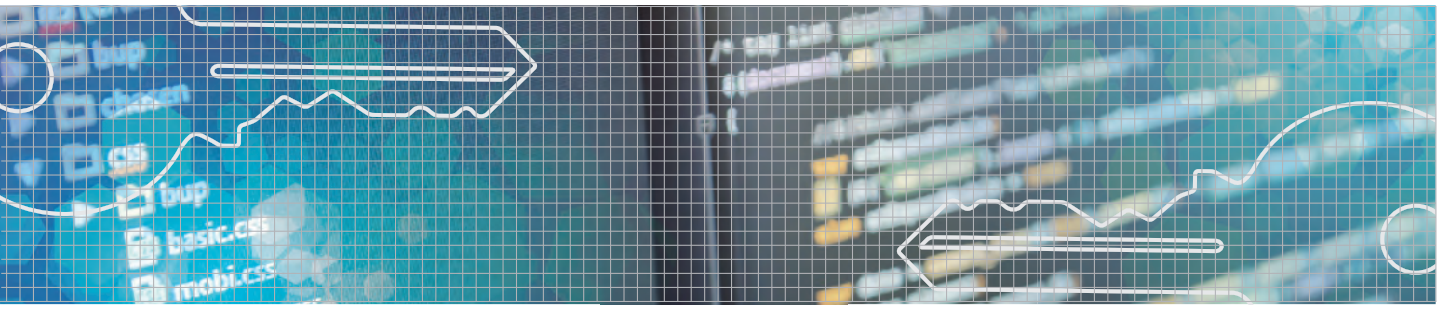
National Institute of Information and Communications Technology

Cybersecurity Research Institute



Cybersecurity Laboratory

Security Fundamentals Laboratory

Planning Office

Cybersecurity Research Institute

Message

In the Internet of Things (IoT) era, many objects, sensors and other devices in our surroundings will be connected to networks. This allows us to enjoy convenient and smart lives; however, security countermeasures for such devices are becoming a pressing issue behind the scenes. The scope that should be covered by cybersecurity is expanding daily, such as protection from information leakage and privacy violations in the case of utilizing the big data collected by such IoT devices. We conduct Research and Development (R&D) to deal with the latest pressing concerns and upcoming issues in our information society.

Advanced cybersecurity technologies

We conduct R&D on cyberattack monitoring, analysis supporting technologies for the increasingly sophisticated and evolved cyberattacks against the government and other important infrastructure. We also engage in research on collecting and analyzing huge amounts of data from these diversifying cyberattacks, and aim to utilize it in automatic cyberattack countermeasures. We also strive to achieve quick R&D outcome deployment through application and verification in NICT's own cyber incident response system to strengthen the technology.

Security testbed development and operations technology

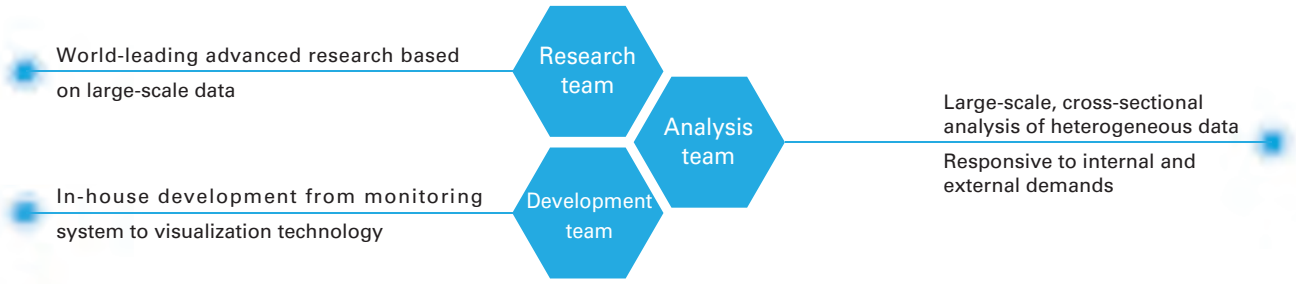
We oversee R&D on technologies for emulating cyberattacks in a safe environment, the construction of a security verification platform that is indispensable for verifying newly developed protection technologies and verifying cyberattack countermeasure technologies in an emulation environment.

Cryptographic technologies

We handle R&D on functional cryptographic technologies providing new functionality to meet the new social needs accompanying the IoT evolution, and security evaluation of cryptographic technologies contributing to the promotion and standardization of new cryptographic technologies, and to the construction of safe and secure ICT systems. We also engage in R&D on privacy enhancing technologies for the practical utilization of personal data and the promotion of technical support activities for appropriate privacy measures.

