from the previous page

ICSCoE Members

members can bring back the techniques and knowledge they got through these tests to each company. This was our prime motivation. We had a precious opportunity to conduct nearly-real penetration testing in advanced environments using some multicasting techniques. Through these efforts, we can collaborate with people from different industries and improve our knowledge while sharing information with colleagues in a setting where are no need to consider the budget of each enterprise.

—— Are there any key findings about a new vulnerability through the activity of this year?

There was no critical vulnerability unique to 400Gbps image transmission. However, we found that we could face the impacts on backbone availability very easily, caused by a few malicious packets or techniques, even though we have built state-of-the-art network infrastructures like 400Gbps.

Besides, we found some issues with the new standards, NMOS. We found there were some risks, which led to unintended behaviors with the video aggregation system caused by malicious codes. It is because NMOS is the "widely open" standards for interoperability, which utilizes Web and API mechanisms in order to control video equipment.

Our stacked efforts through these four years are that we could cover impressive penetration techniques for many protocols and communication methods used in the broadcasting industry. We have conducted 150 test scenarios in total for four years...!!

—— When we hear about organizing the security team, I think a hierarchical command structure, like a pyramid, would be suitable. What do you think?

When it comes to the penetration testing team, I believe it works better away from a hierarchical command structure. We have been autonomous-decentralized structure where each member makes decisions about his/her next action and acts independently. Especially I focus on this way as the organizer because we have members with various motivations for penetration tests, such as not only just interests in image transmission but also our willingness to try advanced penetration testing against state-of-the-art technologies of broadcasting systems, for further development. The ICSCoE offers lectures regarding penetration testing, and we feel free to plan, design, discuss, and conduct the verifications under the instruction of Professor KOBAYASHI Kazumasa's team. Basically, we call for broad participation from experienced to younger trainees under a "gather round" system. That's why I expect the member who has interested in expanding his/her skill or knowledge will come in spontaneously.

—— Please tell us your future plan.

We will appropriately provide feedback to the engineers who offered equipment and coorpetation for our demonstration experiments this year. We will challenge new technologies and techniques without changing basic stances in the coming year and beyond. We are eager to provide feedback on the outcomes of our efforts possible only by the ICSCoE, which gathers people with diverse expertise and backgrounds and advocates fostering white hackers.

I have a dream that broadcasting technologies and user experience will enhance dramatically by being integrated with IP network technologies near future; Of course, it is secure by design. We think it is important that both attackers (red team) and defenders (blue team) can put their heads together, discuss issues, and draw up strategies about how to identify risks and how to face them. That's why we would like to continue these activities in the future.

☞ **Please visit our website for more information on our demonstration experiments this time.**
"The World's First Successful 400Gbps Network Connection Between Multiple Organizations and Penetration Testing on Video over IP"
https://www.ipa.go.jp/icscoe/english/news/news20220426.html

Message from Deputy Director General of the ICSCoE

I am KAKEGAWA, appointed Vice Director of the Industrial Cyber Security Center of Excellence, effective in July 2021.

The strength of this center is, I believe, the Core Human Resource Development Program, through which trainees can practically learn cybersecurity from the lecturers, who have engaged in this field for years.

This program is not a place to only absorb knowledge and skills but to develop a thorough understanding of cybersecurity from its background. We provide our trainees with opportunities to acquire abilities to update information and keep working on cybersecurity measures even after returning to each dispatching company. Besides, trainees collaborate with their colleagues from various industries and engage in lots of tasks enabling them to develop the competence to respond flexibly to unpredictable events they might face. I believe the demonstration experiments published in this volume also brought us many successful outcomes creating vertical-horizontal bonds among the core human resources who acquired abilities through the program while building organic links with various organizations outside our community.

In this center, we would like to create a place to generate new approaches and outcomes by meeting and collaborating with individuals engaging in cybersecurity regardless of industries, governmental agencies, or academia in the future.

Ms. KAKEGAWA Masako,
ICSCoE Deputy Director General

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

Industrial Cyber Security Center of Excellence

3.31.2022

vol. 12

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

Ministry HAGIUDA Visited ICSCoE Exercise Facility

Minister HAGIUDA (Left) had a briefing on the simulated plant.

Minister HAGIUDA received the explanation on in-vehicle control systems.

In December 2021, Mr. HAGIUDA, the minister of Economy, Trade and Industry, visited the exercise facility of ICSCoE in Akihabara. This facility installs simulated plants equipped with nearly actual machines to learn cybersecurity measures for control systems.

