Open Innovation

National Cyber Training Center

Director General　Michio Sonoda

At the National Cyber Training Center, we are working on training security operators and security innovators for positions in cybersecurity and ICT, and we are also conducting research and development in these fields (Fig.1).

In the training of security operators, we are targeting our efforts at information system managers and other cybersecurity professionals by implementing two types of exercise — CYDER (Cyber Defense Exercise with Recurrence) and Cyber Colosseo — as practical cyber defense exercises using real systems for the purpose of equipping people with incident response skills so they can respond promptly to emergencies where affiliated organizations are subjected to severe cyberattacks.

Security operator training

(a) Overview of CYDER (Fig.2)

In order to address an urgent need for the training of security experts, the National Cyber Training Center conducts cybersecurity human resource development projects based on the Act on the National Institute of Information and Communications Technology (Article 14 part 1 clause 7) by utilizing our technical knowledge of cybersecurity research, together with the NICT's large-scale network environment (StarBED), which can simulate massive practical network environments. As part of our human resource development projects, CYDER provides short-term practical training courses based on the latest cybersecurity threats. This sort of practical cybersecurity training is now being implemented and deployed nationwide.

Trainees in the courses conducted throughout Japan play the role of IT system administrators of large virtual organizations by experiencing intensive programs covering the entire process of incident response from attack detection to countermeasures and reporting in a single day.

(b) The achievements of CYDER

In FY2017, in order to secure more learning opportunities while preparing exercise scenarios suited to the trainees, we set up a beginner-level course (A-course) in addition to the conventional intermediate-level course (B-course) aimed at local public bodies, government agencies, and the like. As a result of implementing this training program on a larger scale than in previous years, we ran a total of 100 training sessions in all 47 Japanese prefectures, which were attended by 3,009 trainees (approximately twice the number trained in the previous year). CYDER has thus become Japan's largest training program of this sort.

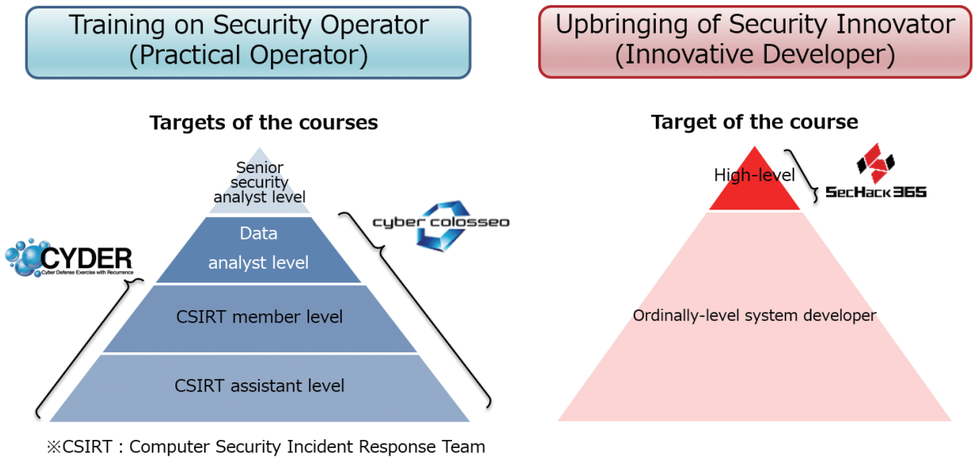

Fig.1 : National Cyber Training Center program overview

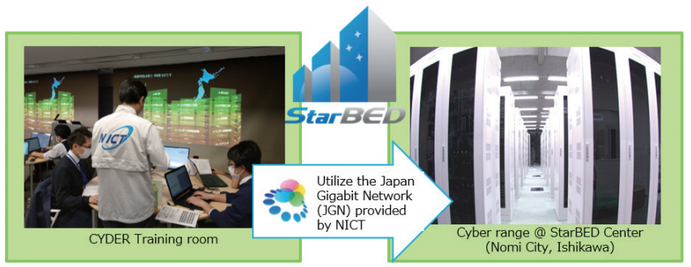

Fig.2 : Virtual network environment for CYDER training

Fig.3 : Battle-oriented cyber training concept

(c) Overview and achievements of Cyber Colosseo (Fig.3)

