NICT NEWS
National Institute of Information and Communications Technology
No.4
2020
Vol.482

FEATURE

No more waiting. Security Human Resource Development.

Interview

Protecting Japanese IT Systems from Worsening Cyberattacks

Preparing with well-planned cyber-defense exercises

CONTENTS

NICT NEWS 2020 No.4 Vol.482
National Institute of Information and Communications Technology

FEATURE

No more waiting. Security Human Resource Development.

Interview

1 **Protecting Japanese IT Systems from Worsening Cyberattacks**
Preparing with well-planned cyber-defense exercises
SONODA Michio / SATOH Hironobu

4 **Aiming to Realize a Sustainable Supply of Human Resources**
National Cyber Training Center Initiatives
ETO Masashi

6 **CYDER: CYber Defense Exercise with Recurrence**
What are the benefits of taking the CYDER?
HANADA Tomohiro / IKARI Harumi / UCHIDA Yoko

8 **Protecting Japanese Cyber Security Even After the Tokyo 2020 Olympic and Paralympic Games**
The legacy left by Cyber Colosseo
YASUDA Shingo / KANAHAMA Nobuhiro

10 **What is SecHack365?**
YOKOYAMA Teruaki / SHIOYAMA Erika

TOPICS

12 **Message from a SecHack365 Trainer**
To Everyone Under 25 Who Uses IT Technology and is Thinking of Applying
INOMATA Atsuo / KASHIWAZAKI Hiroki

13 **NICT's Challengers File 11** ISHIKAWA Hiroki
Planning, Development, and Operation of an Integrated Systems Platform Environment that Supports the Education of Security Personnel

Cover photo: SecHack365 coursework
SecHack365 is a one-year security hackathon for people under the age of 25. SecHack365 holds training-camp style events six times a year as support for research and development. At the group events, shown in the picture, there are lectures and guidance from trainers, and discussions among the trainees.

Upper left photo: Teaching materials used in CYDER
CYDER (CYber Defense Exercise with Recurrence) allows participants to engage in practical defense exercises in an environment that simulates their organization's network environment. At CYDER, it is possible to select from Course A (Beginner) and Course B (Intermediate) according to the degree of difficulty and the participant's purpose in attending. Please see pp. 6–7 of this issue for eligible individuals and available skills.

Interview

Protecting Japanese IT Systems from Worsening Cyberattacks

Preparing with well-planned cyber-defense exercises

National Cyber Training Center

SONODA Michio (left)
Director General
National Cyber Training Center

Completed a doctorate in Engineering. Became a professor in the Faculty of Information Technology and Business at Cyber University in 2014. Joined NICT in 2016 as head of the Cybersecurity Human Resource Development Research Center and became Director General of the National Cyber Training Center in 2017. Ph.D. (Engineering)

SATOH Hironobu (right)
Senior Researcher
Cyber Training Laboratory
National Cyber Training Center

After completing a post-doctoral course in 2008, became an Assistant Professor in Kochi University of Technology.
2009 Assistant professor of Research Organization for Regional Alliances at Kochi University of Technology, 2012 Assistant professor in Department of Electronic and Information Engineering
at National Institute of Technolgy, Kochi college, 2016 Associate professor of Social Design Engineering at National Institute of Technology, Kochi College. Engaged in developing applications using neural networks. Joined NICT in 2017. CISSP, Ph.D. (Engineering)

Fierce battles are taking place, day and night, in cyberspace, and computer networks connected to the Internet are constantly exposed to cyberattacks.

In order to defend against these cyberattacks, it is necessary to strengthen IT systems and, at the same time, have highly-skilled security officers. The more personnel inside an organization who are knowledgeable about security, the stronger that organization's defenses can be, but the domestic IT security field currently has a shortage of approx. 200,000 people.

The NICT's National Cyber Training Center has launched the Cyber-Defense Exercises to develop security personnel, but what kind of program is it? To learn more, we interviewed Sonoda Michio, Director General of the National Cyber Training Center, and Satoh Hironobu, Senior Researcher at the National Cyber Training Center's Cyber Training Laboratory.

——The National Cyber Training Center was established in April 2017; how has it evolved over the last three years?

SONODA It is composed of three training programs: CYDER[*1], the practical cyber-defense exercises, Cyber Colosseo for the Tokyo 2020 Olympic and Paralympic Games, and SecHack365.

CYDER is exercises for people who work at governmental agencies, at local public institutions, or at specified corporations that oversee critical infrastructure. The number of trainees has been increasing each year, and last year there were a total of 11,019 participants, making it one of the largest cyber training programs in Japan.

While the purpose of CYDER is for participants to have basic cybersecurity knowledge, specialized in defense, Cyber Colosseo is focused on the operators of the Tokyo 2020 Olympic and Paralympic Games, so attack and defend battles are held after splitting participants into 'attack' and 'defense' sides. The goal is for participants to have advanced, practical skills so that they can deal with actual cyberattacks. The Olympics were postponed, unfortunately, so we are now assessing the situation.

SecHack365 aims to foster innovators in the security field; it is a program to discover and nurture individuals who can carry out creative technology development in the security field, and is open to young people aged 25 and under (Figure).

——Is the security field one of Japan's weaknesses?

SONODA Cyberattacks on governmental agencies and defense-related companies / research institutions are frequently occurring, however, Japan doesn't really have many of its own original security software or security appliances. This is an unfavorable situation in terms of national security. It is necessary to train engineers and researchers who can make security-related software by themselves, and as such, we launched this kind of program (SecHack365).

The climate in Japan makes it difficult for venture businesses to grow, and this isn't just limited to the security field. Overseas, and especially in the United States, people really take on new challenges, so it's relatively easy to start a business when somebody has a good idea. They are supported on management and operations aspects, with society as a whole helping to nurture the business. I think that Japan still falls short in terms of this kind of

Interview

Protecting Japanese IT Systems from Worsening Cyberattacks

Preparing with well-planned cyber-defense exercises

Figure Participation in the SecHack365 Hokkaido Development Encouragement Course

Working from home has increased as a result of efforts to prevent the spread of the unexpected new coronavirus, and as a result, both companies and individuals are relying on networks more than ever; security technology will become even more important in the future. The number of attacks increase as the number of people relying on the internet increases, and that increases the need for individuals who can respond to these attacks. I think that the National Cyber Training Center's cyber-defense exercises can contribute to this need.