The Minister Toured Our Simulated Plants

During this visit, instructors of the Core Human Resource Development Program demonstrated potential cyber attacks using our plants simulating social and industrial infrastructures: building maintenance, electric generation, and vehicle control systems. Besides, the instructors emphasized the potential impacts and damages on societies caused by cyber attacks while explaining the efforts of the Human Resource Development Program organized by the ICSCoE.

Mr. HAGIUDA Exchanged Ideas with ICSCoE

Minister HAGIUDA enthusiastically questioned risks and security measures, the training contents of the Human Resource Development Program promoted by the ICSCoE, and security personnel and its community. Eventually, we could have a lively exchange of views with Minister HAGIUDA.

Minister HAGIUDA described, "the ICSCoE is an extremely crucial institution, concentrating the world-level human resources, techniques, and know-how, and a core hub responsible for developing top human resources, who will lead the whole industry." Furthermore, he demonstrated the further significance of this center.

Minister HAGIUDA exchanged his views on the foresight of cybersecurity measures.

On the following page, we will introduce the image of our demonstration experiment conducted at our exercise facility located in Akihabara this February.

【Wide-Area Video Distribution Experiment Using Ultrahigh-Definition Video】 Performed Demonstration Experiment on Cybersecurity for IP Remote Production for Broadcasting Industry

The Industrial Cyber Security Center of Excellence (ICSCoE) participated in a demonstration experiment transmitting the ultra-high-resolution videos (4K/8K non-compressed videos) associated with the Sapporo Snow Festival between three locations: Tokyo, Osaka, and Okinawa. This demonstration experiment has been performed by the National Institute of Information and Communications (NICT) under the collaboration among industry, government, and academic organizations since 2019 to realize the next-generation high-speed transmission. To demonstrate IP remote production and its cybersecurity were our key themes of this fourth-year experiment.

Mr. IMANARI Ayumu: Business Promotion Office (Broadcasting personnel) of Ikegami Tsushinki Co., Ltd.

Challenges in NMOS, multicasting, and 400Gbps

Mr. IMANARI Ayumu, responsible for broadcasting technologies of Ikegami Tsushinki Co., Ltd. (Ota, Tokyo), a private company participating in the demonstration experiment, told us,

“One of the highlights of this year was IP remote production. Ikegami Tsushinki has been participating as a cooperating company for four years and myself for two years. We have two main themes: security experiments and content production in remote environments. The word - ‘Integration of broadcasting and communications’ - has been told for years. However, it is the first challenge as IP remote production in an ultra-high-definition transmission technology using IP networks. We challenged much higher technology objectives this year.”

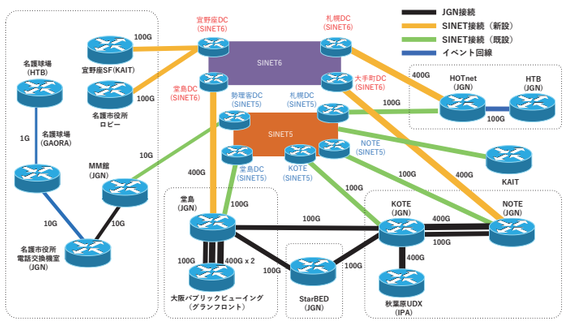
Our technological challenges this time were to 1) validate NMOS standards, 2) apply multicasting techniques, and 3) implement 400Gbps ultra-broadband lines.

First, NMOS (Networked MediaOpen Specifications) is the international standards established by AMWA(Adavenced Media Workfolw Accosiate). Our goal this year was to broadly apply these standards in Sapporo, Tokyo, and Osaka. Eventually, we succeeded in the experiment and could demonstrate the broadcasting technologies using high-speed IP networks over unprecedentedly long distances.

Second, the multicasting techniques are data communications, which specify an address and transmit data from a single sender to multiple receivers. Multicasting is a halfway distribution technique between unicast (one-to-one) and broadcast (one-to-many). Thus, ensuring security was an issue when utilizing multicasting in the broadcasting industry.

The verification of vulnerabilities in the multicasting techniques started in 2021 and has been conducted by a hybrid team, including communication equipment manufacturers, telecommunications carriers, broadcasters, and alumni and current trainees from the Core Human Resource Development Program offered by the ICSCoE. They conducted a penetration test this year and demonstrated replacement with arbitrary videos.

