

FEATURE

## Cyber Security Fighting on the Vast Net

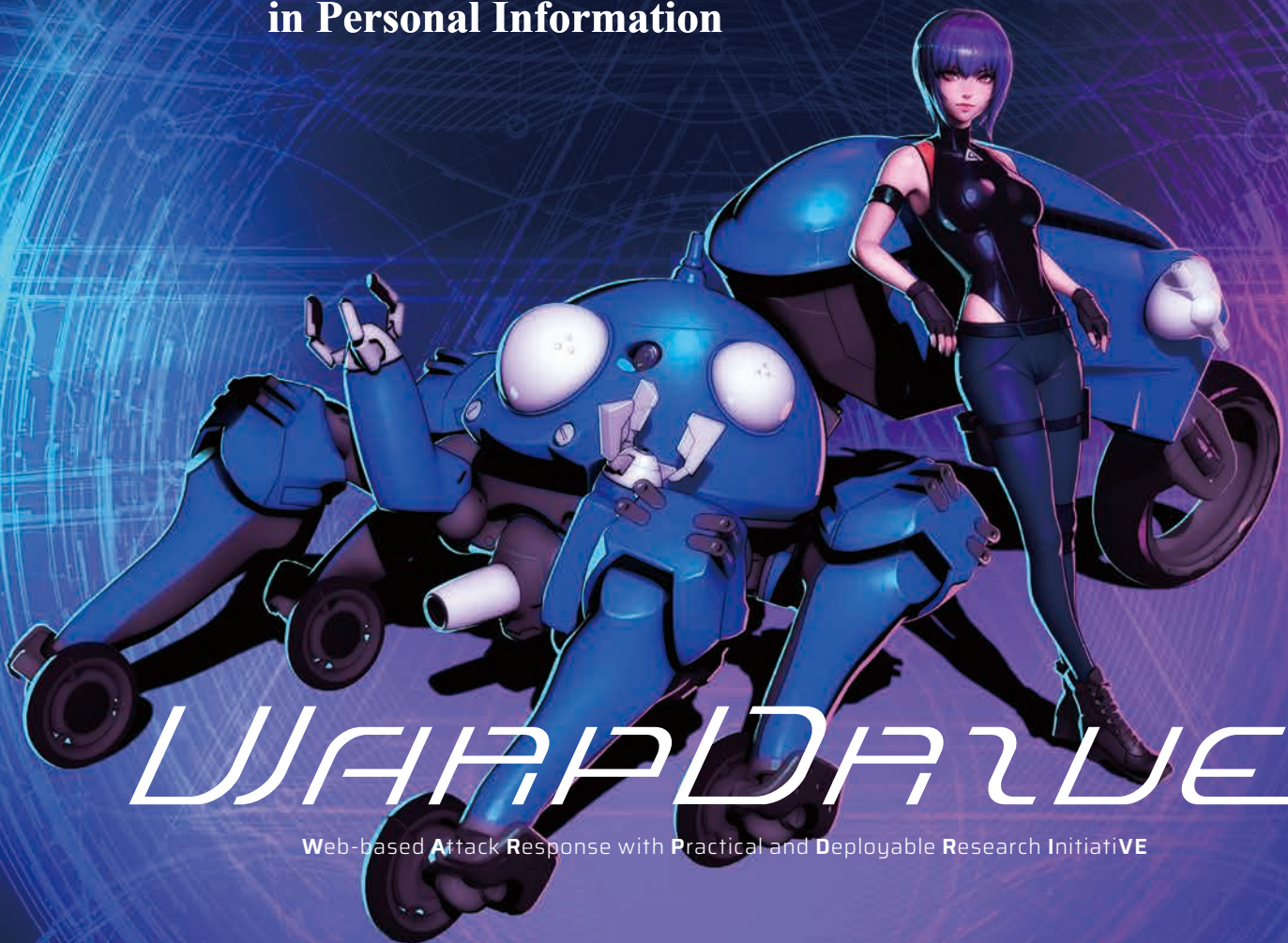
VR Artist

Director General, Cybersecurity Research Institute

DIALOG

**SEKIGUCHI Aimi × INOUE Daisuke**

Discussing Brain Security with a VR Artist  
Our Brains Are the Ultimate Domain  
in Personal Information



# WARPLAVE

Web-based Attack Response with Practical and Deployable Research Initiative





### Cover Page

WarpDrive is a user-participatory project to grasp the actual situation and improve countermeasures for web-based cyberattacks. In a tie-up with the animation work *GHOST IN THE SHELL: SAC\_2045*, the software TACHIKOMA Security Agent was developed with the motif of the character "TACHIKOMA" appearing in the same work.

### Photo Upper left

TACHIKOMA Security Agent Mobile is a free app for Android smartphones. This image is from the app's game function, which is designed to allow users to learn about real-life cybersecurity and IT through immersive gameplay in the world of the *GHOST IN THE SHELL: SAC\_2045* series.

## 1 Message from the President

Dr. TOKUDA Hideyuki

### FEATURE

## Cyber Security Fighting on the Vast Net

### 2 Discussing Brain Security with a VR Artist Our Brains Are the Ultimate Domain in Personal Information

SEKIGUCHI Aimi × INOUE Daisuke

### 4 Cyberattacks Lurk Right Around the Corner Every Time You Access the Internet

KASAMA Takahiro

### 6 Overview of R&D Activities at Security Fundamentals Laboratory

SHINOHARA Naoyuki

### 8 Human Resource Development Programs Offered by the National Cyber Training Center

SONODA Michio

### 9 Toward the Realization of a More Secure and Safe IoT Environment

ETO Masashi

### 10 CYNEX Alliance: "A nexus of Cybersecurity," for Industry-Academia-Government in Japan

YASUDA Shingo / KANAHAMA Nobuhiro

### TOPICS

### 12 Panel Discussion Featuring Women Thriving in the Cybersecurity Industry! Organization of the NICT Cybersecurity Symposium 2025

General Planning Office, Cybersecurity Research Institute

### 13 NICT's Challenger File 31 Looking at Cybersecurity Training Programs from a Career-Track Perspective

SUGIMOTO Sara

### INFORMATION

### 14 NICT Exhibits at MWC25 Barcelona



President of the National Institute of  
Information and Communications Technology

**Dr. TOKUDA Hideyuki**

## Message from the President

Celebrating the start of 2025, we would like to express our heartfelt greetings in this season.

Thank you for your kind understanding of and cooperation with the National Institute of Information and Communications Technology (NICT).

Last year, the Noto Peninsula was hit by a large earthquake in January and again suffered damage caused by heavy rain in September. These repeated disasters made it even more difficult for the afflicted regions to recover, and also made us recognize the importance of enhancing the resilience of information infrastructures. In April of the same year, NICT marked the 20th anniversary of its founding, which was done through a merger between the Communications Research Laboratory and the Telecommunications Advancement Organization. We would like to express our gratitude to all our stakeholders who have given NICT a range of support over the past two decades, including those engaging in the industrial, academic and governmental sectors as well as former NICT officers and staff. Your invaluable contributions have shaped NICT into what it is today.

