National Institute of
Information and Communications Technology

NICT NEWS

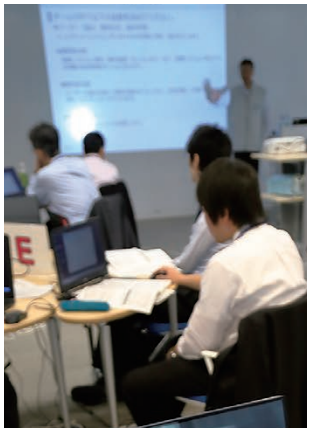
2018
No. 1
Vol. 467

FEATURE

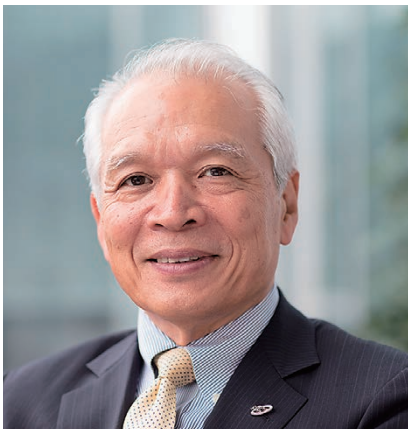
Protect Society from explosive ever-increasing cyber attack

NICT NEWS 2018 No.1 Vol.467
National Institute of Information and Communications Technology

CONTENTS



Cover photo
This photo is from SecHack365, a personnel development project for young people, in which trainees learned ways of generating new ideas. SecHack365 offers a variety of content supporting their research and development (p. 6-7, this issue). The photograph on the upper-left of this page is from CYDER (CYber Defense Exercise with Recurrence) (p. 8-10, this issue).



President of the National Institute of Information and Communications Technology
Dr. Hideyuki TOKUDA

This past year the USA, with President Trump, and many other countries came under new leadership. As ever, there were frequent terrorist acts in locations around the world, and there was a pervading feeling of tension. Closer to home, cyberattacks such as WannaCry are becoming familiar and attacks on IoT and other devices by malware such as MIRAI have increased in scale and frequency. Such circumstances this past year have drawn much attention to information and communications technologies such as IoT, Big Data, AI, and cyber security, and the importance of these technologies has been strongly recognized.

As the sole national research and development agency in the field of information and communications in Japan, NICT's mission is to solve issues in society and create new value using advanced ICT. We work together every day, to research and develop world-leading advanced technologies, promoting collaboration and open innovation to expand and implement them in society.

NICT conducts information and communications R&D in the five fields of Sensing Fundamentals, Integrated ICT, Data Utilization and Analytics Platform, Cybersecurity, and Frontier Research. Last year, to further promote these results, we also established the National Cyber Training Center to plan and promote practical cyber training, and the AI Science Research and Development Center to promote R&D in AI. Together with the MIC and with broad cooperation from many involved people, we also began operating Translation Bank, to gather and use translations from various fields, so that automatic translation systems can be applied in many fields and accuracy can be improved. We are also working with research agencies, enterprises, universities and local governments on various joint research and demonstration projects, promoting activities to use NICT technologies in enterprise, and working with bodies such as ITU and IEEE on international standardization.

Since I became President in April of last year, I introduced three concepts to my management policy that I want the staff to keep in mind constantly: Collaboration, Open-mind and open innovation, and Challenger spirit. Then, in an effort to organically integrate and realize these policies last year, we held events such as ideathons, to boost interaction between departments, encourage creation of new research themes, and draw out a diversity of new views with open discussion throughout the organization. We also promoted initiatives with various other agencies to tackle regional challenges domestically and internationally. We also held events to collect ideas on how to develop the ICT field further, to get opinions from the general public on R&D issues that we should be focusing on in the future. We will continue these initiatives and use them in operation of the Institute.

At NICT, we have received input from a wide range of people, and will continue our efforts to further advance the field of ICT, cooperating and improving ourselves with the help of all involved, and encouraging collaboration among industry, academia, and government. We hope for your continuing support and cooperation in the future as well.

In conclusion, I hope that the coming year is wonderful for all of you, and wish you the best for the New Year!

INTERVIEW

Building Personnel and a Core R&D Community

The topic of cyber-attacks has been addressed frequently in the mass media recently, and the techniques being used are becoming more and more diverse and malicious. The National Cyber Training Center was established on April 1, 2017 as an organization to deal with this situation using knowledge gained in earlier cyber security R&D, and to plan and promote practical cyber training in society. We spoke with Dr. Michio SONODA, Director General of the Center, Dr. Masashi ETO, Director of the Cyber Training Laboratory at the Center, and Tomohiro HANADA, a Technical Researcher at the Cyber Training Business Promotion Office, regarding how the Center came to be established and its activities.

The shortage in cyber security personnel

——To begin with, can you tell us about how the National Cyber Training Center came into being?

ETO: A big news story in 2011 was how major enterprises were subject to large-scale cyber-attacks, and since then, in the early 2010s, there have been a series of information leak incidents targeting major enterprises. There is an increasing sense of crisis prompted by incidents such as these, and a shortage of personnel qualified to handle security has been identified in society. The Ministry of Economy, Trade and Industry (METI) has also issued a report regarding this issue, suggesting that by the year 2020, there would be a shortage of 193,000 people in this area ("Survey results on the latest trends and projections in IT Personnel: Report Summary," June 10, 2016).

