

NICT NEWS

National Institute of
Information and Communications
Technology

No.5

2022

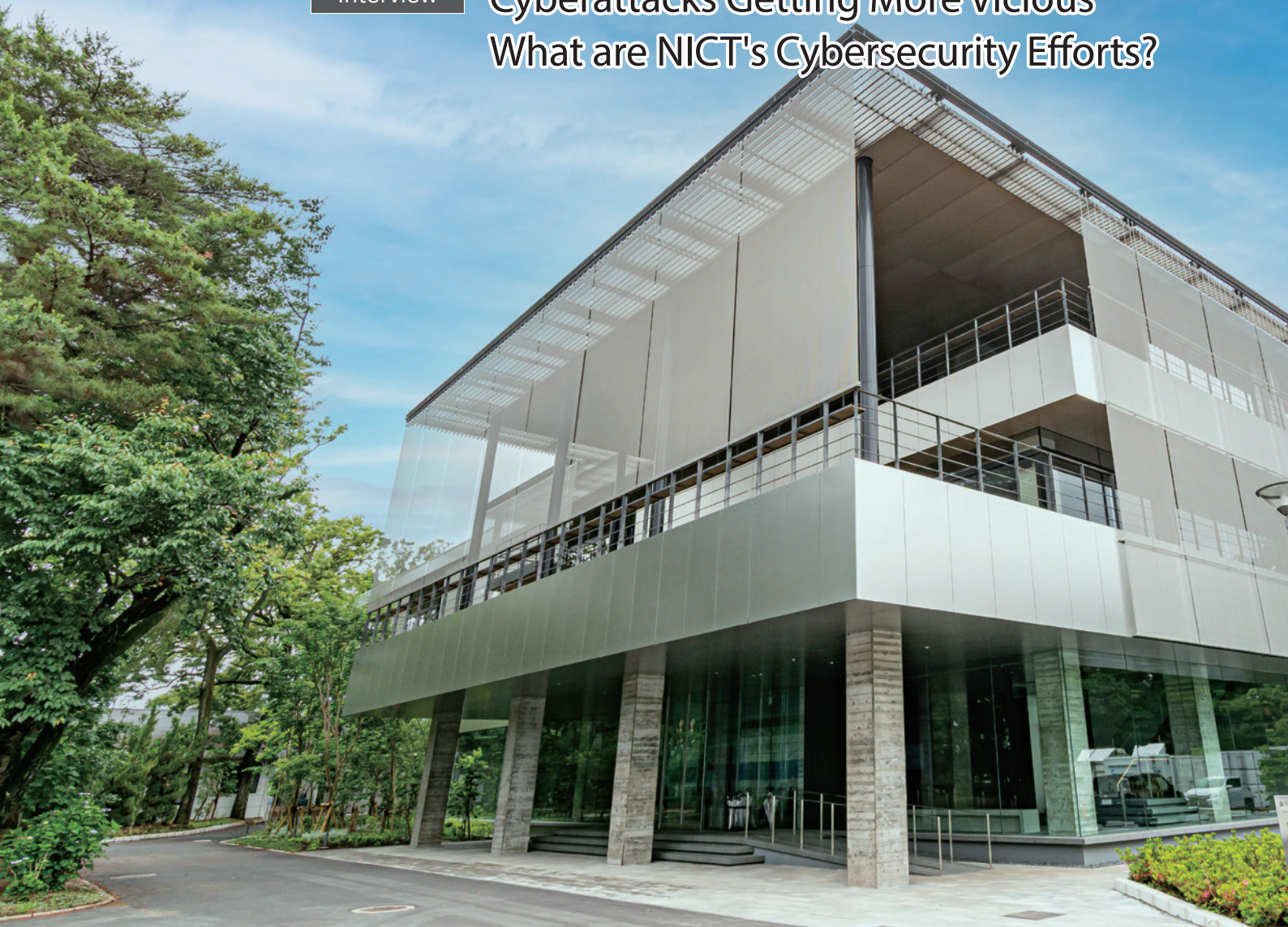
Vol.495

FEATURE

Cybersecurity for All

Interview

Cyberattacks Getting More Vicious
What are NICT's Cybersecurity Efforts?



FEATURE

Cybersecurity for All

Interview

1 Cyberattacks Getting More Vicious What are NICT's Cybersecurity Efforts?

MORIAI Shiho / INOUE Daisuke / SONODA Michio

4 Data-driven Practical Cybersecurity Research for Breaking the Vicious Spiral

KASAMA Takahiro / TAKAHASHI Takeshi / INOUE Daisuke

6 Secure Data Utilization Technologies / Cryptanalysis for Quantum Computing Era

EMURA Keita / SHINOHARA Naoyuki / NOJIMA Ryo

8 Toward the Realization of Cyber Security that Leaves no one Behind

- Efforts of NICT National Cyber Training Center -

HANADA Tomohiro / SHIMADA Kouichi / SONODA Michio

10 Toward the Nexus of Japanese Cybersecurity

YASUDA Shingo / INOUE Daisuke

12 Efforts for Safe and Secure Utilization of IoT Devices

INOUE Daisuke / TANUMA Tomoyuki / MORIAI Shiho

TOPICS

13 NICT's Challenger File 22 Ayako A. Hasegawa Developing Truly Usable Security Systems by Understanding Users' Concerns

INFORMATION

14 Awards



New NICT Fellow

NICT awards the title of "fellow" to individuals who have produced outstanding results in R&D. On May 26, 2022, NICT awarded the title to R&D Advisor YANAGIDA Toshio of the Center for Information and Neural Networks, Advanced ICT Research Institute.

NICT awards the title of "fellow" to individuals who have produced outstanding results in R&D. On May 26, 2022, NICT awarded the title to R&D Advisor YANAGIDA Toshio of the Center for Information and Neural Networks, Advanced ICT Research Institute.

Since 1998, Dr. YANAGIDA has pioneered a new research field integrating neuro science with ICT at NICT. In 2011, he had made a great contribution to establish the Center for Information and Neural Networks (CiNet) to create a global R&D center.

He is the first researcher in the world to elucidate that biological systems, such as muscles and cells, which operate with far less energy than that of artificial systems, including semiconductor processors, effectively utilize "thermal fluctuation," clearly demonstrating its potential applicability to engineering. At CiNet, he proved the applicability of the "fluctuation" principle to information processing in the brain. As Director General of CiNet, he promoted

R&D to achieve unified understanding and application of various brain functions based on the center's common goal of "creating the CiNet brain." With his leadership CiNet's scientists developed technologies to understand brain information and control an energy-efficient and fault-tolerant information network. They have developed a brain-machine interface using wireless technology.

CiNet is already a world-class research center for measuring and analyzing the human brain. In addition to fostering promising young researchers in Japan, it also serves as a center for international exchange. CiNet also conducts research on brain-based AI and promotes R&D on information communication technology that understands feelings. Dr. YANAGIDA's unique research accomplishments and leadership have been recognized both within Japan and abroad with numerous awards, including the Imperial Prize and the Japan Academy Prize, and selection as a Person of Cultural Merit and a member of the Japan Academy.

Cover photo, Upper left photo :
Quantum Security Collaboration
Building

The building was constructed so that visitors can find their favorite space, start interacting with others through repeated visits, and share opinions and ideas. Part of the building is also used by the Cybersecurity Research Institute.



YANAGIDA Toshio

NICT Fellow and R&D Advisor,
CiNet, Advanced ICT Research
Institute

FEATURE

Cybersecurity for All



Interview

Cyberattacks Getting More Vicious What are NICT's Cybersecurity Efforts?

The prevalence of remote working during the COVID-19 pandemic as well as drastic changes in the international situation have inevitably highlighted the importance of cybersecurity. People have never been more aware of how critical information protection is. What is needed now is NICT's technology as a research institute specializing in information and communications. We asked three key persons about NICT's front-line efforts in the cybersecurity area.

■ Current state of cyberattacks

—What are the recent trends in cyberattacks?