Third, the aims of implementing 400Gbps ultra-broadband lines were to perform demonstrations under the dynamic route-switchable state-of-the-art test-bedding environments utilizing EVPN-MPLS networks and verify the utilities of IP remote production and vulnerabilities in video equipment. Audio equipment manufacturers, broadcasters, and telecommunications carriers discussed altogether: “which cyber attack will an attacker be able to launch against the synchronized information of PTP (Precision Time Protocol), a critical cryptography for broadcasting technologies?” and “how can we apply cryptography (a vital technology of cybersecurity) in broadcasting mechanisms?” Such things could never happen to the broadcasting industry alone in the past.



Network configuration diagram

“Why do we need this highly advanced environment to demonstrate cybersecurity?” NAKAYAMA Akira, Manager of the ICSCoE, said,

“Traditionally, cybersecurity was a distant topic to the broadcasting industry. As moving toward the next-generation broadcasting using IP networks; however, preparing for disturbance by malicious groups and attacks caused by geopolitical risks should be crucial. Our demonstration experiments showed that a single computer itself could launch an attack like overriding ultra-high-resolution videos; we had never expected to carry it out that easily.”

Innovation of broadcasting technologies using IP networks

What innovations will be created by integration between broadcasting and broadband internet technologies? Mr. IMANARI, who has been engaging in onsite broadcasts like live sports, said, “The contents of broadcasting will change.”

“Integration with general IP network technologies will make broadcast production much more open. Moreover, Japan has recently established a flow enabling ordinary people to develop video content like YouTube; thus, by opening broadcasting technologies on IP networks, I think that the know-how centered on the broadcasting industry will also be integrated with both video content worlds and eventually broadened. By doing so, the broadcasting equipment and services we handle will improve.” (Mr. IMANARI)

The level of broadcasting technologies in Japan, especially in the live broadcasting area: such as coverages and relays, is internationally high. Thus, we expect improvement in the next-generation broadcasting technologies with IP networks will bring great competitiveness to Japan.

We expect to apply the technological outcomes of cybersecurity and IP remote production gained through this demonstration experiment Ikegami Tsushinki performed in its fourth year to the future coverage and sports relay areas. Those outcomes derived from the collaboration with audio equipment manufacturers, broadcasters, and telecommunication carriers, who performed this demonstration experiment, and alumni and trainees of the ICSCoE were immense; however, we plan to keep conducting those demonstration experiments expansively.

We brought back the experimental equipment to the ICSCoE locations and performed experiments.

A Hybrid Team Performed Penetration Tests by Utilizing Skills Accumulated in Different Fields

In the demonstration experiments of broadband image distribution using ultra-high-resolution videos this year, we used IP networks developed by the participating audio equipment manufacturers and telecommunications carriers and conducted penetration tests to verify cybersecurity in transmitting videos. We asked Mr. INOUE Yuji, the hybrid team leader of alumni and trainees from the ICSCoE Core Human Resource Development Program, for his stories.

Mr. INOUE Yuji, NTT Communications Corporation
（2nd-cohort graduate of the ICSCoE Core Human Resource Development Program）

—— Please tell us your efforts of this year.

Since the utilization of IP networks has advanced as the technologies used for the next-generation broadcasting industry, establishing cybersecurity for video transmission technologies has been an urgent matter.

Following the last year, the alumni and current trainees from the ICSCoE Core Human Resource Development Program collaborated with the equipment manufacturers, and as a hybrid team, we conducted penetration tests for video transmission using IP networks.

The overall picture of penetration testing was to connect SINET developed by the National Institute of Informatics (NII) and JGN to each location - Sapporo, Tokyo, Osaka, and Okinawa - and verify vulnerabilities within video transmission equipment set in those locations. Until the last year, we conducted these penetration tests against image transmission through 100Gbps-based backbone infrastructure testbed. But this year, it has been upgraded to a 400Gbps-based one partially due to the strong passion of the professor, who managed the entire demonstration project.That’s why our penetration tests team also could accomplish several tests using these ultra-broadband networks for 400Gbps.

—— Please tell us the diversity of members and their motivations.

The hybrid team consisting of the alumni and current trainees of the ICSCoE Core Human Resource Development Program organized a penetration testing team (responsible for IP remote production, backbone infrastructure, and image transmission equipment). In addition, we organized an incident response role in the team so that we can verify a series of flows of identification, defense, detection, response, and recovery. I (Mr. INOUE) managed the entire testing in order to avoid duplicate tests against the same target by multiple testers because it might lead to some kinds of complicated results.

Many members belong to critical infrastructure companies, such as the electronic, broadcasting, and telecom industries. Furthermore, most of us have participated in penetration testing demonstrations in the past. The

to the following page →