IPA Better Life with IT

ICSCoE REPORT
Industrial Cyber Security Center of Excellence
8.29.2025
vol. 22

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

OT Security Training Conducted for Practitioners from the ASEAN Countries

From July 21 to 23, 2025, an Operational Technology (OT) Security Training program was conducted in Bangkok, Thailand, in collaboration with the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC). The training targeted practitioners from government agencies and infrastructure-related organizations across the ASEAN countries.

AJCCBC
Operational Technology (OT) Security Training - (37th Training JI4&-wP17)
21st - 25th July 2025

OT Security Trainers and ICSCoE lecturers

As cyber-physical convergence rapidly accelerates in modern society, OT technologies—underpinning critical infrastructure such as energy, water, transportation, and manufacturing—are growing in importance. At the same time, the risk of cyberattacks targeting these systems is on the rise, making it imperative to enhance the skills of frontline personnel and strengthen cybersecurity and resilience across the region.
The training program was designed in response to these challenges, providing participants with a comprehensive learning experience covering both foundational knowledge and practical skills in OT security. A total of 18 participants from eight ASEAN countries—Thailand, the Philippines, Vietnam, Indonesia, Malaysia, Brunei, Cambodia, and Laos—took part in the three-day training, engaging in lectures and hands-on exercises to deepen their understanding of OT-specific risks and countermeasures.

Attack demo exercise using an OT environment simulation plant

The first day featured a keynote speech by Professor Youki Kadobayashi from the Nara Institute of Science and Technology (NAIST) and a lecturer at ICSCoE, who introduced initiatives and shared insights related to OT security human resource development in Japan. This was followed by a workshop featuring a simulated company scenario. Under the guidance of Professor Kadobayashi (NAIST), Professor Daisuke Miyamoto from the National Graduate Institute for Policy Studies (GRIPS), and lecturers from Mahidol University in Thailand, participants actively exchanged views, discussing challenges and best practices across their respective countries and sectors.
On the second and third days, participants took part in hands-on training sessions using tools and scenarios simulating real OT environments. Led by ICSCoE instructors—Assoc. Professor Takuho Mitsunaga, Asst. Professor Satoshi Okada, and Lecturer Koki Watarai from Toyo University—participants observed attack demonstrations and incident response simulations, gaining practical knowledge and strengthening their response capabilities.
Feedback from participants was highly positive, with comments such as, "The hands-on exercises were very practical and meaningful," and "Discussions with participants from other countries offered new perspectives." The effectiveness of the training was widely recognized.
The Government of Japan established the ASEAN-Japan Cybersecurity Capacity Building Centre in 2018 to provide training programs in collaboration with the ASEAN Secretariat and the Government of Thailand, with the aim of strengthening cybersecurity capabilities across the region. Through practical training, including cyber defense exercises, the Centre continues to promote human resource development and knowledge sharing throughout the ASEAN region.
ICSCoE is committed to supporting the enhancement of OT security and the sustainable development of human resources in the ASEAN region, which maintains strong economic ties with Japan. Moving forward, it will continue its efforts in capacity building and information sharing.

Exhibiting at “Interop Tokyo 2025”

Cross-Industry Bonds Turn into Strength: ICSCoE Graduates Thriving on the Frontlines

In June 2025, "Interop Tokyo 2025" took place, and the instructors and graduates of the Core Human Resource Development Program delivered their presentations at the IPA/ICSCoE booth.

Advancing Security Education Across the Financial Sector

In the presentation “SECURITY ASSEMBEL - The Training Was the Beginning of the Journey…! A Chronicle of the Challenges Faced by the Third Cohort of the ICSCoE Graduates Back in the Field,” four graduates discussed buidling mutual support over five-year following program completion.

Mr. TANAKA Katsuyuki of Japan Post Insurance System Solutions Co., Ltd. has played a central role in both educational and operational perspectives by establishing the SOC office, responsible for the businesses of Japan Post Insurance, and the Cybersecurity Office for in-house CSIRT.