INOUE Cyberattacks have existed since the dawn of the internet. Until the late 20th century, many of them were launched just for fun. However, in the 21st century, attacks have tended to have more of a specific purpose, such as defrauding people out of their money. As cyber criminals' tactics and technology continue to advance, we also need to innovate. However, the fact is that the defensive side is short of human resources.

In regions like Europe and North America, where neighboring countries share borders, the issue of security, including military matters, is regarded as being extremely important. In Japan, however, being an island nation, neither business nor government have fully recognized the importance of security.

In 2000, however, we saw cyberattacks in which a number of government websites

were defaced all at once. In 2011, defense-related industries were victimized by targeted attacks. In 2015, cyberattacks on the Japan Pension Service stole personal data of about 1.25 million enrollees. Of particular concern nowadays are increasing attacks on medical agencies, which may lead to life threatening situations, directly affecting people's lives.

In addition, remote working has been growing due to the pandemic over the past few years, and many people now recognize the importance of security.

—It is said that cyberattacks are becoming more sophisticated and complex.

INOUE They are shifting from indiscriminate to targeted attacks, and further to ransomware attacks. A division of labor has been established among attackers, and newly developed, dedicated tools have expanded their horizons. While many attacks still target TCP port 23 (Telnet, a remote control proto-

MORIAI Shiho (center)

Director General,
Cybersecurity Research Institute

After graduating from university, she worked for Nippon Telegraph and Telephone Corporation and Sony Corporation, and then entered NICT in 2012. Current position from 2001. She has engaged in R&D on cryptography, information security and privacy protection technologies. Ph.D. (Engineering).

INOUE Daisuke (left)

Director General, Cybersecurity Nexus
Research Executive Director/
Director of Cyber Observation Operation Office,
National Cyber Observation Center,
Cybersecurity Research Institute

After graduating a doctoral course, he joined CRL(Currently NICT) in 2003. He started network security research based on NICTER, NICT's incident analysis center, from 2006. Current position from 2001. Ph.D.(Engineering).

SONODA Michio (right)

Director General,
National Cyber Training Center,
Cybersecurity Research Institute

Completed a doctorate in Engineering. He became a professor in the Faculty of Information Technology and Business at Cyber University in 2014. He 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).

col that has been around since the early days of the internet), overall, attacks on IoT devices continue to increase. IoT devices including home routers and surveillance cameras often have weak security settings, which are vulnerable to attack.

MORIAI To defend against these attacks, since 2019, NICT has been undertaking the

Interview

Cyberattacks Getting More Vicious
What are NICT's Cybersecurity Efforts?

NOTICE (National Operation Towards IoT Clean Environment) project with the Ministry of Internal Affairs and Communications and internet service providers (ISPs). For more than 100 million IP addresses in Japan, we have defined nearly 600 ID and password combinations frequently exploited by hackers and have investigated whether attempted logins can actually succeed. If so, the users of the devices will be alerted via their ISP so that they can take necessary action. Progress on the project is published every month on the NOTICE website. The effort has successfully decreased the number of vulnerable IoT devices by 21% from its peak. However, new devices are constantly being connected to the internet, so it is important to continue these kinds of measures.

INOUE A factor that led to the launch of NOTICE was the emergence in 2016 of a malware called Mirai that targeted home routers, network cameras, and other IoT devices, causing significant damage. This malware scans vulnerable devices and logs into them. Devices infected cause DDoS attacks (a Distributed Denial of Service attack floods a system with large amounts of data to bring it down) and also become zombie agents to hack into other devices.

■The importance of cryptographic technology for secure data utilization and next generation

—Research on cryptographic technology is ongoing, isn't it?

MORIAI While personal and confidential information must certainly be protected, the increased use of such data while ensuring privacy and secrecy will enhance society. For example, the mutual use of data owned by different companies will make it possible to solve various social challenges.

Thus, we have developed DeepProtect, a privacy-preserving federated learning technology. Federated learning is an AI technology for machine learning of decentralized local data, allowing users to run secure and interorganizational machine learning of confidential data while still preserving privacy.

As a specific example, by learning the account activity data from multiple banks using DeepProtect, suspicious transactions can be immediately detected. The more financial transaction data we learn, the more precise the detection can be.

Experiments conducted with several banks have proven a high accuracy model, and we aim to put it into practice in the near future.

Another major pillar is the research on cryptographic technology for the forthcoming quantum computing era. It is known that existing RSA cryptosystem will be broken if large-scale quantum computers are ever built, so it is necessary to develop Post-Quantum Cryptography (PQC) capable of resisting them. The US National Institute of Standards and Technology (NIST) is working on the standardization of PQC and will announce cryptographic standards in the near future.

■CYNEX aiming to be a nexus for cybersecurity

—NICT is promoting Cybersecurity Nexus (CYNEX) as a cybersecurity effort. Could you tell us about it?

INOUE CYNEX is an organization established with the aim of becoming a nexus in the cybersecurity area to improve the low security self-sufficiency rate in Japan. It started in April 2021 in our medium- to long-term plan. In NICT, the Cybersecurity Laboratory has collected and analyzed a massive amount of cyberattack data, and the National Cyber Training Center has worked on human resources development. Based on this, the new

organization aims to be a nexus connecting the government, industry, and academia and to enhance Japan's cybersecurity capabilities.

CYNEX has four projects ongoing in parallel: (1) Data collection and analysis, (2) Fostering of analysts for the Security Operation Center (SOC), and dissemination of information, (3) Establishing a test environment for security products made in Japan, (4) Support for human resources development by establishing an open platform for cybersecurity exercise.

In the first fiscal year, more than 30 organizations joined CYNEX. In functioning as a nexus connecting government, industry, and academia, CYNEX will expedite data collection and analysis as well as human resources development.

■Development of human resources in cybersecurity

—It is said that Japan lacks cybersecurity human resources. What efforts are being made to address this?

SONODA The National Cyber Training Center which I oversee, carries out three projects. The first is CYDER, a practical cyber defense training program in which security operators from national and local governments and the private sector learn how to cope with a simulated cyberattack in practice. We have about 3,000 participants every year.

The second is RPCI, a practical cyber training program designed for Registered Information Security Specialists to help them renew their licenses. The technical level of RPCI is higher than that of CYDER. The third is SecHack365, a program to foster young (under 25 years old) security innovators, targeting graduates, undergraduates, students of colleges of technology, and so on.

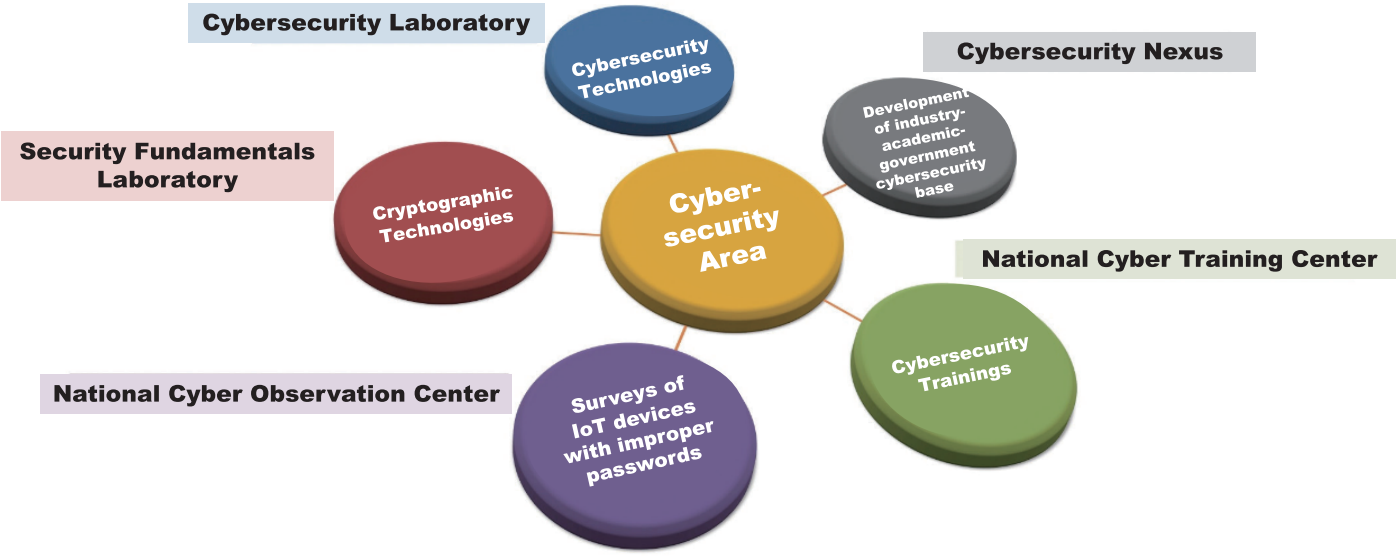


Figure NICT's efforts in the area of cybersecurity

SONODA It is said that Japan is facing a human resources shortage of more than a hundred thousand cybersecurity engineers. Across the ICT area as a whole, the yearly number of students who finish university is only a few tens of thousands. It is not easy to eliminate the shortage if we just follow conventional approaches. While fostering young talent, we need to lower hurdles to security-related operations with new technologies so that people from other areas can readily enter the cybersecurity area.

