Information Security

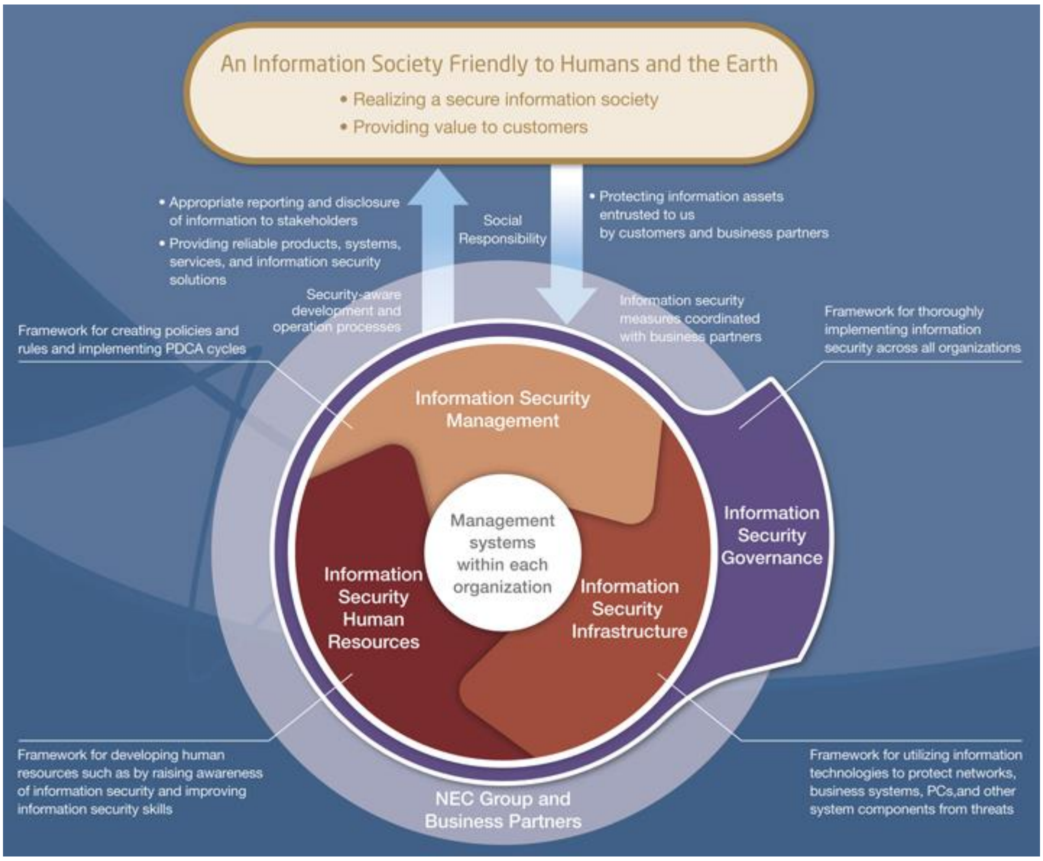
The NEC Group positions information security as an important management activity and pursues its activities so that everybody can use information and communications technologies with a sense of security, leading to the creation of a prosperous society.

Policy

NEC recognizes that it is our duty to protect the information assets entrusted to us by our customers and business partners as well as our own information assets in order to provide better products and services and contribute to the development of society. Accordingly, we have codified this commitment in the NEC Information Security Statement.

Moreover, the NEC Group has established an information security promotion framework to fulfill our responsibilities to society as a trusted company. This framework enables us to realize a secure information society and provide value to our customers by protecting the information assets entrusted to us by our customers and business partners; by providing reliable products, systems, and services; and by properly reporting and disclosing information to our stakeholders.

To protect information assets, we combine the following four elements (information security management, information security platform, information security human resources, and information security governance) to comprehensively maintain and enhance information security on multiple levels.


