IPA Better Life with IT

Industrial Cyber Security Center of Excellence ICSCoE

ICSCoE REPORT

Industrial Cyber Security Center of Excellence

5.23.2024

vol. 19

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

Mr. SAITO Ken, Minister of Economy, Trade and Industry Visited the ICSCoE Akihabara Training Facility

In February 2024, Mr. Saito, Minister of Economy, Trade and Industry, visited the ICSCoE Akihabara training facility. Trainees of the Core Human Resource Development Program from various industries created cybersecurity scenarios that could occur in their industries and demonstrated cyberattacks for the Minister as part of their advanced level training.

Cyberattack demonstration targeting the control systems conducted by the trainees

The trainees presented and explained how attacks will impact and cause damages, also effective ways to prevent attacks from the attackers' point of view which were discussed in their active learning. Minister Saito asked in-depth questions regarding the actual attacks on control systems and expressed concern about the security risks posed by these systems. Minister Saito also inquired about various issues during the discussion, such as abilities of trainees after completing the year-long ICSCoE training, the time and cost required for human resource development, and the activities of ICSCoE graduates. He emphasized the signeficance of the ICSCoE's role in promoting the development of security personnel.

Minister Saito emphasized the importance of security personnel training during the discussion

Wide-area video distribution experiment using ultrahigh-definition video

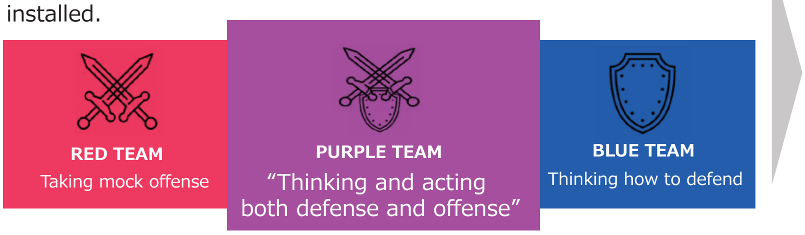
In February 2024, the IPA security penetration testing team consisting of graduates, current trainees, and lecturers of ICSCoE participated in "Demonstration Experiment of Wide-area Video Distribution using ultrahigh-definition video" organized by the National Institute of Information and Communications Technology (NICT)

This year's testing marks our sixth consecutive year of participation since 2019. We interviewed the team leader, Mr. Inoue about the key points of it.

Mr. INOUE Yuji (2nd cohort)

■What is a Purple team testing?

In Purple team testing, the tester always keeps in mind that "where can we break the conditions of a particular cyberattack" in order to develop and execute a test plan, and simultaneously evaluate the detection/protection status with the security products that have been installed.



RED TEAM
Taking mock offense

PURPLE TEAM
"Thinking and acting both defense and offense"

BLUE TEAM
Thinking how to defend

Purpose and Benefits

- ➢ Easier to identify which security measures are most realistic and effective
- ➢ Easier for system owners to know what and how to take measures
- ➢ Easier to envision a series of incident responses

This year, we performed penetration testing on the latest video transmission technology, control devices, and backbone networks, which will be the industry standards in the future. Until last year, we have gone ahead separately by the red team on the offensive side and the blue team on the defensive side. This year, we finally introduced the concept of "Purple team testing", in which members always consider in the point of view both the offense and defense sides in one team.

In the Purple team testing, we could involve some companies in the Broadcasting industry (business owners) and system owners (such as System Integrators). We discussed various issues as one team. Although there have not been many cases of implementing the purple team testing in video streaming and broadcasting field, we believe that the penetration test should not be divided into offense and defense but be consolidated. At this time, for example, when considering a scenario in which a malicious third party attacked the business, we can examine the impact on the business if such a scenario were to occur, and what countermeasures we should take to prevent the conditions under which the scenario could take place. We believe that the three parties working together allowed us to achieve more precise verifications. Our activity extended beyond the tabletop exercise; we reproduced and demonstrated various scenarios, which resulted in more in-depth discussions.