Therefore, R&D on security automation technology will be of great significance. The key to automation is a technology where daily monitoring and analysis activities can instantly detect any unusual signs and invasions. Humans can't analyze several hundred million security alerts per day. Therefore, we carry out research to merge AI and cybersecurity.

■Concept of diversity & inclusion

MORIAI In order to expand the scope of security personnel and to develop new technologies, we need to open the door to a wide variety of researchers including women and foreign nationals.

In terms of cybersecurity research, the field of usable security is gaining attention. The field studies human behavior and thinking patterns to address cybersecurity issues. For example, it deals with actions to take when one comes across disinformation on social media. People who have studied psychology and sociology also join the research.

We value the creation of a diverse and inclusive environment (inclusion beyond nationality, gender, age, etc.) and combining the forces of diverse researchers to carry out R&D.

—What direction is the NICT heading in the cybersecurity area?

INOUE It is often said that cybersecurity is a game of cat and mouse. Measures are being devised, but new threats emerge one after another. We need to struggle with them patiently. Since NICT is a national research institute, we have a great advantage in being able to carry out research from a long-term perspective.

SONODA When it comes to human resources development, it is essential to provide human resources and expand their scope. Meanwhile, we must also focus on finding exceptional talent such as super hackers.

MORIAI The important thing is to protect social safety through cybersecurity technology. We will promote diversity and inclusion and contribute to society by involving a wide variety of resources.

Data-driven Practical Cybersecurity Research for Breaking the Vicious Spiral



KASAMA Takahiro

Associate Director of Cybersecurity
Laboratory, Cybersecurity Research
Institute

After completing a doctoral course, he joined NICT in 2011. He has been engaging in observation and analysis of cyberattacks and IoT security. Ph.D.(Engineering)

**TAKAHASHI Takeshi**

Associate Director of Cybersecurity
Laboratory, Cybersecurity Research
Institute

After working at Tampere University of Technology, Finland and Roland Berger Strategy Consultants, he joined NICT in 2009. He has been engaging in research of cybersecurity and AI technology. Ph.D.(International Information Communication)

INOUE Daisuke

Director of Cybersecurity Laboratory,
Cybersecurity Research Institute

After completing a doctoral course, he joined Communication Research Laboratory (currently NICT) in 2003. He has been engaging in research and development of network security and initiated NICTER, security incident analysis center since 2006. Ph.D.(Engineering)

Nowadays, the world is awash with stories about cyberattacks, and we face new cyber threats every day. In order to defend against cyberattacks, which are getting more sophisticated and diverse, we expedite practical cybersecurity research based on the two pillars of data-driven cybersecurity technology and emerging cybersecurity technology by taking advantage of our neutrality as a national research institute.

■ Real-world data is essential for cybersecurity research

The Cybersecurity Laboratory is conducting R&D based on two pillars in the fifth medium- to long-term plan (Figure 1).

The key to cybersecurity is data, i.e., the point of the R&D is how to build a system in which fresh and real data are collected and accumulated constantly on a large scale. In the cybersecurity area, the market is unfortunately dominated by foreign products, which makes it harder to gather cybersecurity-related real data in Japan. Less data hampers efficient R&D and human resources development, and as a result, domestic technology cannot be created, resulting in a negative spiral of even less and less data.

In order to stop this spiral, we are developing CURE (Cybersecurity Universal Repository)(Figure 2), a security information integration platform, by conducting R&D on

monitoring technology to collect a wide variety of massive amounts of cybersecurity data in real time, including darknet traffic over 20 years (Figure 3), malware samples captured by honeypots, security appliance alerts, URLs of malicious websites, and threat data. Using security big data accumulated in CURE, we advance R&D on data-driven cybersecurity technology to establish automated defense technology that makes full use of visualization and AI technologies.

Meanwhile, new technologies emerging in society certainly come with new security threats. We are conducting R&D on security verification technology capable of dealing with emerging technologies, such as the latest communication devices, connected cars, and 5G/Beyond 5G. For example, we built security verification environments for hardware, including electronic circuits, chips, and real cars, and also a 5G verification network using emulation technology. Through threat analysis and attack scenario evaluation, we try to identify security-related issues and address them. In security, humans (users) are also an important element. We carry out R&D on usable security that analyzes users' behavior patterns, mental models, and decision-making processes to implement security measures without compromising usability.

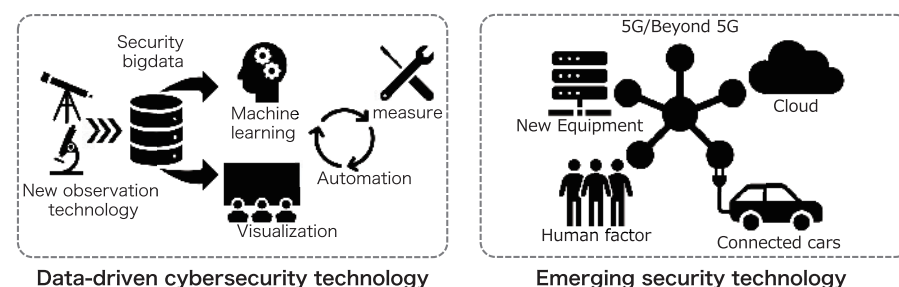


Figure 1 Two pillars of cybersecurity laboratory's activity

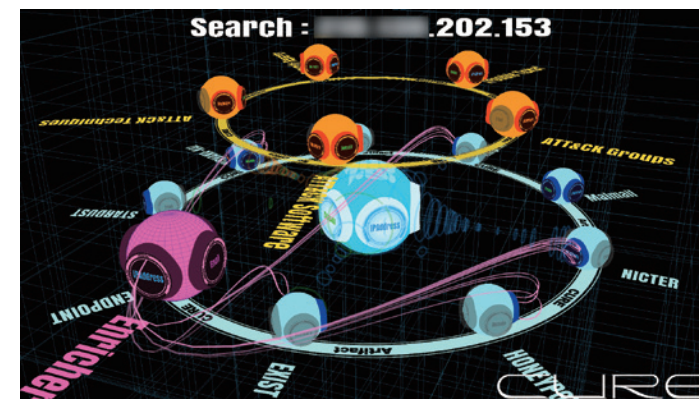


Figure 2 CURE: Cybersecurity universal repository

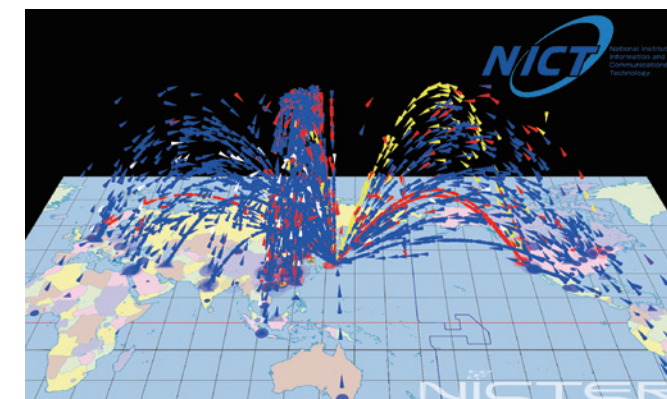
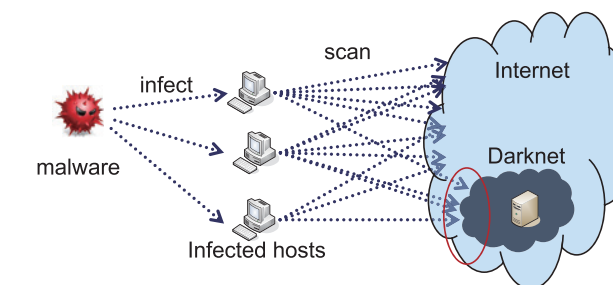


