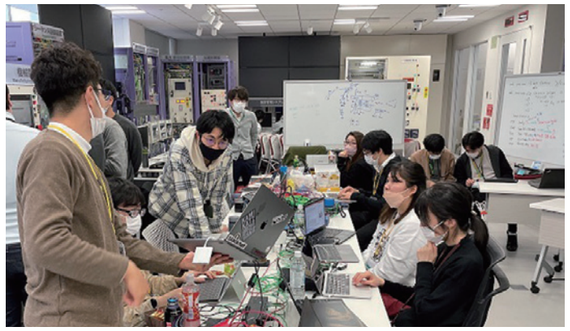
Challenges to Penetration Testing for the Next Generation Broadcasting Technologies

In February 2023, the National Institute of Information and Communications Technology (NICT) held a "Demonstration Experiment of Wide-Area Video Distribution Using Ultrahigh-Definition Video" realized by bringing technologies, human resources, and equipment of approximately 70 organizations from industrial, governmental, and academic fields. The graduates and trainees of the Core Human Resource Development Program (ICSCoE) formed a penetration testing (hereinafter called "Testing") team and participated in this experiment. We interviewed the team leader and members about the demonstration experiment this year, which we have attended for five consecutive years.



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: 5 days from Feb. 5 to 10 (40 hours per person))

■ Leader

Mr. INOUE Yuji
(2nd cohort graduate)

Our team challenged the penetration testing for IP remote production - the next-generation broadcasting technologies - and the 400Gbps-based IP video transmitting backbone. We tackled Testing this year by considering quality more than quantity. For example, we reduced the number of Testing scenarios from 81 last year to 29 this year. This was because we wanted to keep much more time for discussing each Testing item within the team carefully. Finally, we could understand the result and mechanisms of some new technologies (e.g., NMOS) much deeper than last year.

Moreover, the IP production team members, who had built the video transmitting environment, and the Testing team could bring each insight and keep the time for exchanging remarks. Broadcasters and testers have different concerns; thus, by sharing them, each team could find an opportunity to recognize issues only one party cannot think of.

From my point of view, the trainees of the sixth cohort participated in the penetration testing after fumblingly studying how to conduct the Testing beforehand. Their proactive attitudes were fantastic.

■ Member

Mr. YOSHIHARA Naofumi
(6th cohort trainee)
Japan Broadcasting Corporation

I had always wanted to undertake security for video transmission; therefore, I built its environment and learned the Testing techniques. In addition, I felt the significance of penetration testing utilizing emerging technologies (e.g., IP remote production) and broadband; thus, I decided to participate in this demonstration experiment. When I received the pre-briefing by Mr. INOUE, I felt "I do not just participate in the Testing but learn it more." As a result, I held a study session with other trainees and challenged the experiment.

On the day of penetration testing, many professionals – the graduates of the ICSCoE, lecturers, and experts from video transmission and broadcasting industries, attended the experiment, and the penetration testing was very high-level I had never experienced before. Especially the graduates shared their insights into the philosophy of Testing not limited to the broadcasting industry and the concrete procedures on how to proceed with the Testing.

The broadcasting industry has a mission, "broadcasting videos stably." Therefore, it was beneficial for me to gain the opportunity to find our issues from the Testing. I would love to participate in future events and challenge to understand the Testing protocols I did not handle this time and verify security measures based on the Testing results.

NICT "Demonstration Experiment of Wide-Area Video Distribution Using Ultrahigh-Definition Video (In Japanese)"
https://testbed.nict.go.jp/event_new/yukimatsuri2023.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 Industrial Cyber Security Center of Excellence

ICSCoE REPORT

3.31.2023

vol. 15

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

Minister of Economy, Trade and Industry NISHIMURA Yasutoshi Visited the ICSCoE Exercise Facility.

Minister NISHIMURA had a briefing on the simulated plants.

