CYBERSECURITY RESEARCH INSTITUTE

Cybersecurity Laboratory
Security Fundamentals Laboratory
Cybersecurity Nexus
National Cyber Training Center
National Cyber Observation Center
General Planning Office

CYBERSECURITY
Research Institute

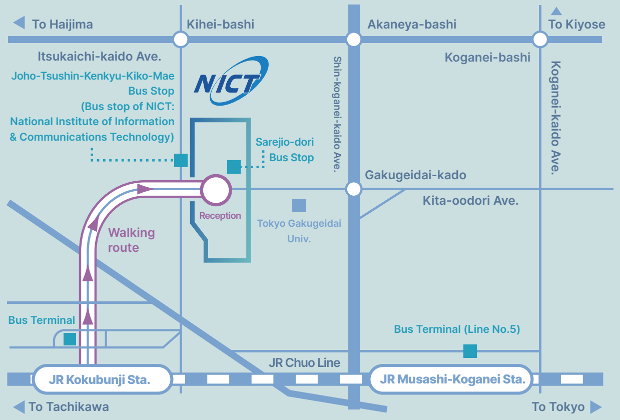
NICT
National Institute of Information and Communications Technology

4-2-1, Nukui-Kitamachi, Koganei, Tokyo
184-8795, Japan
URL : https://www.nict.go.jp/en/

Cybersecurity Research Institute

E-mail : cyber-info@ml.nict.go.jp
URL : https://csri.nict.go.jp/en/

Other inquiry regarding NICT
TEL: +81-42-327-5392 FAX: +81-42-327-7587
E-mail: publicity@nict.go.jp



Towards a Global Center of Excellence for Cybersecurity R&D

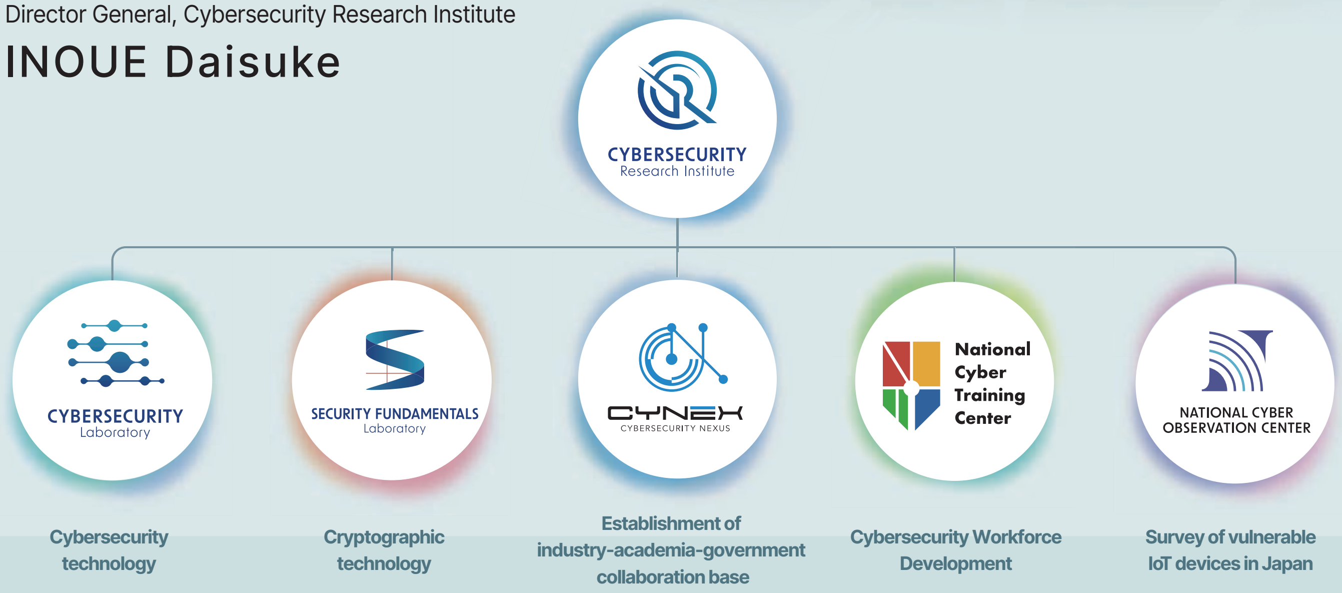
Countermeasures against increasingly sophisticated and complex cyberattacks have become an urgent national issue, and social demands for NICT's role in cybersecurity are growing. To protect Japan from a wide variety of cyberattacks, the Cybersecurity Research Institute aims to become a global center of excellence in cybersecurity research and development by leveraging NICT's neutrality and close collaboration with industry and academia. Based on government policy, NICT conducts cybersecurity training programs, promotes cybersecurity measures for IoT devices, and strives to become a nexus in the cybersecurity domain, connecting industry, academia, and government.

