



ICSCoE REPORT

Industrial Cyber Security Center of Excellence

8.31.2026

vol.
26

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

From Protecting to Developing the People Who Protect Interop Tokyo 2026: Report from the IPA/ICSCoE Booth

Interop Tokyo 2026 was held at Makuhari Messe from June 10 to 12, 2026. At the IPA/ICSCoE booth, graduates and trainees of the Core Human Resource Development Program took the stage to share insights gained through their work with visitors.

Showcasing “Control System Incident Response Training”

One exhibit that drew particular attention was “Control System Incident Response Training,” developed as a final project by trainees from the ninth cohort. The exhibit links a simulated plant with a Human-Machine Interface (HMI), allowing visitors to see and hear a simulated cyber incident and experience it firsthand as part of a cybersecurity awareness exercise.

This exercise targets field operators in the chemical industry. The power industry has established comprehensive guidelines and conducts public-private cybersecurity exercises targeting the electricity sector. In contrast, the chemical industry has not conducted exercises for the chemical sector on a comparable scale or under a similar framework, and such efforts have not yet progressed sufficiently. The project began with challenges identified by trainees from a range of industries, bringing together their respective knowledge and concerns.

The team chose to target operators because they are responsible for monitoring the plant and spotting abnormalities as early as possible. Early intervention depends on operators speaking up when they notice something unusual. However, e-learning and scenario-based exercises alone can make it difficult to visualize what is actually happening. That is why the team focused on creating an environment where participants can see and hear what is happening and gain a more tangible understanding of incidents.



Mr. TODA Kosuke (9th cohort)

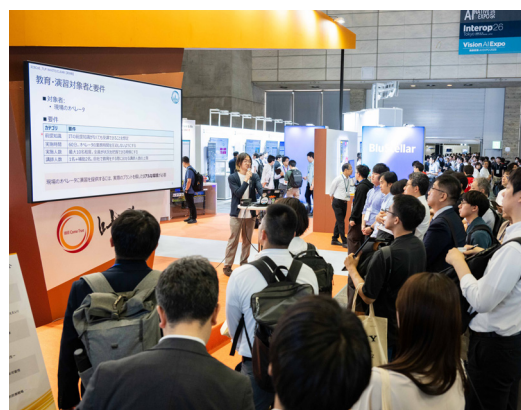


Simulated gas supply plant and HMI screen

An immersive Exercise Raises Awareness of Cyber Risks

The trainees developed a simulated gas supply plant as their final project. The plant replicates a system that supplies gas to customer facilities at constant pressure, using compressed air from an air compressor instead of gas. The HMI screen shows how the controller compares the pressure setpoint with the measured pressure and adjusts the control output to bring the pressure closer to the setpoint. The simulated plant demonstration featured threat scenarios involving anomalies on the HMI screen and in the plant, helping visitors experience the risks.

The simulated plant is compact enough to fit in a suitcase, making it highly portable. After the event, the trainees plan to bring the simulated plant to their dispatching enterprises and use it for exercises, allowing their colleagues to experience the scenarios. The team will ensure that its members can continue to leverage the simulated plant in exercises at their enterprises after completing the program.



Event venue

Graduates of the Core Human Resource Development Program Share His Insights

Designing A System to Keep Cybersecurity Personnel in Their Roles

During the mini-session, Mr. KUMAGAE Takumi, a graduate of the Core Human Resource Development Program (2nd cohort), gave a talk. He first introduced a common concern among managers of enterprise cybersecurity teams: well-trained cybersecurity personnel may be reassigned to roles outside cybersecurity.

Mr. KUMAGAE identified a professional career track as a solution. At ALSOK, R&D staff can pursue a "R&D Specialist" career path separate from the line management path. Since specialists can only be transferred to departments related to their expertise, becoming a cybersecurity specialist makes it less likely they will be reassigned to roles outside cybersecurity operations. Mr. KUMAGAE currently serves as ALSOK's only information security specialist who holds the position of Chief Engineer.

The specialist career system not only helps employees pursue careers in their expertise but also ensures their performance receives appropriate recognition. Although we defend against cyberattacks, our contributions to cybersecurity are often difficult to see, making it harder to evaluate our work properly. If we incorporate these contributions into the evaluation system for specialists, they can receive more appropriate recognition, Mr. KUMAGAE emphasized. He has currently reported on the progress of the cybersecurity initiatives to the CTO every six months and receives an evaluation.