Current state of cyberattacks

——What kind of cyberattacks are being conducted?

SONODA The main types of attacks are DDoS attacks, which send such a large volume of requests to servers that they become essentially unusable, website tampering from unauthorized access, attacks that steal data from databases, attacks that attach executable files to spoofed emails so as to spread malware, and ransomware, which uses a type of malware to encrypt files and then demands money for decryption.

There are a lot of attacks from overseas, some of which seem to involve national organizations; these attackers are very skilled, so there are cases where they erase logs after accomplishing their purpose of collecting information or destroying data. This makes tracking difficult.

Moreover, the defenders also need to constantly be studying and collecting information because these attack methods and software vulnerabilities are quickly being shared and spread around the world.

SATOH We are defending at multiple layers, which is called defense in depth, in order to counter that kind of situation. One of those defensive layers is people (staff), and it is necessary to educate them.

Details of exercise content

——How do you create the exercise scenarios?

SATOH We start with something that looks like it will be a trend for the year and then use that as a starting point. In a year with a lot of targeted attacks, for example, we will create a situation in which suspicious emails are the incident's starting point of incident. We set situations that are more likely to occur, with an emphasis on reality.

We then gradually unfold the story, add the security knowledge we want participants to acquire, and motivate them to think for themselves about incident response methods.

Every year we make many kinds of scenarios, and we plan to prepare three scenarios in FY2020. The aim of our exercises is to learn about incident handling.

The first event happens when you start the exercise. For example, suppose that you get a call from an outside agency saying that there appears to be evidence of an intrusion. What will you do after receiving that report? How will you investigate the specifics of the intrusion? How much damage is there in an organization's network, and what can be done to minimize it?

In following a scenario like this that may actually arise, you will learn how to analyze logs, how to consider counter measures and steps, and how to improve for a defense and reliable response.

SONODA Just like in a novel, the exercise scenario has a story, and it uses the classic 'kishoutenketsu' story structure of introduction, development, twist, and conclusion. The introduction section requires the most change, but it can be adapted in line with the topic at that time. By preparing a variety of stories as "parts," including their subsequent development, you can then combine them to build a realistic story with changes.

SATOH The network environment for the exercises is virtualized using NICT's StarBED (Hokuriku StarBED Technology Center, Nomi City, Ishikawa Prefecture) testbed environment for hands-on exercises. We have also developed CYDERANGE, an automated cyber-exercise automation system, and it allows us to present problems while keeping in mind the participants' progress.

——What are the difficulty levels for the exercises?

SATOH In 2020, CYDER has a single course A for the beginner level and a pair of course Bs for intermediate level participants for a total of three courses. A single lesson has about 30 participants, and they are held about 100 times a year in various prefectures nationwide.

For course A, each lesson has one instructor and four tutors who act in support roles. Participants will work with them and learn how to respond to incidents, one by one. Participants will also be required to learn some basic pre-learning on the Internet, but they don't need skill of programming languages.

SONODA There are individuals from a variety of departments within the organization, and the purpose of the exercise is to reduce the damage from cyberattacks by raising the security literacy of people in each and every role.

SATOH The exercises are devised so that participants can acquire not only technical knowledge, but also soft skills. For example, the ability to communicate using technical terms is necessary in order to smoothly stay in touch with related parties such as external security engineers and cyber security companies.

——Can participants get some sort of qualification from CYDER?

SATOH There isn't a qualification that participants can acquire, but there is a requirement to take a renewal course every three years for the Registered Information Security Specialist (RISS*) qualification from the Information-technology Promotion Agency (IPA), and we plan to apply for new CYDER courses to be specified as courses for this renewal requirement.

Learning purpose

——What is important while learning cybersecurity?

SATOH Information science is the foundation of cybersecurity. First, learn the basics of computers and networks. Additionally, security technology advances extremely quickly, so continually studying is essential.

Even in the sense that security technology advances quickly, it is important to keep cultivating and nurturing young people. However, the challenge is that Japan has a social structure in which it is difficult to increase young people's motivation.

Qualifications are directly related to your career and salary advancement in the United States. For example, you can earn $40,000/year if you have CompTIA Security+, and your salary jumps to $100,000/year if you have a qualification such as CISSP*4.

In Japan, it doesn't really work like that, and as such, I think we need to provide a way to change the social structure to security engineers' increase motivation.

——What is your role as a national research institution?

SONODA We want to do things that can't be done in the private sector. NICT is a large-scale cybersecurity observation network like NICTER, and we also have a wealth of technical knowledge obtained through many years of research. We believe that it is our role to take advantage of such vast resources for exercises and play a part in transforming Japan's networks and social structures into safe and resilient ones.

---

*1 CYDER：Cyber Defense Exercise with Recurrence
*2 IPA：Information-technology Promotion Agency
*3 RISS：Registered Information Security Specialist
*4 CISSP：Certified Information Systems Security Professional

This interview was conducted with consideration to the number of people, social distance, time, ventilation, and hand washing, etc.

Aiming to Realize a Sustainable Supply of Human Resources

National Cyber Training Center Initiatives

ETO Masashi

Director of Cyber Training Laboratory
National Cyber Training Center

He joined NICT in 2005. He had been a researcher of Cyber Security Laboratory until 2016. He became senior researcher of (Cyber Security Research Center[-CYREC] Cyber Tactics Laboratory) and got current position since 2017. His research interests include network monitoring, intrusion detection, malware analysis and auto-configuration of the Internetworking. He received the Best Paper Award at the 2007 Symposium on Cryptography and Information Security (SCIS 2007) and the Commendation for Science and Technology by the Minister of Education、Culture、Sports、Science and Technology in 2009. Ph.D. (Engineering).

Cyber-attacks targeting critical infrastructure such as electrical, gas, and water utilities, even government agencies have become a daily occurrence in the news. On the other hand , it has been pointed out that there is a chronic shortage of security personal despite the promotion of security measures for the public and private sectors. The National Cyber Training Center, in order to eliminate this serious shortage of security personnel and to realize a society that can supply security personnel sustainably, promotes three initiatives: the CYDER practical cyber-defense exercises, the Cyber Colosseo cyber exercises for the Tokyo 2020 Olympic/Paralympic Games, and the SecHack365 training initiative for security innovators, and is also advancing other measures (Figure).