In April 2025, the final fiscal year of the Fifth mid-to-long-term plan will start. In this five-year plan, we set five priority R&D areas, which are areas for advanced electromagnetic technology, innovative networks, cybersecurity, universal communication, and frontier science. Moreover, in line with the Japanese government's strategies, we have been proactively conducting research in four strategic fields: "Beyond 5G," "AI," "Quantum ICT," and "Cybersecurity." We believe that advanced technologies for these fields are indispensable to build a next-generation ICT foundation to create Society 5.0 as soon as possible. In particular, in the "AI" field, the use of generative AI has spread throughout society while various social issues are becoming more apparent. Under these circumstances, NICT opened the Global Partnership on AI (GPAI) Tokyo Expert Support Center in July 2024 and then established the AI Research and Development Promotion Unit to speed up R&D on AI in September of the same year. Moreover, Additionally following the revision of the Act on NICT, we have been implementing the new NOTICE project while also expanded CYNEX Alliance activities. These efforts aim to transform NICT into more than just a conventional research institute, positioning it as a national hub that fosters collaborative research across universities, private companies, and other institutions throughout Japan.

In the "Beyond 5G" field, in addition to R&D into Non-Terrestrial Networks (NTNs), space-time synchronization technologies and terahertz communication technologies, we are proactively participating in international joint research projects and international standardization activities and have already made some achievements. These accomplishments will be presented at the Mobile World Congress 2025 in

Barcelona this March.

In the "AI" field, based on the Global Communication Plan 2025, we succeeded in advancing long-used multilingual translation technology with the VoiceTra app, which provides simultaneous interpretation service. This technology will be widely used at Expo 2025 Osaka, Kansai, Japan, to be held starting in this April. Also, with regard to our Large Language Model (LLM) that is set for further development, we are accelerating R&D to develop a Japanese language-oriented generative AI based on a large dataset of Japanese text and by leveraging past R&D results, including those about the WISDOM-X system.

In the "Quantum ICT" field, we launched the Quantum ICT Collaboration Center, which has been leading the development of new collaborative research fields by providing the following four functions as Japan's quantum security technology research center: "Research and development," "Open testbed," "Dissemination activities towards society," and "Human resources development." Notably, the Center has made significant progress with initiatives such as the NICT Quantum Camp and the Young Researchers Lab to foster talent in this field.

In the "Cybersecurity" field, we launched Cybersecurity Nexus based on the cybersecurity skills and know-how that we have accumulated for more than 20 years. We use it to widely share cybersecurity information and as a platform to develop experts in cybersecurity across industrial, academic, and governmental sectors to enhance Japan's cybersecurity-related capabilities. We are also proactively conducting research into AI system security in addition to applying AI technologies to the security field.

Further, for public services—which are part of NICT's important operations—we will steadily provide services for Japan Standard Time, calibration of wireless devices, cyber training programs including CYDER, and space weather forecast. For the space weather forecast service, the sun will reach its solar maximum period of greatest activity in 2025 in the 11-year solar cycle. We have already been cautioning citizens regarding each large-scale solar flare activity since last year and will continue to diligently provide the space weather forecast service.

We hope that you will kindly continue to support us in implementing measures to achieve our vision: Beyond human intelligence, co-create new standards for future society.

In closing, we extend our heartfelt wishes for a healthy and prosperous New Year to you.





SEKIGUCHI Aimi

VR Artist

DIALOG

INOUE Daisuke

Director General, Cybersecurity Research Institute

## Discussing Brain Security with a VR Artist Our Brains Are the Ultimate Domain in Personal Information

SEKIGUCHI Aimi is a world-renowned VR artist known for the three-dimensional objects she creates in space. The fusion of cutting-edge technology and art gives birth to fresh forms that we have never seen before. In cyberspace—a metaverse of the near-future that transcends the limits of our human bodies—these are what constitute “reality.”

However, where there is light, there can also be darkness. How should we adapt to this era in which everything, both art and real life, is increasingly becoming virtual? The following conversation takes us from discussions on the “creative brain” and on to “brain security.”

**INOUE** Ms. SEKIGUCHI, you are a VR artist, meaning you use cutting-edge virtual technology to create 3D art in space. Your work has been attracting worldwide attention. What led you down this road?

**SEKIGUCHI** I was fascinated by how VR can virtually create three-dimensional shapes in empty space; it felt almost like magic. That’s what got me started.

**INOUE** You’re currently active worldwide, right?

**SEKIGUCHI** Yes, in addition to Japan, I’ve given VR performances in countries like the United States, Germany, France, and Dubai in the UAE. I’ve been blessed by how the audience is moved by the forms that I create in

space in real time with my VR goggles on. I’ve also been invited overseas to exhibitions related to digital technology. I recently visited Africa’s largest exhibition, which was held in Morocco. There as well, young people from other countries showed great interest in my art.

Dr. INOUE, what kind of research do you conduct at your laboratory?

**INOUE** At my laboratory, we do research and development into technologies that protect important information and systems from malicious attacks in cyberspace.

Specifically, we are developing technologies that can quickly detect cyberattacks and block or neutralize them. We also do research on cryptography to protect information that flows through cyberspace, as well as re-

SEKIGUCHI Aimi (left)

President, MUSOU Inc.,

She has been performing 3D-painting in Metaverse since 2016.

She has performed in various countries including Japan, USA, Germany, France, Russia, UAE, Singapore, Thailand, Malaysia, Saudi Arabia and Morocco.

She also contributes to Japanese government’s policy making such as METI’s “Research Meeting of the Creation of Creator Economy at Web3.0 Era, and Cabinet,” Cabinet Office’s “Government-Private sector meeting on the legal issues of contents on Metaverse,” as a member of board.

INOUE Daisuke (right)

Director General, Cybersecurity Research Institute and Cybersecurity Nexus

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 2024. Ph.D. (Engineering).

search into methods of attack, and analysis of malware. In the area of detecting cyberattacks, a major characteristic of our work is how we were able to visualize the parts of the network that are under attack so that we can identify them at a glance. Visualization allows us to detect attacks quickly, and we can easily ascertain the details of the attack and the damage it is causing. Through the wide use of this visualization system, we can enable inexperienced system administrators and young engineers with little experience to instantly understand the situation with a

cyberattack.

Our lab also provides training to security personnel to help them learn practical cybersecurity knowledge and skills. About 3,000 people take our courses yearly.

**SEKIGUCHI** Technologies advance quickly, so it’s essential that we update our knowledge and skills on an almost daily basis. This just goes to show how rapidly cyberattack technologies could also be evolving.

**INOUE** It’s like a game of cat and mouse. While a large number of cyberattacks are indiscriminate, targeted attacks are also on the rise. In recent years, attacks on hospitals have been quite prominent. Attackers encrypt and lock their target’s data, and then demand that they pay a ransom to restore their data! We’ve seen a large number of these ransomware tactics.

### Every Device is a Cyberattack Target

**INOUE** Given how IoT has spread, we can say that any device connected to the Internet is now at risk of being targeted by a cyberattack. I mean all types of devices—including PCs and smartphones, as well as broadband routers, surveillance cameras and multi-function printers. So, security measures are essential. That being said, there’s no need to worry too much. You’ll usually be just fine as long as you keep up to date with your security updates.

The bright side of new technologies is that they are convenient and enrich our lives, but they also have a dark side in that they can be used for illegal purposes.

**SEKIGUCHI** Can VR goggles like the ones I use also be targeted for cyberattacks?

**INOUE** VR goggles are also a type of computer, so yes, they naturally become a target. Research institutes overseas have published several papers on cases of attacks involving VR goggles. They have found that if a goggle is attacked, it could lead to personal information theft, including what the goggle user’s real-world room looks like or the passwords they type in cyberspace.

**SEKIGUCHI** That also goes for smartphones, right? They’re just loaded with personal information. Anyone can find out when, where and who you met with, or even what you ate. But this kind of digital technology also forms the basis of my art, so I would like to see an environment in which everyone can enjoy

these technologies in safety.