Figure 3 NICTER: Global Cyberattack Monitoring System

■ Automation of security operations by AI technology

To protect organizations from cyberattacks, it is important to promptly detect security incidents with proper security operations and to understand the situation. However, the existing model to defend against attacks at the boundary between an inhouse network and the internet is reaching its limit due to increased use of cloud services and teleworking, and security operations are increasingly burdened with the need to analyze a wide variety of data in an integrated manner. We aim to automate security operations and implement DX by applying various types of AI technologies, such as machine learning, to collected security big data and converting the advanced know-how of security operators and analysts into systems.

In particular, through MITIGATE, a research project sponsored by the Ministry of Internal Affairs and Communications, we work with domestic universities and companies in automated analysis and collection of data on darknets, malware, cyber threat intelligence, etc. to develop a hybrid analysis platform technology that will automatically issue comprehensive security reports and significantly reduce the burden on operators. As an example of the benefits of this technology, it will allow us to automatically and rapidly detect the occurrence of new malware activities, determine its identity, and collect, integrate, and post analysis of the behavior and coding of the malware, vulnerabilities exploited, and other detailed reports on the malware in real time. Detection of new malware has become possible by our unique technology that detects synchronization of scan packets emitted by devices infected with the malware (Figure 4). We are also conducting R&D on technology to extract critical information requiring action from among numerous security alerts, as well as technology to instantly



Detecting synchronization of scan packets arriving at darknet space

Figure 4 Technology for automated and prompt detection of new malware

detect new malware requiring detailed analysis, by clustering IoT malware in a fast and highly accurate manner, thereby supporting more operations. An important challenge is developing a technology capable of justifying and verifying a system's judgments and presenting them in a tangible format.

- **Towards a global R&D hub through domestic and international collaboration**


Cyberspace is vast, so there are limits to the R&D we can perform on our own, including data collection and the securing of human resources. Hence, the Cybersecurity Laboratory is proactively advancing collaboration in research with both domestic and international entities. For example, NICTER operates darknet monitoring using one of the world's largest monitoring networks, with about 300,000 IPv4 addresses built in collaboration with dozens of organizations in more than 10 countries. By centralizing the monitoring results of multiple networks, we are now able to grasp and analyze the state of cyberattacks on the internet more precisely. While it is important to utilize the data collected in this way between organizations, there is certain confidential information that cannot be disclosed to others. Therefore, we are promoting the safe and effective utilization of security-related data. For example, in an R&D project with a Taiwanese organization on a method to detect malware activities on the

internet, we share only the learning results of each other's data without disclosing the original data. Furthermore, we are not only focusing on data but also the development of human resources by actively accepting interns and trainees, with the aim of becoming a global R&D hub.

■ Future prospects

Under our medium- to long-term plan, the Cybersecurity Laboratory will conduct R&D on both data-driven cybersecurity technologies and emerging cybersecurity technologies, based on the continuous evolution of data collection and analysis technologies that we have been steadily implementing for some time. Cybersecurity is a difficult but interesting research field where the situation is constantly changing with the emergence of new technologies and the evolution of attackers. We therefore aim to produce national cybersecurity technologies through aggressive R&D by constantly observing the situation and evolving our goals, thus building global resilience through active international collaboration.

Secure Data Utilization Technologies / Cryptanalysis for Quantum Computing Era



EMURA Keita (left)

Research Manager, Security Fundamentals Laboratory, Cybersecurity Institute.

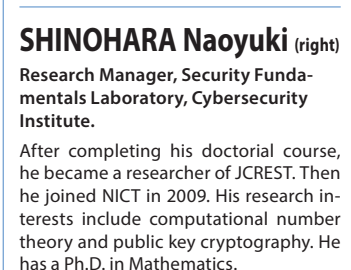
After completing his doctoral course, he became a post doctoral researcher at JAIST. Then he joined NICT in 2012. His research interests include public-key cryptography and information security. Ph.D (Information Science).



SHINOHARA Naoyuki (right)

Research Manager, Security Fundamentals Laboratory, Cybersecurity Institute.

After completing his doctoral course, he became a researcher of JCREST. Then he joined NICT in 2009. His research interests include computational number theory and public key cryptography. He has a Ph.D. in Mathematics.



NOJIMA Ryo

Director of Security Fundamentals Laboratory, Cybersecurity Institute.

He joined NICT in 2006. His research interests include information security and privacy enhancing technologies. Ph.D.(Engineering).

The security fundamentals laboratory aims to conduct research on cryptography and privacy-preserving technologies, including post-quantum ones, and perform cryptanalysis.

Secure data utilization technologies

Searchable Encryption and its Applications

End-to-end encryption (E2EE) is desirable for preventing information leakage of files/messages preserved on external storage. Typical encryption does not provide keyword search because a service provider does not obtain information on files/messages due to E2EE. We investigate E2EE storage and chat systems based on searchable encryption (Figure 1) that provides keyword search functionality in encrypted files/messages. Our systems can reduce information leakage risks because keywords that are searched are not leaked to the service provider.

Technologies for providing integrity and availability

In the guidelines related to the Space Activity Act (November 2018), the transmission of signals related to safety-critical systems should have security measures in place, including appropriate encryption and authentication, to prevent interference or takeover. We have conducted a feasibility study for achieving the highest security level, called information-theoretic security, in the context of spacecraft communication using currently available, low-cost electronic devices. In the latest flight test conducted on July 31, 2021, we confirmed all onboard encryption and authentication operations were performed correctly. We have also conducted research on zero-knowledge proofs and their applications to anonymous authentication. Zero-knowledge proofs allow a prover to prove the possession of data satisfying a statement (e.g., I am a

member of a group) without revealing the data. By employing the proof system, a user can anonymously prove their membership of a group. Although such an anonymous authentication is attractive for providing a privacy-preserving authentication protocol, it is difficult to trace nonlegitimate users whose rights have expired. We study such a system providing anonymity and traceability/revocability simultaneously along with a privacy-preserving protocol on the blockchain and their application.

Secure Data Utilization for Data obtained from Multiple Organizations or Healthcare Information

We propose a privacy-preserving federated learning system, DeepProtect, which employs a homomorphic encryption scheme in a symmetric key setting (Figure 2). For example, DeepProtect can be employed to tackle financial crimes, including money laundering, illegal money transfers, and bank transfer scams, by collecting transaction data from multiple banks in a privacy-preserving manner. We also investigate how to simultaneously guarantee security and utility for data anonymization methods, how to easily recognize a privacy policy to examinees when collecting personal data, how to improve security in a usable security context, etc.