CYDER: Raising the level of personnel responding to security incidents

In order to appropriately deal with cyber-attacks, it is important to take independent and proactive measures, while bearing in mind regular system operations, instead of letting IT vendors take care of all security measures on a daily basis.

The National Cyber Training Center promotes CYDER, a practical cyber-defense exercise, with the aim of "acquiring a series of response actions" that IT systems personnel should take in the event of a cyber-attack. CYDER can be attended free of charge for public institutions such as governmental agencies and local entities, and is also available to private companies for appropriate fee. With CYDER, NICT has prepared the latest exercise scenarios based on actual cyber-attack cases and the knowledge that NICT has accumulated over its many years of cybersecurity research. Built on NICT's large-scale computing environment, IT systems personnel can utilize an exercise environment that mimics the LAN environment of actual organizations and acquire the ability to respond to cyber-attacks while using practical and hands-on skills.

IT systems personnel who participate in CYDER bring practical experience and knowledge gained from the exercises back to their own organizations, and the exercise content is focused on employing this knowledge and experience at their own workplaces. In addition, there is also a support system in place to meet the skill levels and progress of participants, making attendance possible even for security beginners.

Cyber Colosseo: Towards a stable realization of the Tokyo 2020 Olympic/Paralympic Games

Large-scale international events that attract world-wide attention, such as the Tokyo 2020 Olympic/Paralympic Games, are attack targets for hackers, and it is expected that they will be subject to more subtle and advanced cyber-attacks.

National Cyber Training Center, in order to support a smooth implementation of the Tokyo 2020 Olympic/Paralympic Games, is promoting cyber exercises and the Cyber Colosseo initiative for the security personnel of organizations related to the Tokyo 2020 Olympic/Paralympic Games. Cyber Colosseo consists of two types of hands-on exercises, the Colosseo Exercise and the Colosseo College, which are conducted for staff of the Tokyo 2020 Organizing Committee and its contract vendors. The Colosseo Exercise work to train personnel to a level higher than CYDER (the pre-advanced level in the figure) through real-world exercises in a simulated environment set during the Tokyo 2020 Olympic/Paralympic Games, and consist mainly of offensive and defensive techniques related both technologies. Colosseo College offers lecture seminars that aim to supplement the prerequisite knowledge required to attend the aforementioned Colosseo Exercise, and enable participants to acquire a wide range of cybersecurity-related knowledge.

Cyber Colosseo prepares various educational content according to the technical level and expertise of the participants and plans to improve, right up until the Olympics start, the security response capabilities of people involved with the Tokyo 2020 Olympic/Paralympic Games.

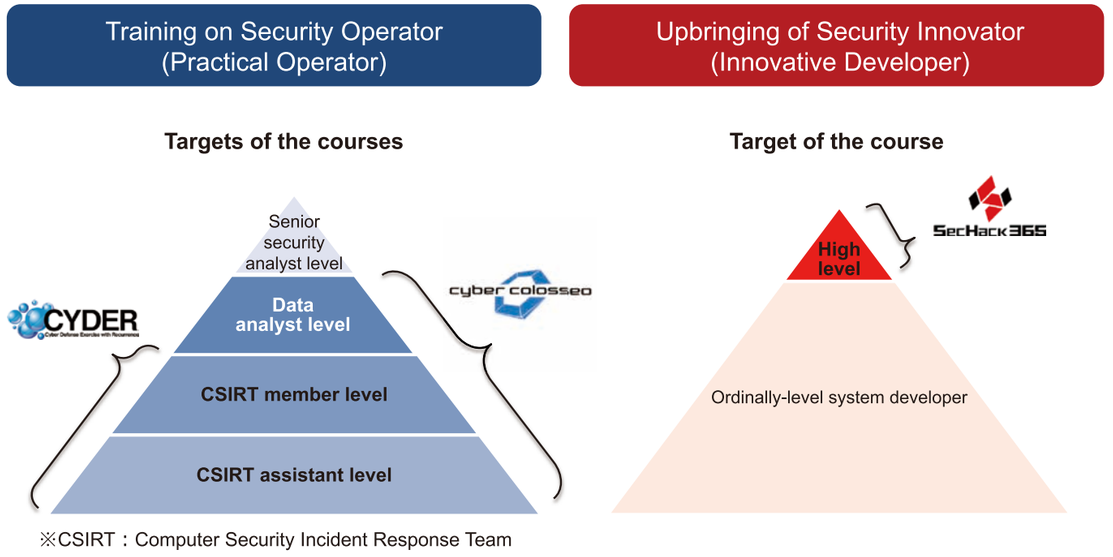


Figure　Three areas of initiatives by NICT National Cyber Training Center

SecHack365: Aiming to improve the security self-sufficiency rate

The presence of Japanese vendors in the global cybersecurity market is by no means large, and, currently, it is common for domestic companies and institutions to use black box products from overseas. Japanese society must improve its security self-sufficiency rate in order for us to protect the safety of our society with our own hands, and this means that, instead of merely operating existing overseas products, we must construct development systems for domestically produced security systems through fostering human resources who can research and develop new products.

Regarding this issue, the National Cyber Training Center is promoting the SecHack365 initiative, aimed at creating future cybersecurity researchers and developers, which provides full-fledged guidance on the research and development of security-related technologies for young ICT human resources. SecHack365 is a long-term hackathon that provides an opportunity to create by researching, developing, testing, and presenting cybersecurity-related software over the course of a year, and is open to students and working adults aged 25 and under, with approximately 40 individuals being selected to participate. These participants, through interacting with top researchers, engineers, and trainees nationwide, are nurtured into human resources (security innovators) who can create their own security-related software.

This initiative started in FY2017, and its 3rd year has already been completed. Graduates so far have already achieved remarkable results in both domestic and overseas security-related businesses and events. There isn't enough time or space here to list all of the successes, but a few examples include the team chosen in the first year competing at a famous overseas hackathon event and winning the sponsor award, alumni who received the IPSJ Excellent Student Award grand prize at the Information Processing Society of Japan's Junior High School and High School Informatics Research Contest, and alumni who started a business using their SecHack365 project and won the METI Minister’s Prize in a domestic business plan contest.

NICT has been implementing each of these initiatives since FY2016, but it is still far from meeting society's demand. At NICT's National Cyber Training Center, in parallel with the three initiatives introduced so far, we aim to achieve a sustainable supply of human resources by working on the research and development of more effective and efficient methods for fostering human resources.

