Information Security and Cyber Security

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. Based on this concept, NEC has placed “security to maximize ICT possibilities” as one of its “materiality,” the priority management theme from an ESG perspective, and has established an “Information Security Statement,” under which it promotes efforts to ensure both information and cyber security.

Based on the “Information Security Promotion Framework” (figure at right), NEC is striving to realize a secure information society and provide value to its customers.

To protect information assets, NEC is implementing cyber attack measures, providing secure products, systems and services, and promoting information security in collaboration with business partners. At the same time, we have positioned information security management, information security infrastructure, and information security personnel as the three pillars of the information security governance framework within the NEC Group, thereby maintaining and improving our comprehensive and multi-layered information security.

- NEC Information Security Statement
- Information Security Report
- Priority Management Themes from an ESG Perspective - Materiality

Information Security Promotion Framework

Activity Objectives, Achievements and Progress

Objectives for the Mid-term (from fiscal 2019 to 2021)

As a global company that provides ICT essential to social infrastructures, NEC will contribute to society by protecting information assets entrusted to us by customers and business partners and its own information assets, as well as further enhance security in the entire supply chain. NEC is also realizing a secure information society and providing value to customers by implementing secure development and operation and providing safe, secure and reliable products, systems and services. 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.

Objectives, Achievements and Progress, and Degree of Completion

(Degree of completion: ◎Achieved, ○Mostly Achieved, △Some Progress, ×No Progress)
In fiscal 2019, NEC will engage in the activities below to achieve the objectives of “minimize the effects of serious security incidents” and “promote our own information security practices as a reference that can be used for our customers” which are set as objectives of “materiality.”

Objectives for the Mid-term	FY2018 Objectives	FY2018 Achievements and Progress	Degree of Completion	FY2019 Objectives
1. Strengthen measures against cyber attacks (Japan, overseas)	• Operate GCAPS[*1] in NEC Corporation and its Group companies in Japan and deploy it in overseas Group companies. Further, expand the deployment scope of cyber-attack countermeasures such as detection of unknown attacks, integrated log management and intensified monitoring, CSIRT[*2] establishment, in overseas Group companies.	• Deployed GCAPS in NEC Corporation and its Group companies in Japan (about 180,000 units). • Expanded the deployment of detection of unknown attacks and integrated log management at overseas Group companies.	◎	• Deploy GCAPS overseas. • Enhance the global CSIRT system. • Enhance the use of threat intelligence. • Enhance deployment of EDR (Endpoint Detection and Response) products. • Validate the effect of advanced measures so that the cyber security measures can be used as a frame of reference by customers.
2. Establish global security infrastructures	• Increase the level of information security, both in terms of employees’ awareness and IT frameworks, at overseas Group companies to the level in Japan.	• Implemented information security education, including latest topics for all employees, and raised their information security awareness. • Conducted Network Security Audit/Security Inspection and confirmed information security status at overseas Group companies.	◎	• This objective is removed from activities that should be a focus in FY2019 and later, but NEC will continue to work on achieving this goal.

Objectives for the Mid-term	FY2018 Objectives	FY2018 Achievements and Progress	Degree of Completion	FY2019 Objectives
3. Strengthen the improvement of secure products, systems and services	• Contribute to business expansion by improving guidelines, enhancing the IT system, and continuously providing safe and secure products, systems and services by supporting secure development and operations in business projects on the front line.	• Newly created and improved security measure guidelines for the OS and middleware used in each business project. • Enhanced the IT system that supports secure development and operations and engaged in efforts to develop the ideal IT system.	○	• Improve a system that visualizes the progress status of security measures and enhance the vulnerability measures. • Continue enhancing and improving the guidelines and streamline the security measures. • Support secure development and operations in each business project, and provide safe and secure products, systems and services to customers. • Promote security-embedded products, systems and services.
4. Improve security in cooperation with business partners	–	–	–	• Support business partners by checking and understanding the security status of the partners in real time. • Minimize risks by deploying awareness-raising activities against new threats to business partners and ensure supply chain security.

*1 GCAPS: Global Cyber Attack Protection System
*2 CSIRT: Computer Security Incident Response Team