NICT is committed to promoting research and development of technologies for the large-scale collection, accumulation, and cross-cutting analysis of data related to cyberattacks. Under the fifth mid-to-long-term plan launched in April 2021, we aim to improve Japan's cybersecurity response capabilities by advancing these technologies, forming a domestic community of analysts to analyze cybersecurity data, and establishing an open platform to develop a cybersecurity workforce throughout society.

Achieving a secure and safe cyberspace requires technologies that securely utilize data while ensuring both security and privacy. Additionally, there are concerns that the security of current cryptographic technologies will be compromised if large-scale quantum computers are realized. Therefore, we will evaluate the security of new cryptographic technologies for the quantum computing era, such as post-quantum cryptography, as well as the cryptographic technologies currently widely used in electronic government systems.

Director General, Cybersecurity Research Institute

INOUE Daisuke



Cybersecurity technology

Cryptographic technology

Establishment of industry-academia-government collaboration base

Cybersecurity Workforce Development

Survey of vulnerable IoT devices in Japan

Cybersecurity Laboratory

OUTLINE

To contribute to the continuous improvement of cyberattack response capabilities and counter the diversifying cyberattacks, we are conducting research and development around two pillars: data-driven cybersecurity technology and emerging security technology. In particular, we are working on the research and development of technologies for attack observation, analysis, visualization, and countermeasures to address increasingly sophisticated and complex cyberattacks, cross-analysis of large and diverse information related to cyberattacks, and verification technologies for improving security in emerging network environments. We also aim to disseminate research and development results and implement them in society.

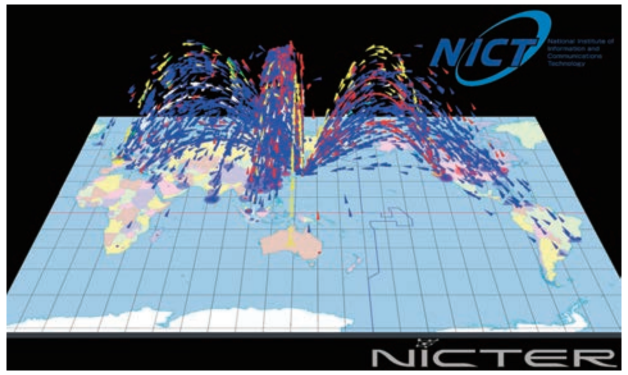
PROJECTS

Data-driven cybersecurity technology

We conduct research and development of practical cybersecurity technologies to respond to changes in cyberattack trends. Specifically, we are working to establish and advance technologies for observing sophisticated and increasingly complex cyberattacks including indiscriminate and targeted attacks from multiple aspects, supporting situational awareness through visualization technologies, and developing automated analysis and countermeasure technologies that make full use of AI technologies such as machine learning. In addition, we are actively promoting the social application of the technologies we have developed, the attack data we have collected, and the knowledge we have gained.

