Reinforce Information Security

Relevant GRI Standards: 102-12/103-2/203-2

Policies and Concepts

With the progressing digitalization of society and the economy and changes in international circumstances, security threats are becoming more serious and sophisticated, particularly cyber-attacks. Within this environment, the NTT Group has a responsibility to protect ICT service infrastructure and customers' basic rights, freedoms, and information assets, as well as to provide a sound foundation for the growth of the digital economy.

When formulating our medium-term management strategies in 2018, we made it our mission in terms of security to contribute to the building and development of a free, open, and safe ICT platform for supporting the infrastructure of the digital economy. We also made it our vision to realize the digital transformation of both customers and NTT itself, and for that reason, we will be chosen by customers.

In order to realize these, we will strive to engage in research and development that leverages the scale of the Group, realize superior abilities for early detection and rapid response, cultivate human resources who share the values of sincerity and advanced skill, and transcend profit-focused principles to transmit pioneering knowledge to society.

The appropriate handling of personal information is a focus of growing interest worldwide and it is also important to have countermeasures to large-scale, sophisticated cyber-attacks targeting things like international events. As a member of the global community building the digital society, the NTT Group will contribute to solving social issues through our security business.

NTT Group Information Security Policy

NTT Group will continue to provide safe and secure services and to be a trusted company, as a responsible carrier in the information and telecommunication industry. NTT Group will strive to ensure information security and contribute to the sound development of society in accordance with the following policies.

1. NTT Group will (a) be fully aware of the importance of information security in society, (b) strive to establish a safe, secure and convenient communication network environment and (c) strive to ensure information security.

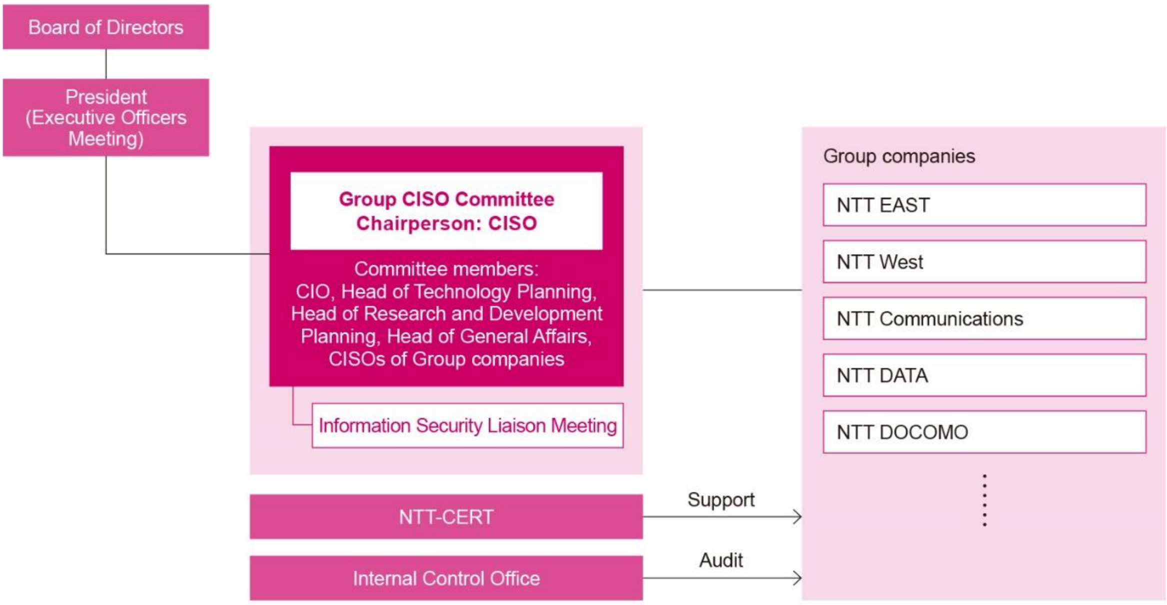
2. All NTT Group employees, executives will (a) be fully aware that the protection of information is the basis of NTT Group's business activities and corporate social responsibility, (b) protect the secrecy of telecommunications and comply with relevant laws and regulations, including “the Act on the Protection of Personal Information”.