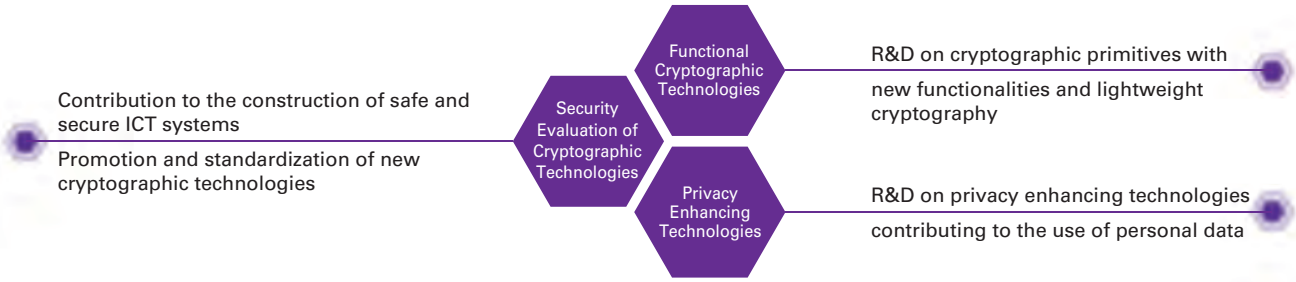
Organization of the Cybersecurity Research Institute, NICT

Cybersecurity Laboratory



1. R&D on collecting and analyzing data technology with the world's largest-scale cyberattack monitoring system, aiming to automate cyberattack countermeasures
2. R&D on security testbeds, including visualization technology, which is applicable to training for the human development of cybersecurity
3. R&D on large-scale and massive data analysis, storage and sharing technology through active, multimodal cyberattack monitoring against advanced persistent threats

Security Fundamentals Laboratory

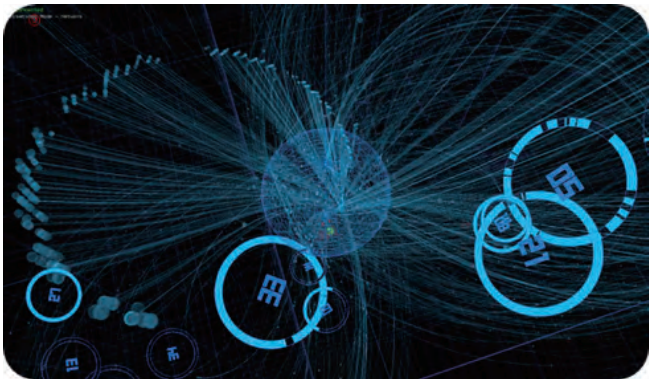


1. R&D on cryptographic primitives having new functionalities to circumvent issues due to the development of IoT
2. R&D on security evaluation of cryptographic technologies contributing to the promotion and standardization of new cryptographic technologies, and to the construction of safe and secure ICT systems
3. R&D on privacy enhancing technologies for the practical utilization of personal data

Cybersecurity Laboratory

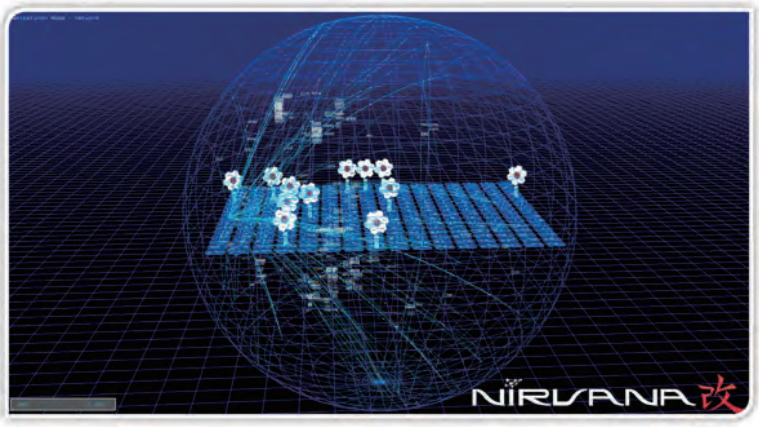
Overview

We work on R&D for cybersecurity techniques to cope with sophisticated cyberattacks and unknown and potential threats, such as ones for emerging IoT devices. We also work to automate countermeasures against cyberattacks by collecting, accumulating, and analyzing large amounts of information on diversified cyberattacks, including indiscriminate and targeted ones. Moreover, we verify the effectiveness of our research outcomes by applying them to our own cyberattack analysis, and then disseminate them to society.



