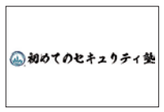
The Core Human Resource Development Program for 5th Cohort - Final Projects Published on our Website

We publish the outcomes of our final projects, including the ones we have introduced in the on the ICSCoE website.
Please visit our website for more details.

▶ Industrial Cyber Security Center of Excellence
The Core Human Resource Development Program
Final Projects (only in Japanese)

https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project.html

Defense!! Security Juku (Security School)



A security educational material in IoT implementation and supply chains for employees

DX Strategies and Organizational Theories for Middle Management

A material outlining essentials that middle management pursuing DX must conduct

IT Sec for Users:5 Minutes to Understand IoT Security Risks

A material for utilizing various guidelines regarding IoT security

Cybersecurity Class for Future Children ～ No SEC, No Life ～

Educational content enabling children to use in classrooms (texts, videos, games)

Encouragement to Shift Toward Zero Trust

A material summarizing considerations to shift toward zero trust

AI Handbook for Security Personnel

A referenced material to proceed to strengthen AI Security

Secure Management for Data-Utilized Smart Cities

A material outlining personal data・privacy risks・management procedures for smart cities

Handbook for Implementing Security by Design

Introduction to implementing security by design on system development sites

English Reading for Security Engineers

Vocabulary flashcards and study materials unique to security

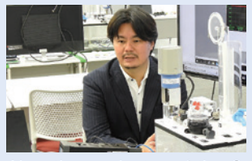
Handbook for Secure ICS Cloud

A referenced material to consider implementing cloud in the OT system environment on manufacturing sites

◆◆◆ International Collaborations Proceeded by the ICSCoE ◆◆◆

We Shared Cybersecurity Perceptions Regarding OT Systems for the Indo-Pacific Region.

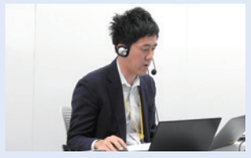
The Industrial Cyber Security Center of Excellence (ICSCoE) and the Ministry of Economy, Trade and Industry (METI) held "JP-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region" in collaboration with the United States government and the European Commission. The ICSCoE provided the participants with a hands-on exercise program utilizing its simulated plants.



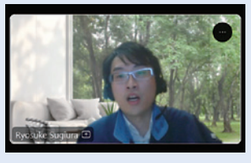
Dr. MITSUNAGA Takuho provided the hands-on exercise program.
(Lecturer of the Core Human Resource Development Program; Associate Professor of Information Networking for Innovation and Design, Toyo University)

Also, the graduates of the Core Human Resource Development Program participated in this program at every meaningful point. They disseminated their findings and learnings obtained through the ICSCoE to the world.

Mr. HASEGAWA Hiroyuki led the discussions as a moderator throughout the seminar presented by experts from Japan, the US, and the EU (Graduate of 2nd Cohort, Chubu Electric Power Grid Co., Inc.)



Mr. TAHARA Jumpei shared his findings on the final project, "Handbook for Secure ICS Cloud." (Graduate of 5th Cohort, Azbil Corporation)



Mr. SUGIURA Ryosuke presented the outcomes from the final project with the theme, "Optimization of Security Enhancement Activities Based in Newly Developing Nations." (Graduate of 5th Cohort)

▶ IPA Website

"JP-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region" was held in FY2022

https://www.ipa.go.jp/icscoe/english/news/news20221031.html

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

ICSCoE REPORT

Industrial Cyber Security Center of Excellence

2.9.2023

vol. 14

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

The Core Human Resource Development Program for 5th Cohort

Introducing Our Efforts in Final Projects Second Series

A final project is that our trainees utilize their knowledge and experience absorbed through our lectures and exercise programs and tackle the issues set for their dispatching company and industry as a team.

A Guide to Prioritize Security Measures for OT Systems

Backgrounds and Issues

It is vital to propel security measures for OT systems to counter mounting cyber attacks; however, there are various obstacles from planning through implementation.