Cyberattack observation and analysis system "NICTER"

Network Incident analysis Center for Tactical Emergency Response



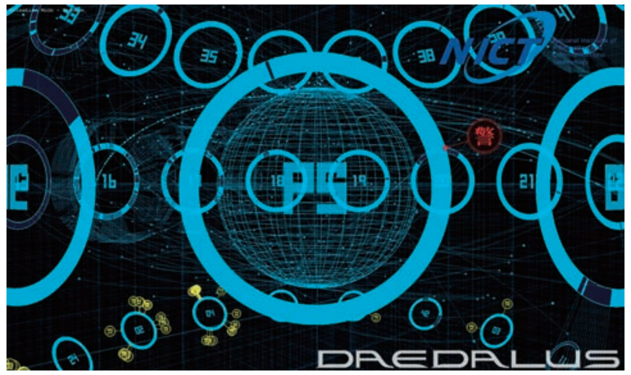
▲Real-time visualization of cyberattacks with NICTER

Emerging security technologies

We conduct research and development on security verification technology to address security issues and measures related to emerging technologies, such as Internet of Things (IoT) devices, 5G/Beyond 5G, and connected cars, in order to contribute to the security of new technologies that emerge in society. We also analyze human (user) behavior patterns, mental models, and decision-making processes, and are engaged in research and development on usable security to achieve high security without compromising usability.

Darknet-based real-time alert system "DAEDALUS"

Direct Alert Environment for Darknet And Livenet Unified Security



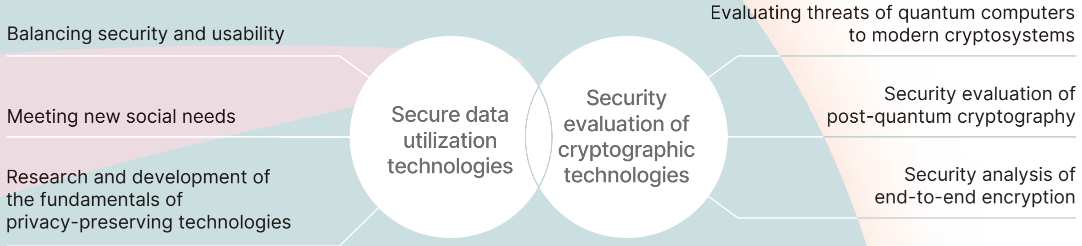
▲Visualization of DAEDALUS which issues alerts for malware-infected devices

Security Fundamentals Laboratory

OUTLINE

The Security Fundamentals Laboratory conducts research and development of cryptography, authentication, and privacy-preserving technologies.

We also evaluate the security of currently used cryptography as well as the security of emerging ones including post-quantum cryptography to promote proper implementation and standardization for secure information systems.



Secure data utilization technologies

- Balancing security and usability
- Meeting new social needs
- Research and development of the fundamentals of privacy-preserving technologies

Security evaluation of cryptographic technologies

- Evaluating threats of quantum computers to modern cryptosystems
- Security evaluation of post-quantum cryptography
- Security analysis of end-to-end encryption

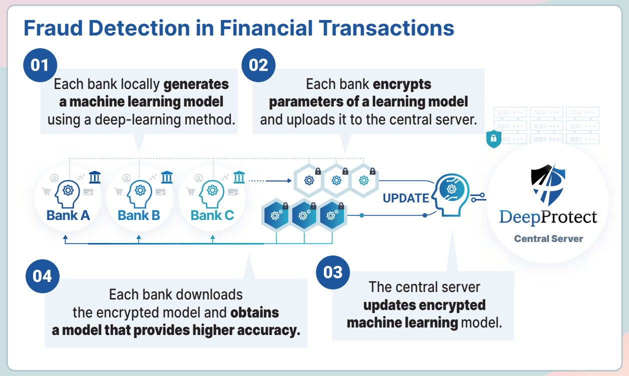
PROJECTS

Secure data utilization technologies

To ensure security and privacy at each stage of data provision, collection, storage, analysis, and deployment, we conduct research and development on access control technologies such as anonymous authentication and privacy-preserving data evaluation technologies such as secure computation.