3. NTT Group will continuously take necessary information security measures such as (a) establishing the information security management system, (b) taking strict security measures, both on the physical and technological aspects, in order to prevent unauthorized access and information loss, falsification, and leaks, (c) ensuring employee education, (d) providing appropriate supervision of outsourcing contractors.

💻 **NTT Group's Information Security Policy** https://www.ntt.co.jp/g-policy/e/index.html

Organization for Implementation

The NTT Group enforces information security management under the charge of the Chief Information Security Officer (CISO), and is thorough in its information security management. We have also established a Group CISO Committee, and formulate Group information security management strategies, plan and implement related measures, undertake human resources training, and otherwise engage in activities in collaboration with companies across the Group.


Board of Directors
President (Executive Officers Meeting)
Group CISO Committee Chairperson: CISO
Committee members: CIO, Head of Technology Planning, Head of Research and Development Planning, Head of General Affairs, CISOs of Group companies
Information Security Liaison Meeting
NTT-CERT
Internal Control Office
Support
Audit
Group companies
NTT EAST
NTT West
NTT Communications
NTT DATA
NTT DOCOMO

Main Initiatives

Strengthen Service Security

Information communication services are an important social infrastructure and a foundation for the digitalization of society and the economy, so to provide these services in a safe and secure manner, we are working to strengthen the security of telecommunications equipment, IT service environments, and all services provided by smart cities, smart buildings, and the like.

Global Cooperation within the NTT Group

With the integration of our global businesses, we are advancing global partnerships in the security field. This NTT Group cooperation includes many businesses and regions and incorporates an approach to risk-based management, the introduction of a framework that acts as a shared language, and the setting of standards that should be met by all Group members in regard to identification, defenses, detection, response, and recovery.

Engaging with and Contributing to the Global Community

We are engaging with the cybersecurity initiatives of governments and industries around the world, particularly in North America and Europe, by sharing information and best practices in regard to security threats and building a community of companies and organizations based on mutual trust.

Training Security Experts in the NTT Group

As a measure to enhance security personnel development with the aim of improving in terms of both quantity and quality, NTT Group companies are implementing human resource development measures based on the types and levels of security personnel.

NTT Group's Security Personnel Hierarchy

		Title	Job classification		
			Security management consulting	Security operation	Security development
Level	Advanced	Security master	Produce first-rate experts with best performance in the industry		
		Security principal			
	Intermediate	Security professional	Reinforce the pool of specialists with deep experience and judgment		
	Beginner	Security expert	Raise the level of workers who can do their work with the required knowledge		

Information Security Training

Each Group company seeks to raise information security literacy by organizing training for all employees as well as the employees of partner companies. Training is offered through e-learning, and all employees are obliged to participate in the course once a year. Looking ahead, we are considering unifying training content throughout the Group to provide employees with a standard level of knowledge on information security required in their business operations. By doing so, we will seek to enhance the security capabilities of the NTT Group and reinforce its human resources to deliver safe, secure services for our customers and society at large.

Research and Development Initiatives

In addition to advancing the technological development of service security, we are focusing on developing elemental security technologies. In 2019, we established a global research center for research into cybersecurity and encryption technology centered around some of the world's leading researchers.

Management of CSIRT

The NTT Group established NTT-CERT in 2004 to function as a computer security incident response team (CSIRT). This team collects information regarding security incidents associated with the Group. It then offers support for addressing these incidents, formulates measures to prevent recurrence, develops training programs, and provides security-related information. As a central element of the NTT Group's security initiatives, NTT-CERT provides a reliable venue for consultations regarding information security. The team also collaborates with organizations and specialists inside and outside the NTT Group to offer support for detecting and resolving security incidents, minimizing damages, and preventing occurrence. NTT-CERT is thereby contributing to better security for both the NTT Group and societies that are permeated by information networks.