In addition, to ensure higher quality discussions, we have refined the scenarios for this year. Through the careful examination of the scenarios that would have the biggest impact on the industry, the three parties were able to actively exchange opinions from their respective viewpoints, engage in thorough discussions, and ultimately reach a conclusion that was satisfactory to all parties. We believe that we were able to achieve the results that only the Purple team can provide. The main benefit of this testing was that we were able to confirm the cyber risk scenarios that concerned both business and system owners are the same as the perspectives we had envisioned.

This is my sixth year participating in this experiment. My motivation is not only to improve my own knowledge, but also to reciprocate to the Telecommunication industry and the ICSCoE lecturers who have been a tremendously helpful to me. In the past few years, I have witnessed the trainees who have participated in the experiment have made great progress, and their progress influenced and motivated the graduates and lectures of the ICSCoE. When you join the experiment, everyone may struggle with their abilities at first. However, with a common understanding of the issues, and working together as a team, their abilities will improve over time. This year, we gave business owners the opportunity to experience the risk scenarios we have developed and explained how the demonstration worked. I saw their eyes sparkled in response, which is only possible at the ICSCoE.

Finally, I would like to appreciate the purple team members for agreeing to the purpose despite our short notice of the request and actively participated in the lengthy discussions. I feel that the purple team testing was a great success because everyone on the team put in a lot of effort. I am really grateful and would like to take this opportunity to express my gratitude.

The participants implemented the verification of various security vulnerabilities against video control devices and network equipment, including video distribution/ emerging technologies in the broadcasting field.
(Participation: 4 days from Feb. 5th to 8th (32 hours per person))

ICSCoE-related Personnel Participated in the Largest OT Security Conference in Japan

CIP
重要インフラ
サイバーセキュリティコンファレンス
ICS
産業
サイバーセキュリティコンファレンス

Lots of personnel engaging in OT systems partook

In February 2024, "the 8th Critical Infrastructure Cybersecurity Conference and the 5th Industrial Cybersecurity Conference" were held in person at the Tokyo Conference Center Shinagawa and in a webinar in which many ICSCoE-related personnel, such as the alumni of the Core Human Resource Development Program, participated.

During the panel discussion entitled Cybersecurity Ecosystem/ Establishment of Inter-organizational Collaboration ～ Deciphering from the Development of Local Communities ～ Mr. MEGURO Yuki, a lecturer of our Core Human Resource Development Program, and Mr. HASEGAWA Hiroyuki, an alumni of the second cohort of the program, served as a panelist and facilitator, respectively.

Throughout the discussion, each participant expressed an enthusiasm for local activities: the importance of fostering human resources that function in virtuous cycles within each region and organization and the necessity of tackling human resource development as a whole community, not enterprise alone, to enhance cybersecurity measures.

Mr. MEGURO Yuki
Lecturer of the Core Human Resource Development Program

When raising the nature of local communities among the attendants, Mr. MEGURO stated, "The center of establishing the communities is participants, not community managers. We should determine how to ensure personnel who engage in our community and collaborate with them." Based on his experience keep the community activities, he also explained the difficulty and importance of continuing the communities while considering the generation change of the position to lead.

Mr. HASEGAWA Hiroyuki (2nd cohort)
Chubu Electric Power Grid Co., Inc.

At the end of the session, Mr. HASEGAWA concluded, "I could reaffirm communities are effective in connecting between organizations." He respected the passion of the personnel operating communities while addressing, "I strongly recommend you to refer our discussion and cases if you want to participate in communities and even establish your community."

Mr. HASEGAWA closed the session while wishing for the realization of intensifying future community activities.

Introducing our Short-term Programs the ICSCoE Provides

The Industrial Cyber Security Center of Excellence, ICSCoE, provides the audience with programs to acquire skills and knowledge of cybersecurity measures essential to protect organizations in a short time that we conduct numerous times a year. We are introducing two programs we held in January and February 2024.

Cyber Security Planning Exercise for Managers (CyberSPEX)

The Cyber Security Planning and Exercise (CyberSPEX) program was held over four days in January and February 2024. This program was newly established in FY2023 and was attended mainly by managers from companies and organizations involved in social and industrial infrastructure.