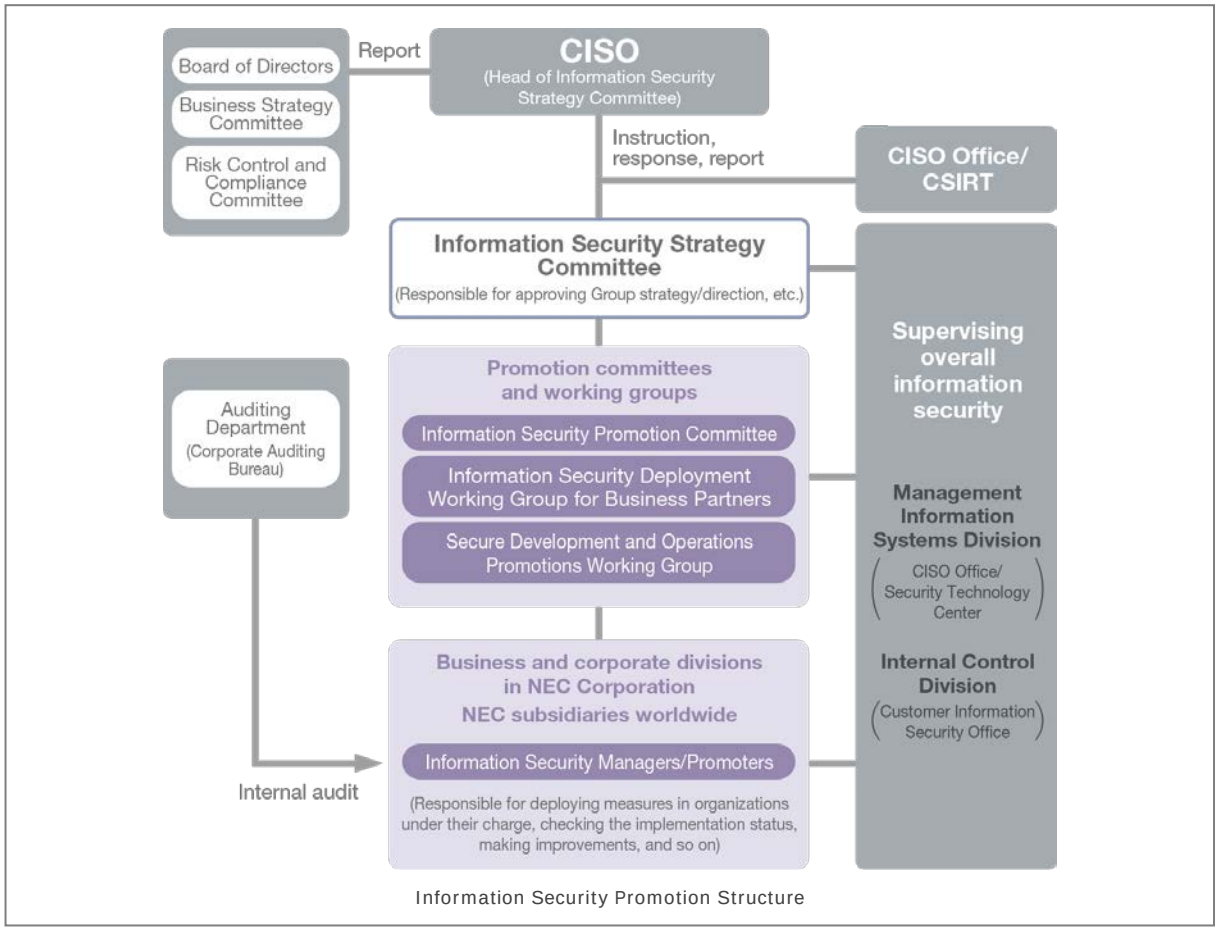
Promotion Framework

The information security promotion organizational structure of the NEC Group consists of the Information Security Strategy Committee, its subordinate organs, and the promotion structure at each organization level.

The Information Security Strategy Committee, headed by the CISO[*1], 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 to 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 CSIRT[*2], 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.
The Information Security Strategy Committee and 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.

[*1] CISO: Chief Information Security Officer
[*2] CSIRT: Computer Security Incident Response Team



Information Security Promotion Structure

Main Activities and Results for Fiscal 2018

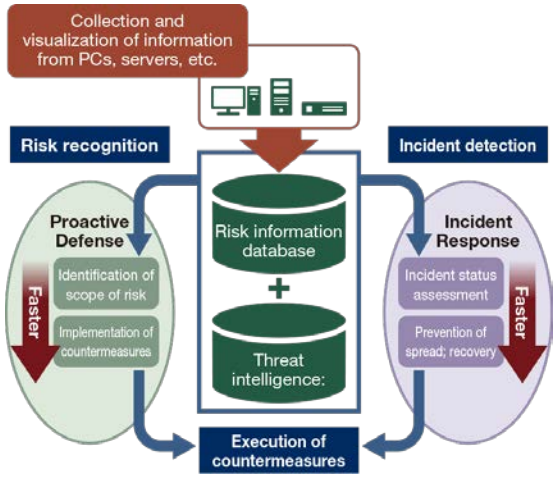
Strengthening Measures against Cyber Attacks

Cyber attacks that occur in daily business operations include targeted attacks against specific companies or organizations, ransomware that is a kind of malware that encrypts files and then demands a ransom in exchange for decryption, BEC (Business Email Compromise), indiscriminate email attacks that aimed at unspecified, large numbers of people, and are becoming more and more advanced and sophisticated. As a means to counter these attacks, we are deploying the Global Cyber Attack Protection System (GCAPS[*1]) within NEC Corporation and all its Group companies 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 2019 onwards, we will gradually introduce GCAPS also to overseas Group companies.

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

In addition, if the system is infected by unknown malware, the unauthorized communication will be blocked automatically from infected devices 24 hours a day together with SDN[*2], thus preventing the spread of secondary infection and minimizing security risks.