Advanced cybersecurity technologies

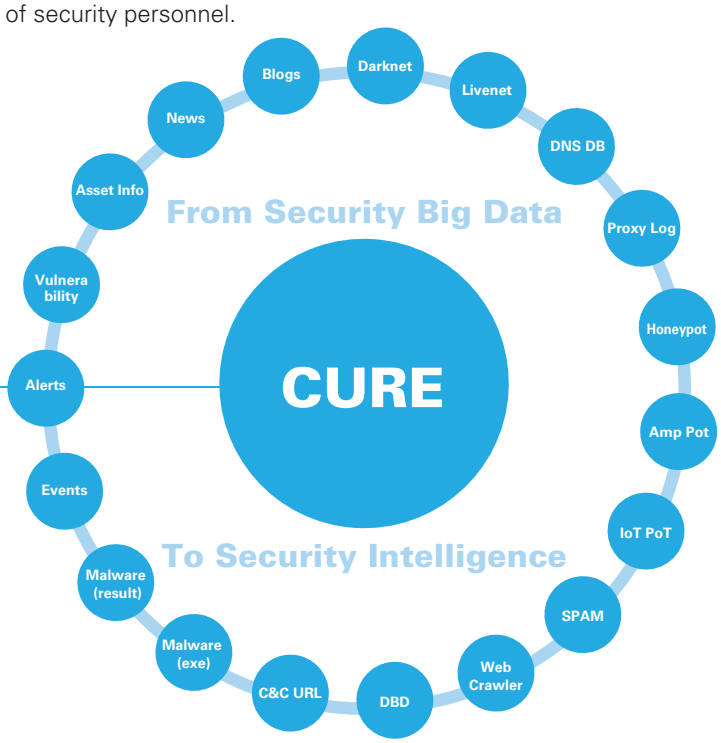
In order to reinforce the capabilities for responding to cyberattacks against governments or critical infrastructures, we work on R&D for visualization-driven security operation techniques, security techniques for IoT devices, etc. in addition to the active and exhaustive monitoring, machine-learning based analysis, and analysis across multiple information sources.



Cybersecurity Universal Repository

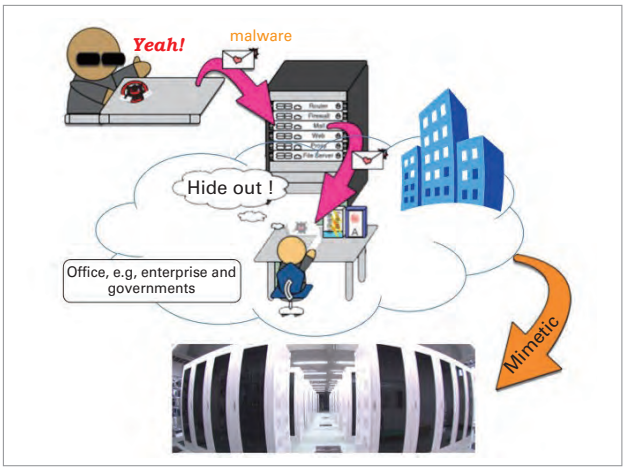
We are building a cybersecurity universal repository to accumulate a large amount of cybersecurity related information, which enables us to securely share the information in a convenient and usable manner. We also conduct R&D on automated countermeasure techniques using the repository. Moreover, we are building a semi-open research platform using technology to assist the development of security personnel.

C U R E : Cybersecurity Universal Repository



Techniques for the use of the Security Verification Platform

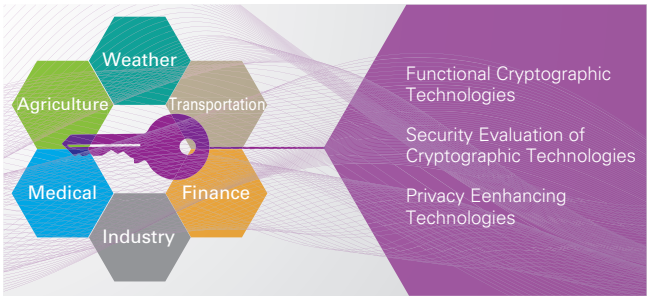
In order to facilitate R&D on cybersecurity technologies, we are building a verification platform that reproduces cyberattacks within a secure environment and that verifies secure protection techniques. We also work on techniques for using mock environments and information as well as security testbed techniques.