**INOUE** What’s scary now is that in addition to cyberattacks, we also have disinformation and misinformation that spread through channels like social media. We now know that false information was deliberately spread in past U.S. presidential elections. Especially in the world of VR, where we continuously receive visual and auditory information in an immersive space, if it’s manipulated in some illicit way, your brain will directly receive false, inaccurate information. That’s why we need to have mechanisms that can properly verify the authenticity of information coming in and going out.

As of now, there’s been little research into what happens in the brain when wearable devices such as VR goggles are subjected to cyberattacks, so we plan to do research in this area going forward.

### Brain Security

**SEKIGUCHI** Ever since generative AIs came out, we have been seeing more and more fake videos. The videos are so realistic. You wouldn’t know if they were fake or not at first glance. It really is a battle for perception. Dr. INOUE, do you also do brain research?

**INOUE** NICT has an organization called the Center for Information and Neural Networks (CiNet), which is located in Suita city, Osaka Prefecture. Our Cybersecurity Research Institute has just begun research into brain security in collaboration with CiNet.

**SEKIGUCHI** So, brain security is already a thing. What specifically will your team be doing?

**INOUE** Research is going on worldwide into brain-computer interfaces (BCIs). BCIs take thoughts from the brain and output them as virtual body movements to operate things like robotic hands. This is important research for people who are frail due to illness or old age. Since it extracts brain signals directly, you could say that this is the ultimate personal information concern. At NICT, we used functional magnetic resonance imaging (fMRI) to analyze brain activity when people are shown certain images, and succeeded in reconstructing the original images from that data.

However, as I mentioned earlier, in order to use brain information in the real world as we go forward, we need to verify whether the information input to and output from the

brain is correct. And on top of that, we need to verify whether there are any unintended biases in our own brain activities. The more advanced brain information systems become, the more important brain security becomes.

**SEKIGUCHI** It’s still quite some time before we get there, right?

**INOUE** It could be 30 years from now, or even 10 years.

**SEKIGUCHI** Seriously? 10 years from now? That’s just around the corner. I was fascinated to learn about all the research you are doing at NICT in our conversation today. It looks like brain information communication is something that everyone will be involved in one way or another going forward. If you think about it, anyone can find themselves unable to move their body for one reason or another. It seems that just being able to say “yes” or “no” with our brain under those circumstances could make a huge difference in a person’s life.

I now see that cybersecurity isn’t just about protecting information. It’s about protecting all the things in one’s life.

**INOUE** Thank you very much for today. It would be great if we could have a collaboration between VR art and cybersecurity.

**SEKIGUCHI** I’d love to. Please let me know, and thank you very much.



# Cyberattacks Lurk Right Around the Corner Every Time You Access the Internet



**KASAMA Takahiro**  
Director of Cybersecurity Laboratory,  
Cybersecurity Research Institute  
Dr.KASAMA joined NICT in 2011. His  
research interests encompass a broad  
range of cybersecurity topics, including  
network monitoring and analysis, mal-  
ware analysis, and IoT security.  
Ph.D. (Engineering).

It's been almost 30 years since the release of the anime "Ghost in the Shell," in which a character remarked: "The net is vast and infinite." Microsoft released Windows 95 the same year, and people who got their hands on a personal computer entered the vast and infinite world of the Internet. Over the past 30 years, technologies once depicted in science fiction have become a reality thanks to advances in ICT, while the threat of cyberattacks continues to grow. In this environment, our Cybersecurity Laboratory is conducting research and development on technologies to counter cyberattacks that may occur now and shortly.

## Cyberattack Communications Arrive Once Every 14 Seconds

Our research and development in the Cybersecurity Laboratory's Fifth Mid- to Long-Term Plan is centered around two pillars (Figure 1). In "data-driven cybersecurity technology," we focus on research and development in technologies for performing routine and large-scale observations of various cyberattacks over the Internet. To develop

effective technologies to counter cyberattacks, it is essential that we understand the reality of cyberattacks and collect actual data, such as malware samples, attack traffic, and malicious web content to use in our research and development. For example, attack traffic related to indiscriminate attacks observed by NICTER—a darknet observation system that we have been researching and developing for 20 years—have consistently been on the rise since we began observations, with approximately 620 billion packets observed in the year 2023 (Figure 2). This means that some device connected to the Internet using a single IPv4 public address receives attack traffic at an average rate of about once every 14 seconds. As a result, if a device with subpar security is connected to the Internet, it can become a cyberattack victim in a matter of minutes. Unless you monitor these attacks, it would probably be challenging to understand the reality of these Internet threats.

Also, cyberattacks often occur in conjunction with real-world events.

When Russia began its invasion of Ukraine on February 24, 2022, NICTER detected a sharp increase in backscatter (bounces of DDoS attacks) from Ukraine within the

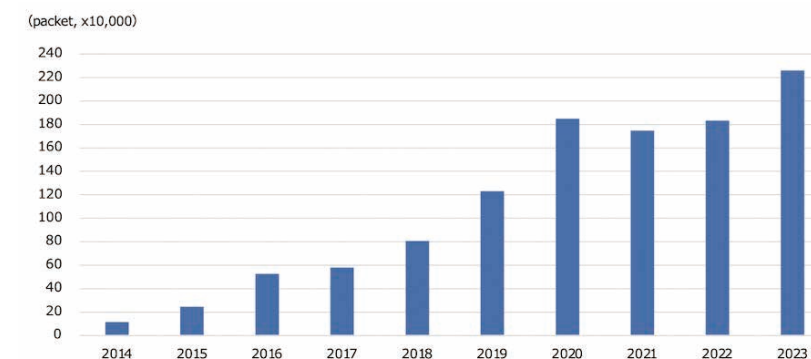


Figure 2 Trends in indiscriminate attack-related traffic observed by NICTER

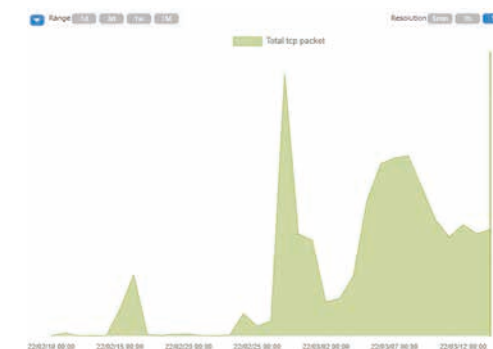


Figure 3 Changes in backscatter from Ukraine

same timeframe (Figure 3). These DDoS attacks targeted government websites, national banks and others. It is unclear how much of an impact these cyberattacks actually had, but this shows how real-world and cyberspace events are closely related.

We ascertain the reality of these cyberattacks in real time, and based on data that we collect on a large scale, we advance our research and development on effective technologies for countering cyberattacks.

## Studying Risks from an Attacker's Perspective

Meanwhile, in "emerging security technology," we carry out research and development with a focus on cyberattacks and new threats that may potentially occur in the near future. New technologies that appear in our society (emerging technologies) often entail threats that we have never seen in already existing technologies. We identify potential threats by considering how these new technologies could be exploited from an attacker's perspective and conduct research and development on reducing risks and verifying safety.

For example, there have been remarkable technological advances in connected cars in recent years. Fully driverless, self-driving

taxi services have been launched in the United States, China, and other countries. Unlike conventional standalone cars, these connected cars have many modules that interact with the outside world, such as wireless communication devices, vehicle-to-vehicle communication systems, and various sensing systems. At the Cybersecurity Laboratory, we have developed a verification environment where we use actual vehicles in demonstration experiments of attacks against Intelligent Transport Systems (ITS) (Figure 4) and other experiments, based on which we conduct our research and development in the area of risk assessment and countermeasures for connected cars.