An Information Society Friendly to Humans and the Earth
• Realizing a secure information society
• Providing value to customers
• Appropriate reporting and disclosure of information to stakeholders
• Providing reliable products, systems, services, and information security solutions
Social Responsibility
• Protecting information assets entrusted to us by customers and business partners
Security-aware development and operation processes
Information security measures coordinated with business partners
Framework for creating policies and rules and implementing PDCA cycles
Framework for thoroughly implementing information security across all organizations
Information Security Management
Management systems within each organization
Information Security Human Resources
Information Security Infrastructure
Information Security Governance
Framework for developing human resources such as by raising awareness of information security and improving information security skills
Framework for utilizing information technologies to protect networks, business systems, PCs,and other system components from threats
NEC Group and Business Partners

Information Security Promotion Framework

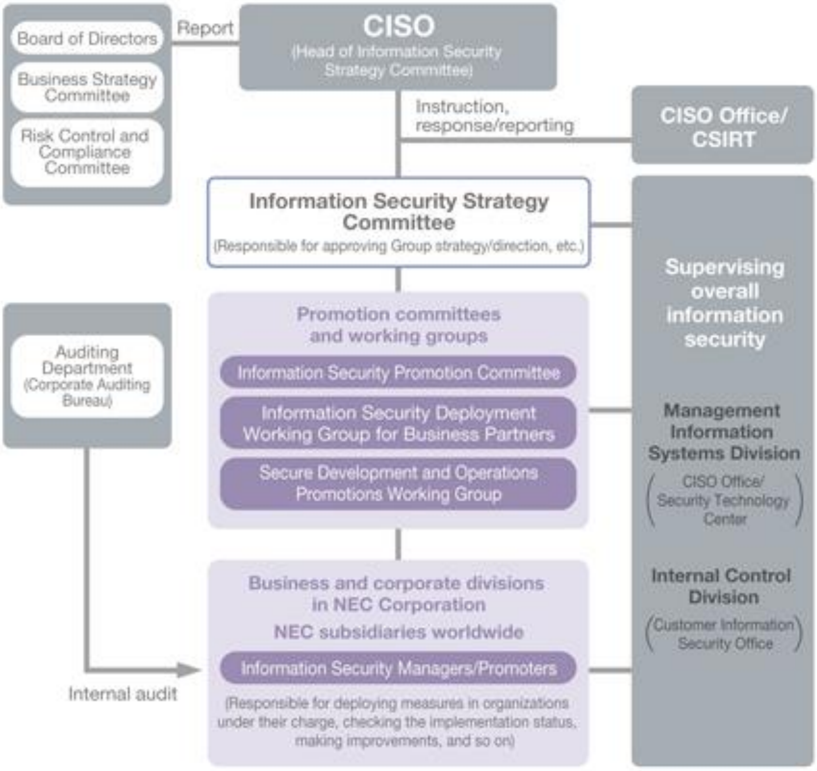
- NEC Information Security Statement
- Information Security Report

Promotion Framework

The information security promotion organizational structure of the NEC Group consists of the Information Security Strategy Committee and its subordinate organs as well as the information security managers and promoters at each organization. The Information Security Strategy Committee, headed by the Chief Information Security Officer (CISO) 1) evaluates and discusses how to improve information security measures, 2) discusses the causes of major incidents and the direction of recurrence prevention measures, and 3) discusses how to apply the results to NEC's information security business to address information security risks, including risks related cyber security. The CISO also heads the CISO office, whose job is to receive direct instructions from the CISO and promote cyber security measures, and the Cyber Security Incident Response Team (CSIRT), whose job is to monitor for cyber attacks and when an attack is detected, immediately analyze it, identify the cause of the incident and implement measures to bring the situation to normal. Under the Information Security Strategy Committee, three subordinate organs (a sub-committee and two working groups) discuss and coordinate security plans and implementation measures, enforce instructions to achieve them, and manage the progress for group companies worldwide, for business partners, and for driving the Secure Development and Operations initiative, respectively.

The information security manager in each organization has primary responsibility for information security management including the group companies under their supervision.

They continuously enforce information security rules within their organizations, introduce and deploy measures to assess the implementation status, and implement further improvement measures to maintain and enhance information security.


