IPA Better Life with IT

ICSCoE Industrial Cyber Security Center of Excellence

ICSCoE REPORT

12.24.2024

vol. 20

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

8th Core Human Resource Development Program Started

On July 1, 2024, the Industrial Cyber Security Center of Excellence, ICSCoE, held an opening ceremony for the eighth Core Human Resource Development Program and welcomed 57 trainees anticipated to be responsible for Japan's social infrastructure in the future.

IPA Commissioner Yutaka Saito inspired trainees to achieve their professional goals with skills and knowledge enhanced through the program. He also encouraged them to build cross-industry professional networks, connecting the classmates, graduates of the past seven programs, and experts across the globe.

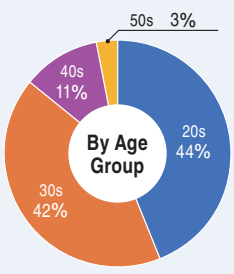
Mr. SAWADA, Director General of the ICSCoE, addressing the trainees.

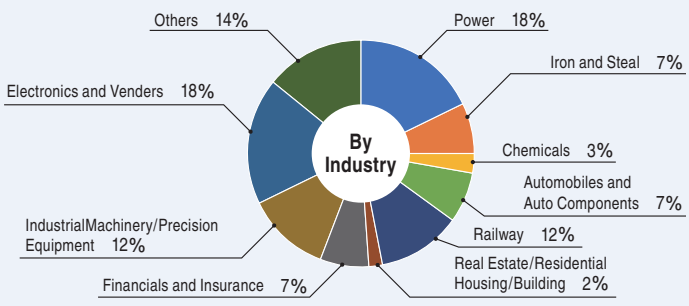
Mr. SAWADA, the newly appointed Director General of the ICSCoE, expressed two expectations for the trainees. The first expectation is for them to become top-class leaders who can respond to cyberattacks by proactively thinking on his/her own. Recent attacks have become more sophisticated with the use of AI and existing knowledge alone is not sufficient to confront them. The second expectation is to make use of the human network including the lecturers and alumni, and grow their capabilities through the interaction among the 57 eighth-term trainees.

Our guest speaker, Mr. NOHARA Satoshi, the Director-General of Commerce and Information Policy Bureau of the Ministry of Economy, Trade and Industry, delivered his great encouragement, saying that he hopes the trainees will become industrial cybersecurity experts whose capabilities are necessary for various situations and that they will actively engage in their dispatching company, but also for the entire industries, throughout Japan and even in the global after completing the program.

Results of 8th Core Human Resource Development Program participants

Fifty-seven trainees from various sectors and industries participate in this program, intending to become core human resources who will lead Japan's future in the cybersecurity field.





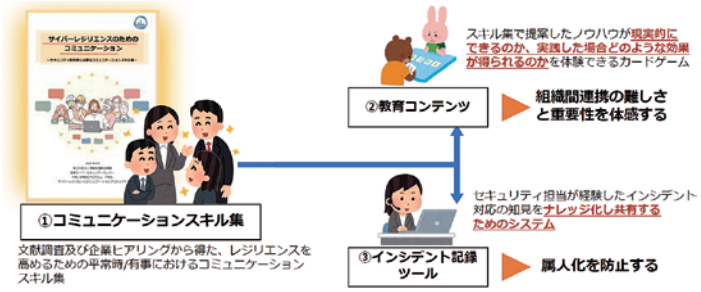
Communication for Cyber Resilience

Backgrounds and Issues

When cyber incidents occur, we must share information with other departments, comprehend situations, and issue instructions accordingly for prompt recovery. In this project, the team focused on incidents when occurring and ordinary circumstances, clarified the capabilities of flexibly responding to incidents by collaborating among organizations and communication techniques to maintain high cyber resilience, and summarized measures.

Issue-Solving and Outcomes

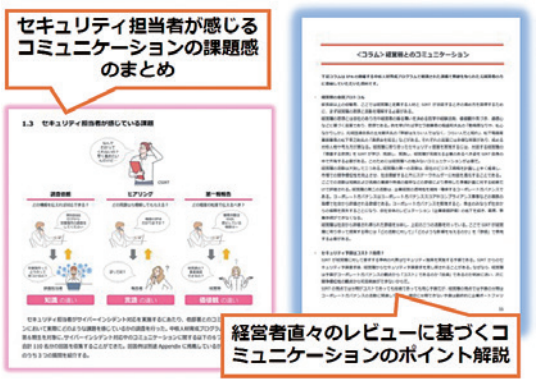
In this project, the team developed a communication skill book, educational content, and incident recording tools for all parties involved in incident responses for cybersecurity.