Additionally, in collaboration with the Center for Information and Neural Networks (CiNet) at the Advanced ICT Research Institute, we have begun research into brain information security as our new research topic. In 2021, clinical trials began for a Brain Machine Interface (BMI) that uses an electrode-equipped cerebrovascular stent developed by Synchron. In 2024, Neuralink, founded by Elon Musk and others, began clinical trials of a BMI for paralyzed patients that can be implanted in the brain, bringing us closer to achieving a "cyber brain" world. We do not yet have any clear answers as to

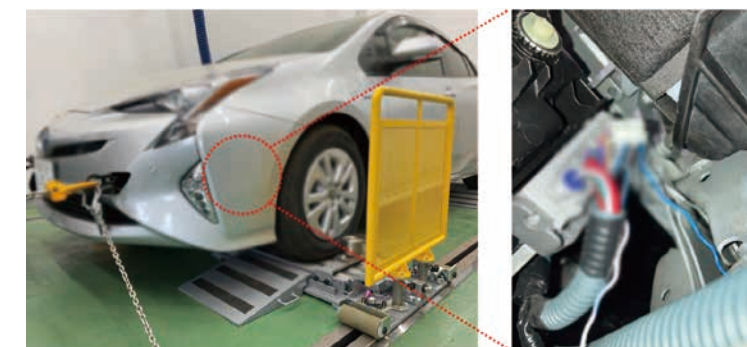


Figure 4 Security verification using actual connected cars

what kind of cybersecurity we will need in a world where brains are connected to computers, and brain information can be easily obtained using inexpensive devices. This is why it is important that we quickly identify the potential threats we may face from emerging technologies and use what we learn to implement security by design before they become widely used in society.

## It is Important that We Do not Stop Under Any Circumstances

The field of cybersecurity is a challenging and fascinating area of research, with situations constantly changing due to the emergence of new technologies and how attackers evolve over time. Attackers sometimes target not only technical vulnerabilities but also our human psychological weaknesses. Just as the crime count in the real world will never reach zero, cyberattacks will also likely never go away. Even so, in order to reduce the damage caused by cyberattacks as much as possible and create a world where people can enjoy the benefits of ICT in safety, we believe it is important that we never stop our research and development in the area of cybersecurity.

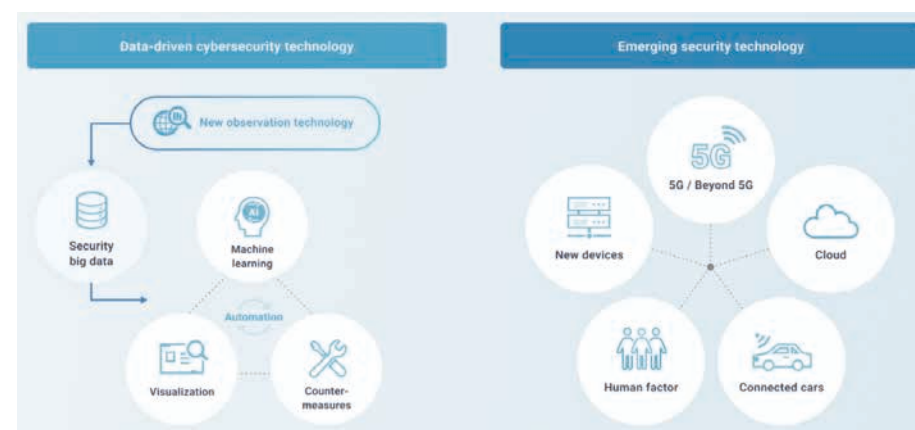


Figure 1 The two pillars of the Cybersecurity Laboratory

## Overview of R&D Activities at Security Fundamentals Laboratory



**SHINOHARA Naoyuki**

Director of Security Fundamentals Laboratory, Cybersecurity Research Institute

Dr. SHINOHARA received his Ph.D. in mathematics in 2008. He was a researcher at the Japan Science and Technology Agency from 2007 to 2009 and a post-doctoral fellow at Rikkyo University in 2009. He joined NICT in 2009. He was a researcher at NICT from 2009 to 2014, a senior researcher from 2014 to 2020, and a research manager from 2020 to 2023, and has been a director at NICT since 2023.

His research interests include computational number theory, computer algebra, and the cryptanalysis of public key cryptosystems. Ph. D. (Mathematics).

Newly developed technologies in quantum computing and machine learning as well as improvements to their performance are increasing the need for encryption and privacy protection technologies. At the Security Fundamentals Laboratory, we are evaluating the threat of quantum computers to modern cryptography and researching cryptography that is difficult to decrypt even with a quantum computer. We are also conducting research and development on DeepProtect, which aims to enable organizations to use their own data for machine learning safely and securely.

### Research and Development on Privacy-preserving Federated Learning Technology, DeepProtect

In machine learning, the more training data available, the more effective the learning tends to be. Therefore, it is considered good for organizations owning training data to share it. However, if the training data contains sensitive information, it is generally difficult for them to share. One way to solve this difficulty is federated learning, in which organizations perform machine learning without sharing training data and share information necessary to improve learning models obtained through machine learning. However, there is a possibility that organization-specific training data may be leaked from the information.

To solve this problem, the Security Fundamentals Laboratory is conducting research and development on a technology for federated learning that preserves privacy. Called DeepProtect,

it enables learning models to be improved and shared with information necessary to improve them, keeping it encrypted with homomorphic encryption, which allows additive operations while keeping training data encrypted. The Laboratory is also conducting demonstration experiments using DeepProtect and data actually used in the financial field (Figure 1), aiming for the social implementation of DeepProtect.

### Evaluation of the Security of Cryptographic Technologies for the Quantum Computing Era

The Security Fundamentals Laboratory evaluates the security and performance of cryptographic technologies currently used and expected to be widely used in the future to help ensure their proper implementation and safe operation. Specifically, the Laboratory is engaged in research and development on the evaluation of the security of cryptographic technologies that can be safely used in the quantum computing era, RSA cryptography, which is currently widely used, elliptic curve cryptography, and other relevant technologies. The results of the research are effectively used in CRYPTREC, a national project to verify and evaluate the security of e-Government recommended cryptography and investigate and examine the appropriate implementation and operation of cryptographic technologies.

### Security Evaluation of Modern Cryptography using Quantum Computers

The security of public key cryptography, which is widely used today, is closely related to prime factorization and discrete logarithm calculations, and cryptography is broken by solving these calculations. The computational cost of decryption increases with the longer the key length as the number of digits grows larger, and it is considered practically impossible to solve calculations of several hundred digits with current computers. Thus, calculations with such large key lengths are used in cryptography. On the other hand, it

has been theoretically proven that large calculations can be solved quickly by using a quantum computer with sufficient performance. For this reason, it is an important research topic for the Security Fundamentals Laboratory to confirm through experiments the size of the key length that can be solved by currently available quantum computers and evaluate the specific threats to modern cryptography related to the key length.

The Laboratory has proposed a mathematical definition of calculations that can be solved by a quantum computer, and has succeeded in the world's first experiment of solving discrete logarithm calculations for very short key lengths using a quantum computer. The result confirms that current quantum computers have difficulty solving the large discrete logarithm calculations in the currently widely used public key cryptography, and that quantum computers currently pose no threat to modern cryptography.