Board of Directors
Business Strategy Committee
Risk Control and Compliance Committee
Report
CISO
(Head of Information Security Strategy Committee)
Instruction, response/reporting
CISO Office/ CSIRT
Information Security Strategy Committee
(Responsible for approving Group strategy/direction, etc.)
Promotion committees and working groups
Information Security Promotion Committee
Information Security Deployment Working Group for Business Partners
Secure Development and Operations Promotions Working Group
Auditing Department (Corporate Auditing Bureau)
Business and corporate divisions in NEC Corporation
NEC subsidiaries worldwide
Information Security Managers/Promoters
(Responsible for deploying measures in organizations under their charge, checking the implementation status, making improvements, and so on)
Internal audit
Supervising overall information security
Management Information Systems Division
(CISO Office/ Security Technology Center)
Internal Control Division
(Customer Information Security Office)

Information Security Promotion Structure

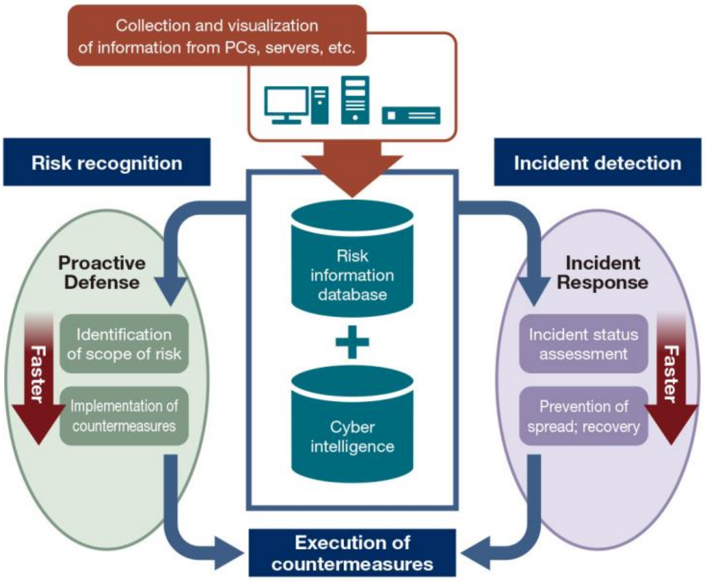
Main Activities and Results for Fiscal 2017

Strengthening Measures against Cyber Attacks

Cyber attacks that occur in daily business operations include targeted attacks against specific companies or organizations, ransomware (a kind of malware that encrypts files and then demands a ransom in exchange for decryption), indiscriminate email attacks (attacks aimed at unspecified, large numbers of people) and are becoming more and more advanced and sophisticated. As a means to counter these attacks, we began the deployment of the Global Cyber Attack Protection System (GCAPS*1) within NEC and all its subsidiaries in Japan, in order to fix vulnerabilities of PCs and servers promptly and to respond to incidents efficiently.

GCAPS reinforces security of PCs and servers from the two standpoints: “Proactive Defense” performed on the basis of risk recognition, and “Incident Response” when an incident is detected. From fiscal 2018 onwards, we will gradually introduce GCAPS also to overseas subsidiaries.

[*1] GCAPS: Global Cyber Attack Protection System. Sold under the Solution name: NEC Cyber Security Platform（NCSP）


Collection and visualization of information from PCs, servers, etc.
Risk recognition
Incident detection
Proactive Defense
Identification of scope of risk
Implementation of countermeasures
Faster
Risk information database
+
Cyber intelligence
Incident Response
Incident status assessment
Prevention of spread; recovery
Faster
Execution of countermeasures