Issue-Solving and Outcomes

In this project, the team aimed to **decrease the obstacles when implementing security measures** and **developed a guidebook and tool to conduct the steps from security risk assessment through security measure prioritization.**

The project team describes three steps through security measure prioritization in this guidebook. Users can input their enterprise data into the tool and derive the priorities for security measures specific to their organization.

STEP 1 Security Risk Assessment

Risk analysis adopting frameworks enables users to determine attack scenarios (risks) for OT systems and their security measures.

STEP 2 Prioritization of Security Measures to be Implemented

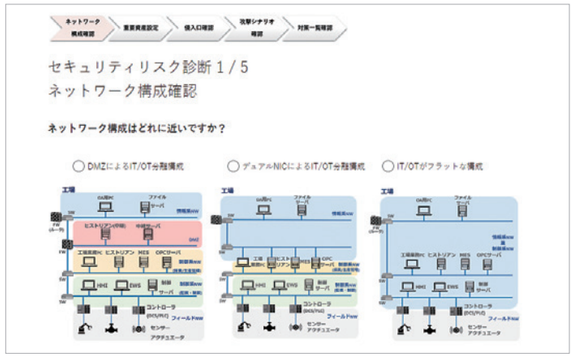
The project team describes potential cyber attacks based on the results of their risk assessment and the methodologies to prioritize security measures considering organizational security strategies.

STEP 3 Prioritization of Security Measures Based on Restrictions Specific to Enterprises

Furthermore, the project team shows the procedures to prioritize security measures considering restrictions unique to organizations: budgets and a condition of system operations. Thus, users can analyze the assessments in the cost consciousness and obstacles when implementing each security measure.

Prioritization Tool

This tool corresponds to the guide and enables users to easily derive their priorities by inputting their enterprise information into a form.



▶ **Please visit our website for more information on the guide and prioritization tool (only in Japanese)**

https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project/yusenpj.html

Interview with A Graduate

Mr. KUBOTA Yu
Mitsubishi Electric Corporation

What is your utmost benefit from this project?

I could share my awareness of issues I had held in practice with many people and enrich my knowledge by discussing with them from various perspectives.

This is unique to the ICSCoE!

I could hear honest opinions from the graduates of the Core Human Resource Development Program, who have been active in the front line of the cybersecurity field. I could pursue the practical deliverables from the on-site perspectives by incorporating the insights gained from the graduates into the project.
Because we took the same program, I could share my thoughts and knowledge with the graduates and exchange our opinions which were dense in excellent content within the restricted time frame.

OT Vocabulary List for IT System Integrators

Backgrounds and Issues

To undertake security measures for OT systems, we must understand both OT and IT systems. Therefore, the trainee launched this project with the theme of “Improving OT knowledge of IT System Integrators” to solve the issue: “IT personnel is unfamiliar with OT environments and terminology.”

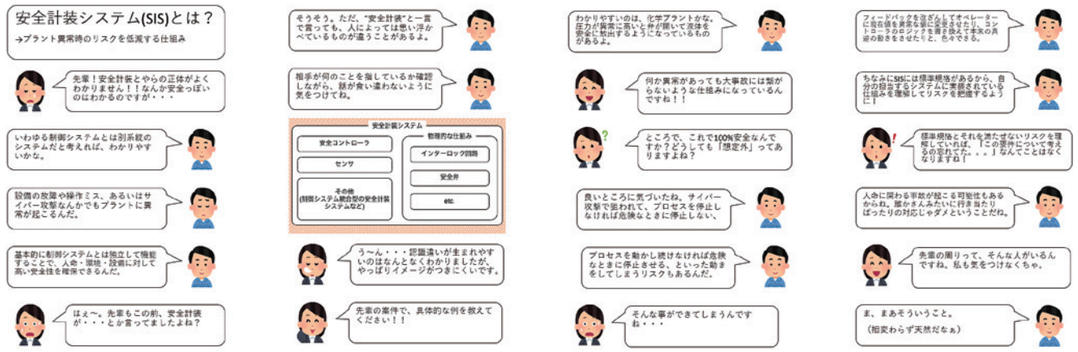
Issue-Solving and Outcomes

As IT System Integrators avoid misunderstanding security measures with OT personnel, they must understand the terminology for the IT field and the various gaps between OT and IT. Consequently, the project team **created the book, “OT Vocabulary List for IT System Integrators”** compiling terms and differences that IT System Integrators must understand.