### Security Evaluation of Quantum-Resistant Cryptography

Quantum-resistant cryptography is a type of public key cryptography usable in environments where conventional types of public key cryptography are usable, and it ensures security for both quantum computers and conventional computers. Specifically, quantum-resistant cryptography is a public key cryptography with which security is based on mathematical calculations and for which high-speed solutions cannot be found, even using quantum computers or conventional computers.

In the Security Fundamentals Laboratory, we are conducting research on the security evaluation of lattice cryptography and multivariate public key cryptography, which are thought to have high potential for quantum-resistant cryptography, and we achieved a world record in the Fukuoka MQ Challenge, a decryption contest for multivariate public key cryptography (Figure 2). The knowledge we obtained through the research is used to formulate the CRYPTREC Cryptographic Technology Guidelines (quan-

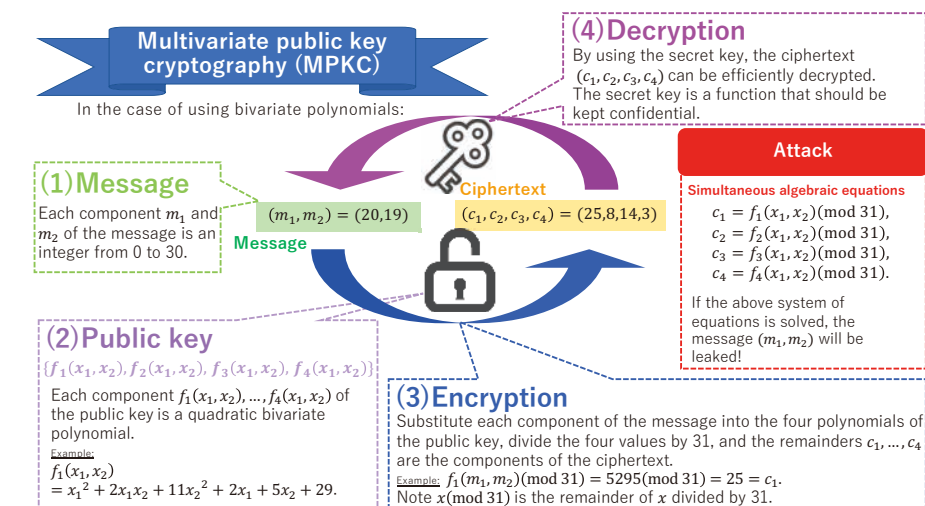


Figure 2 Overview of multivariate public key cryptography

tum-resistant cryptography) described below.

### Activities for Quantum-resistant Cryptography in the CRYPTREC Project

CRYPTREC is a project to evaluate and monitor the security of cryptography technologies recommended by e-Government and investigate and consider appropriate implementation and operation of cryptography technologies. The secretariat of CRYPTREC consists of the Digital Agency; the Ministry of Internal Affairs and Communications; the Ministry of Economy, Trade and Industry; the National Institute of Information and Communications Technology; and the Information-Technology Promotion Agency. CRYPTREC is structured with the Cryptographic Technology Evaluation Committee and the Cryptographic Technology Utilization Committee under the Cryptographic Technology Review Committee.

Activities for post-quantum cryptography are mainly carried out by the Cryptographic Technology Evaluation Committee in which NICT is the leading party, and the Cryptographic Technology Research Working Group established under it. As a specific activity in recent years, CRYPTREC conducted a survey of trends in research on post-quantum cryptography from 2021 to 2022, and based on the results of the survey, formulated the CRYPTREC Cryptographic Technology Guidelines (Post-quantum Cryptography) and published the guidelines in April 2023. In addition, from 2023 to 2024, CRYPTREC is planning to conduct a similar survey and formulate new guidelines based on the guidelines for post-quantum cryptography.

### Future Prospects

This paper introduced some major efforts carried out by the Security Fundamentals

Laboratory in the research and development of cryptography and privacy protection technologies, and research on the security evaluation of cryptography. Regarding DeepProtect, the Laboratory conducted a demonstration experiment using data actually used in the financial sector and found challenges to be addressed. The Laboratory has also identified the possibility of applying DeepProtect to new areas in the medical and other fields, and will tackle new research topics based on this possibility.

With respect to quantum-resistant cryptography, research and various activities are ongoing both in Japan and overseas. In particular, the National Institute of Standards and Technology (NIST) in the United States is promoting the standardization of quantum-resistant cryptography technologies, which will have a significant impact on the selection of quantum-resistant cryptography technologies to be used in Japan. NIST opened the first public call for proposals for quantum-resistant cryptography technologies in 2016, and is in the process of standardizing several technologies as of 2024. In addition, NIST has conducted an additional call for proposals for quantum-resistant cryptography technologies in 2022, and the process for evaluation of the security and implementation performance of selected quantum-resistant cryptography technologies will continue until around 2030.

After that, implementation methods will likely be improved, side-channel attacks against the improved implementation methods will be discovered, and other possible problems will likely occur. Therefore, the Laboratory staff believes that research into quantum-resistant cryptography will remain an important task for the Security Fundamentals Laboratory until around 2035.

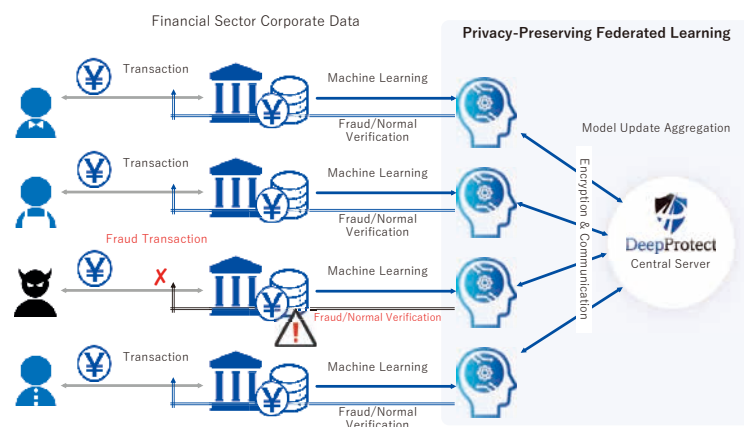
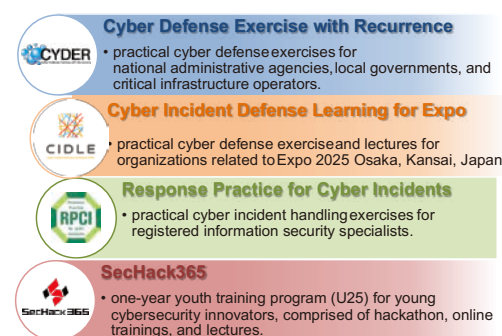


Figure 1 Example of a demonstration experiment using DeepProtect



## Human Resource Development Programs Offered by the National Cyber Training Center



**SONODA Michio**

Director General,  
National Cyber Training Center,  
Cybersecurity Research Institute

After Completing a doctorate in Engineering, Dr. SONODA 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).

The National Cyber Training Center currently provides four programs called Cyber Defense Exercise with Recurrence (CYDER<sup>\*1</sup>), Response Practice for Cyber Incidents (RPCI<sup>\*2</sup>), Cyber Incident Defense Learning for EXPO (CIDLE<sup>\*3</sup>), and SECURITY + HACKATHON 365 DAYS (SecHack365<sup>\*4</sup>). CYDER, RPCI, and CIDLE offer practical exercises for practitioners, while SecHack365 is a program for young professionals, such as engineers and researchers, aged 25 and under.