In February 2023, Minister of Economy, Trade and Industry NISHIMURA visited our ICSCoE exercise facility in Akihabara. During this visit, our instructor utilized our plant, which simulates control systems for critical infrastructures, to demonstrate potential cyber attacks and explain the possible consequences and damages caused by these attacks.

During the dialogue session, Minister NISHIMURA questioned the actual situation of cybersecurity measures and the ICSCoE's human resource development projects and expressed his considerable concerns and awareness of cybersecurity-related issues.

Graduates of the Core Human Resource Development Program Participated in Japan's Largest OT Security Conferences

In February 2023, "the 7th Critical Infrastructure Cybersecurity Conference & the 4th Industrial Cybersecurity Conference" were held online, and eight graduates from the "Kanae-kai," the graduate community of the ICSCoE, participated as special supporters.

During the keynote lecture, Deputy Director General UEMURA introduced the ICSCoE and cited the development of security personnel as a critical issue to secure safety in cyberspace. He also articulated the purposes of the ICSCoE, "It has been setting not only its one-year course but also short-term programs and promoting the development of human resources and provision of up-to-date information." In addition, Mr. UEMURA described the graduates who join the Kanae-kai as they share a firm bond of trust since they have perceptions of the same challenges and objectives. He concluded that he would aim together to promote security.

Mr. UEMURA Masahiro
Deputy Director-General for Cybersecurity and Information Technology
Ministry of Economy, Trade and Industry

修了者によるパネルディスカッション

The graduates who participated in the conferences disseminated their insights by setting the theme of challenges and measures related to security, examples of in-house human resource development, and the paradigm for communication that the security department must have.

The graduates of the 5th cohort participated in the conferences (Mr. KUROKI, Mr. TAHARA, and Mr. FURUSAWA, from left)

Please see the following page for the interviews with graduates participating in the conferences.

Interview with A Graduate | Applying Experience Derived from the ICSCoE at Cybersecurity Sites

In “the 7th Critical Infrastructure Cybersecurity Conference & the 4th Industrial Cybersecurity Conference,” many graduates from the IPA ICSCoE and interested parties participated. We interviewed Mr. SATO, the second cohort, and Mr. YUASA, the third cohort, from the graduates participating in the lectures and panel discussions regarding their activities conducted through the Core Human Resource Development Program and their current careers.

"Three Deliverables" Derived from Participating in the ICSCoE

Mr. SATO Yoshinori
(2nd cohort graduate)

Manager, IT Promotion Department
Mori Building Co., Ltd.

Please tell us your current tasks and motivation for participating in the ICSCoE.

I have been affiliated with the Information System Department for 20 years and am currently a member of the security group of the IT Promotion Department. I used to be responsible for groupware. But I became in charge of the project of web infrastructure integration: It was a trigger to join the Core Human Resource Development Program to deepen security insights for IT and OT (building systems).

During participating in the ICSCoE, what activities did you engage in?

Since my participation in the ICSCoE duplicated the disclosure dates of the building security guidelines published by the Ministry of Economy, Trade and Industry (METI), I joined the working group for guideline establishment within the METI while submitting public comments. As guidelines tend to express abstractly, we created the manual for these guidelines categorizing by measure, contributed them to industrial journals, and gave external seminars to explain their contents in an easy-to-understand manner.

What is the philosophy for securing cybersecurity your company has?

We initiated the concept, moving toward "Cities to escape to, rather than flee from." and upheld the vision for comprehensive disaster countermeasures: earthquake-proof structures and disaster preparedness. We apprehend that cybersecurity is part of them.

Security risks under building construction and urban development will not stop with damage to facilities but be fatal to human lives. Moreover, I believe protecting information is the mission of building companies.

What insights could you obtain from the ICSCoE activities?

Of course, I could gain technical skills and knowledge in addition produce three main outcomes.

The first outcome is “networking.” I built personal connections among trainees and various networks with lecturers and external agencies, including foreign authorities; therefore, I have the good fortune of collecting and disseminating information by using these networks.