Mr. KUMAGAE also points to the effectiveness of the Core Human Resource Development Program in encouraging younger employees to choose cybersecurity as their career path. The specialized knowledge acquired during a one-year full-time program, along with the professional connections built through a community of approximately 500 graduates, has become a precious asset to his enterprise. "We can learn what cybersecurity personnel of other enterprises are focusing on through individual connections, rather than through exchanges among enterprises. Building these connections is a major benefit of the program," Mr. KUMAGAE says.



This chart shows the career path for R&D positions at ALSOK. Mr. KUMAGAE joined ALSOK's R&D department and now works as a Chief Engineer in R&D.

My Experience in the Program Shaped My Career as a Cybersecurity Specialist

“

I joined the Core Human Resources Development Program without any prior experience in cybersecurity operations. I experienced an attack on a lighting system that caused the overhead lights to flash repeatedly. I was struck by the opportunity to analyze how the system worked, reproduce the attack myself, and even test defensive measures in the same environment. These experiences sparked my interest in cybersecurity and ultimately led me to choose a career as a "Security Specialist," a career path that had not previously existed at ALSOK.

”



ALSOK Co. Ltd.
Mr. KUMAGAE Takumi (2nd cohort)

Designing and Leveraging a System for Specialist Personnel to Harness Diverse Strengths

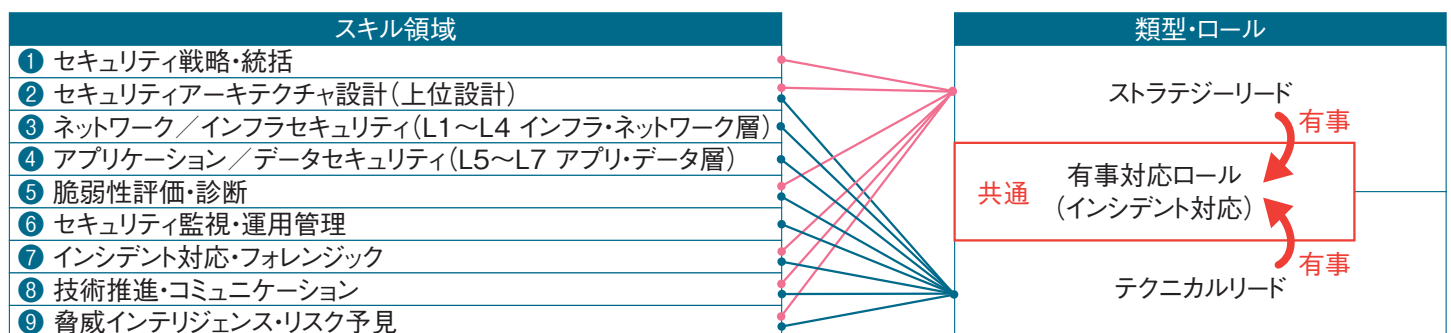
"Cybersecurity is an incredibly broad field; one person cannot cover everything," Mr. TERAMOTO Tsubasa (4th cohort) and Mr. KAWAZOE Kyohei (8th cohort) emphasized during the mini session. They presented on the theme of "How organizations utilize cybersecurity personnel."

Mr. TERAMOTO first introduced Kansai Electric Power's cybersecurity framework. The company defines "Cybersecurity Engineer" as a specialist role and recruits personnel through two channels: internal applications and external hiring. It develops cybersecurity personnel through two complementary approaches: input activities, such as sharing intelligence within the enterprise and incorporating knowledge and expertise from out

side the enterprise, and output activities, which apply those skills to improve cybersecurity operations and other areas.

Mr. KAWAZOE next explained the specialist role framework he has been developing since returning to Kansai Electric Power. The framework is designed to allow each employee to leverage their strengths in their respective areas of expertise rather than treating specialist personnel uniformly as generalists. Under normal circumstances, specialists are assigned to the following roles: "Strategy Lead," responsible for cybersecurity strategy and governance, or "Technical Lead," responsible for planning and designing the technical infrastructure. During an incident, they take on a shared "Incident Response Role," working together across their respective areas of expertise. The enterprise is also organizing skills into nine domains and visualizing them in a radar chart to support human resource development, personnel placement, and career progression.

"What I strongly realized was the importance of leveraging the strengths of people with diverse backgrounds and characteristics and complementing each other in areas where others have greater expertise. This allows the organization as a whole to cover a broader range of cybersecurity areas," said KAWAZOE.