### ■ Cyber Defense Exercise with Recurrence (CYDER)

CYDER has been conducted since the establishment of this center, with an annual target of 3,000 participants and over 100 sessions held each year. It is the largest-scale program among the center's offerings. CYDER focuses on initial response actions immediately after a cyberattack. Participants gather at venues across all 47 prefectures in Japan will engage in practical learning on responding to incidents over one or two days. They are divided into groups of four, each member playing a specific role and working on incident response following a scenario based on an actual event. The training uses CYDERANGE, a proprietary cyber training automation system, to provide each team with a virtual organizational network, which serves as the training environment and platform for investigation and analysis.

The lineup features A Course, a beginner and introductory program; B Course, an intermediate program; and C Course, a semi-advanced program. While C Course is a two-day program, both A and B Courses are one-day programs with a few additional hours of online pre-training.

In addition, in response to various recent needs, the center has been offering an online self-study style pre-CYDER program since fiscal year 2023, through which participants can learn the basics of incident response quickly. This program provides essential knowledge of cybersecurity and features

multiple case study videos (each about 10 to 20 minutes long) that delve into actual incidents. Furthermore, organizations unable to participate in collective training, an online version with content equivalent to the collective training is currently being tested and is scheduled to be available soon.

### ■ Response Practice for Cyber Incidents (RPCI)

RPCI follows the same format and training environment as CYDER, consisting of one-day collective training plus pre-learning. However, RPCI provides scenarios with difficulty levels adjusted for security professionals.

### ■ Cyber Incident Defense Learning for EXPO (CIDLE)

CIDLE is a program designed for the Japan Association for the 2025 World Exposition, the organizer of Expo 2025 Osaka, Kansai, Japan. While its main focus is on incident response training, as with CYDER and RPCI, CIDLE also provides lectures and hands-on training in various fields and topics primarily related to hosting mega-events. Additionally, like CYDER, CIDLE offers short-duration online self-study exercises.

### ■ SECURITY + HACKATHON 365 DAYS (SecHack365)

SecHack365 is entirely different from the other three programs. It holds six events annually, along with intensive online communication, inspiring young professionals and producing individuals capable of taking action. Now in its eighth year, the program continues to evolve gradually each year.

### ■ Future Prospects

For CYDER and RPCI, we plan to identify and address user needs more thoroughly, particularly by developing content that is user-friendly for both hosts and participants, similar to Pre-CYDER. Through SecHack365, we aim to produce even more individuals capable of creating innovative solutions to the cybersecurity workforce shortage.

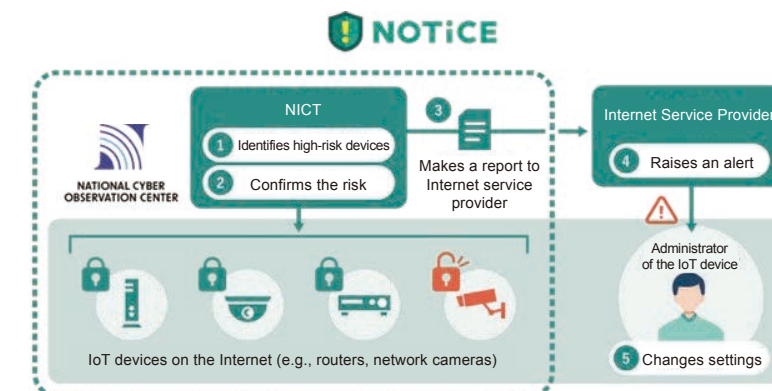
## Toward the Realization of a More Secure and Safe IoT Environment



**ETO Masashi**

Director General,  
National Cyber Observation Center,  
Cybersecurity Research Institute

Dr. Eto joined NICT in 2005. Has since been at the forefront of research and development in cybersecurity technologies, focusing on areas such as the NICTER project, IPv6, ITS, and IoT. His work has extended to international standardization, development of cybersecurity workforce, and policy formulation to foster innovation in the field. Ph.D. (Engineering).



Overview of NOTICE

With the development of the Internet, IoT devices have become indispensable in the lives of ordinary people. However, cyberattacks against IoT devices are increasing, seriously affecting their lives.

In light of this situation, the National Cyber Observation Center (NCO) is working with the Ministry of Internal Affairs and Communications and telecommunications carriers (Internet service providers, hereinafter referred to as ISPs) to promote the NOTICE project\* to improve the security of IoT devices and prevent damage from cyberattacks.

NCO's main role in the NOTICE project is to identify IoT devices in Japan that may be exploited in cyberattacks and notify ISPs about the identified devices. To do this, we mainly conduct the following investigations:

### ■ Investigation of Devices with ID/Password Vulnerabilities

If an IoT device has an ID and password that are easily guessed (a simple string or a small number of characters), it is more likely to be accessed illegally and exploited. Thus, NCO attempts to log in to IoT devices by entering an ID and password that are easily guessed in order to investigate vulnerabilities that may allow unauthorized intrusion. When the attempt is successful, the device is determined to be vulnerable, and NCO alerts the administrator of the device via the ISP concerned to urge the administrator to change the password to an appropriate one.

### ■ Investigation of Devices with Firmware Vulnerabilities

Vulnerabilities in IoT device firmware can pose serious security risks, such as having their functions be exploited or allowing unauthorized remote control of the devices.

Thus, NCO is investigating to find if there are any devices with security holes that may allow attacks to be made through firmware vulnerabilities. If a vulnerability is found on a device, NCO alerts the administrator of the device and recommends that the administrator update the firmware to the latest version.

### ■ Investigation of Devices Infected with Malware

Using NICTER's observation network, NCO is investigating devices infected with malware such as Mirai, which is designed to target IoT devices. In the investigation, NCO identifies IoT devices suspected of being infected with Mirai from communication data collected by NICTER and analyzes how the devices are running. When an infected device is confirmed as a result of the investigation, NCO alerts the administrator of the device and recommends that the administrator eliminate the malware.

### ■ Future Prospects

As a result of these efforts, in 2023, NCO discovered more than 10,000 devices with improper settings through an investigation of devices with ID and password vulnerabilities in Japan and reported these devices to their respective ISPs. As NCO has been conducting the investigation and reporting to ISPs for more than five years, the number of alerts regarding problematic devices has been steadily decreasing.

However, there are still many vulnerable IoT devices with improper settings in Japan, and it will be necessary to respond to unknown threats caused by newly developed technologies or changes in the ICT environment, so NCO is determined to promote the NOTICE project while improving its investigation capabilities and work efficiency.

\*1 CYDER: Practical cyber defense training conducted primarily for national government agencies and local governments, and also extended to independent administrative institutions, public organizations, and the private sector

\*2 RPCI: A specialized training program designed for the national qualification of Registered Information Security Specialist (RISS), focused on the initial response to incidents, based on the CYDER framework

\*3 CIDLE: A cyber defense training program built on the Cyber Colosseo initiative, which provided exercises, lectures, and hands-on training for the Tokyo Olympic and Paralympic Organizing Committee

\*4 SecHack365: A security workforce development program targeted at individuals aged 25 and under, designed to cultivate professionals who are aware of security challenges and capable of proposing innovative solutions to address them, and who are committed to driving change in society through technology

\* NOTICE: National Operation Towards IoT Clean Environment




# CYNEX Alliance: “A nexus of Cybersecurity,” for Industry-Academia-Government in Japan



**YASUDA Shingo**  
 Director of CYNEX Research, Development and Operations Laboratory, Cybersecurity Nexus, Cybersecurity Research Institute

After working as a postgraduate researcher, Dr.YASUDA joined the National Institute of Information and Communications Technology in 2013. Engaged in research on automation technology for building emulated environments for reproducing and verifying cyber-attacks, and he also managed the Cyber Colosseum project, a security training project for Tokyo 2020 Games officials. Ph.D. (Information Science), CISSP.