By using these technologies, we aim to promote the utilization of data, including cross-organizational collaboration, and contribute to solving social issues such as providing secure telework.

Privacy-preserving federated learning system: DeepProtect



Fraud Detection in Financial Transactions

01 Each bank locally **generates a machine learning model** using a deep-learning method.

02 Each bank **encrypts parameters of a learning model** and uploads it to the central server.

03 The central server **updates encrypted machine learning model.**

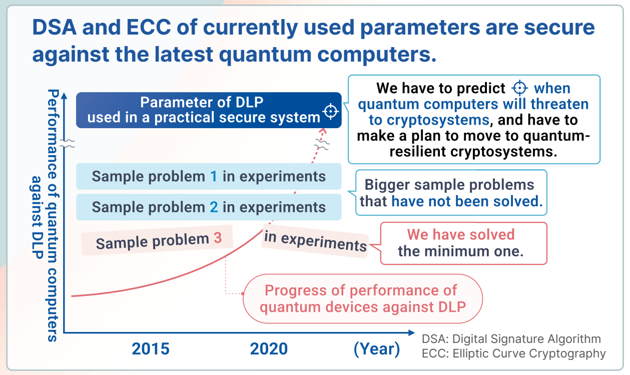
04 Each bank downloads the encrypted model and **obtains a model that provides higher accuracy.**

▲ DeepProtect enables data analysis shared by multiple organizations without disclosing sensitive data such as personal information.

Security evaluation of cryptographic technologies

To contribute to the appropriate implementation and secure use of various cryptographic techniques, our laboratory has conducted research and development of cryptographic infrastructure technology. In particular, we are engaged in the research and development of security evaluation of lattice-based cryptography and multivariable public key cryptography, which are expected to become the world standard post-quantum cryptography, as well as RSA cryptography and elliptic curve cryptography, which are currently widely used. Based on the results, we also conduct security evaluations of cryptographic technologies used in e-government systems and other applications.

Predict when quantum computers would break many of the currently-used public-key cryptosystems.



DSA and ECC of currently used parameters are secure against the latest quantum computers.

We have to predict ⌖ when quantum computers will threaten to cryptosystems, and have to make a plan to move to quantum-resilient cryptosystems.

DSA: Digital Signature Algorithm
ECC: Elliptic Curve Cryptography

▲ NICT has succeeded in the world's first experiment in solving a DLP using an actual quantum computer.