Given these conditions, government effort into training cyber security personnel has also gained momentum, mainly at the National center of Incident readiness and Strategy for Cybersecurity (NISC). One particular security personnel training project started by the Ministry of Internal Affairs and Communications (MIC) in FY2013 is the cyber defense training program called CYDER, which is currently operated by the National Cyber Training Center. The CYDER program actually started before our Center was initiated.

The favorable results produced by CYDER led to a desire to expand its scope and enhance the content with new knowledge and technology. On another front, the decision was made to host the Tokyo 2020 Olympics and Paralympics ("Tokyo Olympics"), and the need to train security personnel suitable for that event further increased urgency. As a consequence, management of the CYDER project was given to NICT, with its history of research initiatives and deep knowledge of cyber security, and a new organization was established within NICT to strengthen security measures for the Tokyo Olympics.

As a first step, the Cybersecurity Human Resource Development Research Center was established in FY2016. This was then expanded and reorganized to form the National Cyber Training Center in April 2017. Its business included three main projects: CYDER, a practical cyber defense training program transferred from MIC; CYBER COLOSSEO, a practical cyber training program for the Tokyo Olympics; and a new program called SecHack365, to train young security personnel with a perspective looking farther into the future.

Experiencing cyber-attacks on a virtual network with CYDER

——Can you tell us about the content and status of the first project, the CYDER cyber defense training project?

SONODA: Various organizations have been damaged by cyber-attacks in recent years. If an organization does not respond appropriately immediately after a cyber-attack, the damage to the organization can expand rapidly. Even though it is difficult to prevent damage completely, organizations must act with appropriate decision-making to prevent expansion of dam-

From the left: ETO, SONODA, HANADA (See p. 5 for profiles)

age. The immediate response after an incident is important in minimizing the damage. CYDER provides training for this sort of initial response.

As an example, when many people are injured during a disaster, medical personnel must prioritize care according to urgency. This is called triage, and there is a similar need when it comes to security. It is particularly necessary to prioritize and handle incident response according to urgency. So, what areas are potentially more urgent, and how do they manifest? And what adjustments should the organization make as their next step? Decisions must be made and action taken quickly. CYDER training incorporates simulation of such situations.

CYDER trainees first receive approximately one hour of prior online training. Then, they meet at the training venue for a one-day session. Teams of three to four members are formed, with roughly ten teams participating in each session. Virtual networks with virtual terminals for each of the ten teams are built on StarBED, a large-scale computing environment operated by NICT. Each of the teams is able to experience and study cyber-attacks and how to handle them using these virtual networks as a platform.

They look at computer logs for any suspicious data, identify and locate the source of contamination, and attempt to contain it. They then discuss whether the analysis and handling leading to identification of the threat was appropriate, and finally, consider what should be done if the situation occurred at their organizations. This knowledge and experience can then be brought back to their organizations. This is the structure of the CYDER program.

When it was operated by MIC, the CYDER program had approximately 200 participants per year, but when it was transferred to NICT it was expanded to 1,500 participants. It was then doubled to 3000 in FY2017. Initially it was offered primarily to government ministries and agencies, but this has also been expanded to include regional governments and independent administrative agencies. Till last year the program was held in 11 venues, but this fiscal year it was held in all 47 prefectural regions.

Recently, demand to run sessions for organizations beyond government has increased and we have begun offering CYDER training sessions for compensation. Smaller organizations, even with only one security person, can receive this training by joining with other similar organizations and applying together.

A more practical CYBER COLOSSEO and the future with SecHack365

——The second project, CYBER COLOSSEO, is an even more concrete initiative, preparing for the Tokyo Olympics, isn't it?

ETO: CYDER is for personnel from central and regional government organizations, with the intention of broadly raising the overall level of security, but the main objective of CYBER COLOSSEO is to provide intensive training for security personnel in the Tokyo Olympic/Paralympic Organizing Committee. It was also established in FY2016. The first session was run by MIC and later sessions have been run by NICT.

With the Tokyo Olympics as a concrete target, CYBER COLOSSEO must train at a deeper level than CYDER, and in contrast with the de-

Interview

Building Personnel and a Core R&D Community

fensive approaches studied in CYDER, a significant feature of CYBER COLOSSEO is simulation of an offensive and defensive cyber battle format More effective defenses can be mounted by understanding the intent of the attacker.

The 2020 Tokyo Olympics will attract the attention of the world, so it will also attract a high volume of cyber-attacks. At the 2012 London Olympics, there were incidents causing the ticketing sites to shut down due to attacks. Depending on the scope and type of damage, attacks can affect revenue and also cause significant damage to the event brand. Of course, the government and Metropolitan Tokyo are being very sensitive to smooth operation of events and services, and NICT is also collaborating closely with the Tokyo Olympic and Paralympic Organizing Committee to build even better programs.

——SecHack365 is a new project initiated by the Center and is quite different than the previous two. What sort of content does it offer?

HANADA: The objective of SecHack365 is to train young innovators that can do their own R&D, beyond simply operating existing software. It is open to trainees 25 years old or younger from the general public. Trainees in FY2017 ranged widely from a ten-year-old elementary school student to adult working members of society. This range of ages was not selected intentionally, but resulted from selection based only on personal information, answers to application problems, and applicants' enthusiasm and desires.

With SecHack365, trainees stay in contact till the end of FY 2017. Specifically, they use an online development environment and communication platform, and roughly once every two months, they gather for hackathon* retreats, other events for individuals to present development results, and tours at leading enterprises.