Concept of GCAPS

NEC has incorporated Artificial intelligence (AI) to realize leading-edge cyber security. By operating our solution in an actual IT environment as proof of concept, NEC is making efforts on the growth of its focused area as well as the development of an advanced internal reference model. For example, we have implemented ASI[*3], NEC's AI-based self-learning technology that detects abnormal behaviors of a system, into IT environment of NEC Asia Pacific (Singapore), and enabled CSIRT to monitor the environment more effectively. Requirements and points for improvement obtained through these actual operations are provided to the development division as feedback, contributing to the improvement of ASI quality.

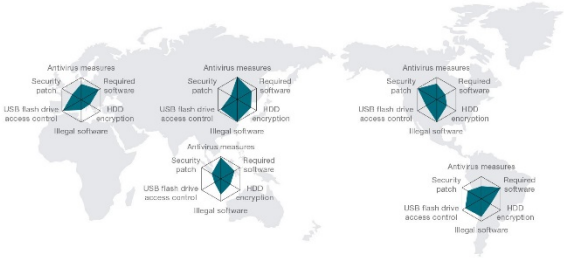
[*2] SDN: Software-Defined Networking
[*3] ASI: Automated Security Intelligence

Strengthening Global Security Infrastructures

NEC has deployed the integrated management platform that enables the visualization[*4] of the status of information security measures for PCs such as installation of security patches, malware countermeasures, and PC encryption, at overseas Group companies.

NEC also implemented information security education including the latest topics for all employees by using the Global ID Management Platform and has raised information security awareness. We have also carried out Network Security Audit/Security Inspection and confirmed the information security status at local Group companies.

[*4] “Visualization” in this context refers to a system for quantitatively confirming the implementation status of information security measures in overseas Group companies. 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 Corporation 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 NEC.

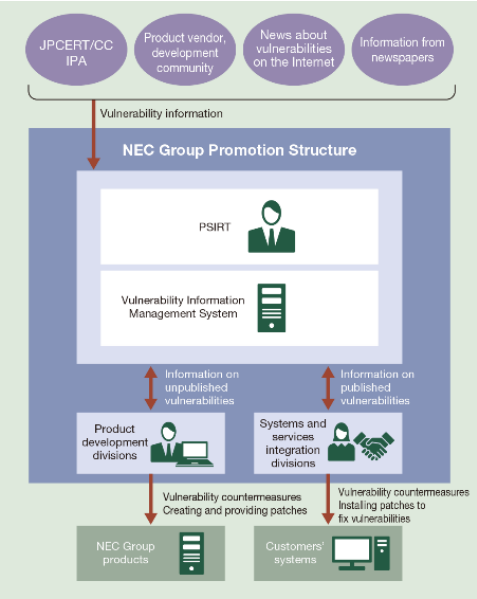


Visualization example: “Overview of information security implementation by region”
(The graph above shows only sample data and does not indicate any actual information.)

Strengthening Promotion of Secure Products, Systems and Services

NEC implements a PSIRT[*1] that manages vulnerabilities in order to quickly respond to the huge amount of vulnerabilities that are discovered on a daily basis. The PSIRT, with external organizations such as IPA[*2] and JPCERT/CC[*3], collects and analyzes vulnerability information and functions as PoC[*4] for communications. A framework has been established for enabling the entire NEC Group to share vulnerability information collected principally by the PSIRT.

We operate our own vulnerability information management system as infrastructure for deploying and managing the acquired information within NEC Group. Using this system, we are steadily disseminating and managing vulnerability information.



Vulnerability Response Promotion Structure

By visualizing security risks in customers' systems early on, we undertake security-related risk assessments to minimize those risks as much as possible. In response to the increasing threats of cyber attacks on control systems in recent years, we are focusing on implementation of a risk assessment service for control systems complying with standards such as ISO/IEC27001 or IEC62443.

[*1] PSIRT: Product Security Incident Response Team
[*2] IPA: Information-technology Promotion Agency, Japan
[*3] JPCERT/CC: Japan Computer Emergency Response Team Coordination Center
[*4] PoC: Point of Contact

Monitoring and Improvement

Information Security Assessment Activities

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

In fiscal 2018, information security assessments were carried out at NEC Corporation and its 68 Group companies 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 its 34 overseas Group companies, 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 Corporation and its Group companies 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 Corporation and its Group companies in Japan. On the other hand, for overseas Group companies, since the level of implementation has not reached that of the Japanese Group companies, the overseas Group companies were given instructions to implement measures based on the results of assessments, and the status of their implementation was regularly validated.

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 of business partners through web-based self-assessments and onsite assessments. We provided business partners with feedback on evaluation results, and thoroughly implemented improvements.

In fiscal 2018, web-based self-assessments were carried out at approximately 1,500 companies and onsite assessments at approximately 100 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

To ensure security in products, systems and services, NEC uses a checklist. The "Secure Development & Operation Check System" is used to visualize the status of security measures based on this checklist. This system manages about 7,000 business projects and managers can effectively inspect and audit the status of the security measures in place.