CYDER: CYber Defense Exercise with Recurrence

What are the benefits of taking the CYDER?

HANADA Tomohiro
Senior Technical Researcher
Cyber Training Business Promotion Office
National Cyber Training Center

Joined NICT in 2017. Previously involved as project manager in development and operation, the core of banking systems at an IT vendor. Besides work, I founded the first information security community in Kyushu, and organized many events and study groups. Currently involved as a senior technical researcher in the projects at the National Cyber Training Center: CYDER, SecHack365 and building CYDERANGE. Chairman of SECCON.

IKARI Harumi(left), UCHIDA Yoko(right)

IKARI Harumi
UCHIDA Yoko
Cyber Training Business Promotion Office
National Cyber Training Center

A variety of organizations have suffered damage from cyberattacks in recent years, and damage rapidly spreads if the organization does not properly deal with the cyberattack immediately after falling victim to it. In the event of a cyberattack, it is important to take action quickly to minimize damage and prevent damage from spreading. CYDER lets organizations train for a series of steps using actual computers, including initial actions and from incident occurrence to reactive responses (Table 1).

Being prepared before an incident

Just as it is necessary for healthcare providers to conduct triage, the post-disaster prioritizing of treatment for certain patients based on their severity, cybersecurity also requires a similar response and performs incident handling after an incident occurs, wherein certain actions and responses must be prioritized based on the damage and severity of the incident.

Once you understand the importance of triage, what do you think should be confirmed and how should it be assessed when an incident occurs? A variety of events must occur in parallel after an incident occurs; decisions must be made, and actions must be taken in a short amount of time. There are also things that need to be prepared before an incident occurs, such as being able to confirm what happened in your IT systems, and knowing how to coordinate as an organization with relevant parties, etc.

CYDER allows participants to conduct practical training using actual computers by generating artificial cyberattacks situation and by providing IT system environments that have been attacked, allowing them to gain an awareness of how to detect attacks and what to do to minimize damage from an attack.

Table 1 CYDER basic information

Purpose	To acquire practical measures to minimize the damage caused when organizations suffer a cyberattack.
Eligibility	National institutions, designated corporations, independent administrative agencies, local public institutions, critical infrastructure providers, private companies, etc.
Course Length	1 hour of pre-learning + 1 day of group exercises *Annual attendance is recommended
URL	https://cyder.nict.go.jp/

Table 2 Skills that participants will acquire

	Course A (Beginner)	Course B (Intermediate)
Target	• Those who are just starting to be involved with IT systems • Those who have to responds when an incident occurs • Those who want to operate IT systems safely • Those who want to learn how to prepare for an incident	• IT system administrators and operators • Those involved in IT system procurement, planning, and development • Those involved in managing and directing the response and responders when an incident occurs
Skills Acquired	• Understand what to do in preparation for an incident • Read and understand reports from vendors and share information appropriately • Understand the response flow when an incident occurs	• Audit logs of PCs, servers, and network equipments, etc. • Share information with CSIRT members, bosses, vendors, etc., and independently respond to incidents • Review your organization's security policy

CYDER curriculum

The people administrating IT systems are busy on a daily basis, and it is difficult for them to have enough time for training and drills. Based on feedback such as this, CYDER has carefully selected and condensed the necessary skills for incident handling, providing a 1-hour online pre-learning course and 1-day group exercises (Table 2).

In the pre-learning course, you can learn the basic content for attending the group exercises and you can learn how to use the tools used in the group exercises. It can be accessed from anywhere via the Internet, similar to common e-learning.

In the group exercises, you can experience a series of incident handling events using actual computers. You will also split into groups of 3–4 people and respond to the security incidents as a member of the organizations that appear in the exercise scenarios (Figure).

Each group is provided with the IT systems environment of the organizations that appears in the exercise scenario. Providing independent environments for each group lets you freely experience and learn about cyberattacks and countermeasures within the environments. These environments also make it possible to execute commands that you would hesitate to carry out during your regular duties, such as making drastic settings changes.

The cyberattacks and incident handling that appear in the exercises are based on NICT's thorough analysis of the latest trends in actual cyberattacks, and up-to-date scenarios are prepared every year. (Table 3)

Why CYDER?

It is difficult to acquire emergency coping skills while only carrying out every-day tasks. It is necessary to use non-crisis times to sufficiently improve response capabilities so that a swift and accurate response can be carried out when an incident actually occurs. Previous participants have made comments such as "Things didn't work as expected when I actually tried them, and it made me realize the importance of drills and training."

Similar to holding annual disaster drills for earthquakes, etc., it is important to prepare for cyberattacks as well. With CYDER, you can enhance your ability to understand the meaning, effects, and impacts of individual elements by repeatedly experiencing different scenarios. You can expect to improve your organization's ability to deal with incidents by bringing back what you learned at CYDER and sharing it with colleagues.

Table 3 Examples of Exercise Scenarios

While teleworking, Mr. S, a government employee, had his computer infected by malware after a vulnerability in software he uses was exploited. The malware infection then spreads when Mr. S goes to work and connects his PC to the system at his government agency.
An attacker exploits a vulnerability in a web application managed by Mr. M, an employee of Saida City, and gains access to the system. The attacker steals information on the internal server.

CYDER until now, CYDER in the future

CYDER was started in 2013 as a Ministry of Internal Affairs and Communications demonstration experiment, and the initiative was then transferred to NICT, which has been strengthening the implementation systems and enhancing the contents. It is currently operated in 47 prefectures all over Japan, approximately 100 times a year, and has a capacity of more than 3,000 attendees. The training environments use the CYDERANGE training infrastructure, developed by the National Cyber Training Center. Going forward, NICT plans to work on advanced research and development, such as making available online the training environments provided to each group in the group exercises.

Figure Exercise scene

Messages from the Cyber Training Business Promotion Office

IKARI Harumi

I hope that you will take the CYDER course if you aren't confident in your knowledge of IT security. For the course A (Beginner) in particular, it's OK not to be confident; our experienced instructors and tutors will offer support and guidance if you have difficulties.

With CYDER you can experience what to do in the event of an emergency while actually operating PCs, and you can also become more aware of high security and answer questions such as "Are incidents caused by things like this?" and "Is there a lot of work after an incident occurs?"

We carry out our daily duties behind the scenes so CYDER can run smoothly, to convey CYDER's merits to everyone in Japan, and to have as many people as possible take the course.

