The 4th Core Human Resource Development Program

Functional Improvement in IMANE-CARD and PC

Backgrounds and Issues

As we cast an eye on the current trend in security threats to enterprises, especially threats targeting employees – individual users – have been increasing. Accordingly, our challenges are to provide those employees with security training they can actively work through and obtain highly educational effects. Therefore, **the team tried to improve active learning formatted security training materials for employees, the "IMANE*1 series", by making its functions easier to use.**

The "IMANE series" is a set of training materials developed by the laboratory of Professor HASHIMOTO Yoshihiro at Nagoya Institute of Technology, and the ICSCoE has been using this series for its exercises in the Core Human Resource Development Program, especially for OT incident responses and BCP*2. The "IMANE-CARD", a part of this series designed for group work exercises using cards, enables participants to discuss and examine inter-organizational collaborations required for incident responses. Another series is the "IMANE-PC", game-style training material for PC allowing participants to simulate incident responses and visualize activities made by players; thus, they can recall and analyze specific actions.

*1 Incident **MAN**agement **E**xercise
*2 **B**usiness **C**ontinuity **P**lanning

- IMANE Series
  Training materials enabling to simulate responding methods in case of incidents
  Allow us to respond to various incidents by applying different training scenarios
  - IMANE-CARD
    Allow us to visualize an overview of incident response procedures as an enterprise by utilizing "Action Cards"
  - IMANE-PC
    A training material leveraging PC browsers
    Allow us to simulate inter-organizational collaborations in case of incidents
  - IMANE-DRAW
    A software creating training scenarios for PC
    Create scenario data combining Draw-IO and Excel macros

Details of IMANE Series

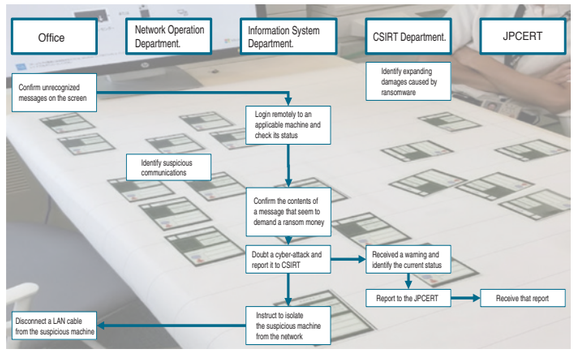
Issue-Solving and Outcomes

1. A Manual for Facilitators

The team developed a facilitator manual that **ensures every instructor can effectively conduct in-house training where participants utilize the IMANE-CARD and IMANE-PC.** To develop this manual, the team examined its contents through the eyes of both facilitators and participants that would enable the participants to actively discuss and reflect on incident responses as developed this manual. Especially in a reflection of this exercise, the team considered which discussion would deepen participants' thoughts and illustrated their training procedures using some concrete examples.

2. Creating New Scenarios and Adding Functions for IT Enterprises

Using the IMANE-CARD, the team created several scenarios that enable participants to learn incident response methods when an office computer gets infected with ransomware. Therefore, the team reviewed actions to be taken in case of incidents and shaped these actions into trainable formats. Also, to make these exercises more effective, the team considered it essential that participants act according to circumstances rather than memorizing their incident response methods formulaically. Thus, the team devised the new functions and implemented these functions into the IMANE-CARD so that the participants could consider potential risks behind actions and address those risks. We expect that enterprises will enhance the response capabilities of each employee to security threats by utilizing the IMANE-CARD.



A sample scenario: Learn how to handle incidents when they occur

Interview with Graduates

Mr. USHIYAMA Takuya
NHK Technologies, Inc.

What is Your Utmost Benefit from the Project?

There is no perfect answer for incident responses; however, this project helped me realize the importance of simulating suitable incident responses like emergency drills. For putting myself in the position of creating educational materials, I could widen my perspectives on the importance of raising on-site and in-house security awareness and the methodology, including the IMANE series.

Methods for Utilizing Project Outcomes

I would like to propose to utilize the IMANE series for in-house security training for my company and other enterprises. It would be wonderful if our project outcomes contribute to raising security awareness throughout society.

This is Unique to the ICSCoE

I was the only member among the fourth cohort participating in this project, a collaborative project with the laboratory of Dr. Hashimoto at Nagoya Institute of Technology. I could absorb knowledge and gain various inspirations from academics with whom I did not generally have an opportunity to interact in my routine work environment.

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 Industrial Cyber Security Center of Excellence
ICSCoE REPORT 8.31.2021 vol. 10
The ICSCoE Report is a public relations newsletter on ICSCoE's activities.

