Information Security and Cyber Security

Policy

As information threats continue to evolve daily, information security has become an essential management priority in our sophisticated IT-based society.

NEC recognizes that it is our duty to protect the information assets entrusted to us by our customers and business partners as well as the Group's 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," priority management themes from an ESG perspective, and has established an "Information Security Statement" as the basis for promoting efforts to ensure both information and cyber security.

NEC Corporation selects priority risks as those that are evaluated as having a particularly large impact from the perspectives of the need for countermeasures and the magnitude of the possible damage to corporate business and society. In fiscal 2020, "risk related to information security" was selected, and we promoted countermeasures in line with the Groupwide management policy.

Based on the "Information Security Promotion Framework" (figure at right), and making reference to NEC's Purpose, NEC is working to realize a secure information society and provide value to its customers.

To protect information assets, NEC is taking the following approach:

- Implementing cyber attack measures,
- Providing secure products, systems and services
- Promoting information security in collaboration with business partners

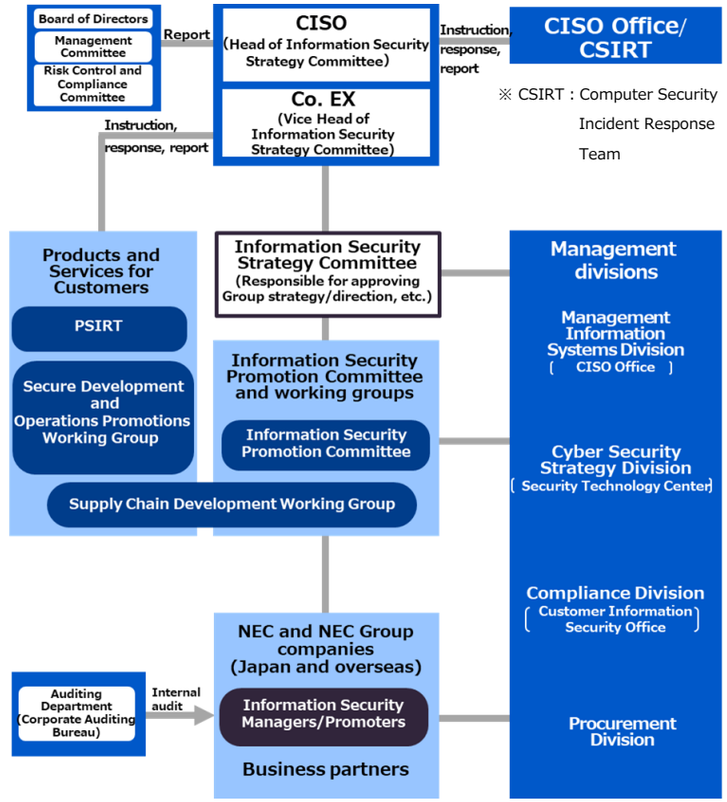
At the same time, we have positioned information security management, information security infrastructure, and information security personnel as the three pillars of the information security governance framework within the NEC Group, thereby maintaining and improving our comprehensive and multi-layered information security.

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

Information Security Promotion Framework

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. Under the directions of the Chief Information Security Officer, each company in the NEC Group works together to promote information security measures.



NEC Group Information Security Promotion Structure

Strategies and Main Activities and Results for Fiscal 2020

Measures against Cyber Attacks

As cyber attacks grow increasingly complex and sophisticated, the NEC Group focuses on protection of information assets entrusted by customers and business partners as well as its own. To this end, we have implemented total cyber security management by conducting uniform and advanced measures worldwide based on cyber security analysis, and established an incident response framework with our Computer Security Incident Response Team (CSIRT).