Security Fundamentals Laboratory

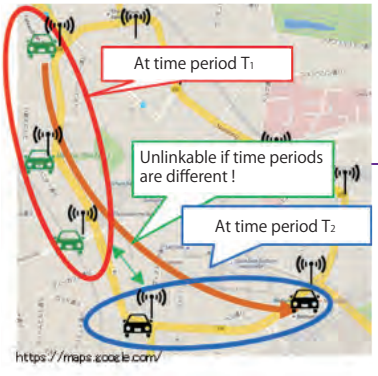
Overview

The Security Fundamentals Laboratory conducts R&D on cryptographic primitives with new functionalities and lightweight cryptography to circumvent issues due to the development of IoT. We also evaluate the security of currently used cryptographic techniques to contribute to securing ICT systems, and the security of emerging cryptographic techniques to promote market deployment and standardization. Furthermore, we promote research on privacy enhancing technologies for personal data use and support technical countermeasures to privacy threats.



Functional Cryptographic Technologies

We propose cryptographic primitives with new functionalities that meet social demands that arise from emerging technologies. The target technologies include searchable encryption, anonymous authentication, secure key revocation and updates, and lightweight cryptography tailored for implementation in constrained IoT devices, etc.



Example of functional cryptographic technologies
A lightweight group signature scheme with time-dependent linking for collecting linkable information

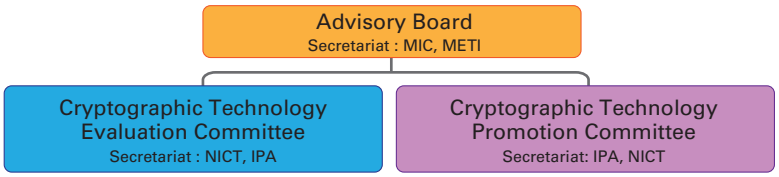
Security Evaluation of Cryptographic Technologies

We evaluate security of cryptographic technologies currently used for e-government and in ordinary society to keep them secure. We also research the security of new cryptographic technologies such as pairing-based cryptography, lattice-based cryptography, and so on.

Security evaluation of lattice-based cryptography
TU Darmstadt Lattice Challenge
https://www.latticechallenge.org/

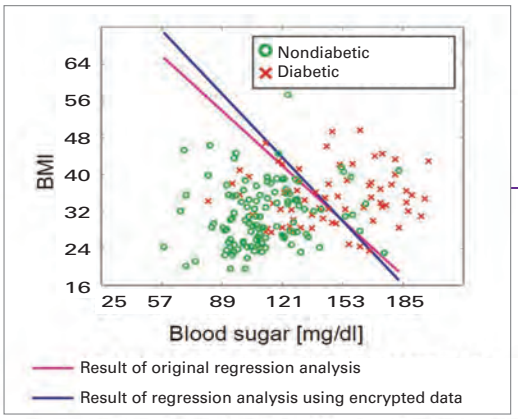
CRYPTREC

Since 2000, we have organized CRYPTREC (CRYPTography Research and Evaluation Committees) to monitor and evaluate the security of e-government recommended ciphers and investigate and examine the appropriate implementation and operation of these cryptographic techniques.
URL : http://cryptrec.go.jp/english/index.html

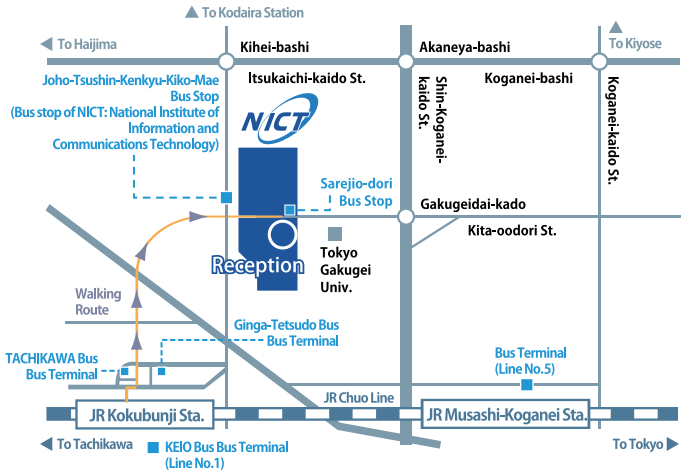


Privacy Enhancing Technologies

We propose technologies for personal data utilization without infringing on privacy. Our proposals include privacy preserving cryptographic technologies based on lattice theory. We also evaluate the privacy-risk of widely known technologies.



Privacy preserving data analysis
Clustering encrypted big data by logistic regression



National Institute of
Information and Communications Technology

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

Cybersecurity Research Institute
Tel: +81-42-327-5807
E-mail:cyber-info@ml.nict.go.jp
URL:http://www.nict.go.jp/csri/

For inquiries about NICT, please contact Public Relations Department.
Tel : +81-42-327-5392 Fax : +81-42-327-7587
E-mail:publicity@nict.go.jp

Feb. 2017