Usually, hackathon organizers decide on a single theme or direction, but a major feature of SecHack365 is that individual trainees decide what they will create or research based on their own interests, and members of the Executive Consultation Committee provide continuous support as trainers. In fact, we have quite a rich variety of themes. Another strength of SecHack365 is the depth of support provided by our layer of trainers, and we intend to increase our number of trainers in the future. The 365 in SecHack365 refers to 365 days a year, and it also raises the challenge of what ambitious

SecHack365, Aug. 23-25, 2017 (Fukuoka course)


Left/right photos: CYDER practicum, June 20, 2017 (MIC Auditorium)

trainees can achieve in such a dense learning environment.

A larger, more flexible core framework to handle security

——Projects at the Center to train personnel for the approaching 2020 Tokyo Olympics and beyond are very interesting, but can you tell us about other directions and aspirations of the Center in the future?

SONODA: I believe that the National Cyber Training Center as an organization must operate on a still broader scale. This goes beyond simply expanding our current projects. We are training security personnel, including defending against cyber-attacks, and passing on technology and know-how, but there are still areas we are not covering.

So, what do we need to do to cover these areas?

Some issues can be resolved using personnel and financing, such as by sending personnel to trainees if they cannot come to us, but there is still room for other approaches. One example is to create other mechanisms for providing training to those that cannot attend our current sessions. We want to increase the number of such mechanisms in the future, as possible only with environments and opportunities at NICT and the Center.

The same also applies to the members of the SecHack365 Executive Consultation Committee; we want to create mechanisms enabling many people from within and outside the Center to participate in the project, regardless of their level of commitment. It will become a platform to enhance various R&D initiatives and create a structure for cooperation during emergencies. I would like to see our Center function as the core for that sort of platform.

* Hackathon: A word combining "hack," used in software and engineering, with "marathon." Used for events mainly in software development, where programmers and engineers gather for intensive development sessions.

Michio SONODA
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.

Masashi ETO
Director
Cyber Training Laboratory
National Cyber Training Center

Joined NICT in 2005 as a researcher in the Cybersecurity Laboratory till 2016, and at his current position since then. Engaged in cyber security related R&D including network operations and management technology, application trace-back technology, the NICTER project, IPv6 security, and ITS security, as well as international standardization and human resource development. Ph.D. (Engineering).

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

Joined NICT in 2017. Previously involved as project manager in development of banking systems. Besides work, founded the information security community in Kyushu, holding study groups and other events. Currently involved as a technical researcher in the three major projects at the National Cyber Training Center: CYDER, CYBER COLOSSEO, and SecHack365.

SecHack365 https://sechack365.nict.go.jp/

SecHack365: A Year-long Personnel Development Project for Young People

SecHack365 logo built by the Executive Committee

Hironobu SATOH
Ph.D., CISSP
Senior Researcher, Cyber Training Laboratory, National Cyber Training Center
Visiting Researcher, Kochi University of Technology
SECCON Executive Committee
Security Camp Instructor
SEC Dogo Program Committee
SecHack365 Implementation Consultation Committee

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 Technology, 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.

SecHack365 is a portmanteau of "Security" and "Hackathon," and the name of a program started in 2017 to improve security technical capabilities and industrial competitiveness in Japan, by cultivating researchers and developers with advanced technical skills.

Security products made in Japan do not have a large share of the global market, so it is necessary to use products from overseas, without knowing their internal details or what algorithms are used in them. SecHack365 was planned as a program to overcome this situation, giving guidance in research and technical development to young people under 25 years of age and producing cyber-security researchers and entrepreneurs for the future.

Program Overview

SecHack365 is composed of the following content.

- **Hackathon**

  This is an event in which technologists gather at a venue for a fixed amount of time, compete on ideas and results in software and other areas, and gain R&D experience in advanced security-related technologies. This is supported by members of the implementation consultation committee specializing in fields such as security and software development.

- **Remote development training**

  Ongoing R&D from home by connecting through a VPN[*1] to the "NONSTOP" remote security-development environment prepared by NICT.

- **Contest exercises**

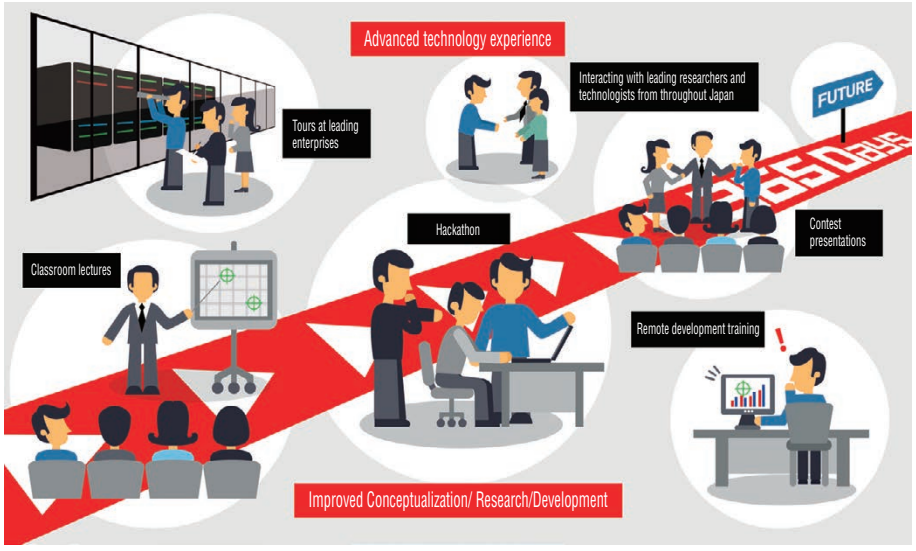
  A contest is held to utilize the capabilities of all participants, without focusing on a particular technical domain.