**KANAHAMA Nobuhiro**  
 Director of CYNEX Business Promotion Office, Cybersecurity Nexus, Cybersecurity Research Institute

He joined NICT in 2016, after working at a hardware vendor and as an instructor and developer of educational materials related to cybersecurity. He has primarily engaged in scenario development for cybersecurity Trainings. Hobby is experiencing “4DX” around the world.cyber-security. He has primarily engaged in scenario development for cybersecurity Trainings. Hobby is experiencing “4DX” around the world.

The Cybersecurity Nexus (CYNEX) was established in 2021 as a nexus for industry-academia-government cooperation on cybersecurity information analysis and human resource development in Japan. For sustainable development of the initiative, a new framework, the CYNEX Alliance, was formed after the preparation period, on October 1, 2023. The CYNEX Alliance aims to be an organization in which partners and members share their issues and objectives and autonomously carry out activities. It adopts the chair system, under which experts from NICT and partners are appointed to chair Co-Nexuses (described later) and action policies and other matters are decided through discussion. Joint steering by NICT and the partners encourages Co-Nexuses to be self-propelled to carry out independent activities involving the partners. CYNEX and the secretariat support such activities by Co-Nexuses.

## CYNEX Alliance and four Co-Nexuses

To move forward a wide range of cybersecurity-related activities in parallel, the CYNEX Alliance implements concurrent multi-faceted activities under four sub-projects, or “Co-Nexuses” (figure 1). One year since the establishment of the CYNEX Alliance, cooperation between NICT and partners has advanced and the activities of each Co-Nexus have increased. With these increasingly active movements, the number of partners is sharply increasing, reaching a total of 86 organizations as of November 1, 2024 (table 1).

### Co-Nexus A

Co-Nexus A (Accumulation & Analysis) currently has 36 participating partners. Using

R&D results from the Cybersecurity Laboratory and CYNEX, Co-Nexus A collects and accumulates cybersecurity information and lends analysis infrastructure and offers data to alliance partners to foster a community of analysts and facilitate joint analysis.

### STARDUST

STARDUST is developed by the Cybersecurity Laboratory, is a platform for luring cyberattacks, mainly targeted attacks. Currently, STARDUST is being loaned out to more than 20 partners, each of which uniquely uses it for cyberattack analysis. Meanwhile, STARDUST user organizations are leading analyst community activities for sharing analysis results and knowledge. About 90 domestic analysts gather for regular meetings that are held quarterly.

### WarpDrive Project

WarpDrive is a user-participatory project in collaboration with the animation work GHOST IN THE SHELL: SAC\_2045. CYNEX conducts R&D and distributes free of charge the TACHIKOMA Security Agent (TACHIKOMA SA), in which amination characters appear. Data on web-based cyberattacks that is provided by users is collected and accumulated for analysis by partners and used in R&D to improve detection technologies. Users receive feedback in the form of security application functions based on the results (figure 2).

As a result of the addition of a game function, improvement of basic security software functions, and other measures for promoting long-term use by users, the data volume collected by TACHIKOMA SA increased by about 7 times in the most recent two years to 7 million URLs/day.

### LETTICE

LETTICE is a threat observation team

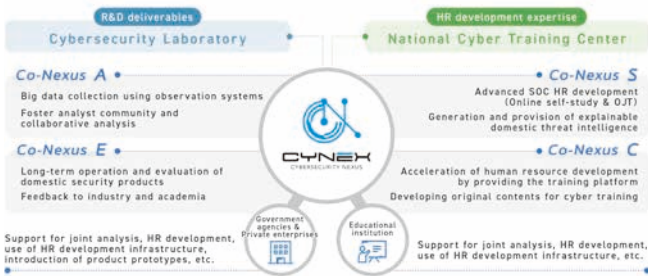


Figure 1 CYNEX and Four Co-Nexuses

newly founded under Co-Nexus A in February 2024 for joint analysis of various threat information. In STARDUST and WarpDrive, partners independently conduct observation and data analysis to share obtained knowledge to the extent possible. In LETTICE, volunteers are invited from partners participating in Co-Nexus A or S to conduct joint analysis of threats as a team.

### CURE

Co-Nexus A has opened up CURE, a security information integration platform developed by the Cybersecurity Laboratory, to partners participating in Co-Nexus A or S. CURE provides the function of searching for malicious information obtained by partners and determining how such information is acquired on information infrastructure that NICT observes.

### Co-Nexus S

In cooperation with the analysis team from the Cybersecurity Laboratory, which is also a member of NICT-CSIRT, Co-Nexus S (Security Operation & Sharing) conducts continuous analysis of darknets, livenets, and so on, generation of domestic threat information and provision of data based on primary data accumulated by Co-Nexus A and secondary data obtained from the outside. Meanwhile, for the development of advanced Security Operation Center (SOC) human resources, Co-Nexus S accepts people from partners to the analysis team, where they take OJT and online self-study courses. So far, online courses have been completed by 46 individuals.

### Co-Nexus E

Co-Nexus E (Evaluation) uses NICT’s internal network as a test bed to connect domestic security products developed by partners for long-term operation and verification. Co-Nexus

E uses unique simulated attacks by CYNEX’s top engineer team (red team) as well as live traffic and standard cyber-attack patterns in conducting functional and non-functional verification of products and comparison with existing products, and provides developer organizations with feedback on evaluation results to support R&D of technologies in Japan. Co-Nexus E has conducted verification, including ongoing verification, for eight products and provided their developer vendors with feedback on the results.

### Co-Nexus C

Co-Nexus C (CYROP) continuously develops extensive security-related training content aligned with the NIST NICE Cybersecurity Workforce Framework (NICE Framework) and provides partners with the content as standard training material to facilitate the development of security human resources in Japan. As of fiscal 2024, more than 70 types of training materials have become available, and coverage based on the NIST NICE Framework, which is an indicator for the security knowledge area, is about 50%. Co-Nexus C plans to create business-specific training materials, such as training for critical infrastructure, in addition to general-purpose content going forward.

## Future Prospects

Currently, CYNEX is promoting Co-Nex-



Figure 2 WarpDrive ©Shirow Masamune, Production I.G/KODANSHA/GITS2045



Figure 3 Image of Co-Nexus E implementation

Table 1 Number of CYNEX partners (Figures for Co-Nexus include partners that participate in multiple Co-Nexuses)

Entire CYNEX Alliance (Unique organizations)	86 organizations
Co-Nexus A	36 organizations
Co-Nexus S	18 organizations
Co-Nexus E	8 organizations
Co-Nexus C	61 organizations

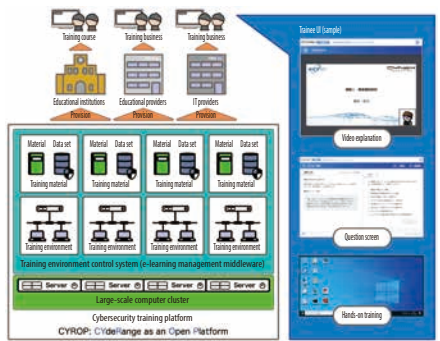


Figure 4 Cybersecurity training platform CYROP

uses activities together with 86 partner organizations. CYNEX shares activity results mainly among partners, but is planning to provide information to the general public using the CYNEX and WarpDrive websites.