The 4th Core Human Resource Development Program was completed

The Industrial Cyber Security Center of Excellence (ICSCoE) held a completion ceremony for the fourth-cohort trainees of the Core Human Resource Development Program in June 2021. Under adequate infection control measures for the COVID-19 pandemic, we conducted the ceremony at an external venue and invited people from the dispatching companies of each trainee to provide them with an excellent opportunity to feel the growth of trainees through our one-year-program.

During the ceremony, the graduates of the fourth cohorts received a video message from Mr. KAJIYAMA Hiroshi, Minister of Economy, Trade and Industry. In this video message, Minister KAJIYAMA encouraged the graduates, "I would like you to be aware of being a guardian of the digital world and play an active role responsible for the security of Japanese society at large".

Mr. KAJIYAMA encouraged the graduates in his video message.

Mr. AKIMA Kazuhei (right) (J-Power Telecommunication Service Co. Ltd.) received a certificate of completion from Dr. ENDO, Director General of ICSCoE

Address by Graduate

Ms. TAMADA Hikari,
NIPPON STEAL CORPORATION

As the representative of the fourth cohort, I have three things to talk about.

Firstly, I highly appreciate it letting me join this one-year-program even under the COVID-19 pandemic. I genuinely express my gratitude to all lecturers and staff members for their efforts, which committed to continuing the practical hands-on exercises only learned from the actual plants provided by the ICSCoE.

The trainees from the first to third cohorts had had overseas deployment exercises physically visited abroad though the trainees of the fourth cohort participated in all activities remotely. Nonetheless, these online exercises had some advantages of enabling us to look up unfamiliar English words and ask questions while attending the lectures offered by overseas experts. Since our hands-on exercises were connected online to the training environments abroad, we could carry out these exercises repetitively and deepen our understanding. We could experience fruitful learning from overseas activities without leaving Japan.

Secondly, I would like to mention communication among trainees. The ICSCoE incorporates many group work exercises in its curriculum, and the trainees pursue their careers in different specialized fields: such as IT and OT. We complemented our expertise and compensated for each of our weaknesses to tackle the training tasks. Since the trainees are from various industries, we could gather new insights from other colleagues and generate good outcomes. Through these group exercises, we could deepen our friendships and make many friends with whom we could talk about anything from our personal lives to business matters, regardless of industry or age.

Thirdly and finally, I would like to express our future aspirations. When I think of the opening ceremony held a year ago, I had little security knowledge. However, I have absorbed knowledge and skills of security through this program. Now I feel, "I want to learn more with my colleagues. I don't want to complete this program" in my heart of hearts. On the other hand, I have started finding many ambitions and challenges for security measures, which I desire to tackle proactively once returning to my company. I believe that every member of the fourth cohort feels the same way. What an encouraging thing it is! We, the fourth cohort, have valuable relationships with senior colleagues, lecturers, and experts we met at the ICSCoE. After returning to each company, we will continue to work on operations, with a strong sense of mission, seeking to enhance cybersecurity measures applied not limited to our industries but also social and industrial infrastructures. I truly appreciate all of your supports over the past year. Thank you very much.

Final Projects

46 trainees undertook 15 projects. We will introduce some of those projects serially in two volumes.

Enhance Security Levels of the Entire Supply Chain

Backgrounds and Issues

Today, enterprises have been facing pressures to consider security measures for not only their own company (contractors) but also the entire supply chain: such as clients and their business partners, affiliates, and group companies (buyers), to run a business. One of the project teams established this project for "enhancing security levels of the entire supply chain".

First, the project team held multiple study sessions to identify issues for this project and examine Government measures and guidelines for supply chains and support systems for small and medium-sized enterprises (SMEs).

Second, the team interviewed 15 organizations from five different categories: public institutions, universities, enterprise groups, supporting organizations, and SMEs, to become familiar with security measures for SMEs. As a result, the team identified the following seven issues:

1. Increase security awareness
2. Consolidate and disseminate security incident cases SMEs have been facing
3. Visualize security measures
4. Ease burdens of security education on supporting organizations
5. Utilize security experts
6. Derive benefits from security measures
7. Declare major corporations (buyers)

Issue-Solving and Outcomes

The project team created two evaluation frameworks for cybersecurity measures applied to supply chains while authoring some articles in the newsletters published by the Chamber of Commerce and Industry (CCI) to address their identified issues.

1. Authored Articles in the Chamber of Commerce and Industry Newsletter

With the aim of "raising the SMEs' security awareness level from zero to 0.1" in mind, the team interviewed the Chambers of Commerce and Industry in Osaka, Sapporo, and Nagoya, where the number of SMEs is high, to learn the actual circumstances of security measures taken by SMEs in each area. The team **took the issues faced by the companies, the readers of the CCI newsletters, into account and published two easy-to-understand articles on security.** We expect that these activities will contribute to improving security awareness among SMEs.