Cybersecurity Nexus

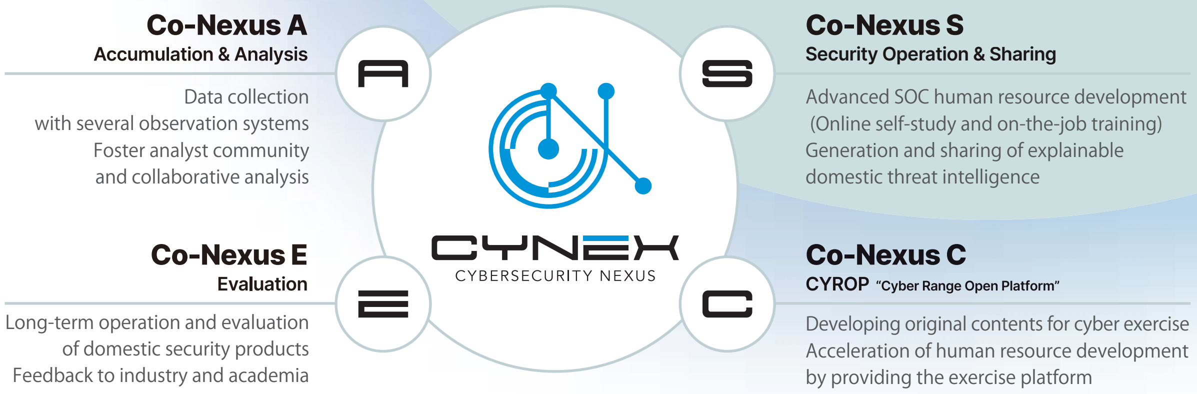
OUTLINE

CYNEX (Cybersecurity Nexus) has been newly organized to build an advanced infrastructure that will serve as a "nexus" for industry, academia, and government in Japan's cybersecurity field, utilizing the vast amount of data on cyberattacks, research and development achievements, and knowledge gained from developing cybersecurity workforce collected by NICT. CYNEX will collect, store, analyze, and provide cybersecurity information domestically and release a common platform for nurturing cybersecurity personnel throughout society, aiming to enhance Japan's cybersecurity response capabilities.

PROJECTS

CYNEX Structure: 4 Co-Nexus

CYNEX will promote four sub-projects, "Co-Nexuses," concurrently.



Co-Nexus A
Accumulation & Analysis

Data collection with several observation systems
Foster analyst community and collaborative analysis

Co-Nexus S
Security Operation & Sharing

Advanced SOC human resource development (Online self-study and on-the-job training)
Generation and sharing of explainable domestic threat intelligence

Co-Nexus E
Evaluation

Long-term operation and evaluation of domestic security products
Feedback to industry and academia

Co-Nexus C
CYROP "Cyber Range Open Platform"

Developing original contents for cyber exercise
Acceleration of human resource development by providing the exercise platform

WarpDrive

Web-based Attack Response with Practical and Deployable Research InitiatiVE

We are currently recruiting users to join the attack observation network.

Cyberattacks continue to become more diverse and sophisticated, and there is no end to the damage caused by web-based attacks that infect you with malware just by browsing a website. The WarpDrive Project, led by CYNEX Co-Nexus A, has developed the web-based attack countermeasure software "Tachikoma Security Agent," inspired by the character "Tachikoma" from the anime series "Ghost in the Shell: SAC_2045." By constructing the attack observation network with user participation, we aim to clarify the actual state of attacks and develop countermeasures against them.

National Cyber Training Center

OUTLINE

In order to protect the safety of society from increasingly diverse and malicious cyberattacks, it is necessary to accelerate the development of cybersecurity workforce who will take on this responsibility on a national level. Against this background, in response to the passage of the 2017 budget by the Ministry of Internal Affairs and Communications, the National Institute of Information and Communications Technology (NICT) established the National Cyber Training Center on April 1, 2017. The center aims to plan and promote practical cybersecurity training by maximizing the technical knowledge gained from years of research on cybersecurity.

PROJECTS

The National Cyber Training Center promotes the following three projects:

Cyber Defense Exercise with Recurrence

“CYDER”

CYDER allows practical defensive exercises in an environment that simulates an organization's network. By providing CYDER, we aim to train security operators in the thousands in national administrative agencies, local governments, critical infrastructure operators, etc.

Practical Cybersecurity Exercise Response Practice for Cyber Incidents

“RPCI”

RPCI is a highly practical incident-handling exercise utilizing NICT's large-scale exercise environment and the expertise in CYDER. This is the first specific course for Registered Information Security Specialist (RISS) offered by a public institution.

Development of young security innovators

“SecHack365”

SecHack365 is a program for ICT personnel under the age of 25, aimed at developing cybersecurity innovators who can tackle various security challenges with creative ideas. The program provides full-scale guidance over the course of one year by taking advantage of NICT's long-standing research and development expertise and the environment.