Security evaluations for cryptographic technologies in the quantum era

Evaluating how the latest quantum computers threaten standard cryptographic schemes

Many fundamental/industrial organizations have been promoting their research and development of quantum computes as a means to solve multiple social problems. However, a large-scale quantum computer could threaten the security of some de fac-

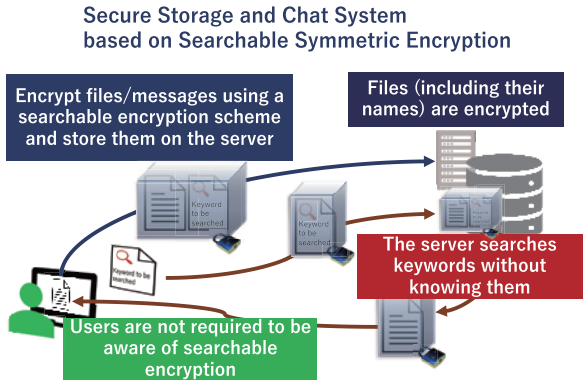


Figure 1 End-to-end encrypted storage and chat systems based on searchable encryption

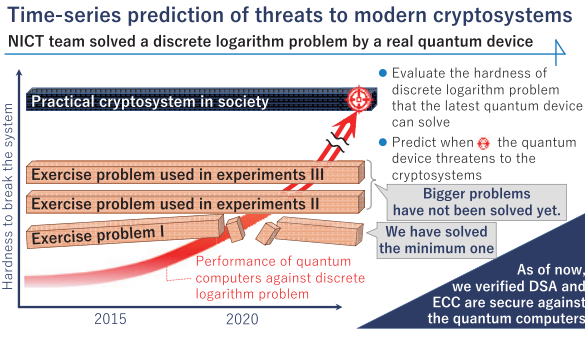


Figure 3 Time-series prediction of threats to modern cryptosystems based on DLP.

to standard cryptographic systems, such as RSA, ECC, DH, and DSA, because such a computer could solve the very large size integer factoring problems and discrete logarithm problems (DLPs) that such systems use as their security base. To the best of our knowledge based on our survey, the largest number factored by a real quantum computer using Shor’s algorithm is 21, whereas, in practice, standard RSA cryptosystems use numbers longer than 2048 bits. In other words, it is necessary to factor an integer greater than 2^{2048} to compromise these systems. Because this factor is much greater than 21, the latest quantum computers do not pose a direct threat to current cryptosystems. In collaboration with Keio University, Mitsubishi UFJ Financial Group, and Mizuho Research & Technologies, we successfully performed experiments to solve a 2-bit discrete logarithm problem. Additionally, we propose a rough version of a future roadmap to verify that the latest quantum computers do not pose a threat to DH, DSA, and ECC and to predict when such computers will pose a threat to cryptosystems.

Security evaluation of multivariate public key cryptosystems

Post-quantum cryptography (PQC) refers to a cryptographic system that is secure

against attacks by quantum and classical computers. The development and standardization of PQC is underway worldwide. Multivariate public key cryptosystems (MPKCs) are potential candidates for PQC. The security of MPKC depends on the hardness of solving a system of multivariate quadratic equations and the fact that the hardness increases with increasing numbers of variables. For the secure use of MPKC, it is necessary to evaluate the largest number of variables such that a system of multivariate quadratic equations can be solved using the most effective algorithm. In collaboration with Tokyo Metropolitan University, we succeeded in solving such a system with 37 variables using our proposed algorithm; this constituted a world record for solving such systems. The data attained from this success will contribute to evaluating the secure parameters of an MPKC.

Security analysis of end-to-end encryption (E2EE) schemes

In the wake of the global COVID-19 pandemic, remote conference systems have become essential not only for business purposes but also for private, academic, and educational uses. Therefore, it is important to evaluate the security measures, such as E2EE, used in these systems. In collaboration with the

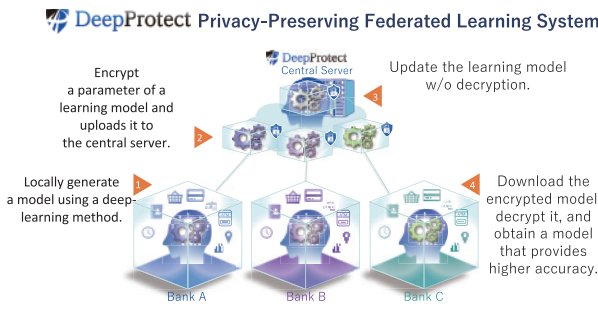


Figure 2 DeepProtect: Privacy-Preserving Federated Learning System

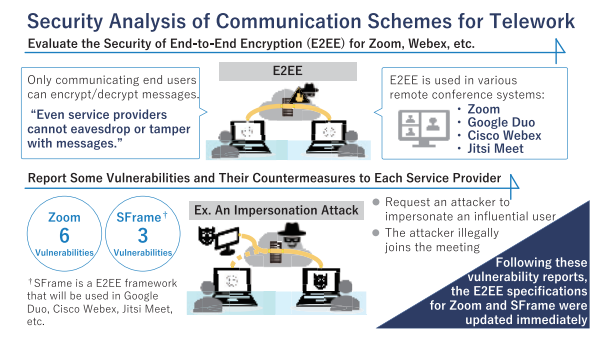


Figure 4 Security analysis of communication schemes for telework.

University of Hyogo and the NEC Corporation, we evaluated the E2EE schemes for various remote conference systems, such as Zoom, Google Duo, Cisco Webex, and Jitsi Meet, and contributed to enabling the trusted and secure operation of these systems (Figure 4). In this study, we identified several vulnerabilities in the E2EE scheme for these systems, proposed various attacks (e.g., impersonation, tampering, and denial of service attacks) based on these vulnerabilities, and then quickly reported our findings and their countermeasures to each service provider. Following these vulnerability reports, the service providers immediately updated their E2EE specifications.

Toward the Realization of Cyber Security that Leaves no one Behind

Efforts of NICT National Cyber Training Center



HANADA Tomohiro

Director of Cyber Training Laboratory, National Cyber Training Center, Cybersecurity Research Institute

Joined NICT in 2017. Previously worked for an IT vendor and worked as a project manager for the development and operation of core banking systems. He is currently engaged in projects such as CYDER, SecHack365, and CYDERANGE development at the National Cyber Training Center as the director of the laboratory. SECCON Executive Committee Chairperson.

SHIMADA Kouichi

Director of Cyber Training Business Promotion Office, National Cyber Training Center, Cybersecurity Research Institute

Joined Radio Research Laboratory, Ministry of Posts and Telecommunications (currently NICT) in 1980. Since FY 2016, as the head of the Business Promotion Office, he has led the launch of the National Cyber Training Center, and various businesses in line with the enactment of the revised NICT Law.

SONODA Michio

Director General, National Cyber Training Center

Completed a doctorate in Engineering. He became a professor in the Faculty of Information Technology and Business at Cyber University in 2014. He 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)

National Cyber Training Center (NCT) is an organization with a mission to foster human resources for cybersecurity. We established on April 1, 2017, to plan and promote practical cyber-related training by entirely using the technical knowledge, research outcomes, and facilities of NICT, the only public research institute specializing in information and communications in Japan. NCT is currently conducting three projects: CYDER, Cyber Defense Exercise with Recurrence; RPCI, Response Practice for Cyber Incident; and SecHack365 (Figure 1). The following sections describe the features of each project and NICT's strengths.

CYDER, Cyber Defense Exercise with Recurrence

CYDER is a project to foster thousands of security operators by providing practical defense training in an environment simulating an organization's network for IT personnel from the national and local governments, critical social infrastructure providers, and others.

We prepared the environment simulating an entire organization using NICT's notable large-scale computer environment. The training is group work of up to four people, providing experience of actual incident handling in a scenario based on our long-term observation and research on cyberattacks(Figure 2). Some trainees successfully addressed incidents that occurred soon after the training,



and we are constantly improving the content to promote repeated courses to make them more applicable.

After being launched as a demonstration experiment of the Ministry of Internal Affairs and Communications (MIC) in FY 2013, CYDER was transferred to NICT from MIC, where we have reinforced the system and improved the contents. Currently, we provide 100 sessions for about 3,000 participants in all of the 47 prefectures nationwide every year. The training was only classroom instruction, but now online training is available using R&D outcomes of CYDERANGE, a training platform developed by NCT.

RPCI, Response Practice for Cyber Incident

In FY 2021, we began to provide RPCI, Response Practice for Cyber Incident, as the first specified training*1 provided by the public sector for Registered Information Security Specialists(RISS). Taking advantage of the large-scale environment and knowledge developed by NICT through CYDER, RPCI meets the needs of those who want technical-oriented training as per the curriculum and scenario tailored to the specific training for the Specialists.

The participants of RPCI form a team of up to four people as a CSIRT*2 and handle a simulated cyberattack in a realistic practice environment simulating a network of a virtual organization as in CYDER. They can learn incident handling procedures from A to Z using actual equipment in a scenario likely to happen in reality.