Kansai Electric Power has organized cybersecurity skills into nine areas and established evaluation criteria to help individuals deepen their expertise while enabling the enterprise as a whole to cover a broad range of cybersecurity areas.

A Rewarding Year of Learning Across IT and OT

“

Having worked exclusively in IT, I found it highly rewarding to spend a year learning about OT. I was also impressed by the hands-on environment, which allowed us to put our ideas into action immediately. Through the program, I strongly appreciated the importance of cybersecurity professionals who understand a broad range of domains beyond their own specialties and can explain them to senior management.

”



Kansai Electric Power Co. Inc
Mr. TERAMOTO Tsubasa (4th cohort)



Kansai Electric Power Co. Inc
Mr. KAWAZOE Kyohei (8th cohort)

Building Connections to Become a Hub for Protecting Society

“

My experience through the program has been a valuable asset; I spent a year learning alongside colleagues from various industries and positions, ranging from their 20s to 50s. As cyber threats become increasingly complex, no single company can protect against them on its own. I hope to keep the connections built through the program, share information whenever we have the opportunity, and serve as a hub that helps protect society as a whole.

”

Graduation Ceremony for the 9th cohort of the Core Human Resource Development Program

The graduation ceremony for the ninth cohort of the Core Human Resources Development Program was held on June 29, 2026. A total of 55 trainees completed the year-long program and embarked on a new chapter as Industrial Cybersecurity Experts.

A Graduate Representative Greeting



Mr. HAMAMOTO Seiji (9th cohort)

We would like to extend our deepest thanks to the instructors, IPA, and the Ministry of Economy, Trade, and Industry for their ongoing support in providing this highly beneficial learning opportunity. We are also sincerely grateful to the companies that allowed us to participate in the program and supported us throughout the year.

The program offered an extensive and highly practical curriculum, with final projects addressing topics such as the challenges our enterprises face, generative AI, and issues specific to our respective industries. As the project progressed, we encountered various challenges. With support from our instructors and fellow trainees, we completed every project successfully.

From our instructors, we learned methods and approaches to assess threats, make decisions based on limited information, determine what to protect, and propose measures to senior management as core cybersecurity professionals.

The program offered more than technical knowledge and skills. Through practical exercises and final projects, we learned the importance of engaging in discussions with people from different backgrounds and explaining technical topics in a comprehensible manner.

We also formed invaluable connections with people across industries, companies, and ages, with whom we shared challenges and successes and had open and honest discussions. These connections are our priceless asset, and we will continue to cherish them.

Once we return to our enterprises, each of us will face different circumstances, challenges, and constraints, and what we learned through the program may not always translate directly into practice. Rather than keeping what we learned here to ourselves, we believe that our role is to apply it to our circumstances and serve as core cybersecurity professionals who bridge the gaps between senior management and the front lines, IT and OT, and across departments, enterprises, and industries.

Cybersecurity cannot be achieved by one individual, one department, or one enterprise. Through the connections established through the program, we will enhance cybersecurity across industries.

Opening Ceremony for 10th Cohort of the Core Human Resource Development Program

On July 1, 2026, the Industrial Cyber Security Center of Excellence (ICSCoE) held the opening ceremony for the 10th cohort of its Core Human Resources Development Program, welcoming 65 participants expected to play a key role in securing Japan's future social infrastructure.

Mr. SAITO, Chairman of the IPA, encouraged the trainees to challenge each other and discuss issues across industries as AI capabilities evolve and cybersecurity professionals need extensive skills. He also expressed his hope that they would become leaders of the cybersecurity field who harness AI as a partner to strengthen cybersecurity across industries in Japan.



Chairman, IPA
Mr. SAITO Yutaka

Mr. SAWADA, Deputy General of the Industrial Cyber Security Center of Excellence (ICSCoE), outlined three expectations for the trainees. First, he encouraged them to remain committed to continuous self-improvement. Second, he urged them to recognize that their work directly contributes to developing and stabilizing society, as cybersecurity is closely connected to every aspect of society. Third, he emphasized the importance of building strong connections with leading instructors, fellow trainees, and graduates participating in the Kanaekai, and leveraging those connections effectively in the years ahead. He expressed his hope that the trainees would continue to value these connections and contribute to the developing society in their respective roles.



Director General, ICSCoE
Mr. SAWADA Jun

