3 ＜Building industry team＞
Activities to improve security levels in the Building Automation industry

Overview

Recently, examples of remote monitoring and maintenance over the Internet are increasing with the needs of more efficient building systems' operation and the introduction of IoT as a background. Also, some individual equipment systems are connected to the integrated network to interconnect their functions. In addition to changes in the environment surrounding buildings, METI (Ministry of Economy, Trade and Industry) just released a guideline* aimed at ensuring the security of building systems. This opportunity became the trigger of our activities to start this project.

This project made many recommendations through the submission of public comments so that various stakeholders across the industry could use this guideline to consider security as a common language and their own issue. The team also prepared an explanation book for the guideline. It would encourage them to take the “FIRST STEP” by accelerating the understanding of security risks, impact by cyberattacks, and more practical countermeasures. The explanation book also presents the following content independently.

＊Guidelines for Cyber-Physical Security Measures for Building Systems
https://www.meti.go.jp/english/press/2019/0617_005.html

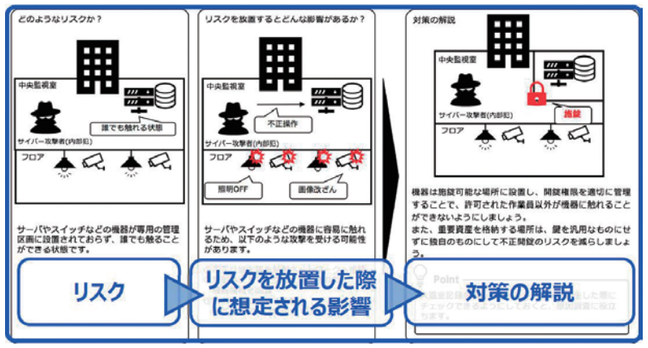
① **Proposals on how to proceed with the measures using the guideline,**
② **Measure map which visualizes the control points of the whole building automation system and around it,**
③ **Measure catalog which illustrates security risks, incidents, measures, and mapping to the guideline with easy-to-understand diagrams,**
④ **Case studies of risk analysis to determine the priority of measures.**

Comments of members

Trainees from various industries related to buildings came together to this project. We were able to work with other ICSCoE trainees without distinction and beyond the lines of the dispatching companies. We could not have completed the explanation book without the solidarity of all project members, and the book was a culmination of the one year training at ICSCoE. The content of this book is a must read for those who are going to tackle security in this industry.

We are pleased if our cultivated knowledge at ICSCoE could make any contribution to developing cyber security awareness in the building industry and a circle of understanding among stakeholders.

Example of the explanation book (measure catalog)



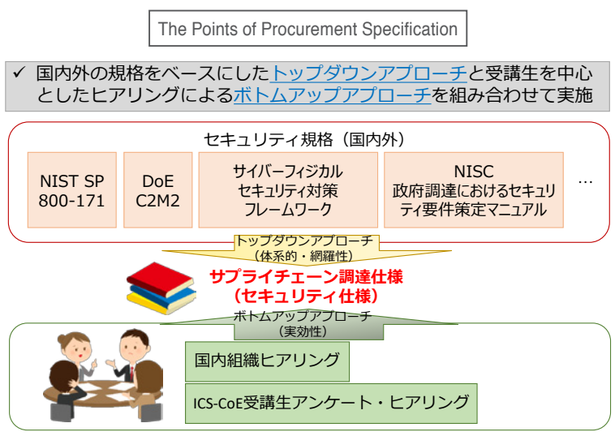
4 ＜Power industry team＞
Supply chain security study

Overview

The team prepared a procurement specification specific to the supply chain. Trainees from the power industry led the creation of the specification with other trainees from critical infrastructure operators and vendors. This specification deals with potential risks of malicious codes (malware) contamination in the supply chain from ordering to delivery.

The team created the specification by combining both a top-down approach (a systematical and comprehensive reflection of procurement specifications based on national and international security standards) and a bottom-up approach (an enhancement of the effectiveness of procurement specifications through interviews with ICSCoE trainees and organizations in Japan). Its primary advantage is that the procurement specification is conscious of theory as well as actual usage.

The Points of Procurement Specification



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

IPA Better Life with IT

Industrial Cyber Security Center of Excellence

ICSCoE REPORT

9.30.2019

vol. 05

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

The 3rd Core Human Resource Development Program has started.

