take into consideration the needs of the control system department as well. As my own superiors and the senior officers of the control system department interact with one another, and contact with the personnel of the control system department has increased, I am now able to motivate them and provide them with specific advice on how to do things while also taking their aims into consideration. Acting as an intermediary, I take the lead in coordinating the work between the two departments.

After returning to work, I became more aware of security, including areas which are not directly related to my duties, such as news stories, trends in other industries and so on. I think this is thanks to my participation in the program while also maintaining my own unique awareness of the problems. I kept asking myself "what my role is" during the one-year course, and I am sure that trainees who are continually exploring would have the same attitude.

After the Interview

I felt the need to attend the program with a sense of awareness of the issues and to consider the "expectations" on my own, and to make sure that the results are fully utilized in his work. Playing an active role as a coordinator, Mr. Kimura commented that "communication between the information system department and the control system department is important when implementing security measures across the company". I look forward to observing what kind of achievements will result from what he learned at the Core Human Resource Development Program.

New Initiatives of ICSCoE

◆ New seminar for managers of administration departments

The key word "strategic management layer", for personnel who deal with risks in management and business strategy, was incorporated into the cyber security strategy adopted by the Cabinet in July 2018. To meet the development needs of such new cyber security personnel, a "strategic management seminar" was set up for managers involved in general risk management, strategic planning, public relations and other management departments. A total of 7 weekly sessions were held in the evening from November to December 2018.

The seminar consisted of two parts, lectures by experts and case studies conducted in groups. During the discussion, participants in different positions and from different industries actively discussed the functions required for security measures in organizations.

Comments of participants

- "I got some hints on what should be considered when it comes to 'security'".
- "I got some useful insights on how to explain security to top management."
- "I had no prior knowledge but I was able to get a better understanding of security through the seminar."
- "I was able to share issues and learn how other companies think through discussions with people inside and outside the industry."
- "I managed to network with other people by exchanging opinions a total of 7 times within the same group."

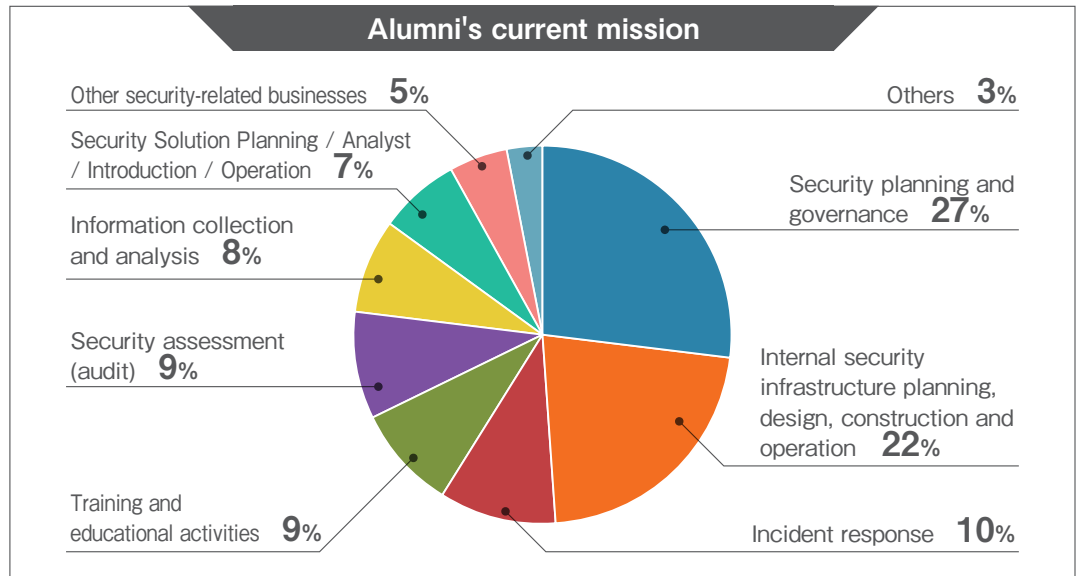


Scene of group work by participants

FACT & DATA

(From the questionnaire results etc.)

Almost all the alumni are active in cyber security work such as security planning, operation, training, incident response and so on.



After completing the program (Alumni interview)

Mr. Yasuhito Suzuki Chubu Electric Power Co., Inc.

Although I was in charge of IT before attending the program, my position was simply to implement security measures according to the predetermined rules. Due to a lack of knowledge, I used to overreact to cyberattacks, treating them as simply “dangerous” and “scary”.

By participating in the program, however, I learned more about attack techniques and defense techniques and I was able to experience first-hand how dangerous attacks can be and how far attacks can be tolerated. I also still continue to maintain contact with associates across different industries who share the same concerns. This is an advantage that cannot be obtained elsewhere.

Based on my knowledge of risk sensitivity acquired in the current course, I am drawing up the rules and security measures taking into account examples of the latest incidents which have occurred. My aim is to achieve a consensus within the organization.

Mr. Takahiro Tanaka JFE Steel Corporation

With my experience in both information and control systems, I was naturally inclined to attend the Core Human Resource Development Program because of trend in control system security in recent years as well.