UCHIDA Yoko

Are you able to properly respond to a cyberattack without any knowledge or preparation? CYDER is a training program that enables you to properly respond to cyberattacks. From beginners to experienced system operators, you can experience the flow of incident handling while receiving help and support from instructors and tutors. We look forward to seeing you at CYDER courses in the future, both those who have attended the training before and especially those who will be attending for the first time!

Protecting Japanese Cyber Security Even After the Tokyo 2020 Olympic and Paralympic Games

The legacy left by Cyber Colosseo

YASUDA Shingo

Senior Researcher
Cyber Training Laboratory
National Cyber Training Center

He joined NICT in 2013 after working for graduate school.
He is interested in construction and operation for large-scale network experiments, and Application to cyber security training and human resource development. Ph.D. (Information Science).

KANAHAMA Nobuhiro

Senior Technical Researcher
Cyber Training Laboratory
National Cyber Training Center

He joined NICT in 2016 after working as a hardware vendor and as an instructor and developer of educational materials related to cybersecurity. He is primarily engaged in scenario development for cybersecurity exercises. His hobby is soldering.

The Olympics and Paralympics have been targeted by cyberattacks at every Games since the cyberattacks that targeted the London 2012 Olympic/Paralympic Games. Cyber Colosseo is supporting the smooth operation of the Tokyo 2020 Olympic/Paralympic Games, and will be implementing a variety of curriculum even after the Tokyo 2020 Olympic/Paralympic Games so that the security personnel who can support Japan will be left as a legacy.

Cyber Colosseo overview

The Olympic and Paralympic Games of recent years have become attractive targets for cyberattacks by criminals. The National Cyber Training Center is conducting Cyber Colosseo, a cybersecurity human resources development project, in preparation for these kinds of cyberattacks at the Tokyo 2020 Olympic/Paralympic Games and to support the smooth operation of the Games (Figure 1).

Cyber Colosseo is recruiting participants from staff of the Tokyo 2020 Organizing Committee (hereinafter "the Organizing Committee") and its contracted vendors through the Organizing Committee. The project, which started in FY2017, has gradually been expanding in scale, and in 2020 is aiming to train 220 individuals with the three Colosseo Exercise levels (beginner level, intermediate level, and pre-advanced level), which will be described later. In addition to the Organizing Committee-related organizations, there are external organizations that support the Tokyo 2020 Olympic/Paralympic Games. Cyber Colosseo has secured a wide range of target organizations by collaborating with CYDER, which is practical cyber-defense exercises put on by the National Cyber Training Center for local public institutions, and is focusing on training staff that are connected to the Organizing Committee.

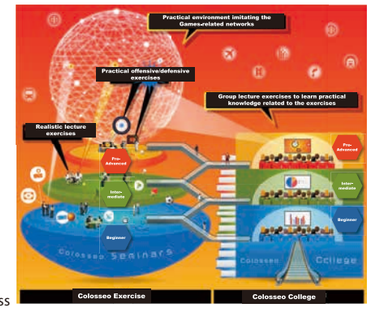


Figure 1 Cyber Colosseo business

Cyber Colosseo curriculum

The Olympic and Paralympic Games are some of the world's largest events, and it is expected that there will be an array of cyberattacks against them for financial purposes and terrorist plots. In order to hold the Games in that kind of situation, it is necessary to have not just the protective skills and technology of individual people, but also the organizational strength of defensive skills and technology that come from the trust, cooperation, and collaboration between departments. As such, Cyber Colosseo works in close collaboration with the Organizing Committee to provide training through two types of curriculum, the Colosseo Exercises and the Colosseo College, which are aimed at both real experiences/raising the level of technical skills and at fostering collaboration between organizations and departments.

Colosseo Exercises: Knowing the attacker's unexpected mindset and polishing defenses

As shown in Table 1, the Colosseo Exercises consist of three levels: beginner level, intermediate level, and pre-advanced level, consisting of multiple courses at each level, in consideration of abilities and organizational professions, for a total of seven courses. Training with exercises from the attacker's perspective are also conducted in addition to incident response training particularly for the intermediate level courses and higher (Figure 2).

Table 1 Types of Colosseo Exercise Scenarios

Types of Colosseo Exercise Scenarios		
Level	Course	Description
Beginner CSIRT Assistant Level (1-day)	Beginner A	Scenarios for participants whose work does not handle personal information, such as purchasing
	Beginner B	Scenarios for participants whose work does handle personal information
Intermediate CSIRT Member Level (1-day)	Intermediate A	Conduct attacks on typical web services using simulated sites. Exercises to confirm the effects of the attacks in logs and do a survey of the impacts
	Intermediate B	Exercise to trace attacks on organizational network systems and to clarify the whole attack. The attacks in the exercise are based on actual attacks on organizational network systems and are traced in order from intrusion discovery.
Pre-Advanced Data Analyst Level (2-day)	Pre-Advanced A	Divide into groups and learn, in CTF format, intrusions into the organization networks of the other groups. Attack and defend battles focused on attacking by examining countermeasures by analyzing attack logs.
	Pre-Advanced B	Penetration test exercises inheriting the CTF format from pre-advanced A and with increased attack variations
	Pre-Advanced C	Attack and defend battles focused on defense, with course staff and instructors (red team) attacking, and participants defending their organization's network

Figure 2 A snapshot at the Colosseo Advanced Exercise

General cybersecurity exercises place emphasis on hands-on training in defense techniques and incident response. However, if students better understand the attacker's perspective, mentality, and tactics, they will be more confident in defending against the attacker.

Movies and TV shows depict cyberattackers penetrating deep inside systems in moments, but in reality, it involves a significant amount of simple work and patience.

Therefore, the intermediate level has exercises that include the experience of attacking, and the pre-advanced level's A/B exercises where the participants are divided into teams and conduct attack-and-defend-style exercises, such as invading each other's simulated environment. Participants learn the difficulty in attacking and the mentality of attackers, answering questions such as "What is the time scale of attacks that are usually recognized in logs and alerts?" and "What do target systems look like from the attacker's point of view?" Exercises are designed so that participants will be able to appropriately respond while feeling a sense of alarm. Then, after learning the attacker's point of view, participants in the pre-advanced level C course will engage in red team / blue team exercises, with the operator team (blue team) defending a simulated Organizing Committee system from the attacking team (red team), which is composed of course staff and instructors.