Dr. Endo, Director of ICSCoE, inspiring trainees

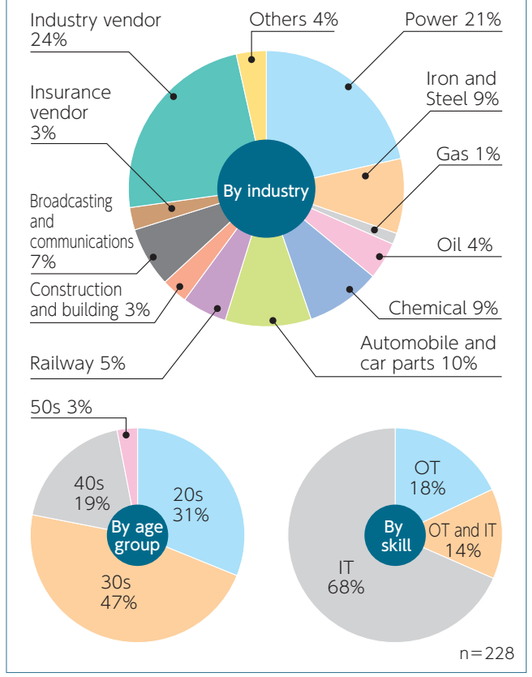
In July 2019, Industrial Cyber Security Center of Excellence (ICSCoE) accepted 69 trainees to the 3rd Core Human Resource Development Program. The opening ceremony took place on July 1st, the first day of the program, as the first step for all trainees to renew their determination.

Dr. Tomita, IPA Chairman, gave a warm message: "I expect everybody aims for height with many peers, leveraging their strengths cultivated in their companies."

Dr. Endo, Director of ICSCoE, indicated the importance of collective defense to protect systems from attackers as recent technology innovation had been remarkable. He highlighted that spending one year together would nurture the robust trust relationship and that bond with trustworthy peers would become a significant power to protect Japan.

Mr. Keita Nishiyama, Director-General, Commerce and Information Policy Bureau of METI, peering over the trainees’ faces, said: "Feel uneasy whether you could make it through for one year. That’s quite normal and important." He also inspired the trainees: "The purpose of this one-year program is to change what you have been. To that end, ICSCoE offers you a unique program only available here in the world."

Core Human Resource Development Program FACT & DATA
(Profile of the 1st to the 3rd cohorts)



The 3rd cohort of 69 trainees attended the opening ceremony.

The 2nd Core Human Resource Development Program was completed.

The 2nd Core Human Resource Development Program Completion Ceremony (June 2019)

In June 2019, the 2nd Core Human Resource Development Program was completed. At the completion ceremony, each completer received encouragement letters from Mr. Seko, then Minister of Economy, Trade and Industry, in addition to words of encouragement from other guests. In response to these messages, Hiroyuki Hasegawa (Chubu Electric Power Co., Inc.), representing the completers, contemplated the one year. He renewed his determination on how he would act as an “Industrial Cyber Security Expert," a title given to the trainees.

Address by Mr. Hiroyuki Hasegawa (Chubu Electric Power Co., Inc.) on behalf of the 2nd cohort,

As taking this program for one year, I have three deeply memorable things, which today I want to share with you briefly.

The first is the acquisition of technical skills. Through team exercises, various people were actively able to teach and enhance their knowledge with each other. Some trainees had many skills that I did not have, and active learning enabled me to acquire such knowledge.

The second is the overseas experience. In addition to overseas dispatching exercises to France and the U.K., I applied for a training program held by the U.S. Department of Homeland Security. I experienced the cyberattack response exercise, with two Japanese joined into 38 Americans., In France, the industry-government-academia collaboration was very advanced; notably, companies were focusing on research fields.

In the U.K., I had the impression that the government supported start-up companies and that the framework for information collaboration was quite advanced. In the U.S., I witnessed that debate started among students during a lecture and that the lecturer jumped in. Presumably, they have a culture that makes lectures more interactive in their root. I want to incorporate such a culturally-rooted communication skill into Japan appropriately.

The third is about communication. I had a desire to be the best peers with all 83 members in the 2nd cohort. On the very first day of the lecture last July, I proposed preparing a list of all trainees with photos and throwing a drinking party with everyone. I made them happen. At the opening ceremony, a guest said that the 1st cohort was like Columbus that discovered the American Continent. If so, I was hoping to make the 2nd cohort be those who developed the Continent significantly. That was my driving force. We also discussed various opinions along the way, and everything was constructive. Receiving stimulus with each other, I was able to acquire security skills as well as know-how that advanced the project. Extracurricular club activities counted more than 20, and the year-end and the dissolution parties were very exciting with more than 100 participants, including lecturers. It would have taken much longer to develop such a deep relationship where we can talk and discuss anything because the company-to-company relationship is usually businesslike. I believe that this secure horizontal connection would transcend industries and regions and contribute to cyber security in Japan even after we returned to the respective companies.

We would like to steadily expand our contributions to industries, regions, Japan, and the world, and become professionals who can contribute to the cyber security of this era. Thank you very much.

Live Discussion on the Current Cyber Security Human Resources Development Targeted to Top Corporate Executives (May 2019)

In May 2019, right before the date for the completion ceremony of the Core Human Resource Development Program, the Japan Business Federation (Keidanren) hosted the “Fifth Cyber Security Seminar for Top Corporate Executives” and invited three participants from the program as its panelists. During the session moderated by Professor Youki Kadobayashi, the panelists utilized all their knowledge absorbed from the one-year-training held by the ICSCoE and developed an active debate of cybersecurity.

Moderator: Professor Youki Kadobayashi, Nara Institute of Science and Technology
Panelists: Mr. Yuji Inoue (NTT Communications Corporation), Ms. Haruna Go (LAC Co., Ltd.), Mr. Hiroyuki Hasegawa (Chubu Electric Power Co., Inc.)