- **Utilization of latest research data**

  The vast amount of valuable security-related data obtained by the NICT cyber-security research over many years is used.

For the first fiscal year, there were 358 applicants, and from these 47 trainees were selected for enthusiasm and conceptual abilities, based on their application information.

Venues were established in various regions including Tokyo, Fukuoka, Hokkaido, Osaka, and Okinawa, so that trainees can generate free, creative thinking and active collaboration among trainees through an environment with good facilities and surroundings including com-



SecHack365 Program overview

Figure 1 June 2017 Kamata (Tokyo) course

Theme	Become an idea brain!
Objective	Stimulate creativity
Venue	Fujitsu PLY (Fujitsu Inc.)
Trainers and Guests	Fujitsu Inc.: Mr. Kosetsu KAYAMA, Mr. Hidehiro TAKEDA It's Co. Ltd.: Mr. Tatsuya KUBOTA

- Fujitsu PLY had many 3D printer and other devices to stimulate creativity, which were used by trainees to stimulate their "idea brains" and create new ideas.
- Provided an opportunity to study new ways of generating ideas, such as changing the viewpoint or distance, as needed in this era of intense change.

Figure 2 August 2017 Fukuoka course

Theme	Changing gears from Creating ideas to manufacturing!
Objective	Manufacturing through collaboration
Venue	LINE Fukuoka Co. Ltd. Kyukamura Shikanoshima
Trainers and Guests	LINE Co. Ltd.: Mr. Kenji AIKOU

- Trainees present the ideas they have produced so far to other trainees and trainers, receive feedback, and refine them into products in an "Idea trade fair."
- A multi-track hands-on event called "Ennichi" was held. Included a hand-made router using a Raspberry Pi*2, introduction to deep learning, and Intensive Soldering.

pany tours and guest hackers.

To operate SecHack365, the SecHack365 executive committee was organized by NICT members and external security specialists. The implementation consultation committee provided technical support as trainers. SecHack365 was made possible through support from many others as well, including the venues, the implementation consultation committee, the individual trainees' schools, and their families.

There have also been recent reports in the media, of young people being received guidance for creating viruses because they knew about security, but did not understand related ethical and legal issues. SecHack365 goes beyond research and technical development in the hackathon, also including education on ethics and the legal system as it relates to security, with themes such as "Research ethics," "Actual law regarding cyber security," and "Rules that are followed, and rules that are not."

Achievements at SecHack365

At SecHack365, we call this group of trainees sharing the same objectives and values, "collabo" (ration). Of course, doing development individually is accepted, but we also encourage finding "collabo" through the idea trade fair and other interaction. The synergy effects of working with people having different backgrounds—whether in research themes, what they have learned, or experience in society—make it possible to pursue technology that would not have been possible to imagine or develop individually.

Particularly in Fukuoka, we held a practice fair, to expose trainees to the specialized technology and knowledge of the trainers.

The latter part of the Fukuoka hackathon was filled with enthusiasm, due to a combination of inspiration from the idea trade fair and practice fair (see Figure 2) and the picturesque background scenery of the Genkai-nada Sea. Communication on SNS was still active after the event ended, and trainees carried the excitement of the hackathon back into their everyday activities.

Anticipating the meeting to report results

SecHack365 is a one-year project, but the presentation of results is approaching in March, and the first SecHack365 will soon come to an end. Personally, it has been a year in which I have learned much and been stimulated by ideas created by the trainees with different perspectives than my own.

In conclusion, I look forward to the activities of these trainees in the future, and also to meeting and collaborating with new trainees in the next fiscal year.

*1 VPN (Virtual Private Network): A technology for providing safe communication over the Internet and other networks by using encryption.
*2 Raspberry Pi: A computer developed for education by the Raspberry Pi Foundation.

CYDER Cyber Defense Exercise with Recurrence *http://cyder.nict.go.jp/*

Promotion of CYDER: CYber Defense Exercise with Recurrence

Kouichi SHIMADA
Director of Cyber Training Project Promotion Office
National Cyber Training Center
Joined the Communications Research Laboratory (currently NICT) in 1980.

Mana KAWASATO
Assistant Chief, Cyber Training Project Promotion Office
National Cyber Training Center
Joined NICT in 2009.

Cyber attacks have diversified and become more sophisticated in recent years, and attacks on government agencies, regional public organizations and important infrastructure continue to increase. Various cyber security products and services are being introduced to handle these attacks, but this alone does not appear to be sufficient, and preventative measures against cyber attacks are very difficult. On the contrary, it is believed that many organizations have been infiltrated, undetected for long periods of time.

If 100% prevention is not possible, it is important that organizations train to handle cyber attacks appropriately for cases when incidents occur.

NICT conducts a program of practical exercises called Cyber Defense Exercise with Recurrence (CYDER), involving a series of actions to be taken in case of cyber attack, to improve the incident response capabilities of information system administrators and others. This is being done to avoid simply depending on external vendors and to develop highly capable information system administrators that can handle attacks threatening business continuity, while considering everyday system operations.