Since 2017, with the aim of providing phased and systematic training of people with the necessary skills in the run-up to the Tokyo 2020 Olympic and Paralympic Games (which are now less than two years away), we have been providing security personnel from organizations involved in the Olympic and Paralympic Games with training in advanced practical content such as offensive and defensive battles, in addition to the fundamental CYDER knowledge. This culminated in the Cyber Colosseo training program where real systems are used to train people with even more advanced skills. In the first year of this program, we trained 74 security personnel from organizations involved in the Games.

Security innovator training program

(a) Overview of SecHack365 (Fig.4)

In order to provide practical training for the research and development of innovative security software and the like, it is necessary to obtain technical guidance and support based on the experience and achievements of leading researchers and engineers in addition to data related to cyberattacks, such as malware samples and traffic data obtained from them, and R&D environments in which it is possible to conduct research and development using this data safely. At the National Cyber Training Center, by using NICT's NONSTOP remote development environment and R&D knowledge, we are now offering a comprehensive skills development program based on a year-long combination of an ideathon, a hackathon, remote R&D, and exercises (SecHack365).

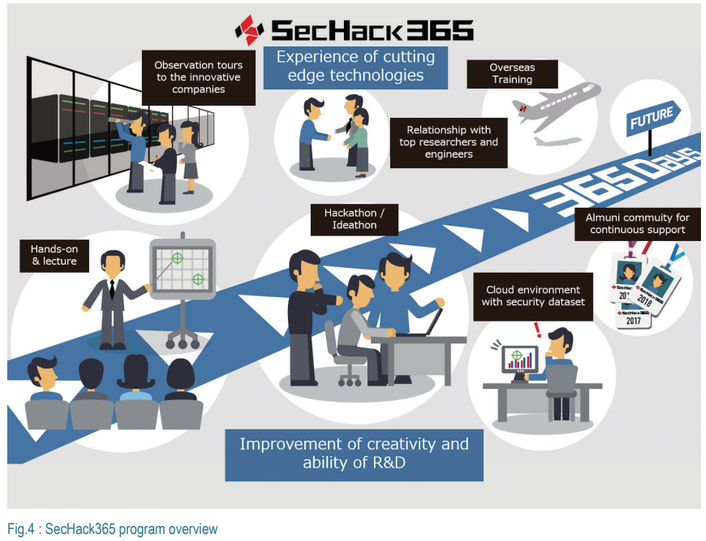

Fig.4 : SecHack365 program overview

(b) The achievements of SecHack365

In the first period (FY2017) of SecHack365, we received 358 applications and conducted cybersecurity R&D training for 47 successful candidates (trainees). These 47 trainees were trained in a total of five group training meetings held throughout Japan in parallel with the remote guidance from trainers and the provision of a remote R&D environment, and presented the results of their research and development at a final presentation meeting. The final presentation and the achievements of each trainee were also publicized in newspaper reports and other media, and drew a lot of attention in Japan as a new solution to the issue of training young ICT professionals by government agencies. In addition, four trainees who had achieved excellent scores were sent to Austin, Texas to take part in the SXSW (South by Southwest) Hackathon (the world's largest creative event of its kind) as foreign observers. Their achievement was judged to be the most creative and was awarded a prize from Cloudinary, one of the companies sponsoring the event. In the future, we aim to employ research assistants with superior grades in order to guide their research and development efforts, and if we find promising research achievements, we plan to follow them up by such means as applying for research and development at NICT. In this way, we aim to maximize the development of human resources by ensuring that this program provides continuity and development potential.