Overviews of Outcomes

We marshaled communication techniques for ordinary and emergency circumstances obtained through the literature research and hearing from enterprises to raise resilience and summarized them into one communication skill book. In this skill book, the members provide various information: explanations of cyber resilience, survey results of challenges the security personnel faces, interview data from enterprises, and communication techniques with higher management.

With this skill book as the main outcome, the project team created educational content for applying the skills into practice, manualized the information acquired from their experiences, and developed an incident recording tool as a sharing system. For more information on the educational content, please check "Security Awareness Content Development Project" on the next page.



Excerpt from the collection of communication skills

Interview with a graduate

Ms. NISHIZAWA Yuri (front row center)
West Japan Railway Company, and members

What is your utmost benefit from this project?

The utmost benefit of our project is that I was able to learn security knowledge and skills from my colleagues, lecturers, and antecessors of the ICSCoE and comprehend how to apply those to enterprises. It is not straightforward to share the necessity and values of security responses with people from different departments and positions. I was able to gain a variety of patterns to utilize knowledge and techniques, such as sharing information from diverse settings and providing easy-to-understand cases, which I have been applying to my current business assignments.

Methods for utilizing project outcomes

We hope security personnel leverage our project outcomes mainly when communicating security. It is essential how to get others involved to strengthen security and protect enterprises. If you attempt to defend the security systems only by your department or enterprise, you may not be able to receive the necessary information and may delay initial measures when an incident occurs. Sharing information alongside camaraderie with the department and enterprise around you enables us to determine approaches promptly. Therefore, we hope that you would utilize our project outcomes in such circumstances.

This is unique to the ICSCoE!

First, the ICSCoE enables us to examine defense mechanisms while analyzing actual behaviors on real equipment from the attackers' point of view. Since I have experienced multiple cyber attacks, I have been able to determine attackers' mental states, widen my view , and judge how far I had to go to determine countermeasures.

Second, the ICSCoE enables us to build broader personal networks.

Before participating in the program, I only had an opportunity to talk to the people working at my company and its affiliated companies. At the ICSCoE, I discussed the security measures with my colleagues in my sector and from other industries; then, I realized each of us we had completely different concepts and methodologies. Moreover, I found more people I can consult with through the personal networks cultivated through the ICSCoE; thus, I can determine security measures by collaborating with the people outside my company recently.

Lastly, the ICSCoE significantly influences our societies due to the outcomes the trainees created through the final projects. Indeed, I saw an interesting scene where participants used the training materials that quoted and summarized our outcomes. This way, the ICSCoE provides us with opportunities to contribute not only to our company but also to our societies from security perspective. I believe that is unique to the ICSCoE.

Security Awareness Content Development Project

Backgrounds and Issues

Although the criticality of the cyber incident measures has recently increased, it is challenging to prevent 100% cyber attacks no matter how far we implement these measures. Besides, standard cyber incident drills for enterprises take formal approaches verifying the manualized measures in responding to anticipated events; thus, we face obstacles to finding communication issues. During actual incident responses, information collaboration is essential since many security personnel will tackle the incidents occurring unexpectedly. However, it is not clear what information each enterprise possesses and needs. To solve these issues, the project team developed awareness content that replicates a flow of information collaboration among organizations during an incident and identifies obstacles to communication.

Issue-Solving and Outcomes

In this project, the members created the learning materials in a gaming format to simulate scenarios damaging OT and IT systems.

Examples of the cards

This project aims to let people experience incident responses and comprehend the importance and issues of information collaboration through simulations. After completing the simulation, the participants review the incident responses; they identify issues by comparing information collaboration between their enterprises and the results obtained and discussing what to improve; thus, they will take the following action to solve them. This card game enables participants to determine who needs the information they have obtained; therefore, they realize when facing inadequacies of information collaboration that will become future considerations.

自社想定時の振り返り時の参考項目（抜粋）

チェック項目	☑
NIST "Computer Security Incident Handling Guide"	
コミュニケーションツールの優先順位が確立され、関係者に周知されている	
緊急時の連絡先情報が用意されており、常に最新情報に更新されている	
連携が必要な外部機関およびその連絡先が整理されている	
インシデントの重要度を決める指標があり、関係者に周知されている	
SANS Institute "Incident Handler's Handbook"	
演習を通じてインシデント対応組織の課題を発見し改善する仕組みがある	
インシデント対応を記録するフォーマットがあり分析できる仕組みがある	
誰がどのようにインシデントを報告するか、どの情報を含めるべきか定められている	

Excerption of the review sheet

Interview with a graduate

Mr. TATSUMI Daisuke
(front row, 2nd from left)
Osaka Gas Co., Ltd, and members

What is your utmost benefit from this project?