These exercises allow participants to experience a variety of on-site responses, such as incident triage, technical response, response recording, and collaborations between departments. The exercises give a practical overall finish to the training so that participants can flexibly act and respond at their actual workplaces.

Colosseo College: Raising individuals' levels and fostering organizational strength

Colosseo College is a group of supplementary lectures and exercises that were newly established in 2018 with the aim of maximizing the effectiveness of the Colosseo Exercises by acquiring prerequisite and peripheral knowledge necessary for the Colosseo Exercises. The Organizing Committee is a time-limited organization, with staff from a variety of backgrounds successively gathering for the Games. Cyber Colosseo was initially an exercise-only initiative, but there were large variations in participants' skills and it was difficult to maintain the level of the exercises, due to weak human relationships. To that end, the subject matter is divided into the three areas of basic knowledge, technology, and tool usage; a set of 20 subjects (Table 2) that will increase the skill levels of participants and enable lateral cooperation through hands-on sessions and group work.

Colosseo College is an elective system, and participants choose lectures depending on the content of their own job, skill improvement plan, and interests, etc.

Cyber Colosseo plans to conduct these trainings until just prior to the Tokyo 2020 Olympic/Paralympic Games, and ultimately there will have been hundreds of participants in the Colosseo Exercises and the Colosseo College. Participants from the various departments in the Organizing Committee will share their experiences through lectures, hands-on sessions, group work, and exercises, and Cyber Colosseo will support the smooth operation of the Tokyo 2020 Olympic/Paralympic Games by fostering the organizational strength of defensive skills that are not just limited to technology.

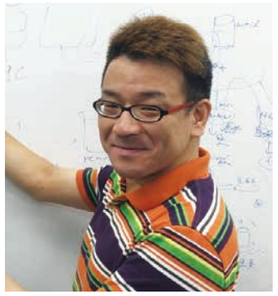
The positive legacy of skills and knowledge that will remain after the Olympics

Cyber Colosseo formulated an Action & Legacy Plan for the Tokyo 2020 Olympic/Paralympic Games that connects outcomes at the Games to the future. Most Cyber Colosseo participants are individuals from companies that normally do business in Japan, and the individuals who attend Cyber Colosseo to learn basic cybersecurity knowledge and practical defensive/analytical skills will demonstrate their skills in a variety of companies and industries in Japan and support Japanese cybersecurity even after the Tokyo 2020 Olympic/Paralympic Games. In addition, the exercise scenarios created by Cyber Colosseo will be utilized as the center's legacy for the development of Japanese cybersecurity personnel after the Games, such as being used in CYDER.

Table 2 Colosseo College

Related Colosseo Course	Colosseo College Course Name
Beginner A/B	Security Basics
Beginner A/B	Intermediate Level Security Tools E
Beginner A/B	Introduction to Incident Response
Beginner B	Laws Related to Personal Information Protection
Beginner All	GDPR
Intermediate All	Latest Security Trends
Intermediate, Beginner A/B	System Architecture
Intermediate, Pre-Advanced	Practical Incident Response
Intermediate, Pre-Advanced	Security Tools M
Intermediate, Pre-Advanced	Vulnerability Diagnosis Practice
Intermediate, Pre-Advanced	Penetration Testing Practice
Intermediate All	Secure Development
Intermediate, Pre-Advanced	Security Tools P
Intermediate, Pre-Advanced	Log Analysis Practice
Intermediate, Pre-Advanced	Micro Hardening
Intermediate, Pre-Advanced	Cyber Intelligence
Intermediate, Pre-Advanced	Forensics Practice
Intermediate, Pre-Advanced	Malware Analysis Practice
Intermediate, Pre-Advanced	Traffic Analysis Practice
Intermediate, Pre-Advanced	Non-Technical Skills IR Exercises

What is SecHack365?



YOKOYAMA Teruaki

Senior Researcher
Cyber Training Laboratory
National Cyber Training Center

He is in charge of SecHack365, which trains young security innovators. He is interested in practical ICT education and the realization of industrial contribution and social implementation through ICT. He is a special associate professor at the Graduate School of Information Technology, Kobe Institute of Information Studies. Ph.D. (Engineering)

SHIOYAMA Erika

Cybertraining Business Promotion Office
National Cyber Training Center

She is in charge of the administration and management of SecHack365.

The name SecHack365 stands for "Security + Hackathon for 365 Days," and is a program to foster young individuals, open to people aged 25 and under. SecHack365 is a unique "long-term hackathon" that provides an opportunity to create, thereby aiming to nurture "security innovators" who can conduct innovative research and development.

Unlike at ordinary hackathons, the SecHack365 attendees (hereinafter referred to as trainees) themselves set as a theme the technology or security area that they are interested in, and then work hard over the course of a year to create something. Over the course of six training camps, the trainees receive first-hand guidance from experts active in a variety of fields, such as security and software development. Throughout the year they will show others what they are making, receive feedback and improve their skills and methods, advancing their work. A major feature of the SecHack365 program is the creation of projects that could not be developed by a single person; both online and offline they repeatedly "Make→Show→Get Feedback→..." with experts and diligently work with other trainees.

From technical development such as program implementation and research results to content creation for security awareness, SecHack365 works to develop human resources who can create a variety of security-related works and produce these results.

Figure 1 shows the SecHack365 schedule from FY2019. Trainees work on their creation at 6 training camp-style events over the course of the year and through online activities, and they learn how to develop progressively and create works that reflect a security perspective by repeatedly "Making→Showing" their creations.

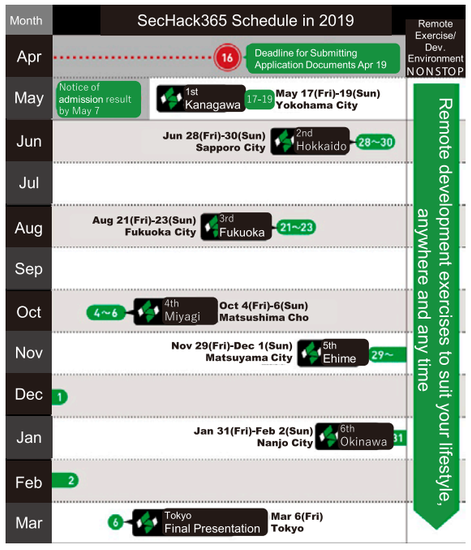


Figure 1 SecHack365 schedule in 2019

What kind of things have been made?