History of CYDER

CYDER was a demonstration program run by the Ministry of Internal Affairs and Communications (MIC) from FY2013 to FY2015. For the program, NICT provided a large-scale training environment built at the Hokuriku StarBED technology center. According to a cabinet decision on cyber security strategy in September 2015, NICT's training platform and technical knowledge of attack monitoring and analysis was to be used for practical training and prac-

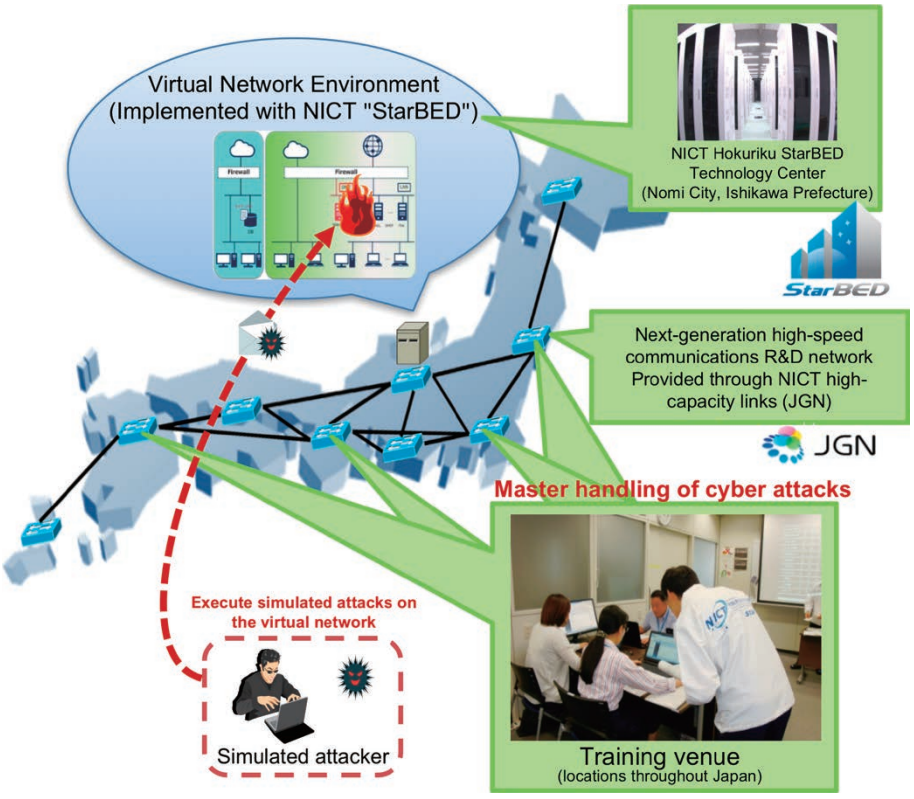


Figure 1 CYDER training overview

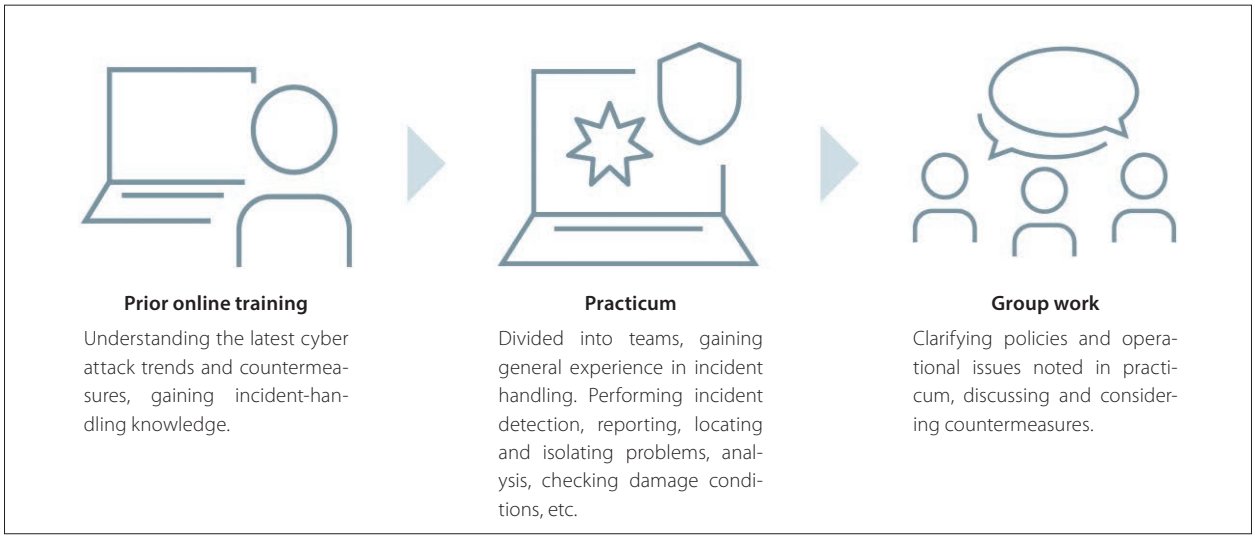


Figure 2 The CYDER curriculum

tice at government agencies and for important infrastructure. Then, in May 2016, NICT was made the operating body for CYDER through revisions to the Institute for Information and Communications Technology Law. This has enabled the program to operate continuously and with stability since then, and the training system has been enhanced significantly.

Overview and Features of CYDER

The most important feature of CYDER is that it can provide the latest training scenarios, reproducing current cyber attack examples based on data accumulated by NICT over many years and a comprehensive analysis of trends in cyber security and cyber attacks particular to Japan. Training is given to teams of three or four trainees who are in charge of information systems at government agencies, regional public organizations and important infrastructures, based on these scenarios.

Specifically, a group of high-performance servers located at NICT's Hokuriku StarBED Technology Center is used to simulate the network environment of an organization. The latest cyber attacks are simulated in this environment, and trainees practice aspects of response ranging from incident detection to handling and reporting. This is done through actual operation of real devices and software.