In this program, participants learned the knowledge required of those in charge of cyber security and business continuity. They then put this knowledge to use in a security strategy planning exercise. As a result, they acquire the skills necessary to promote cyber security (such as systems, budgets, and policies) and learn how to think and use logical thinking to persuade management.

In the team-based exercises, participants carried out a series of simulated tasks, from creating a proposal to persuading the board of directors (played by the instructor). Participants fully used their know-how and worked to improve their skills through active learning.

In the network-building session after the exercises, the participants actively communicated with each other in a friendly atmosphere to share their experiences.

A photo of the simulated board meeting in CyberSPEX

Cyber Crisis Response Tabletop Exercise for Managers (CyberCREST)

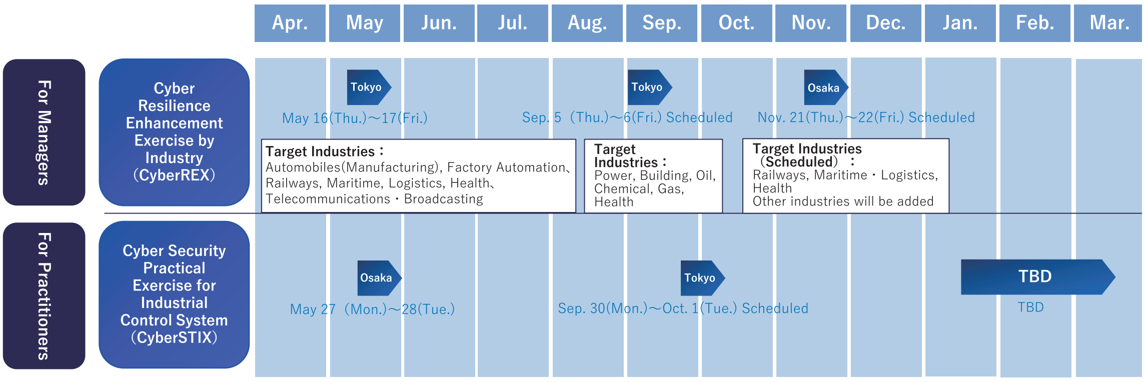
The ICSCoE conducted the Cyber Crisis Response Tabletop Exercise, CyberCREST, for a total of three days in January and February 2024. Its participants were the responsible officials from the enterprises expanding supply chains in Japan and overseas and the companies and organizations possessing OT systems.

In this program, participants can learn strategies and techniques possessed by cyber attackers targeting industrial control systems, trends and measures of cyber threats envisioned from a geopolitical point of view, and impacts on cybersecurity when utilizing rapidly growing generative AI. They can also absorb practical skills to enhance enterprise adaptability and resilience against cyber attacks.

On the last day of this program, the participants implemented our tabletop exercise with a scenar io envisioning a cyber attack occurring. To practice what they had learned through the CyberCREST, the participants examined countermeasures just like an actual stage, and each of them presented decision-making and approaches, which responsive officials should do.

The image of the tabletop exercise in the CyberCREST

FY2024 Annual Schedule of Short-term Programs as of May 2024



Cyber Resilience Enhancement Exercise by Industry (CyberREX)

Tokyo May 16(Thu.)～17(Fri.)

Target Industries：Automobiles(Manufacturing), Factory Automation、Railways, Maritime, Logistics, Health、Telecommunications・Broadcasting

Tokyo Sep. 5 (Thu.)～6(Fri.) Scheduled

Target Industries：Power, Building, Oil, Chemical, Gas, Health

Osaka Nov. 21(Thu.)～22(Fri.) Scheduled

Target Industries (Scheduled)：Railways, Maritime・Logistics, Health
Other industries will be added

Cyber Security Practical Exercise for Industrial Control System (CyberSTIX)

Osaka May 27 (Mon.)～28(Tue.)

Tokyo Sep. 30(Mon.)～Oct. 1(Tue.) Scheduled

TBD

TBD

※ We will announce the dates of other short-term programs once we have decided.

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

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。