National Cyber Observation Center

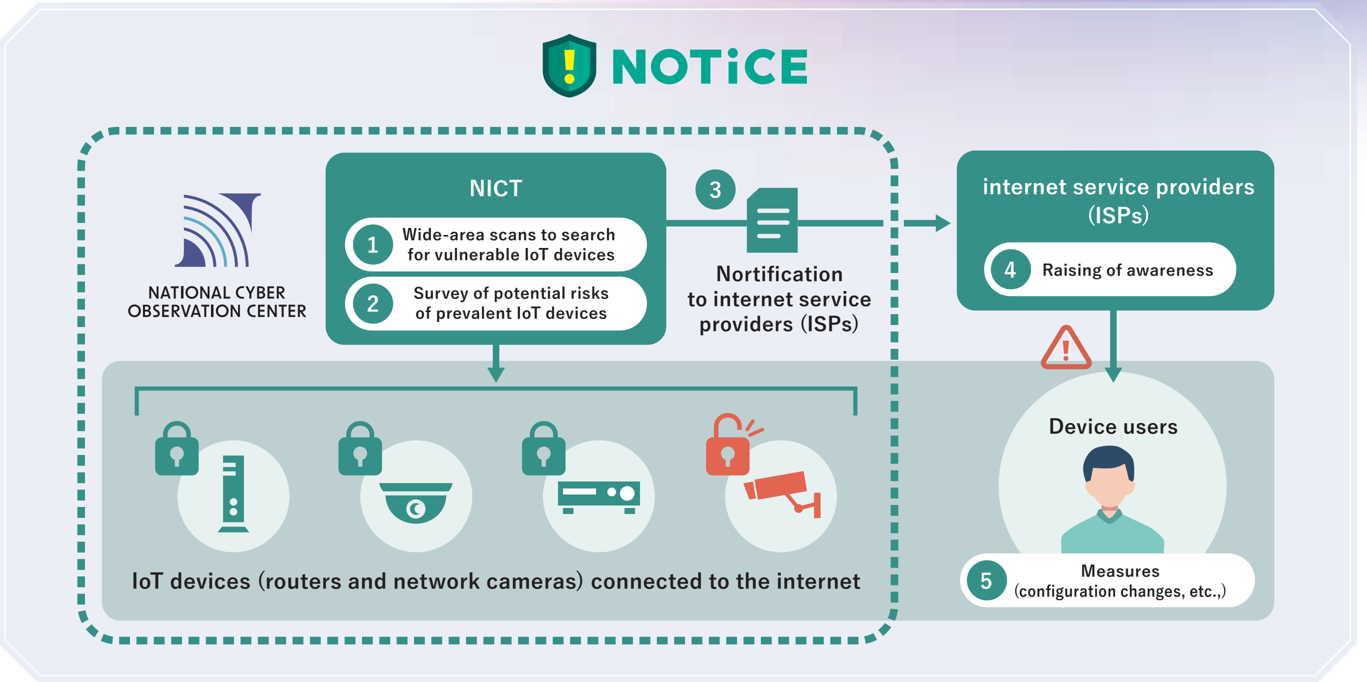
OUTLINE

The National Cyber Observation Center, as the organization responsible for investigations in the NOTICE project, conducts wide-area scans of the internet space within Japan to search for IoT devices that could potentially be exploited for cyber attacks. The information of discovered vulnerable IoT devices is provided to internet service providers and device manufacturers, and is used to promote safety and security on the internet through raising awareness and taking measures among device users.

PROJECTS

NOTICE

National Operation Towards IoT Clean Environment (NOTICE) is a project aimed at suppressing the hijacking of IoT devices and the activities of botnets by improving the security measures of IoT devices such as routers and network cameras that are connected to the internet. The Ministry of Internal Affairs and Communications (MIC), NICT, and Internet Service Providers (ISPs) are collaborating to promote the "observation of IoT devices that are being exploited for cyber attacks, or that have the potential to be" and the "security measures for IoT devices that have potential risks".


NOTiCE
NATIONAL CYBER OBSERVATION CENTER
NICT
1 Wide-area scans to search for vulnerable IoT devices
2 Survey of potential risks of prevalent IoT devices
3
Nortification to internet service providers (ISPs)
internet service providers (ISPs)
4 Raising of awareness
Device users
5 Measures (configuration changes, etc.,)
IoT devices (routers and network cameras) connected to the internet