SecHack365 requires trainees to shape solutions for the security problems that they consider, and the SecHack365 program invites specialists in a variety research and development fields from universities and companies to take on the role of trainers and mentors. The trainees continue making their creations for one year, receiving guidance not just from a technical perspective, but also from the perspectives of maintainability and creativity. Additionally, sharing their creations with other trainees allows them to experience how to communicate with others and how to reflect in their creations the advice they received. SecHack365 is the place to make this kind of creation, and the table is a portion of the results obtained thus far.

Trainees work on making their creations, which have a variety of themes related to security. Some trainees decide on a theme before applying, and some trainees change their theme after participating in SecHack365 activities, and every creation is that trainee's answer to a security issue that they have considered.

In this way, SecHack365's goal is fostering individuals' ability to solve problems that they encounter and to shape and produce creations. Additional creations are also posted on the SecHack365 official web page, and interested readers are invited to go and look at them.

Table Examples of past projects

A team of trainees interested in car security formed a team and used actual vehicles to develop information collection, analysis, and application by using CAN*1
Developing Twitter client software that analyzes and protects the text and images in tweets in order to prevent accidentally leaking personal information
Developing games for security awareness
Wrote Writing a book on learning information security using the Python programming language and learning information security
Used QEMU*2 to implementing and testing security mechanisms on a CPU using QEMU*2

The Importance of building with your own hands and thinking without giving up

Trainees may work on a theme that they decided on before applying to SecHack365, or they may also change their theme after participating in the presentations and discussions. SecHack365 lets trainees experience making a creation, from the initial idea all the way to polishing it and making it better. During this process they will also have the opportunities to present for short intervals. This process, of creating and showing, has trainees be aware of the strengths and weaknesses of their own works and ideas, continuing to work towards making them better while receiving advice from trainers and other participants (Figure 2).

In many cases they can't get exactly what they wanted in one pass, and there many things that they don't understand until they start making their creation, and things that they realize after making and operating it. The burden and pressure of creating new things greatly increases if you think that you can't make something without first predicting or planning everything about it.

Additionally, it is difficult to create a perfect solution in advance when it comes to security problems, and it is important to deal with problems after they occur. SecHack365 allows trainees to learn this through the process of making something small, showing it, and then continuing to work on it, maximizing their movement towards increasing the value of their creation and solving problems that come up, and in this way the trainees are expected to become creative engineers, researchers, and creators.

Awareness gained by showing work to others

Do you like presentations? Showing is as important as making at SecHack365, but there are a lot of people who may think that preparing to show your work to others is difficult. However, showing your work to others is an opportunity to receive a variety of opinions and objectively observe what you have made. And, knowing how to show your work to other people makes the act of creating less lonely. We believe that receiving feedback like this will also lead to an attitude that quickly corrects security problems.

Figure 2 Snapshots at SecHack365

SecHack365 is a place to create and show your work like this, and aims to foster individuals who can continuously make things.

*1 CAN (Controller Area Network: A network standard used within automobiles)
*2 QEMU (Quick Emulator: An open source process emulator, software that runs a virtual computer within a computer.)

Messages from SecHack365 Staff

YOKOYAMA Teruaki

Creating something is the most effective introduction for yourself Through the one-year program at SecHack365 you'll learn methods to create values and polish your security skills. Come to SecHack365 and create what you're envisioning!

SHIOYAMA Erika

The training camp-style events are held at various places nationwide, so there's a lot of traveling involved, and the programs are substantial, so the training camp period is quite difficult. But there was a great sense of unity and connection among the participants after they shared these difficult thoughts, and they continue to keep in touch after finishing the program, even though their environments have changed. SecHack365 is also an opportunity to make friends with the same goals, regardless of age, birthplace, or school, etc., so I hope a lot of people step forward and try it. I look forward to your working as a "SecHack365 graduate" in the future.

Message from a SecHack365 Trainer

To Everyone Under 25 Who Uses IT Technology and is Thinking of Applying

INOMATA Atsuo
Professor, Osaka University

His main research theme is theory of cryptography. Visiting professor of Ritsumeikan University, representative director of Wireless LAN Certification Organization, director of JPCERT coordination center, cyber security advisor of Nara prefectural police, security camp lecturer, etc.

SecHack365 isn't a traditional institution of learning, such as a school. We have a somewhat unusual style, traveling from place to place all throughout Japan and really working on what we want to make. Sharing is important for security. Speaking of training, it is common for trainers to become mentors, and I'll give a little boost or hint when the trainees and I are puzzling over something. Furthermore, the trainers are often envious of the things that the trainees create, and there aren't many places where you can get this excited.
If you'd like to create a happier world through security, then please, by all means, join us. We are preparing to make SecHack365 the best it can be and look forward to seeing you all.

KASHIWAZAKI Hiroki
Project Associate Professor, Center for Cybersecurity Research and Development, National Institute of Informatics

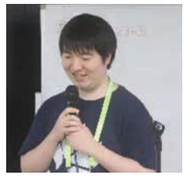
After dropping out of the Graduate School of Engineering at Hokkaido University twice, He worked at Hokkaido University, Tokyo University of the Arts, and Osaka University before assuming his current position. His research achievements involve high availability networks, wide area distributed systems, resilience, and MOE. Ph.D. (Information Science).

There are some teenagers who, even though they have an interest in security, are dispirited because they don't have "a teacher who will instruct them on security" or "a friend with common interests," and then there are the SecHack365 graduates who say, "Being able to earnestly talk with fantastic people of the same age is better than anything." But, looking around me, there aren't really a lot of fantastic trainees at their first stage of SecHack365. Great, fantastic people grow together over the spatiotemporal course of a year, like eggs in an incubator. I think that this, and the diversity that arises from it, is the genuine worth of SecHack365. You will also find friendly rivals who will help push your skills even further. If you're a young person interested in security, then SecHack365 is definitely where you should be.