The second outcome is “trend understanding,” from which I understood domestic trends and the policies and attitudes (philosophy) of various nations from my experiences derived through overseas exercises. I can proactively plan by keeping myself open to emerging trends.

The third outcome is “management perspectives.” I learned methodologies for developing strategies to advance in-house measures/ procedures and techniques for explaining to management. This outcome enables me to illustrate the adequacy of urgently required countermeasures and costs; therefore, I can utilize the enterprise standpoints of cyber risks as an enterprise for developing security policies.

It was very fruitful for me and the enterprise that I could produce the above three outcomes; therefore, I want others considering participating in the program to use them as references.

Cardinal Rules of Disseminating Security Is “Visiting Field Sites.”

Mr. YUASA Takuma
(3rd cohort graduate)

Chief, Security Group
IT Digital Promotion Department, Cybersecurity Division
Toyota Industries Corporation

Please tell us your story about getting engaged in the security field.

I joined the enterprise as a new hire in 2015 and was appointed to the Information System Department. In my second year, the enterprise transferred me to the IT subsidiary. The company offered me the ICSCoE program, and I willingly consented. The enterprise also planned to order me an overseas assignment. However, I chose to become a cybersecurity professional since I might have an opportunity for overseas posting later. I believe I made a good decision.

Why did you choose to be a security professional?

I always like security technologies. Security is like a puzzle-solving of offense and defense – we examine where others will attack from the defenders’ perspectives; on the other hand, we explore where others have security holes from the offenders’ perspectives. Security is similar to the games in which we use our brains strategically.

What are the characteristics of and challenges for securing cybersecurity in your company?

Since my company is a part of the Toyota group, we have crucial responsibilities to protect the fundamentals of Japan’s economy. Handling technology information as a manufacturer is very sensitive. First, we have a cardinal rule, “Do not stop our factories.” Under the furious advancement of IoT, our operations and data environments have also been changing more and more; however, we do not have enough referenced cases or information regarding the security of factories equipped with cutting-edge IoT. Under these circumstances, obtaining hands-on experience is the highest priority issue.

When I returned from the ICSCoE, remote working expanded rapidly due to the COVID-19 pandemic. We had already prepared the remote environment; however, we faced the issue of developing a secure environment tolerating the rapidly increasing number of connections. Moreover, we poorly understood factory security. Therefore, we struggled with implementing and migrating equipment.

What kind of efforts did you launch, indeed?

I disseminated security measures to factories. Although we have the guidelines for factory security published by the government and these in-house manuals, we needed the summaries to instill security in field operators. I developed the strategies since there would be no solutions by filing a one-way notice to our colleagues.

Our first strategy was to create the cards for security incident exercises enabling us to practice specifically predictable incidents and these measures with several people. I received approval from the enterprise; thus, I conducted this card exercise at each site.

The ICSCoE’s final project triggered this card game. In our project, we created a card game as a training tool for new CSIRTs. I contemplated that this card game might develop incident responses and raise our security awareness if we conducted a tabletop exercise utilizing these cards for factory security. However, I could not find off-the-shelf exercise satisfying our needs, so I made the card game for my company. It led to the efforts within the enterprise.

The outcomes produced from the final project.

What do you keep in mind when putting into practice?

I tried to “visit our field sites.” The veterans finally endorsed a request from the headquarters by having a heart-to-heart conversation with them. The enterprise has been proceeding to standardize equipment and facilities; however, there are unique issues factories have. I cannot convey my intentions and understand the problems our sites face through online meetings. I keep in mind to develop empathy by visiting field sites and communicating with the operators many times.

The effects of the table top exercise using the cards created for Toyota Industries Corporation

The card-based training tool, developed in light of the experience derived from the ICSCoE’s final project, enables us to understand the points necessary for factory security. Mr. YUASA designed this training tool to understand the voices from sites and pleasantly learn know-how from planning to implementing exercises through the improvement in incident response abilities of field personnel, communications during training, and implementation reports.