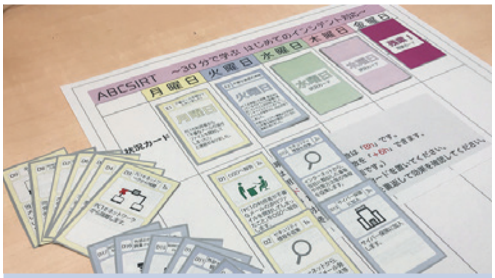
Mr. TANAKA introduced the deployment of an educational tool named “ABCSERT,” created through the final project created by third cohort member, within the financial sector. ABCSERT is a tool allowing users to learn security incident response in a card game format. The content of its card game is practically oriented, enabling users to prioritize incident responses within a limited timeframe based on a fictional bank scenario.

With frequent personnel rotations in financial institutions, this tool is useful for personnel to picture operations without prior experience. Financials ISAC Japan has deployed the tool industry-wide, and Mr. TANAKA created five scenarios relevant to the financial industry: Advanced Persistent Threat Attacks, DDoS, and Phishing, for the next five years. In 2024, Mr. TANAKA received the “Financials ISAC Award.”

Recalling his experience in the Core Human Resource Development Program, Mr. TANAKA said, “This program was extremely valuable for both trainees and their dispatching enterprises. It trained us to deliver an output promptly in response to challenges, a mindset I still carry today. Although the program description emphasizes ‘technical skills spanning both operational skills (OT) and information skills (IT),’ enterprises lacking OT might assume the program is irrelevant to them. However, they will encounter business situations to apply OT knowledge to the workplace someday.”

Mr. TANAKA’s words conveyed a strong sense of mission: we will continue to contribute to the financial industry, and together with other cohorts, help strengthen cybersecurity throughout Japan’s critical infrastructure sectors.

Mr. TANAKA Katsuyuki (3rd cohort)
Japan Post Insurance System Solutions Co., LTD.



CSIRTの業務をゲーム形式で体験・学習するツール。

目的

・インシデント発生時のCSIRTの活動を理解する。
・限られたリソースの中で対応を迫られる状況を体験する。

詳しくは▶ IPA ABCSIRT

ABCSIRT - created by 3rd cohort member as the final project

Addressing ASM Implementation Challenges Through Cross-Industry Collaboration

Mr. SAKATA Naoshi of TOPPAN Holdings Inc. has currently overseen Attack Surface Management (ASM), Threat Intelligence, Factory Security, and the Computer Emergency Response Team (CERT).

His final project at the ICSCoE was "Application of Cyber Threat Intelligence." Mr. SAKATA immediately established an OSINT team to collect and analyze publicly available information and launched ASM activities by leveraging his expertise upon returning to his enterprise.

Mr. SAKATA said, “I joined the program in my second year of security experience, but I obtained fundamental skills that I could immediately apply.” Also, he emphasized,” the greatest value I gained from the ICSCoE was the bonds I built. I understand the colleagues’ personalities through the one-year training, enabling me to continue having genuine, meaningful conversations.”

We can see a clear example of the bonds in the case study introduced by Mr. SAKATA, presenting the introduction of the ASM made possible through

Mr. SAKATA Naoshi (3rd cohort)
TOPPAN Holdings Inc.

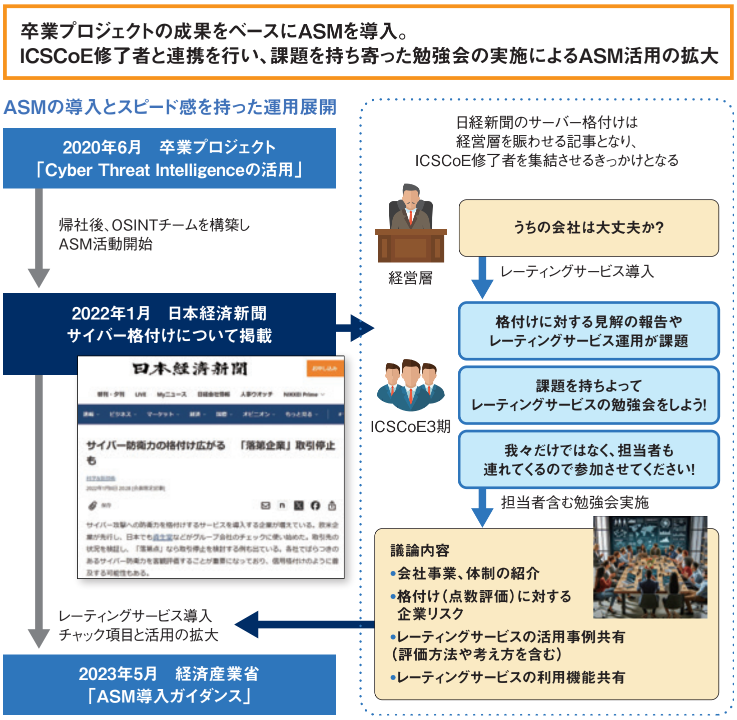
collaboration among the graduates.