The CYDER Curriculum

Trainees complete online study before taking practical training. In this study, they learn foundational and other knowledge required for the practical training.

In the practicum, trainees gain practical experience performing real operations, hands-on with PCs.

In workgroups after the practicum, each team selects a team leader and secretary, and discusses operational and other issues and solutions they encountered in the practicum, and each group gives a presentation to the other teams. We also conduct tests before and after the training, enabling us to check how much knowledge trainees gained.

Through this series of tasks, trainees should be immediately useful for practical work after returning to their organizations. A support system for trainees, accommodating their individual skill levels and progress, is also provided so training can also be given to beginners in the field of security.

CYDER Implementation State

In FY2016, there were 1,539 trainees from 764 organizations trained in 39 sessions in 11 regions throughout Japan, but applicants far exceeded the scale of the program, so we were forced to limit the number of entrants.

As such, the scale of the program was expanded significantly in FY2017, with a total of 100 sessions held in 47 prefectures throughout Japan, and a target of over 3,000 trainees.

This fiscal year, an opening ceremony was held on June 20, 2017 in the MIC Auditorium, coinciding with the start of the first CYDER session of the year, to be followed by a series of sessions in the 47 prefectures.

CYDER in the Future

As the Tokyo 2020 Olympics and Paralympics approach, cyber attacks are becoming more serious and they are expected to increase in sophistication.

To combat cyber terrorism as it becomes more serious, it has become an urgent matter to cultivate cyber security human resources who will be able to deal with cyber attacks, through CYDER training.

Contents of CYDER

(CYber Defense Exercise with Recurrence)

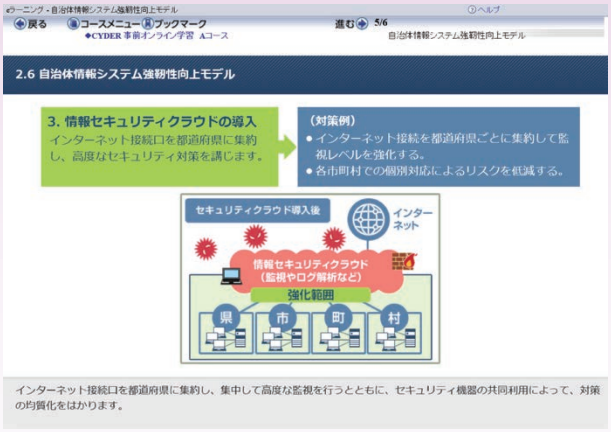
This year, CYDER is composed of prior online training, practice, and group work. Here, we introduce some of the content and underlying environment for this training.

Nobuhiro KANAHAMA
Senior Technical Researcher
Cyber Training Laboratory
National Cyber Training Center

Prior Online Training

The prior online training for CYDER was built on Learning Management System (LMS), and as with ordinary e-Learning, it is a system that anyone can participate in easily. To ensure that participants from anywhere in Japan can access it through the Internet with a Web browser, the environment was built within the StarBED technology center in Hokuriku.

Since participants are usually busy with their other duties, the amount of work required has been kept to a minimum, by concentrating the overall content into the minimum of background knowledge needed for training in incident handling. Thus, it has been reduced to a volume that can be completed in 60 to 90 minutes. Content is also organized in detailed chapters and sections with many illustrations, so that each item can be covered in 3 to 5 minutes. This helps participants complete it a little at a time using small breaks in their other duties, without it becoming too tedious.



Prior online training screen

Practice and Group Work

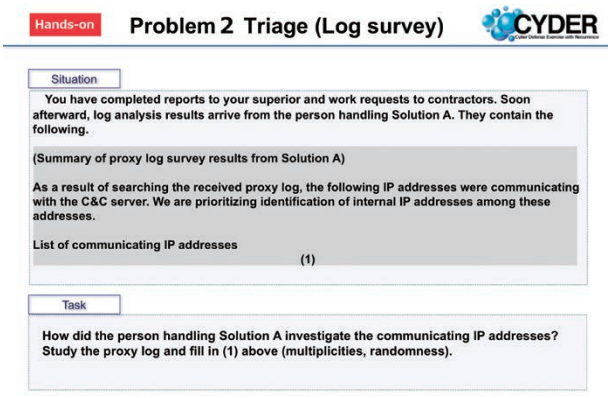
The group training, which is the core of CYDER, is done in groups of three or four in a team. Participants gain practical experience by performing each incident handling step as an "issue" or "milestone," according to the scenario, from "detection or receiving contact" to "isolation" and "creating reports," operating actual equipment and software throughout.

There is a large amount of useful information in real environments, such as logs from proxy servers, and it can be used to identify terminals infected with malware and performing unauthorized communication. Each year, we also create new training scenarios, incorporating the latest advanced findings from the NICT Cyber Security Laboratory. For example, scenarios in this year's Course B include the WannaCry incident that spread throughout the world this year, as well as attacks on vulnerabilities in applications using Apache Struts2.

The training environment is built within StarBED, as with LMS, modeling networks within real organizations.

Then, in the group work at the end, participants discuss how they would implement such measures within their own organizations, environments, and security policies.

In this way, the content is designed to emphasize enabling participants to bring the practical experience gained through all aspects of the CYDER training back for use within their own organizations.