RPCI is a fledgling initiative, but we succeeded in providing practical training that participants cannot experience in their everyday work. And we received positive feedback like “The hands-on training was beyond my usual work and gave me valuable experience” and “I was able to learn and gain practical experience through discussions with the



Figure 1 Three projects of the National Cyber Training Center

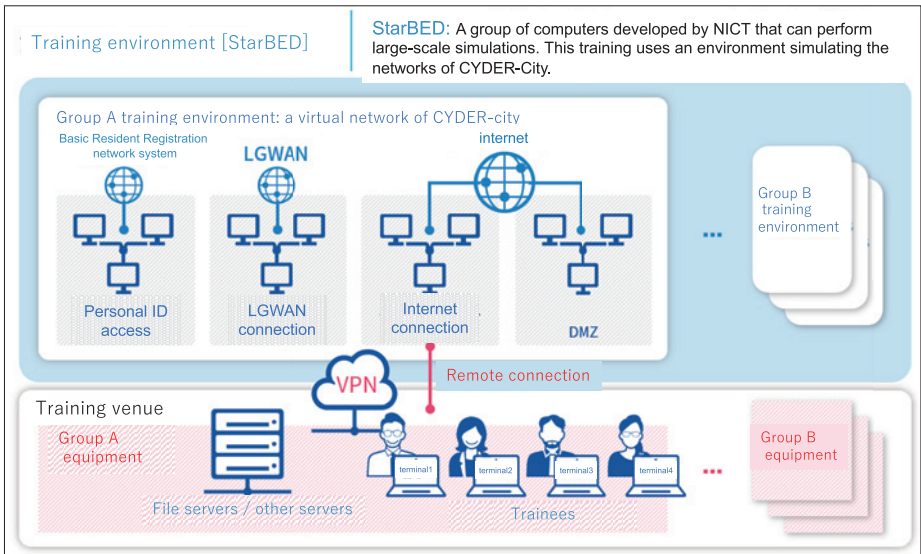


Figure 2 Example of networks provided for each group

members of the team and the instructor.” We also received a summer greeting card from a participant who joined the summer training saying that the training was fruitful with good support from instructors and tutors.

We aim to contribute to a safe and secure society by helping the RISS enhance their incident handling ability through the RPCI training.

SecHack365

SecHack365 is a one-year, full-fledged training program for young ICT people to foster human resources who can produce new things with their hands in cybersecurity (security innovators). It provides them with security-related technical guidance by using NICT's many years of accumulated R&D knowledge, our observed data on cyberattacks, and the environment, which enables safe use of these in R&D.

Trainers who are active in the front lines in ICT and security and assistants who com-

pleted this program instruct about 40 selected people among ICT human resources aged 25 or younger in R&D on security-related technology and how to make the security in general development more sophisticated throughout the year(Figure 3).

Several courses from different development approaches are available to avoid mismatches, and applicants can choose which ones they want to take. We incorporate various inputs, such as lectures by guest speakers and instructions on forming good habits, in training and provide characteristic course work for each course. SecHack365 trainees put effort into completing their work by refining their theme through discussions with other trainees to proceed with the work and presentations.

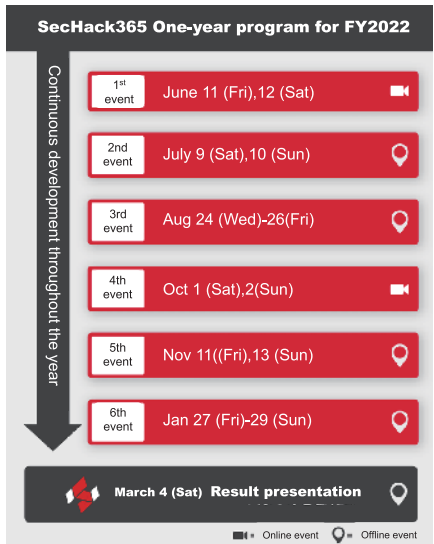


Figure 3 One-year program of SecHack365 for FY 2022

* 1 Specified training: Training defined by the Minister of Economy, Trade and Industry. Registered Information Security Specialists (RISS), a national qualification granted to specialists with the latest security knowledge and skills, are required to take these trainings every three years to renew their license.

* 2 CSIRT: Computer Security Incident Response Team. An organization that handles incidents related to information security. Besides addressing incidents (events and accidents) in their own organization, it collects and analyzes information on incidents, vulnerability, and potential attacks as well as decides policies and creates procedures.

Toward the Nexus of Japanese Cybersecurity



YASUDA Shingo
Research Manager, Cybersecurity Laboratory & Cybersecurity Nexus, Cybersecurity Research Institute

He joined NICT in 2013. He has engaged in the research of construction and manipulation various emulated environments for large-scale verification of network systems, cyber-attacks, and security training exercises. He is also involved in security human resource development projects within and outside NICT, such as the Hardening Project, Cyber-colosseo, and SecHack365.



INOUE Daisuke
Director General, Cybersecurity Nexus, Cybersecurity Research Institute

After graduating a doctoral course, he joined CRL(Currently NICT) in 2003. He started network security research based on NICTER, NICT's incident analysis center, from 2006. Ph.D.(Engineering).

In Japan's cybersecurity field, the security self-sufficiency rate is critically low, as overseas security technologies are introduced and operated in most cases. Overdependence on overseas security technologies has undermined Japan's international competitiveness. In 2019, the R&D Strategy Special Investigation Committee,*1 which is organized by the National center of Incident readiness and Strategy for Cybersecurity (NISC), also pointed out the importance of developing technologies and industry in Japan.

Four sub-projects of Co-Nexus to escape a negative spiral of the data shortage

In cybersecurity, collection of a large amount of data related to cyberattacks, development of human resources, technologies to analyze data and implement appropriate measures are required. In line with the development of technologies such as AI and machine learning, R&D on analysis technology has been actively promoted by using big data. However, actual data related to security is sensitive information and difficult to share. Overseas security vendors with large market shares in the security market collect and possess a large amount of actual data, giving them a business advantage. As a result, Japanese vendors, which rely on overseas security products, do not have the means of collecting actual data and face a shortage of data. The lack of available actual data makes them stuck in a vicious cycle of "losing out due to lack of data" spiral.

To solve this problem, Cybersecurity Nexus (CYNEX) was established within the Cybersecurity Research Institute in April 2021. It is necessary to make multifaceted efforts to reverse this negative spiral. CYNEX forms an alliance that serves as a "nexus" for private companies, educational institutions, and governmental agencies in Japan by combining and providing the R&D results and

security information collection platform of the Cybersecurity Laboratory with the know-how of the National Cyber Training Center to train security experts. Four Co-Nexus sub-projects were launched(Figure 1) to concurrently promote activities on various fronts to improve cybersecurity capabilities in Japan and reverse this negative spiral.

Co-Nexus A

Co-Nexus A (Accumulation & Analysis) aims to foster the community of analysts and joint analysis in Japan by collecting, accumulating, and analyzing cybersecurity information and making the analysis platform available to organizations participating in CYNEX through the utilization of STAR-DUST (a large-scale infrastructure for luring cyber adversaries), WarpDrive (Web-based Attack Response with Practical and Deployable Research Initiative) in collaboration with Ghost in the Shell SAC_2045 which are R&D accomplishment of the Cybersecurity Laboratory.

Co-Nexus S

Co-Nexus S (Security Operation & Sharing) aims to train advanced human resources with high engineering capabilities for the Security Operation Center (SOC) by offering online self-learning education programs and on-the-job training in the CYNEX analysis team to participating organization's employees. In Co-Nexus S, Analysts analyze multi types data utilize the machine learning engine in the SOC operations, thereby generating and providing the threat informations unique to Japan.