大阪ニュース　令和3年(2021年)7月10日　土曜日　(4)

セキュリティ! あなたの会社を守る <1>

サイバーセキュリティの第一歩
「守りたい資産を見つける」

独立行政法人情報処理推進機構 産業サイバーセキュリティセンター 研究主幹 八木 晴信

Appeared in the newsletter published by the Osaka Chamber of Commerce and Industry, "Daisho News" (July 10, 2021 issue)


専門家からの提案書

やってみましょう! セキュリティアクション!

村上 幸司

セキュリティ対策、何からやればいいの?

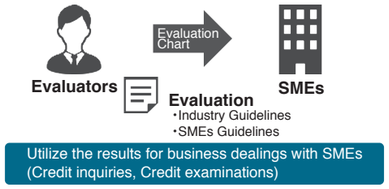
Appeared in the newsletter published by the Sapporo Chamber of Commerce and Industry, "Sapporo Economy" (July 2021 issue)

▶ **Website link to the newsletters published by the Osaka Chamber of Commerce and Industry, "Daisho News"**
https://www.osaka.cci.or.jp/index3-07.html

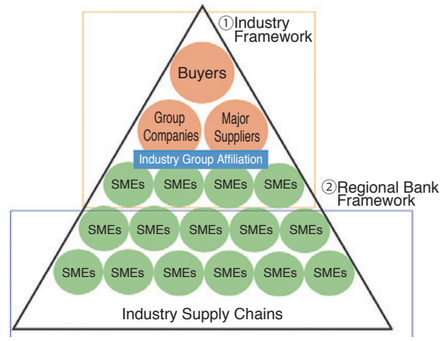
▶ **Website link to the newsletter published by the Sapporo Chamber of Commerce and Industry, "Sapporo Keizai"**
https://www.sapporo-cci.or.jp/web/public/index.html

2. Evaluation frameworks for cybersecurity measures applied to supply chains

The project team developed two frameworks, which allow third parties to evaluate the status of security measures for small and medium-sized enterprises (SMEs) using an evaluation chart and its results for business dealings with SMEs.



There are two types of frameworks: Industry Framework and Regional Bank Framework. The Industry Framework evaluates the status of enterprise security measures by the universal guidelines for each industry. We assume that buyers utilize this framework to appraise the credibility of SMEs. On the other hand, Regional Bank Framework allows regional banks, the closest advisors for SMEs, to use the SME guidelines and evaluate the status of enterprise security measures. We assume that the regional banks employ the evaluation results for credit examinations. The team introduced its framework to the Ministry of Economy, Trade and Industry and the financial industry and could receive their positive feedbacks.



Framework Overview

Furthermore, the project members established the "Supply Chain Cybersecurity Measures Subcommittee" within "Kanae-kai", an alumni community of the ICSCoE. They will leverage their connections among the ICSCoE alumni to continue their activities to promote these frameworks and raise the security awareness of SMEs.

Presentation of the Final Project Outcomes

Following the completion ceremony, the trainees presented the outcomes of four final projects in the same venue. One project team, who had developed a portable simulated plant installed in a suitcase seeking to raise on-site security awareness, assembled that plant and introduced its normal functions and educational scenarios. Another project team searching drone security and summarizing countermeasure plans demonstrated several mock attacks by flying a drone inside the venue and presented their findings on vulnerabilities and countermeasures facing drones.

Each team made their presentations highly realistic; thus, we believe that the graduates did prove their achievements of the year-long training program to the people from their dispatching companies and guests.

Demonstrated a portable simulated plant

Demonstrated the mock attacks by flying a drone in a tent

Interview with Graduates

From Left:
Mr. EMURA Yuki, NEC Corporation
Mr. YAGI Harunobu (Subleader)**,** Central Japan Railway Company
Mr. MURAKAMI Koji, (Leader), Hokkaido Electric Power Co., Inc.
Mr. KAWAI Koji, Electric Power Development Co., Ltd.

Interview with Mr. MURAKAMI, project leader

What is Your Utmost Benefit from the Project?

This project broadened my perspectives on supply chain cybersecurity. Since I could hear the diverse views of people from various positions, I can now see the supply chain cybersecurity through the viewpoints of both buyers and suppliers.

Methods for Utilizing Project Outcomes

I will engage in supply chain-related operations even after returning to my company. I believe I will be able to leverage the ideas defined in the "Industry Framework" as a basis in considering supply chain security measures.

This is Unique to the ICSCoE!

The ICSCoE provided me with great opportunities to visit a variety of business enterprises and organizations, including the Ministry of Economy, Trade and Industry, the Regional Bureaus of Economy, Trade and Industry, the Chambers of Commerce and Industry, on a short-term basis, and I could obtain lively information from them. I believe the ICSCoE is the only place providing me with such opportunities.