My utmost benefit was that I could work on this project as a leader. I desired to give back the knowledge I obtained to my enterprise and industries; therefore, I put myself up for a leader. I feel that I was able to advance in management perspectives by identifying tasks within our project, assigning them to the members, and tracking the progress of our project.

Methods for utilizing project outcomes

After returning to each enterprise, some members have already utilized our project outcome. I want the security personnel to use it first and for in-house security training and awareness-raising activities for related parties. Subsequently, I want to encourage middle managers to take advantage of this outcome. The reason is that although enterprises have cyber incident drills, if they are formal and only verify how to respond, they sometimes cannot take any appropriate actions, such as giving instructions and reporting as an incident occurs for real. I wish for more people to try our project outcome at least once.

This is unique to the ICSCoE!

Everything I experienced here is unique to the ICSCoE, but the best is that I built personal relationships with the instructors and my colleagues. It is not easy to create close relationships with them beyond the business boundaries for the long term, one year, nowhere but the ISCSoE. I could communicate with the people with whom I had not interacted during the regular operations of my enterprise and broaden my knowledge, which I could not have obtained if I had secluded myself in my enterprise or industry. In particular, I could master and comprehend the security initiatives of other enterprises and industries that will be able to nurture me when I operate across enterprises and industries.

The Graduation Ceremony of 7th Core Human Resource Development Program

Mr. Endo, Then Director General of the Industrial Cyber Security Center of Excellence

Mr. ENDO, the then Director General of the Industrial Cyber Security Center of Excellence, made an encouraging speech to the graduating trainees.

I heard the 7th trainees voluntarily worked on the courses and your final projects and stayed late to deal with them every day. When you stand on your own feet, you have to have your own judgment criteria to decide for your life. Since you faced tasks, at which you and your industry have confronted and you thoroughly dealt with them throughout the year, I am sure that you could have broadened your judgment criterion further.
I'm sure that you could obtain many valuable and trustworthy colleagues through spending time together over the past year. Needless to say, It is challenging for one enterprise or even a single country to defend against cyber attacks. It will be essential to take full advantage of the connections, which you established at the ICSCoE, strengthen vertical and horizontal contacts with various industries, cooperate with other nations to defend your enterprises and industries against cyber attacks. I have a high expectation that you will play not only a key role in connecting people between business sites and managers in your entity but also as an active leader to enhance the cybersecurity and resilience of Japan beyond enterprises and industries. Congratulations on your completion of the Core Human Resource Development Program today.

Mr. KUBO Takashi
Hankyu Hanshin Holdings, Inc. (Then)

Mr. KUBO Takashi delivered a speech as the representative of the graduates.

Many of our sixty-five trainees faced security for the first time when joining the Core Human Resource Development Program. I believe some colleagues might have felt anxious at the beginning of the program. However, at the ICSCoE, the instructors thoroughly taught us from the ground up, and we worked hard on exercises with other colleagues every day; we were all able to reach this day together.
The curriculum prepared by the instructors was tremendously valuable for us not only to absorb knowledge and hone practical skills through the hands-on exercises but also to develop the abilities of leadership, communication, and problem-solving as the Core Human Resources. I believe we have gained excellent experiences since we could discuss the opinions with colleagues beyond generations and enterprises from our hearts that we might not be able to express our thoughts frankly in the enterprises.
Even outside of the facilities, the ICSCoE provides varied environments where the trainees can voluntarily participate, such as overseas deployment programs, hardening competitions, and facility tours of various industrial fields; as Director General Endo mentioned, these were extremely valuable and inspiring for us.
From now on, I will support the development of industries from the security perspective with my colleagues I have met through this program. Therefore, I will be committed to continuing to learn and tackle security challenges after returning to my company.
Thank you very much for your support over the past year.

Briefing of Representative Final Projects

After the graduation ceremony, the trainees presented their selected final projects. Dr. UKAI Daisuke presented his final project titled "Visionary Security ～ Security Measurers Starting from Zero ～ " as a project leader, and he pointed out the issues newly established business corporations and start-ups just started expanding; they do not take appropriate actions when increasing security risks. In this project, the team set up three solutions as hypotheses for these issues: organization and systematization of necessary security measures, promoting a security-conscious culture, and establishment of a starter kit for IT environments taken security measures, and Dr. UKAI explained each activity, respectively.

Dr. UKAI Daisuke
Chubu Electric Power Co., Inc. (Then)

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

Bunkyo Green Court Center Office,
2-28-8 Honkomagome, Bunkyo-ku, Tokyo, 113-6591
TEL 03-5978-7554 FAX 03-5978-7513