Back then, many companies were struggling with rating requirements, asking, “How to report our rating assessments to the management?” or “We have implemented rating services, but how to utilize them?” Therefore, Mr. SAKATA organized study sessions together with his colleagues to address these concerns. The graduates from various industries gathered for the study sessions, fostering extensive discussions by involving representatives and supervisors from enterprises.

Mr. SAKATA recalls, “When we shared our insights, the challenges we faced were similar even across different industries.

Based on the insights gained from these study sessions, Mr. Sakata significantly expanded the ASM application within the TOPPAN Group. Today, he provides year-round remedial guidance and support targeting 136 out of 264 group companies that manage corporate domains. Mr. Sakata also implemented a certification system, which integrated ASM and audit for contractors handling personal information and confidential information protected under the Economic Security Act.

Today, the graduates conduct cross-industry study sessions on diverse themes, collaborating beyond the ICSCoE cohorts and industry boundaries to explore solutions for shared challenges.


卒業プロジェクトの成果をベースにASMを導入。
ICSCoE修了者と連携を行い、課題を持ち寄った勉強会の実施によるASM活用の拡大

ASMの導入とスピード感を持った運用展開

2020年6月　卒業プロジェクト
「Cyber Threat Intelligenceの活用」

帰社後、OSINTチームを構築し
ASM活動開始

2022年1月　日本経済新聞
サイバー格付けについて掲載

レーティングサービス導入
チャック項目と活用の拡大

2023年5月　経済産業省
「ASM導入ガイダンス」

日経新聞のサーバー格付けは
経営層を賑わせる記事となり、
ICSCoE修了者を集結させるきっかけとなる

うちの会社は大丈夫か?

レーティングサービス導入

格付けに対する見解の報告や
レーティングサービス運用が課題

課題を持ちよって
レーティングサービスの勉強会をしよう!

我々だけではなく、担当者も
連れてくるので参加させてください!

担当者含む勉強会実施

議論内容
- 会社事業、体制の紹介
- 格付け（点数評価）に対する企業リスク
- レーティングサービスの活用事例共有（評価方法や考え方を含む）
- レーティングサービスの利用機能共有

Training achievement, alumni collaboration, and ASM implementation

Developing a Portable Simulated Plant to Expand Human Resources for OT Security Across Japan

Mr. MEGURO Yuki
Industrial Cyber Security Center of Excellence
Information-technology Promotion Agency, Japan

Mr. MEGURO Yuki, an instructor of the Core Human Resource Development Program, has been leading the security exercises for OT systems since the establishment of the ICSCoE. He is also a practitioner at Toinx Co., Ltd., who engages in penetration testing, risk assessments, and security training for control systems. Under the practical, educational policy of “Identifying security risks from the attackers’ perspective,” he has guided numerous graduates into the field.

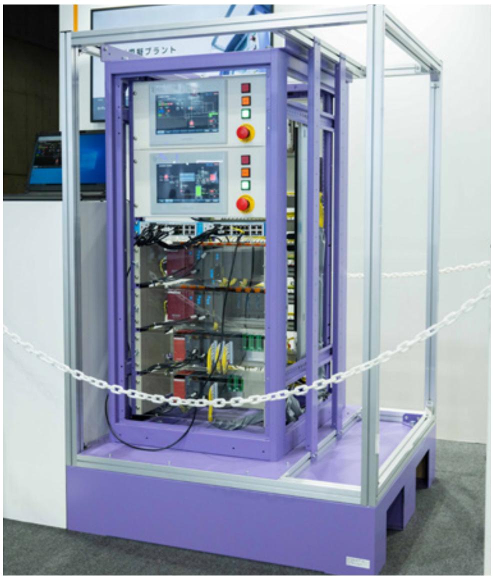
In addition to the Core Human Resource Development Program, the ICSCoE offers cybersecurity training for control systems using the simulated plants in Akihabara, Tokyo. However, companies based far from Tokyo, the distance posed a significant burden, often discouraging them from developing as many cybersecurity professionals as they would like.