## Panel Discussion Featuring Women Thriving in the Cybersecurity Industry! Organization of the NICT Cybersecurity Symposium 2025

General Planning Office, Cybersecurity Research Institute

Do you know what the period from February 1 to March 18 is called in Japan? The answer is "Cybersecurity Month." It was designated by the National center of Incident readiness and Strategy for Cybersecurity (NISC). The Cybersecurity Research Institute has been holding the annual NICT Cybersecurity Symposium during the month for more than 10 years, in which participants make presentations and hold discussions on the latest cybersecurity-related trends. By the way, Cybersecurity Month ends on March 18, or "318," which sounds similar to the pronunciation of "cyber" in Japanese.

Last year's NICT Cybersecurity Symposium 2024 was held in a face-to-face format only at the NICT Innovation Center located in Nihonbashi, Tokyo, on February 16, 2024. On the day, nearly 150 people participated in the event from governmental agencies, companies in the private sector, and research institutes including universities across the country, making the venue almost completely full.

The 2024 symposium was held with a focus on next-stage R&D in the field of cybersecurity, and was composed of three speeches and two panel discussion sessions.

In particular, the panel discussion in which seven women thriving in the cybersecurity industry discussed the empowerment and career paths of women in the industry attracted the greatest attention at the symposium.

SAKUMA Morica (incri Co., Ltd.) served as moderator for the panel discussion and the following six women participated in the event as panelists: NAKAJIMA Asuka (Elastic / security research engineer), Yin Minn Pa Pa (Associate Professor, Institute of Advanced Sciences, Yokohama National University), SHINODA Kana (CEO, BLUE Co., Ltd.), MORIAI Shiho (then Director General, NICT Cybersecurity Research Institute), ANBE Sayuri (Research engineer, NICT Cybersecurity Nexus), and MATSUDA Misato (Researcher, NICT Cybersecurity Laboratory).

At the beginning of the session, they called one another by nicknames, and the event started in a calm atmosphere. However, as they began to talk about the theme, they dramatically changed their expressions and discussed the issues faced by the cybersecurity industry in a very passionate manner and from a perspective that is unique to women. Their attitudes left a great impression on the audience. In the Q&A session, a female participant asked a question about the work styles of women. The panel discussion thus also provided participants with an opportunity to think about diversity, and was truly innovative.

The NICT Cybersecurity Symposium 2025 will be held again at the NICT Innovation Center on Friday, February 21, 2025. This event will be organized both in face-to-face and online formats so that even more people can participate in it from across Japan.

This year's symposium, the theme is "Continuous Security, Connected Security", will be composed of the presentations of latest research reports by the teams of the Cybersecurity Laboratory and speeches by guest speakers. As a special part of the symposium, another discussion by women thriving in the cybersecurity industry will be held! Last year, the panel discussion was so exciting that the time allocated to it, which was as many as 80 minutes, was not enough for the discussion and the Q&A session. We heard that the discussion continued at the wrap-up party, which may or may not be true. Therefore, we're holding a second round this year.\*

Please come to the venue and directly feel the speakers' and the audience's passion about cybersecurity. If you cannot come in person, you can participate and ask questions online. We are looking forward to your participation!

(The speakers have not yet been selected, and not all of the last year's speakers will participate.)



Last year, a panel discussion was held on the empowerment and career paths of women in the cybersecurity industry.



The symposium was held on next-stage R&D in the field of cybersecurity.

## Looking at Cybersecurity Training Programs from a Career-Track Perspective



### SUGIMOTO Sara

Administrative Specialist  
Cyber Training Promotion,  
Cybersecurity Research Institute  
National Cyber Training Center

#### ● Biography

2002 Born in Tokyo  
2024 B.A. in Department of Finance and Public Economics, College of Economics, Nihon University  
2024 Joined NICT Cybersecurity Research Institute  
Assigned to National Cyber Training Center

#### Q&As

#### Q What do you like about working at NICT?

A The biggest appeal for me is that I can engage in cutting-edge ICT research and contribute to society. It's also interesting to get an up-close feel for the kind of research that I don't encounter in my daily life.

#### Q Please give a message to students who are interested in a career-track position at NICT.

A At NICT, you can gain a great deal of knowledge and skills through diverse experiences. Stay curious and keep your passion to learn more. I look forward to seeing you at NICT!

#### Q How do you spend your days off?

A I go out and eat with my friends from university. Recently I have been into eating at local casual-style Chinese restaurants, and I want to explore new restaurants.



As a career-track employee, I have been involved in the work at the National Cyber Training Center. At the center, there are four programs in place: CYDER, RPCI, CIDLE, and SecHack365. I am mainly involved in SecHack365. SecHack365 stands for "Security + Hackathon 365 Days," a long-term hackathon for people under 25 years old. Its goal is to develop security innovators who are capable of solving various security issues with their ideas, while being given unique opportunities to create over a long period of time.

In SecHack365, I am in charge of reimbursement of expenses for the participants, communicating with external business operators, and handling administrative duties as the secretariat of events.

When I joined NICT as a new graduate, my first task was to get a proper grasp of my role in SecHack365 and the center. When the actual work began, I

had to handle duties of the center other than SecHack365 at the same time. I had a hard time getting used to prioritizing multiple tasks and doing them in parallel. In SecHack365, I initially struggled with the reimbursement of expenses in a system that I was unfamiliar with, but now I have become accustomed to the system and method of reimbursement of expenses, so I make fewer mistakes than before. Since SecHack365 is funded by grants, double-checking within the team is a must, and each person is responsible for

entering and checking vouchers. Therefore, I believe that collaboration within the team is extremely important.

At events, I see the participants actively talking about their work. It is challenging to witness the process from theme setting to creating a work, and to see the participants' personal growth over the course of one year. Just as the SecHack365 trainees pursue their themes of work set on their own and give shape to the themes, I want to have an inquisitive mind about my work and take on various challenges at NICT.

#### Five features of SecHack365



Group events held six times a year  
Continuing development by holding ideathon and hackathon events multiple times a year, both online and offline.



Support for Students  
Students are fully subsidized for necessary expenses for the group events. Counseling on balancing studies and career paths is also available.  
Note: Students 25 years of age and under as well as those with no income will receive full subsidies for actual expenses incurred, such as travel and lodging expenses.



Only at NICT  
"NONSTOP" is available, which allows the participants to utilize NICT's cybersecurity research and development know-how and valuable actual attack data.



A variety of lectures and online content  
We also have online content, including materials on ethics and laws, and communicate remotely using chat and task management tools.



Use of online content  
Online content, including ethics and law, is also utilized. We communicate remotely using chat and task management tools.

SecHack365 aims to develop "security innovators" who are capable of tackling various security issues with their ideas by maximizing the use of the above five features and providing opportunities for manufacturing.



NICT will be exhibiting at MWC again this year.

**3-6 MARCH 2025**  
Fira Gran Via, Barcelona



## Contents

NICT are preparing a variety of exhibits about our R & D on Beyond 5G, including tools for a glimpse into the future of life beyond 2030, transmission of uncompressed 4K video using terahertz (300 GHz band) technology, a working demonstration of a service in which drones and robot cars collaborate in the wireless transmission of time-space synchronized multi-view large-volume observation data, and an interactive demo where a drone in Singapore can be remotely controlled using O-RAN that enables cross country control of equipment.