Co-Nexus E

Co-Nexus E (Evaluation) aims to use NICT's internal network as a test bed to connect security products developed by participating organizations in Japan and achieve long-term operation. Functional and non-functional verification of products is conducted by using live traffic, standard

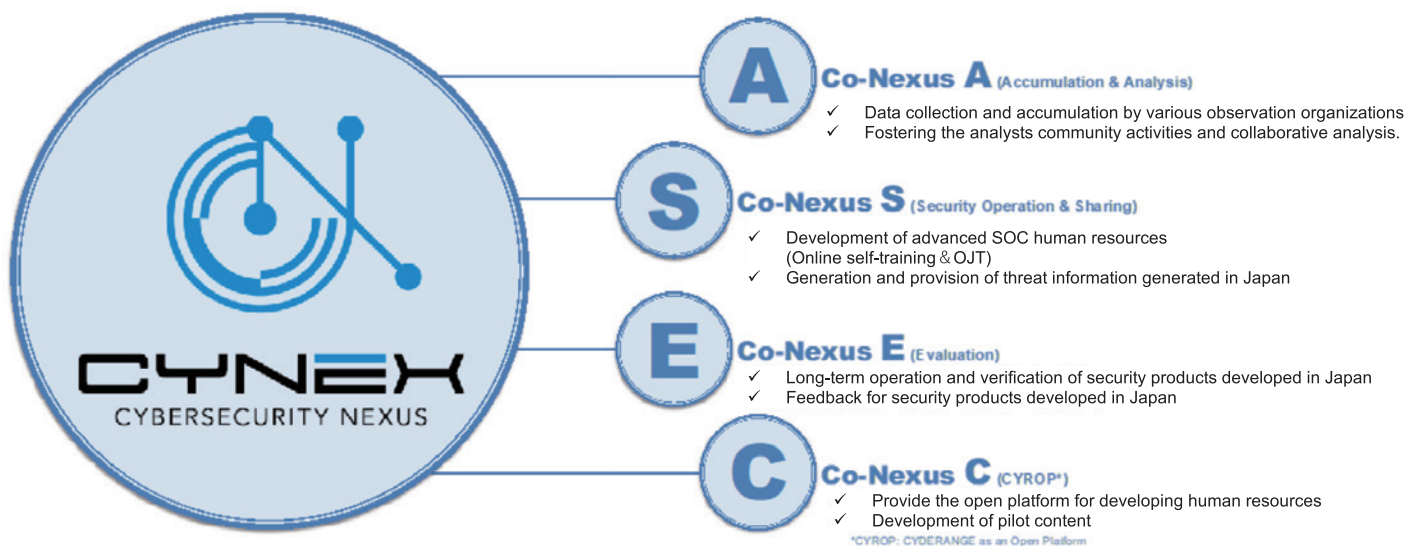


Figure 1 Four Co-Nexus sub-projects

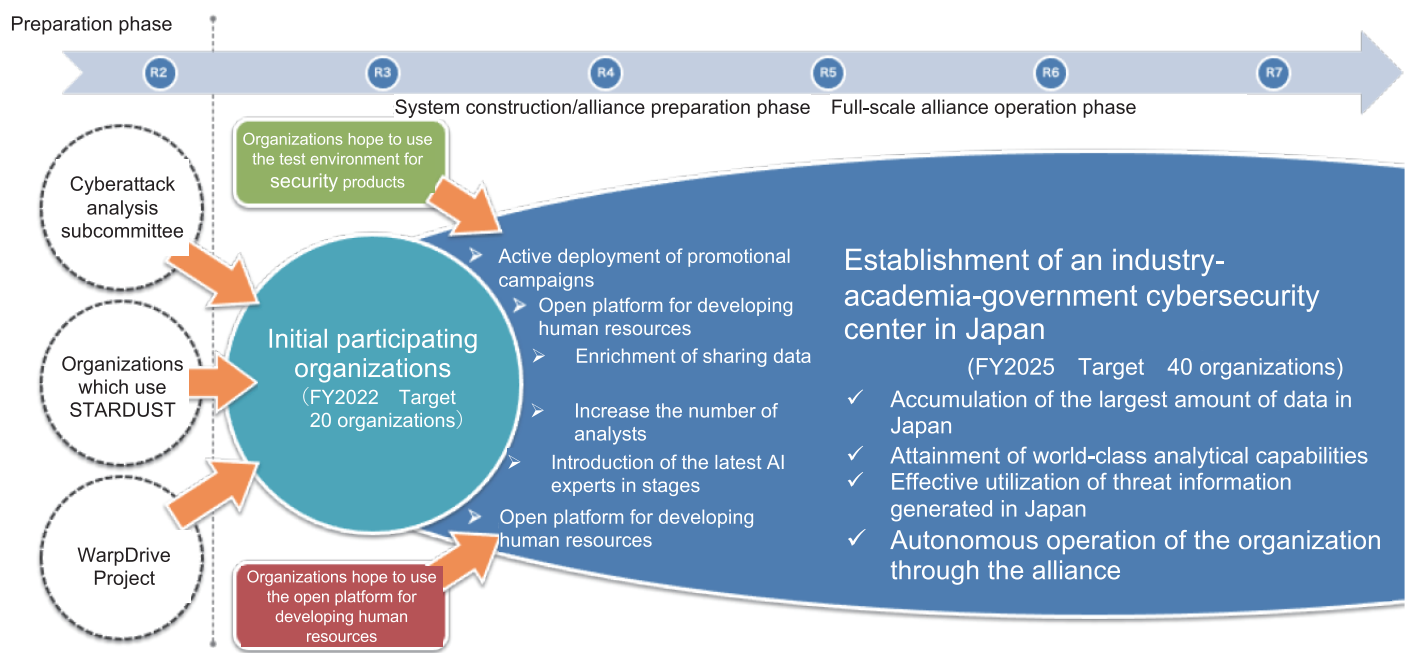


Figure 2 Timeline of the CYNEX plan

cyberattack patterns, and unique simulated attacks by CYNEX's red team. R&D of technologies in Japan is supported through comparison with existing products and feedback of evaluation results to development organizations.

Co-Nexus C

Co-Nexus C (CYROP) aims to promote the project to train security experts in Japan by applying the platform for CYDER (Cyber Defense Exercise with Recurrence) at the National Cyber Training Center to CYNEX.

It continuously develops extensive exercise content for all positions, such as system developers, top management, and students, to meet social needs. It also offers the content as standard exercise scenarios to participating organizations.

Future prospects

CYNEX launched a series of Co-Nexus sub-projects with over 30 initial participating organizations toward full-scale alliance operation in FY2023. It has been implementing projects on a trial basis(Figure 2). CYNEX

aims to create a "nexus" for cybersecurity in Japan by establishing an alliance management system based on feedback from initial participating organizations.

*1 <https://www.nisc.go.jp/pdf/council/cs/kenkyu/dai12/12shiryou01.pdf> (in Japanese)

Efforts for Safe and Secure Utilization of IoT Devices

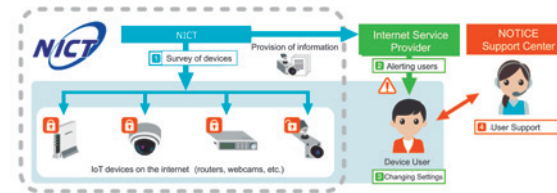


Figure NOTICE project



INOUE Daisuke (right)
Research Executive Director/
Director of Cyber Observation Operation Office,
National Cyber Observation Center,
Cybersecurity Research Institute

After graduating a doctoral course, he joined CRL (Currently NICT) in 2003. He started network security research based on NICTER, NICT's incident analysis center, from 2006. Current position from 2021. Ph.D.(Engineering).

TANUMA Tomoyuki (left)
Distinguished Expert/
Director of Cyber Observation Business Promotion Office,
Cybersecurity Research Institute

After graduating a graduate school, he joined Ministry of Post (Currently MIC) in 1994. He has engaged in making rules of radio management, telecommunication business, R&D, and promotion of international standardization. Current position from 2021.



MORIAI Shiho
Director General,
National Cyber Observation Center,
Cybersecurity Research Institute

After graduating from university, she worked for Nippon Telegraph and Telephone Corporation and Sony Corporation, and then entered NICT in 2012. Current position from 2021. She has engaged in R&D on cryptography, information security and privacy protection technologies. Ph.D. (Engineering).