Main Topics

IT and OT : Based on a common perception that OT security conceptually differs from IT security, the panelists glanced at the natures of industries where the trainees served for and discussed the distinct functional capabilities between IT and OT, inherent issues, and essential observing points to accomplish security measures.

Overseas Initiatives : The panelists introduced their insights acquired from the overseas observation trips: 1) Security policies implemented by other countries; 2) Development of security-related laws where critical infrastructure companies participated in; and 3) Information sharing systems. They also discussed the challenges the Japanese industries might face in the future.

Voluntary Initiatives : The panelists introduced the activities which each of them infused with his or her enthusiasm: 1) Proactive information exchange through lectures and publications, 2) Awareness-raising campaigns for the industries, where the participants belonged to, through the dissemination of guidelines; and 3) Establishment of networking mechanisms to widen and strengthen the systematic relationships among the instructors and all participants who had absorbed the knowledge from this program since 2017.

Unique to ICSCoE:

- I became able to understand cybersecurity in the real world that I could not find through any search engine or in textbooks.
- I had an incredible opportunity to meet security professionals from various fields and became able to build relationships with them beyond the boundaries of companies and industries.
- I had an invaluable opportunity to collaborate even with the competitors as a peer who had a high level of security awareness to strive hard for one objective.

Here are some efforts from the final project of the 2nd cohort.

83 trainees from 69 companies tackled about 35 team projects. Four projects out of them are below.

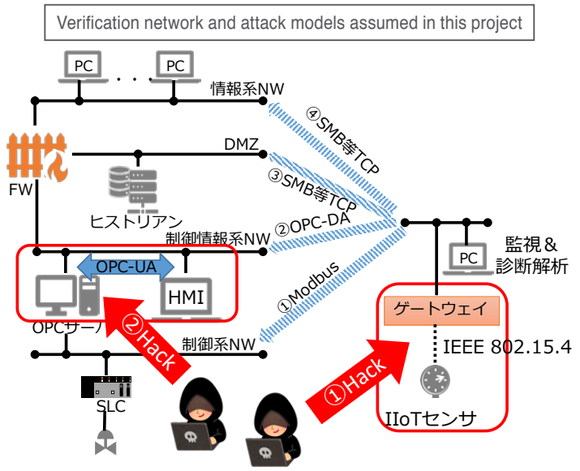
1 ＜Chemicals and gas industries team＞ Verification of IIoT & OPC-UA security

Overview

Although various industries, including the chemical industry, are actively promoting the use of industrial IoT, they have not studied security measures throughly yet. Furthermore, communication protocols used in plants are expected to transit from conventional ones to OPC-UA, which is considered to be theoretically secure. But there are concerns if it is secure from the field's viewpoint, or free from pitfalls in configuration and others.

In this project, therefore, we configured a verification environment with simulated plants and performed security verification against industrial IoT devices and OPC-UA.

Verification network and attack models assumed in this project



In verifying industrial IoT devices, we evaluated their security tolerance and proved that systems might be subject to DoS attacks and alternation of the acquired data. We also suggested the risks of inadvertently connecting equipment to control and control information networks in the report.

In verifying OPU-UA, we conducted a penetration test for each security setting of OPC-UA and evaluated what kind of risks it had. We summarized the results into seven precautions on introducing OPC-UA to publicly disseminate the conclusion that ”Security in plants cannot be guaranteed only by the introduction of OPC-UA."

Seven precautions on introducing OPC-UA

1. **Never use** “Security Policy : None.”
2. **Never use** “Security Policy : None & Anonymous Authentication” as well.
3. Close unused Security Policy.
4. Manage secret keys (certificates) properly.
5. Yet DoS attacks are inevitable.
6. Never forget other security measures.
7. Even OPC-UA products have vulnerabilities.

Comments of members

As a critical infrastructure operator, it is vital not only to pursue convenience and efficiency but also to understand the risk points of secure specifications of devices. While attackers are said to be overwhelmingly advantageous, the ICSCoE training, which allowed us to learn from the attackers' perspective, was significant in considering security measures in the future.

Furthermore, I believe that the formation of personal connections is another major achievement possible only in ICSCoE, enabling close collaboration across industries.

2 ＜Power industry team＞ Considerations on power system security products

Overview

A trainee, who was in charge of OT (Operational Technology) at a power company, had a strong desire to deepen technical knowledge to negotiate with system vendors on an equal basis. Trainees from other power companies agreed with him, and we launched this project.

The purpose of the project is set to develop practical eyes to introduce security products and to improve the technical level of user companies. For that purpose, we examined the survey items from the viewpoint of ease of maintenance and functional survey and verified various products.

We created a video report explaining such as verification status and product settings; it would be easier to reproduce the results and understand the technologies at the dispatching companies.

Comments of members

I had an experience unable to communicate well with vendors due to my lack of expertises; I could not purchase a product with functions required indeed. That bitter experience always makes me think to boost the users' skill level. I believe that this report will improve our companies' skill level. I hope that this report would be used effectively to catch up with and maintain their skill level.