Concept of GCAPS

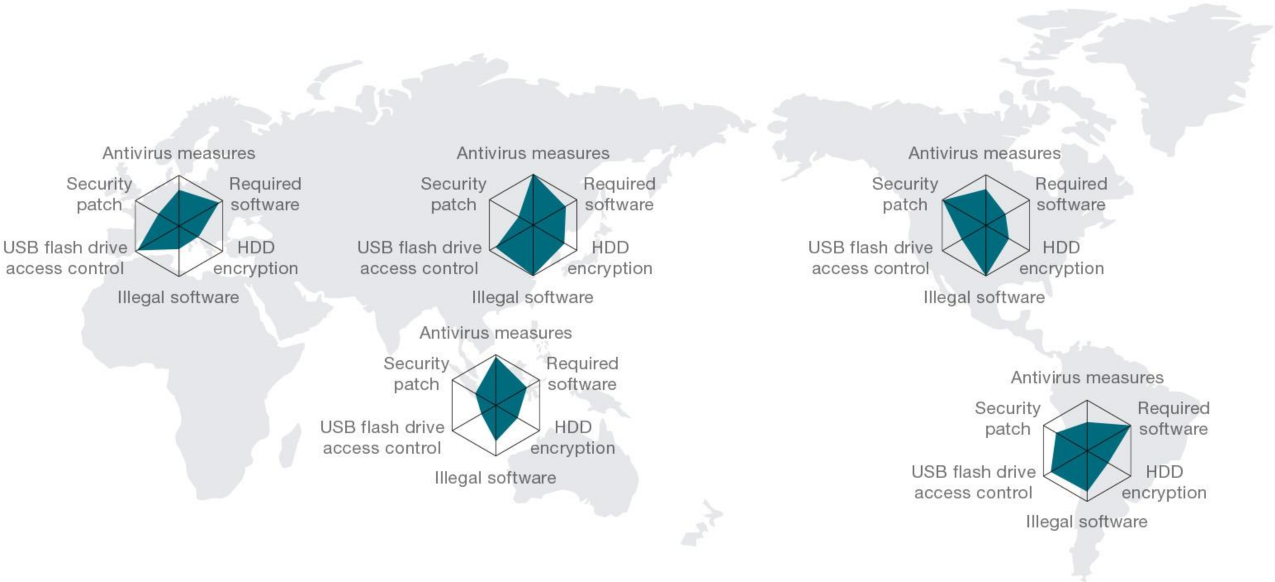
Also, as part of global deployment initiatives, we deployed measures against cyber attacks (detection of unknown attacks, integrated log analysis and intensified monitoring, CSIRT establishment) in the APAC region. We will continue to expand the coverage area for deployment in fiscal 2018.

Further, we conducted targeted attack drills to sharpen employees’ awareness against suspicious emails and “Integrated Cyber Attack Drills” that enable people of each relevant organization including CSIRT to experience incident response and collaboration among divisions, as well as top management to experience press releases that will be required in case NEC becomes the victim of a cyber attack. We also conducted the “NEC Security Skill Challenge,” an internal security contest CTF (Capture the Flag) aimed at improving technical skills of CSIRT personnel and expanding the breadth of our security human resources.

Strengthening Global Security Infrastructures

NEC has completed the deployment of the integrated management platform that enables the visualization*2 of the status of information security measures for PCs (e.g. installation of security patches, malware countermeasures, and PC encryption) at overseas subsidiaries. In regard to the introduction of file encryption tools for PCs, we began deploying InfoCage FileShell, which had already been implemented in Japanese group companies, in overseas subsidiaries in the second half of fiscal 2017. From fiscal 2018 onwards, we will accelerate its implementation and eventually make it a mandate.

[*2] "Visualization" in this context refers to a system for quantitatively confirming the implementation status of information security measures in overseas subsidiaries. The system, for example, shows the security patch installation status and implementation rates for PC encryption measures. This enables Management Information Systems Division of NEC and regional administration companies as well as Information Security Managers of local group companies to confirm the implementation status of security measures and take concrete actions to further improve the information security within the NEC Group.