In the age of IoT/AI, everything is being connected to a network, such as the internet. With the advances in technology, IoT devices are rapidly spreading. On the internet, cyberattacks targeting IoT devices are increasing sharply. Devices with improper security measures may be exploited by them. This article introduces NOTICE, an effort in which NICT is participating for safe and secure use of IoT devices in such circumstances.

What is NOTICE?

NOTICE (National Operation Towards IoT Clean Environment) is a joint effort of NICT, the Ministry of Internal Affairs and Communications (MIC), and internet service providers (ISPs) to detect vulnerable IoT devices by attempting to access them and then alert the users of the devices detected. NICT is responsible for conducting surveys on devices vulnerable to cyberattacks and providing results to ISPs. Based on this information, ISPs alert the users of the devices so that they can change the settings. The MIC has opened the support center to handle inquiries from users via the website and telephone to provide them with guidance on appropriate security measures. This effort has been conducted since February 2019. An outline of the effort is presented in the figure.

NICT established the National Cyber Observation Center in January 2019 for conducting the survey and the information provision work. The activities of the Center have been subsidized by the MIC, and it has been operated under the Cybersecurity Research Institute since the start of the fifth mid-term plan of NICT.

Current Result of Survey

In addition to NOTICE, NICT has been providing alerts about devices which had been infected with malware as a part of the NICTER project since June 2019, and reports on both projects are published on the website

every month. In May 2022, the results are as follow:

-Alerts by NOTICE

1,564 devices were detected, and results were informed to ISPs.

-Alerts by NICTER

An average of 1,025 devices per day were detected, and results were informed to ISPs. (For more details, please visit <https://notice.go.jp/status>.)

Every time we review and enhance the survey roughly once a year by modifying survey programs and adding target IDs and passwords, the number of subjects to be alerted significantly increases, but then gradually decreases every month through consistent cooperative efforts by NICT and other organizations.

Future prospects

We have added target protocols (http/https) since June 2022 to make the survey more complete. Although alerting activities need further enhancement, the number of targets is expected to rise considerably by this addition.

As described above, the NOTICE project is conducted with the full support of the Japanese government, and NICT performs relevant surveys in compliance with the law (Act on the National Institute of Information and Communications Technology; the NICT Act), in which the period is stipulated to be about five years until the end of FY 2023. In line with the efforts made so far, we have now reached a phase where the government, relevant agencies and private businesses are to have discussion on what is needed in the next phase for safe and secure utilization of IoT devices.

Developing Truly Usable Security Systems by Understanding Users' Concerns



Ayako A. Hasegawa

Researcher,
Cybersecurity Laboratory,
Cybersecurity Research Institute

Biography

- 2013 Graduated from the Department of Information Sciences, Faculty of Science, Ochanomizu University
- 2015 Completed master's program in Computer Science, Advanced Sciences, Graduate School of Humanities and Sciences, Ochanomizu University
- 2015 Joined the Nippon Telegraph and Telephone Corporation
- 2021 Joined NICT. Appointed to current position

Awards

- Best Paper Award at EuroUSEC2021
- Best Paper Award at CSS2020

Q&As

Q What is good things to be a researcher?

A I love the moment when I share the joy of having a paper accepted with my co-authors. It is also rewarding to see the results of my research being incorporated in actual systems.

Q What are you interested in other than research?

A Recently I bought a tea incense burner. I enjoy refreshing myself with the aroma of tea leaves. It makes me feel as if I'm in a tea shop.

Q How do you spend your time on holidays?

A I go walking and take care of my home garden. I end up spending long hours in front of my PC on weekdays, so I want to experience nature as much as possible on my days off.



When starting to use a new device or service, most will get excited but at the same time, probably worry whether they are protected by adequate security measures. Although I'm a security researcher, I find it difficult to take security measures as a user. Sometimes I become anxious and ask myself, "Is it safe to click this URL?" or "Is my data protected on this service?" As I understand such concerns very well, I wanted to become a researcher considerate of users' concerns related to security. That's the reason why I started the research called "usable security." In this area, we focus on users' behavior and perception and aim to develop systems that assist users in taking appropriate security measures.

Currently, I conduct various user studies such as online surveys and social media analysis to identify security- and privacy-related concerns and issues that users have in their daily lives. The most frequent concern is how to judge whether a website you are browsing or a message you have received is legitimate. Through

user studies, I found that they do not have enough knowledge about the tactics that attackers use. For example, URL spoofing techniques commonly used by attackers include a fraudulent URL masked to look legitimate by using characters of the name of a popular service in its sub-domain. Many users do not know about such URL spoofing techniques. In light of this situation, I am aiming to provide a security knowledge base and educational content that are easy for users to access and understand. Another thing many users find difficult is the security and privacy settings of devices and services. I became aware of how confusingly the current designs of devices and services are to users. What is particularly troublesome to users is that technical terms are often used to explain security matters of devices and services. In the future, I will look into how this type of explanation can be more comprehensible and work with providers of devices and services to make improvements.

I will continue to put myself in users'

shoes to understand their concerns and issues and address them one by one, thereby contributing to a better society where users can safely utilize digital technology.

On the Radio Wave Day and the Communications Promotion Month, the Award is given to individuals and entities who have contributed to the use of radio waves or the development of communication, and to persons who are expected to create outstanding digital contents.



Awards for FY2022 Radio Day and Info-communications Promotion Month

Minister of Internal Affairs and Communication Award

YANAGIDA Toshio

NICT Fellow and R&D Advisor, CiNet, Advanced ICT Research Institute

- Date : June 1, 2022
- Awarded for: He was instrumental in setting up the Center for Information and Neural Networks at the National Institute of Information and Communications Technology, and as the Director General, has also contributed greatly to the establishment and development of cutting-edge interdisciplinary research between neuroscience and ICT over many

years.

● **Receiver's Comment:** I am honored to receive this prestigious award recommended by the Ministry of Internal Affairs and Communications. I would like to extend my gratitude to everyone who has supported me. As a Fellow and R&D Advisor going forward, I will contribute to the development of the CiNet to the best of my ability.



SHIDA Rinzaburo Award

KOJIMA Shoichiro

Research Manager, Remote Sensing Laboratory, Radio Research Institute

- Date : June 1, 2022
- Awarded for : He has worked on the development of airborne synthetic aperture radar over many years and contributed greatly to advancements in land-surface monitoring technology, which is expected to be applied in disaster management, including his initiative in establishing a world-class technology through empirical monitoring.

● **Receiver's Comment:** I could receive this award thanks to the great support of the members of NICT and the Ministry of Internal Affairs and Communications and those involved in the manufacture of the radar. I am most grateful to them. This award will encourage me to pursue my research further and advance the development of the world's top performance sensors.



Distinguished Achievement and Contributions Award

INOUE Daisuke

Director General, Cybersecurity Nexus/
Director of Cybersecurity Laboratory/
Director of Cyber Observation Operation Office, National Cyber Observation Center/

- Date : June 1, 2022
- Awarded for: He has led extensive projects over many years including R&D on cybersecurity and vulnerability surveys on IoT devices at the National Institute of Information and Communications Technology, and also contributed greatly to the stable

operation of the IT infrastructure of the Tokyo 2020 Games by providing a cyberattack monitoring system.

● **Receiver's Comment:** I am highly honored to receive this distinguished award. I would like to extend my heartfelt gratitude to all the researchers, engineers, analysts, and support staff with whom I work.



Other Awards

- ◆ **The ITU Association Japan, 54th Celebration of World Telecommunication and Information Society Day, The MIC Minister's Award**
SATO Kohei
Invited Advisor, Standardization Promotion Office, Innovation Promotion Department
- ◆ **Telecommunication Technology Committee, FY 2022 Telecommunication Technology Awards, Minister of Internal Affairs and Communication Award**
NAKAO Koji
Distinguished Researcher, Cybersecurity Institute

- ◆ **Sankei Newspaper, 35th Advanced Technology Awards, Minister of Economy, Trade and Industry Award**
TORISAWA Kentaro
Associate Director General, Universal Communication Institute
TANAKA Masahiro
Senior Researcher, Data-driven Intelligent System Research Center, Universal Communication Institute