Moreover, NTT-CERT coordinates with the United States Computer Emergency Readiness Team (US-CERT*[1]) and the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC*[2]) and is also a member of the Forum of Incident Response and Security Teams (FIRST) and the Nippon CSIRT Association,*[3] which enables it to coordinate with domestic and overseas CSIRT organizations. This coordination makes it possible for NTT-CERT to share information on relevant trends and response measures. In addition, NTT-CERT participates in the cross-industry drills held by the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) to share expertise and gather information. NTT-CERT also plays a role in promoting the establishment of CSIRTs at Group companies and helping improve their response capabilities.

NTT-CERT will expand its collection of information on vulnerabilities and attacks to cover areas including the dark web and will strengthen its information analysis platform and further automate and enhance its response to cyber threats in order to continually respond to threats as they change.

*1 US-CERT: An information security preparedness organization under the Department of Homeland Security (DHS)

*2 JPCERT Coordination Center: An organization that collects reports inside Japan, supports responses, monitors situations, analyzes entry points, and reviews and provides advice on measures for preventing reoccurrences from a technical standpoint with regard to computer security incidents such as intrusions through the Internet or service interruptions

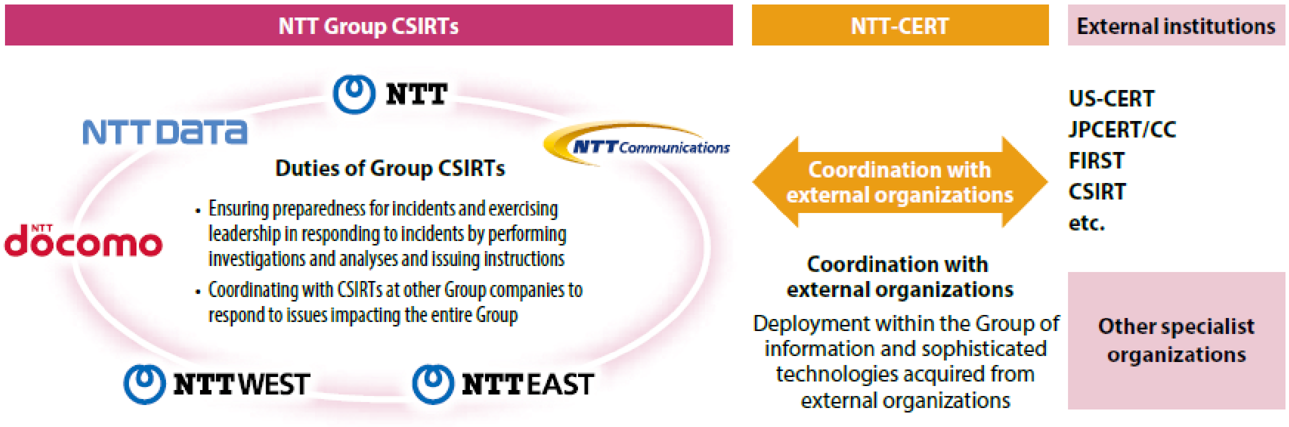
*3 NTT-CERT founded the Nippon CSIRT Association

NTT-CERT https://www.ntt-cert.org/index-en.html

Nippon CSIRT Association https://www.nca.gr.jp/en/

FIRST Forum of Incident Response and Security Teams https://www.first.org/

NTT Group CSIRT Activities



NTT Group CSIRTs

NTT-CERT

External institutions

NTT

NTT DATA

NTT Communications

docomo

NTT WEST

NTT EAST

Duties of Group CSIRTs

- Ensuring preparedness for incidents and exercising leadership in responding to incidents by performing investigations and analyses and issuing instructions
- Coordinating with CSIRTs at other Group companies to respond to issues impacting the entire Group

Coordination with external organizations

Coordination with external organizations

Deployment within the Group of information and sophisticated technologies acquired from external organizations

US-CERT
JPCERT/CC
FIRST
CSIRT
etc.

Other specialist organizations