To overcome these challenges, Mr. MEGURO introduced a “portable simulated plant,” a new educational tool that enables OT security training anywhere in Japan. The model is based on a power plant with two 2,500 kW generators. Although it is the size of a standard server rack, it incorporates actual devices, such as PLCs, providing functionality equal to or even greater than conventional simulated plants.

Mr. MEGURO has developed twelve scenarios based on real-world cyberattacks. Through hands-on exercises with actual equipment, participants learn how attackers exploit control system vulnerabilities to trigger power outages or manipulate operations, while gaining insights into the defensive measures required. After an exercise held at a Nagoya-based company in March 2025, participants remarked, “I realized how we can easily hack systems and gain valuable insights from attackers’ perspectives,” and "Using actual equipment made the exercise far more authentic.”

In March 2025, IPA publicly showcased the portable simulated plant for the first time. Mr. MEGURO commented, “I hope more people will become aware that these resources can be used in regions far from Tokyo.”

Looking ahead, Mr. MEGURO envisions diverse for the training: attack detection and log analysis for blue teams, penetration testing skills for red teams, practical attack-defense exercises for purple teams, and threat awareness training for managers and field staff.


The portable simulated plant

8th Core Human Resource Development Program Graduation Ceremony

In June 2025, the Industrial Cyber Security Center of Excellence held the graduation ceremony for the 8th Core Human Resource Development Program. Fifty-seven trainees have successfully completed the one-year program and are now taking their next steps as industrial cybersecurity experts.

A Graduate Representative Greeting

> **“The most meaningful aspect of this past year was the connections among the fellow trainees. Over the past year, I have gained a deep appreciation: I cannot accomplish effective cybersecurity alone.”**

Mr. ASAKURA Daichi
Nagoya Railroad Co., Ltd.

All fifty-seven members of the eighth cohort have completed the program, appreciating the dedicated support of our instructors, lecturers, administrative staff members, the Ministry of Economy, Trade and Industry, and our dispatching enterprises. We sincerely appreciate each one of you who stood by us throughout this journey.

Looking back on the past year, I am struck by how rich and intense this journey has been. At the opening ceremony a year ago, we received an encouraging message: we will grow into professionals to contribute as industrial cybersecurity experts, not only within our enterprises, but across industries, the nation, and even on the global stage when completing the program. I remember feeling excited but uncertain if I could rise to such expectations.

Some colleagues began the program without strong experience in the cybersecurity field; however, we have built the knowledge and skills expected of the core human resources through basic training, hands-on exercises, and overseas deployment exercises. Since April, we have tackled the final project, focusing on the issues enterprises face and the challenges discovered during the lectures and exercises. Some teams focused on trending subjects, such as generative AI and digital transformation (DX), while others continuously input data into generative AI and created illustrations, texts, and videos, incorporating them into their outcomes. Therefore, we all successfully delivered meaningful results.

Throughout the program, the instructors and trainers recognized our enthusiasm for learning and responded with exceptional dedication. They also coordinated meetings with external experts and relevant stakeholders to deepen our insights when necessary.

The most meaningful aspect of this past year was the connections among the fellow trainees. I gained valuable experience to discuss in depth with them beyond generational and corporate boundaries; thus, I look forward to continuing to foster these relationships in the years ahead.

Over the past year, I have gained a deep appreciation: I cannot accomplish effective cybersecurity alone. Together with the colleagues I met through this program, I will strive to contribute to the development of industries by strengthening cybersecurity. I will also bring the knowledge and skills that I have gained throughout this year back to my dispatching enterprise and integrate them into my work after returning. Thank you again very much.

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

R60 古紙パルプ配合率60%再生紙を使用

リサイクル適性Ⓐ
この印刷物は、印刷用の紙へリサイクルできます。