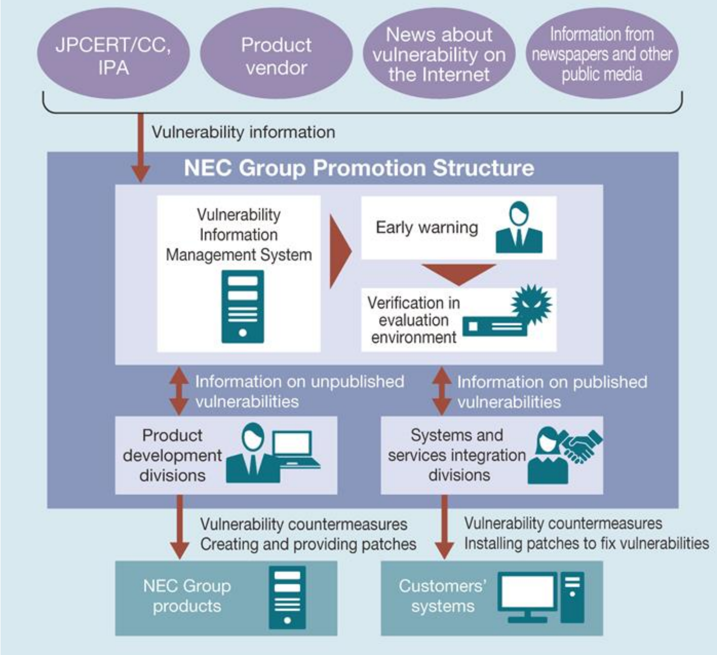


Visualization example: Overview of information security implementation by region
(The graph above shows only sample data and does not indicate any actual information.)

Promoting and Enforcing Secure Development and Operations

Aiming to reduce the burden of our system developers and operators, the NEC Group provides an internal service for evaluating how a patch aimed to fix a vulnerability behaves as well as its impact on customers' systems. Using the service at each business project ensures the implementation of measures for fixing vulnerabilities in customers' systems. Further, the implementation of anti-vulnerability measures is required by the quality protection rules of the NEC Group, which ensures that the service is used properly. Moreover, the implementation status is managed on an individual project basis, and if measures are not implemented, a warning is issued, thereby ensuring systematic and thorough vulnerability handling.

We also developed security implementation guidelines based on the Cybersecurity Management Guidelines formulated in 2015 by the Ministry of Economy, Trade and Industry (METI) and the Information-Technology Promotion Agency, Japan (IPA). These guidelines, along with other offerings, support our business project members in proposing a system with more value to their customers, contributing to the growth of our business. To provide our customers with more valuable proposals, in particular, we undertake security-related risk assessments on customers' systems to promptly make system risks visible and mitigate them to the extent possible conducting risk assessment aimed at "visualizing" security risks in customers' systems early on and minimizing those risks as much as possible. In response to the increasing risks of attacks on IoT devices and control systems in recent years, we performs risk assessments not only for ICT systems but also for IoT devices and control systems, so that we can propose security measures that will assure our customers' business continuity.


JPCERT/CC, IPA
Product vendor
News about vulnerability on the Internet
Information from newspapers and other public media
Vulnerability information
NEC Group Promotion Structure
Vulnerability Information Management System
Early warning
Verification in evaluation environment
Information on unpublished vulnerabilities
Information on published vulnerabilities
Product development divisions
Systems and services integration divisions
Vulnerability countermeasures Creating and providing patches
Vulnerability countermeasures Installing patches to fix vulnerabilities
NEC Group products
Customers' systems

Vulnerability Response Promotion Structure

Monitoring and Improvement

Information Security Assessment Activities

The NEC Group continuously conducts information security assessments to check the implementation status of information security measures and to create and execute improvement plans.

In fiscal 2017, information security assessments were carried out at NEC and 60 subsidiaries in Japan. Assessments were conducted both by general employees as well as by managers of specific security measures to confirm the status of measure implementation based on their respective roles (personal assessment). We were able to improve effectiveness by accurately assessing the actual on-site security situation. Personal assessments were also conducted at 34 overseas subsidiaries, which enabled a detailed grasp of their security measures, and further raised awareness and recognition among them.

These ongoing activities ensure that information security measures for NEC and its subsidiaries in Japan are continually being implemented and improved. There remains, however, room for improvement for some of these measures, and we issued reminders for their thorough implementation to NEC and its subsidiaries in Japan. On the other hand, for overseas subsidiaries, since the level of implementation has not reached that of the Japanese group companies, the overseas subsidiaries were given instructions to implement measures based on the results of assessments, and the status of their implementation was regularly followed up.