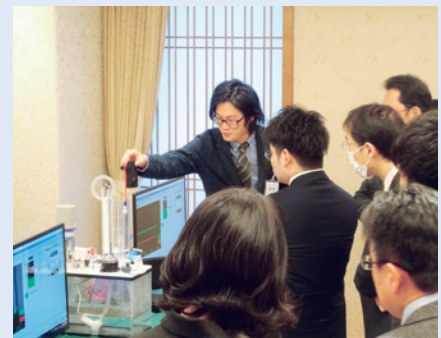
During the program, I was able to work on the actual equipment in building the system, configuring the security devices, going through the accident response training and so on, allowing me to have an invaluable experience that is unique to ICSCoE. I also obtained knowledge that is directly linked to my work such as the systematic knowledge of risk assessment, the concept of product selection and so on.

Currently, I am in charge of security operations for control systems, working on establishing rules and management systems for my company and group companies, and conducting risk assessments that will start in the next fiscal year.

◆ A new seminar to experience the human resource development program of ICSCoE

A “One day extension” seminar was held in Tokyo and Osaka, allowing people to experience, in half a day, the essence of the human resource development program run by ICSCoE.

A keynote speech was first given by GEN. Keith Alexander, a former NSA secretary. This was followed by the introduction of a program for corporate security officers, including the Chief Information Security Officer (CISO) through a practice demonstration of response to a security incident. In addition, Associate Professor Takuho Mitsunaga presented an exercise using a simulated system and a demonstration to introduce the Core Human Resource Development Program. Program alumni were also seen to be discussing current initiatives passionately using the results of the 1-year program, and the connections, skills and personal networks that they have cultivated.



Demonstration using a simulation system

Comments of participants

- “I managed to learn more about the initiatives of ICSCoE, so I would like to make use of this knowledge in future.”
- “I have never actually dealt with a major incident so far but the demonstration provided us with an accurate picture of such an incident.”
- “I could not envisage collaborating with other departments when an incident occurs. So I would like to verify the decision-making in my own company.”
- “Working in the IT sector, I did not understand much about control systems, but I managed to develop a perspective of industrial security that is different from information systems.”
- “I was able to understand the value of this program by listening to the comments of those who had completed the Core Human Resource Development Program.”



Core Human Resource Development Program

Current situation of second cohort

The 2nd Core Human Resource Development Program has completed the “Basic” phase and is progressing to the “Advanced” and “Final Project” phases.

An expansion of the ICSCoE curriculum to overseas locations and the voluntary activities actively undertaken by the trainees will be introduced as below.

Overseas Deployment Exercise

ICSCoE regularly organizes overseas visits to understand the leading initiatives of each country and to build up a personal connections with top class, local institutions.

We recruited applicants from the trainees of the 2nd Core Human Resource Development Program, and implemented it in France and UK.

1st Overseas Visit (France)

The first overseas visit to France with 18 participants was held over 2 days on September 17 and 18, 2018.

During the first day’s exercises, the trainees attended a lecture by a security expert on cutting-edge research in France that was aimed at enhancing cyber resilience. A French government official explained the security-related legal system to protect important infrastructure and a lecturer from industry discussed specific security measures and other examples.

On the second day, the trainees visited the Institute of Research and Technology (IRT) SystemX, a trilateral research institute bringing together the public, private and academic sectors in France. Involving more than 100 domestic and international companies and academic institutes, IRT System X also supports start-up enterprises to bring their research results to the market faster. The latest initiatives including automated driving and block chain research were introduced with demonstrations.

A lively exchange of views was held between the trainees and lecturers/researchers on both days.

2nd Overseas Visit (UK)

The second overseas visit was held on December 3 and 4, 2018 in UK with 33 participants. Representatives of the British government, the automobile industry, the financial industry and start-up companies gave a presentation on cyber security activities and conducted a question-and-answer session. The results of the survey show that “the majority of information leaks are caused by the supply chain”. With regard to ensuring security for the entire supply chain, an issue which is attracting much attention in Japan, it was seen that some of the trainees were also aware of the security risks in the industry.

On the following days on December 5 and 6, interested parties participated in a global information security event called “Black Hat Europe 2018”. In order to improve the details being reported to the participant’s companies, information was gathered on the latest security data, including global trends, technologies, and training methods etc. related to cyberattacks.

Comments of participants

- “I managed to make some connections that are very valuable to infrastructure operators.”
- “I was able to adopt cyber security measures from a multilateral perspective with input from national, corporate and other research institutes.”
- “As a business operator, I feel that I am still very much lacking in my knowledge of cyber security initiatives and concepts.”

▼ Exchange of opinions with researchers at IRT SystemX (France)*



▲ Networking event with security-related officials (UK)

Trainees Voluntary Activities

Participation in the test video transmission of “Sapporo Snow Festival 2019” to check the vulnerability of the equipment



Trainees working on demonstration experiments



Next-generation video transmission equipment etc. used in the demonstration test

Trainees participated in a demonstration experiment (with approximately 200 people from 51 organizations) to distribute high-resolution live videos of the Sapporo Snow Festival to Tokyo and Osaka in real time. Penetration tests were conducted on video transmission devices that are currently used in television

broadcasting and next-generation devices expected to be used in the future. By fully utilizing the knowledge and technology gained in ICSCoE up to this point, the vulnerabilities, including the risk of images being replaced arbitrarily by an intermediate attack, were assessed. Few examples of penetration testing for such video systems have been seen so far, so it could be said that this is a unique initiative from ICSCoE bringing together people from various key infrastructure companies such as broadcasting, telecommunications and other industries.

The trainees will take their gaining knowledge back to their own companies and will study measures to ensure safe and secure broadcasting, in preparation for future global attacks expected in large-scale relay events etc.