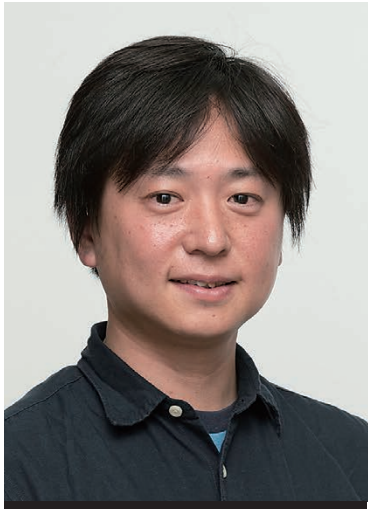


Issue/Milestone Example

cyber colosseo https://colosseo.nict.go.jp

The CYBER COLLOSEO Project

For stable operation of the Tokyo 2020 Olympic and Paralympic Games



Masashi ETO
Director
Cyber Training Laboratory
National Cyber Training Center

The Tokyo 2020 Olympic and Paralympic Games (2020 Tokyo Olympics) will be held in 2020, and as such a large-scale international event with the attention of the world, it is expected to present an attractive target for cyber attackers. To avoid events being suspended and obstruction of related businesses due to cyber attack, and to maintain normal operations, there is urgent need to gain know-how and strengthen personnel in cyber security in addition to regular preparation work.

The CYBER COLOSSEO project, operated by the National Institute of Information and Communications Technology (NICT), provides cyber training for security personnel related to the 2020 Tokyo Olympics, to promote stable operation of the event.

CYBER COLLOSSEO endeavors to provide personnel training at a technical level equivalent to CYDER and still higher levels. This practical training consists mainly of lectures, practice, and battles using both attack and defense technologies, in an environment simulating conditions anticipated during an event like the Olympics.

Among organizations involved in the 2020 Tokyo Olympics, CYBER COLLOSEO training is being given to members of each department of the Olympic organizing committee and employees at system vendors for each department. Training is provided at levels from beginner to pre-advanced, as shown in the table below, and trainees can decide which courses they will take according to their technical capabilities.

Each course, from beginning to pre-advanced, is composed of classroom work and practical work with cyber-security technologies. The pre-advanced course in particular, includes battles specialized to the technical areas of each trainee, such as Web, networking, or forensics.

In these ways, the CYBER COLLOSEO training program has prepared content suited to the technical level and domain of trainees and works to improve their capabilities through repeated, battle-oriented training.

These events will be held continuously, starting this year, in preparation for the 2020 Tokyo Olympics, working to strengthen resilience against cyber attack in related organizations.

	Prior knowledge required for each course	Audience (who are to be trained)
Beginner Course	• Experience operating computers (esp. Windows)	• PC/network users who will engage in security management in the future
Intermediate Course	• Basic knowledge of computers and networks (esp. Windows and TCP/IP) • Basic knowledge of cyber security	• Persons who will take leadership in security management • Persons handling contact and coordination with users and related internal and external departments for incident handling
Pre-Advanced Course	• Knowledge of computers and networks (esp. Windows, Linux, Unix, TCP/IP) • Knowledge of cyber security (esp. network security, binary analysis, forensics, web security, database security, OS security, either strategy or governance)	• Persons able to immediately handle advanced cyber attacks using their own skills • Persons having techniques for detailed analysis of malware samples or contaminated devices

Table CYBER COLLOSEO course configurations

* For advanced level personnel requiring competency higher than "Pre-Advanced," it is preferable to recruit personnel with more experience, such as from security solution vendors, rather than training them through practice. As such, this project focuses on training at the beginner, intermediate, and pre-advanced levels.

Observation of a Fra Angelico Fresco Painting Using Wide-Band Electromagnetic Waves

Dr. Kaori FUKUNAGA
Director of Electromagnetic Applications Laboratory,
Applied Electromagnetic Research Institute

Art conservation treatments applied by conservators over centuries allow us to appreciate historical artworks, such as Renaissance paintings, in the 21st century. Similarly to a medical operation, conservators often use scientific examination before and during the treatment.

Heritage science research has progressed since the 1970s, after the disastrous flood of the Arno River in Florence in 1966. Among the various types of scientific examinations imaging techniques using wide frequency bands from microwave to X-ray are particularly appreciated for the examination of masterpieces, because they can visualize the internal structure of artworks nondestructively.

In 2016, NICT, Istituto di Fisica Applicata "Nello Carrara" (IFAC), and Istituto Per Il Rilevamento Elettromagnetico Dell'Ambiente (IREA) investigated the "Annunciation" by Fra Angelico, a masterpiece of fresco painting in the north corridor of the San Marco Museum, Polo Museale della Toscana.

Initial observations were carried out visually, but at an extremely high resolution. The image at 100 ppi of the 3.2 m wide by 2.3 m tall painting was obtained using an automatic digital imaging system developed by Hitachi Ltd. In this particular case, three digital cameras were simultaneously used to obtain approximately 1500 shots in one day. Figure 1 shows part of the visible image and the effect of edge enhancement, which can show small cracks clearly, allowing the examination of the preparation layer.

Electromagnetic waves from microwave to X-ray are used to investigate the internal structure of an object as well as to identify the materials used in the original artwork and in previous conservation methods. Figure 2 shows a photograph taken during the electromagnetic measurement. The instrument on the left-hand side is a THz imaging system developed by Pioneer Corp. that revealed the condition of the preparation layer. On the right-hand side, the author can be observed carrying out X-ray fluorescence spectroscopy for element analysis, which allowed the identification of the pigments used in the masterpiece.