Examples of SecHack365 Graduates' Successes *Parenthesis indicate their status when participating in SecHack365

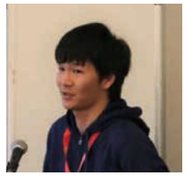
FY 2017: Distinguished Graduate
KITAMURA Takuya (Graduate student)

- Received the Challenge IoT Award 2017 Minister of Internal Affairs and Communications Award
- Nominated for Student CG Contest, Art Division
- Received METI Minister's Award, Business Division Grand Prize, and JVCA Award (Cyship) at the 15th Campus Venture Grand Prix National Convention
- Published "Techniques for Learning Programming from Zero Knowledge" (#1 best-seller in its category on Amazon)
- Special Assistants to the President, Special Assistant Professor, Hiroshima University
- Co-founder of TechChance!, a programming school for elementary, junior high school, and high school students
- Founder and Representative of Cyship Co., Ltd. (https://cyship.net/)
- Student at MAKERS UNIVERSITY, 3rd Term



FY 2017: Distinguished Graduate
KAWASHIMA Kazuki (Vocational school student)

- Cyship exhibition at CISCO DIGITAL JAPAN DAYS 2019
- Established Cyship Co., Ltd.
- 3rd Place, HAL Laboratory, Inc. Programming Contest



FY 2017: Distinguished Graduate
MUROTA Masataka (University student)

- Received the Niigata IT Award 2018 Grand Prize
- Received the ICT Business Idea Contest 2018 in Nagaoka Encouragement Award
- Established Riparia, Inc., a venture company from Niigata University, CEO and Representative Director (https://riparia.jp/)
- Student at MAKERS UNIVERSITY, 4th Term
- Chosen for the Wide Ecosystem Accelerator 2019

FY 2017: Graduate
NINOKATA Rihito (Elementary school student)

- "Sugoude 2019" was chosen for the IT Super Engineer Support Program
- Received the Junior High School Student Research Award Grand Prize at the 82nd Information Processing Society of Japan National Convention's Junior High School and High School Informatics Research Contest

FY 2018: Graduate
KUBOTA Yasuyuki (Junior high school student)

- Received the Japanese Society for Artificial Intelligence Home Robot Challenge Award in the Junior Category at the World Robot Summit 2018
- Received the Junior High School Student Research Award Grand Prize at the 82nd Information Processing Society of Japan National Convention's Junior High School and High School Informatics Research Contest

FY 2018: Graduate
MIHASHI Yuki (Junior high school student)

- Certified as Mitou Junior Super Creators (FY 2018)
- Appeared on BS TV Tokyo's "Startup at 14" documentary program

FY 2018: Distinguished Graduate
SHU Yoshifumi (High school student)

- Received the Junior High School Student Research Award Grand Prize at the 81st Information Processing Society of Japan National Convention
- Presented U25 "Semzhu-Project – A self-made new world of embedded hypervisors and attack detection methods" at the 2019 CODE BLUE Main Track

Planning, Development, and Operation of an Integrated Systems Platform Environment that Supports the Education of Security Personnel

ISHIKAWA Hiroki

Senior Technical Researcher
Cyber Training Laboratory
National Cyber Training Center

Biography

1988 Born in Ibaraki Prefecture
2010 Joined a domestic systems integration company
2017 Joined NICT
2020 Current position

Awards, etc.

2018 Received the Social Contribution Award (Group) from the National Institute of Information and Communications Technology

Q&As

Q What are you currently interested in outside of your research?

A I love cooking, and always look forward to getting cookware made by Japanese craftsmen.

Q How do you spend your time on holidays?

A Taking walks with my camera, riding my motorcycle, traveling, and tinkering with machines, etc.

Q What advice would you like to pass on to people aspiring to be researchers?

A It is exciting to work with people who have a variety of knowledge and different ways of thinking. Don't be shy!

The National Cyber Training Center conducts three initiatives: the CYDER practical cyber-defense exercises, the Cyber Colosseo cyber exercises for those involved in the Tokyo 2020 Olympic/Paralympic Games, and the SecHack365 training for security innovators.

Our platform team in the lab plans, develops, and operates the integrated infrastructure platform that supports these three initiatives, and we currently operate a system that is composed of more than 500 devices with 30 types and at six locations, such as multiple container-type data centers at the Hokuriku StarBED Technology Center and data centers in Tokyo.

When planning an integrated system, we consider what it should be, from design to operation, and then design a plan from an overall, bird's-eye view. During development and procurement, we consider and compare the functionality, quality, and cost balance in order to optimize the design and what we purchase, considering compatibility with existing equipment while also incorporating the latest technology of the day. During operation, we work on in-house production, and we have achieved rapid maintenance operations by adding new functions, by efficiently allocating various resources, and by standardizing and automating. Continuing these efforts enables us to provide a high-quality integrated systems platform.

Knowledge gained from operations is also utilized in SecHack365 to visualize network operations and traffic, and also to make trouble shooting visible to the participants. I am really looking forward to future trainees who are deeply interested in these areas.

The platform team's duties are not something that can be done by just one person, and are accomplished through teamwork and collaboration with team members. Going forward we will continue to support NICT's initiatives by putting our team's heart and soul into the work.

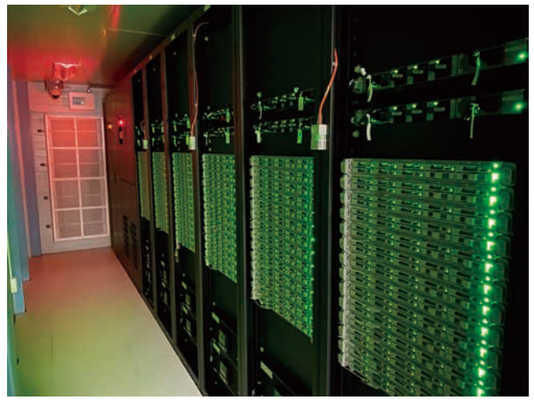


Photo of the inside of a Cy02 container-type data center operating at the Hokuriku StarBED Technology Center

Utilized as the main human resources development platform, the latest high-performance servers are interconnected with a high-speed, high-capacity network.
Equipment for the exercises can be used from exercise venues throughout Japan via the JGN research network and internet lines.
Electricity and cooling for container-type data centers are also primarily operated by members of the platform team at the Hokuriku StarBED Technology Center.

NICT NEWS 2020 No.4 Vol.482
Published by **Public Relations Department, National Institute of Information and Communications Technology**
Issue date: July 2020 (bimonthly)

4-2-1 Nukui-Kitamachi, Koganei, Tokyo
184-8795, Japan
TEL: +81-42-327-5392 FAX: +81-42-327-7587

URL: https://www.nict.go.jp/en/
@NICT_Publicity
#NICT
ISSN 2187-4050 (Online)