Assessment of Business Partners

On the basis of the "Information Security Standards for NEC Group Business Partners", the "Basic Rules for Customer-Related Work for Business Partners," and other related guidelines, we conducted assessments and evaluations of the implementation status of information security measures in business partners (through on-site assessment and Web-based self-assessment by business partners themselves). We provided business partners with feedback on evaluation results, and thoroughly implemented improvements.

In fiscal 2017, Web-based self-assessment was carried out in approximately 1,450 companies and on-site assessment in approximately 50 companies.

These ongoing activities ensure that information security measures for business partners are continually being implemented and improved. There remains, however, measures that have relatively low implementation rates compared to other measures, and we requested concerned business partners to conduct thorough implementation of such measures.

Assessment of Security Measures for Products, Systems, and Services Provided to Customers

By promoting the use of a system that visualizes the progress of security measures for customer projects within the NEC Group, we were able to identify projects for which measures for secure development, operation, and maintenance were inadequate, and continued to make the necessary improvements.

Objectives and Achievements

Objectives for the Medium Term (From fiscal 2017 to fiscal 2019)

As a global company that provides ICT essential to social infrastructures, NEC will contribute to society by protecting information assets entrusted to it by customers and business partners and its own information assets, as well as by providing even more secure, reliable, and trusted products, services, and solutions. Also, NEC will accelerate the creation of mechanisms for defense against cyber attacks, which are foreseen to continually become more sophisticated and advanced, as well as the global deployment of programs to train information security personnel.

Fiscal 2017 Objectives, Achievements and Progress, and Degree of Completion

Objective	Achievements and Progress	Degree of completion
1. Strengthening measures against cyber attacks (Japan, overseas) ・Deploy GCAPS within Japan and expand global deployment of cyber attack countermeasures, in order to strengthen measures against increasingly sophisticated and advanced cyber attacks.	・We began the introduction of GCAPS at NEC and subsidiaries in Japan. ・We implemented cyber-attack countermeasures (detection of unknown attacks, integrated log analysis and monitoring, and CSIRT establishment) in the APAC region.	Mostly achieved
2. Establishing global security infrastructures ・Increase the level of information security at overseas subsidiaries to the level in Japan.	・We began deploying InfoCage FileShell as our standard PC file encryption tool in overseas subsidiaries in the second half of this fiscal year. ・We completed the preparations for introducing GCAPS to overseas subsidiaries.	Mostly achieved
3. Promoting and enforcing Secure Development and Operations ・Implement the mechanisms for efficiently providing customers with secure products, systems, and services in our business projects, educate leaders to drive Secure Development and Operations initiatives in their project for further business growth.	・We incorporated the implementation of vulnerability countermeasures into the quality protection rules of the NEC Group, which ensures that our vulnerability information management system is used properly in all of our business projects. ・We deployed documents based on the Cybersecurity Management Guidelines to support our business project members in proposing a system with more value to their customers. In particular, to promptly make system risks visible and mitigate them to the extent possible, we undertake security-related risk assessments on customers’ systems including IoT devices and control systems using a list of security threats and countermeasures, and started the development and operations based on that list.	Mostly achieved

FY2018 Objectives

1. Strengthening measures against cyber attacks (Japan, overseas)	・Operate GCAPS in NEC and subsidiaries in Japan and deploy it in overseas subsidiaries. Further, expand the deployment scope of cyber-attack countermeasures (detection of unknown attacks, integrated log management and intensified monitoring, CSIRT establishment) in overseas subsidiaries.
2. Establishing global security infrastructures	・Increase the level of information security (both in terms of employees’ awareness and IT frameworks) at overseas subsidiaries to the level in Japan.
3. Promoting and enforcing Secure Development and Operations	・Continue to provide our customers with safe and secure products, systems, and services efficiently and contribute to business growth by improving guides and manuals, reinforcing IT systems, and supporting Secure Development and Operations in our business projects.