First, this book describes the differences with IT: risks unique to OT systems and on-site operational methods. The team **carefully selected and compiled the terms,** from professional to frequently used on-site, **that System Integrators should understand and the information of those terms.**

This vocabulary list has both a printed version and a web version. Thus, the team expects users can check unknown terms on-site, and IT and OT personnel can undertake security measures using a shared language.

Vocabulary List (interactive easily comprehensible explanations in an interactive format)



Interview with A Graduate

What is your utmost benefit from this project?

Since we had decided on a theme for our final project, we could bring back the outcomes that would be genuinely necessary for us. I also felt the necessity of the OT vocabulary list as an IT System Integrator. I met the members with awareness of the same issues and could create handy outcomes on-site.

Methods for utilizing project outcomes

We have held in-house workshops once a month and utilize the vocabulary list as our textbook. The enterprise imposed me on a mission, “You must contribute to the company as N-fold much as you will learn.” Now I feel I’ve been achieving it.

This is unique to the ICSCoE!

The ICSCoE is a place to actualize our idea of “I wish I could.” For example, we planned to create a book through this project, but no members had such experience and knew how to do so. On this occasion, the lecturers with know-how in publishing advised us; therefore, we could make the book step by step.

Visualization of Security-Related Costs

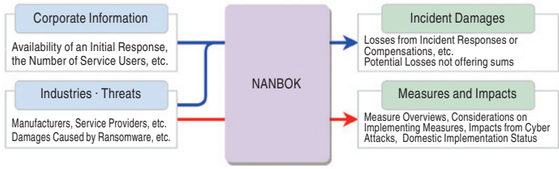
Backgrounds and Issues

When proceeding with security measures within organizations, acquiring budgets is an obstacle we must overcome. For managers to understand the importance of security investment and exercise judgment, a challenge would be that security personnel provides the managers with the necessary information to decide.

Issue-Solving and Outcomes

The project team **developed the tool “NANBOK”* to utilize for providing information to acquire budgets.**

This tool enables us to estimate damages caused by incidents (quantify cyber risks) and project security measures and those impacts by inputting information: incident types, industries, and severities.



*NANBOK Next-generation-scenario in Assembled Notes for security administrator with Bill calculator Optimized by Kawamura model

function 1 Estimating Incident Damages

The project team selects threat types from “Information Security Threats Top 10” published by IPA. The team developed the estimate method based on the “Research Report on Losses from Incident Damages” by JNSA outlined the precedent examples of costs when an incident occurred.

*NPO Japan Network Security Association

function 2 Projecting Security Measures and Impacts

This tool projects security measures (security products・services, etc.), potential impacts, and domestic implementation status by threat. The project team shows security measures and those impacts by linking to possible attack paths using the ideas of cyber kill chains. Thus, this tool enables its users to have concrete images of them.

▶Please visit our website for more information on the guide and prioritization tool (only in Japanese)

https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project/visualization-costs.html

Interview with A Graduate

What is your utmost benefit from this project?

We could take enough time to consider our estimation methods of damages and spending when we encounter cyber attacks. We dealt with the matters, not necessarily urgent but crucial, and incorporated them in concrete form. These were worthwhile in terms of looking into the future.

Methods for utilizing project outcomes

The outcomes enable us to derive reference values to have shared awareness within the enterprise. The tool has parts measuring quantitatively and non-quantitatively; however, this tool lets us take a prompt initial response by deriving reference values quickly.

This is unique to the ICSCoE!

It was I had advice from many experts. The lecturers, of course, and the trainees, who had research experience in this theme, shared their professional perceptions. Also, the lecturers introduced us to some private companies; therefore, we could interview them to learn their reality and actual values. I met the people with whom I could not build a relationship and could obtain deep insights by hearing their stories.