Here, it is important to use as many techniques as possible to gather useful information for the production of a good conservation plan. For example, visible images suggested that the condition of the preparation layer has some discontinuities from the appearance of cracks on the surface, and internal structure observation by THz imaging supported this idea. From an artist's perspective, differences in crack features depend on the skill of the person who made the mortar and on atmospheric conditions, because the fresco technique uses a chemical reaction of mortar and carbon dioxide in air. Photographic techniques, including ultraviolet and infrared imaging, suggested that consolidation was previously performed, and this was confirmed by fiber optics reflectance spectroscopy, which is a type of broadband spectroscopy.

All the results obtained in this case study are introduced in a new book published by Sillabe s.r.l. A digital museum event using high-resolution visible images and scientific examination results is planned. In addition, similar examinations were applied to panel painting analyses in Estonia in 2017, and will be reported in an academic research paper in the near future.

Figure 1: Edge enhancement of high-resolution visible images.

Figure 2: Photograph of scientific examination using electromagnetic waves. Air cap sheets were used to protect the glass plates in front of the wall painting. The instrument on the left-hand side is a THz imaging system developed by Pioneer Corporation. The author carrying out X-ray fluorescence spectroscopy for element analysis can be seen on the right-hand side.

Author:
Kaori Fukunaga received her Ph.D. in Electrical Engineering while she was working at Fujikura Ltd. She also graduated in Art and Design. She joined NICT and is in charge of nondestructive sensing technology. She is a member of the Science Council of Japan.

Awards

The Merit Awards for Industry-Academia-Government Collaboration are presented for instances of great success, which contribute significantly to promoting collaboration among industry, academia, and government, either reaping great success through such activity at corporate, university, or public research institutions, or otherwise conducting pioneering initiatives.
The Red Hat Innovation Awards are awarded to enterprises that have created solutions to IT problems using open source software, have promoted innovation through reform or modernization of information technology, or have achieved improvements in agility or productivity.

Minister for Internal Affairs and Communications Award of 15th Annual Merit Awards for Industry-Academia-Government Collaboration

Yutaka ASHIKARI

Director, System Development Office
Advanced Speech Translation Research and Development Promotion Center

Hearing-impaired people are able to enter questions as text, which is then conveyed as speech. A hearing person is able to answer using just speech, and this is conveyed in the form of text.

Overview

●Description: Awarded in recognition of major contributions to realizing a cohesive society in cooperation with industry, academia and government, developing and expanding the KoeTra smartphone application. KoeTra uses speech recognition and synthesis technologies developed by NICT to convert between speech and text in real time. It facilitates communication with hearing-disabled people. The technology was transferred to Feat Ltd. in January 2015, and has been downloaded 52,152 times as of October 31, 2017.
●Co-recipients: Teruji KOBAYASHI (FEAT Limited), Setsuji ARIKI (Telecommunications Carrier Association)
●Date: August 21, 2017

Comment from the Recipient

We developed KoeTra as an applet to support the hearing disabled after I received an e-mail from Professor Yamada at the Kumamoto Prefectural School for the Deaf.

The applet was found to be useful, and we were able to transfer the technology to a private enterprise for permanent operation. This honor belongs to all involved in NICT's speech translation research. I would like to offer thanks to all these researchers and also to Professor Yamada. We will continue our efforts to develop systems that are useful to society in the future.

Red Hat Innovation Awards APAC 2017

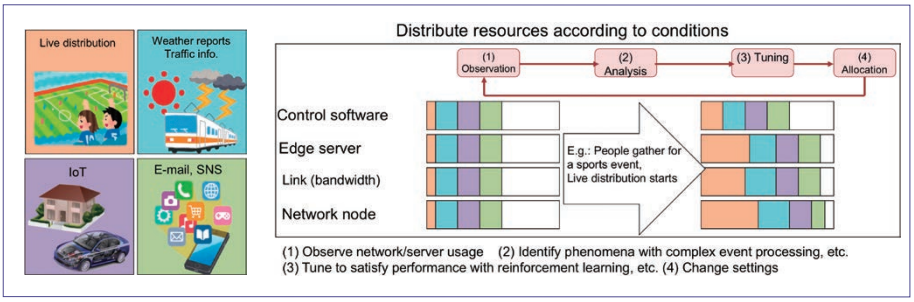
Category: IT Optimization/Cloud Infrastructure

National Institute of Information and Communications Technology*

*Awarded to the organization

Overview

●Description: NICT introduced the Red Hat OpenStack Platform to demonstrate effectiveness of our autonomous control architecture for network and computing resources. We developed verification infrastructure for experimental scenarios that establish both system administration load reduction and stable service quality, and for stable provision of fast and reliable services in a future.
●Date: October 20, 2017



Automating computing and communication resource assignment and arbitration to support stable service quality

Comment from the Recipients

We are honored that our laboratory is being recognized for providing sufficient service quality to potential network users. Future networks should change volume and location of allocated resources elastically in advance and/or in response to changes in personnel mobility and environment. We would like to thank everyone in our research institute for their support in R&D, and many others for their guidance. We will continue in the future, together with laboratory members, implementing systems incorporating with new ideas that have not yet progressed beyond theory, and contributing to standardization.

Comment: Hiroaki HARAI, Director, Network Science and Convergence Device Technology Laboratory, Network System Research Institute

Mr. HARAI is in the center

NICT NEWS 2018 No.1 Vol. 467
Published by **Public Relations Department, National Institute of Information and Communications Technology**
Issue date: Jan. 2018 (bimonthly)

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

E-mail: publicity@nict.go.jp
URL: http://www.nict.go.jp/en/
Twitter: @NICT_Publicity

Subscription applications accepted by
E-mail or on the Web site.

ISSN 2187-4050 (Online)