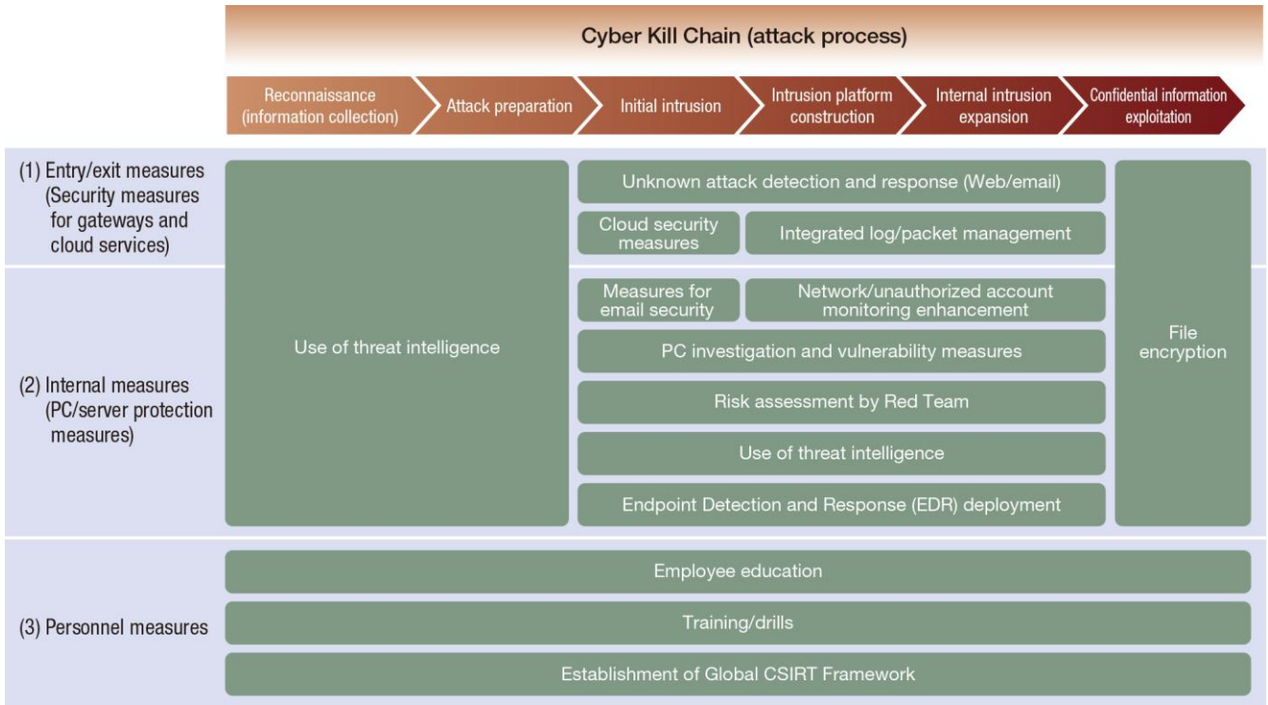
Every year, NEC plans and proposes measures based on cyber security analysis, and implements the measures with approval from the CISO.

In particular, as NEC is offering social solutions worldwide, a comprehensive global cyber security risk response is essential for its business continuity.

We are strengthening our global measures against increasingly sophisticated cyber-attacks based on a multilayered defense approach. In fiscal 2020, we took measures focused on the following five points.

(1) Detection of and response to unknown attacks
(2) Enhanced security of the mobile access environment
(3) Endpoint detection and response (EDR)
(4) Red Team[*1] risk assessment
(5) Use of threat intelligence

*1 Red Team: A team that carries out mock cyber attacks on corporations or organizations based on actual threats to evaluate the organization's attack resilience and risks from the perspectives of policy, CSIRT operation, and systems, and presents improvements and additional countermeasures.



Overview of Our Global Cyber Security Response

(1) Detection and response of unknown attacks
We have built an unknown malware detection system for monitoring incoming and outgoing emails and Web traffic. Based on the malware information obtained through monitoring, we take immediate actions to deal with PCs and servers suspected to have been infected, while continuously improving our filtering system to block illegal traffic more efficiently.
Moreover, we have introduced systems to detect suspicious activity at key monitoring points on the network to strengthen monitoring and response capabilities against infiltration.

(2) Enhanced security of the mobile access environment
Over the past few years, further diversification in work styles has seen an increase in opportunities for working outside of offices, such as working at home and in working spaces. In addition to PCs and smart devices that can be taken outside of the Company, we are also strengthening security for web access points of small-scale locations that do not have connection to the NEC Intranet, offering the same level of security as the NEC Intranet.

(3) Endpoint detection and response (EDR)
NEC is undertaking Groupwide deployment of EDR to enable early detection of threats that broke into the NEC Intranet and establishing more efficient incident response. In addition, we have deployed GCAPS[*2] for fixing vulnerabilities of PCs/servers in a timely manner.
The vulnerability management solution NEC Cyber Security Platform (NCSP) developed based on analysis derived from GCAPS in NEC Corporation enables "visualization" of the vulnerabilities of servers and PCs in the companies where it is installed, for rapid, appropriate security countermeasures.

2 GCAPS Global Cyber Attack Protection System

(4) Red Team cyber risk assessment
We conduct Red Team cyber risk assessments aimed at increasing the NEC Group's cyber-resilience and accountability.

We construct assessment scenarios from the attacker's perspective and mount a simulated attack on key systems within the organization to identify holes and leaks in our existing security countermeasures for further improvement.

(5) Use of threat intelligence
We are using threat intelligence to grasp threats against NEC including their signals in the early stage, thus enabling us to mitigate risks, minimize damage and shorten

response time, even if sophisticated threats break into our environment by passing through existing measures.

Providing Secure Products, Systems, and Services

Following the concept of security by design (SBD), which ensures security from the planning and design stages, NEC implements Secure Development and Operations initiative from the planning to operation phases for its products, systems, and services we provide to our customers. Ensuring security at the early stage of system development brings various benefits such as cost reduction, on-time delivery, and excellent maintainability of the developed system.

At each phase, checklists are used to ensure that required security tasks have been carried out. In the previous security standards and checklists, security measures were determined based on the confidentiality level of information assets. However, with the emergence of new types of cyber threats such as ransomware and denial-of-service attacks aiming at more than mere information stealing, we have to consider not only confidentiality but also integrity and availability. We therefore revised our security standards and checklists to make our secure development and operations more suitable for the current situation.

In addition, to analyze our systems from an attackers perspective, we established a risk hunting team that is skilled at identifying risks that are not easily uncovered with typical tests using tools.

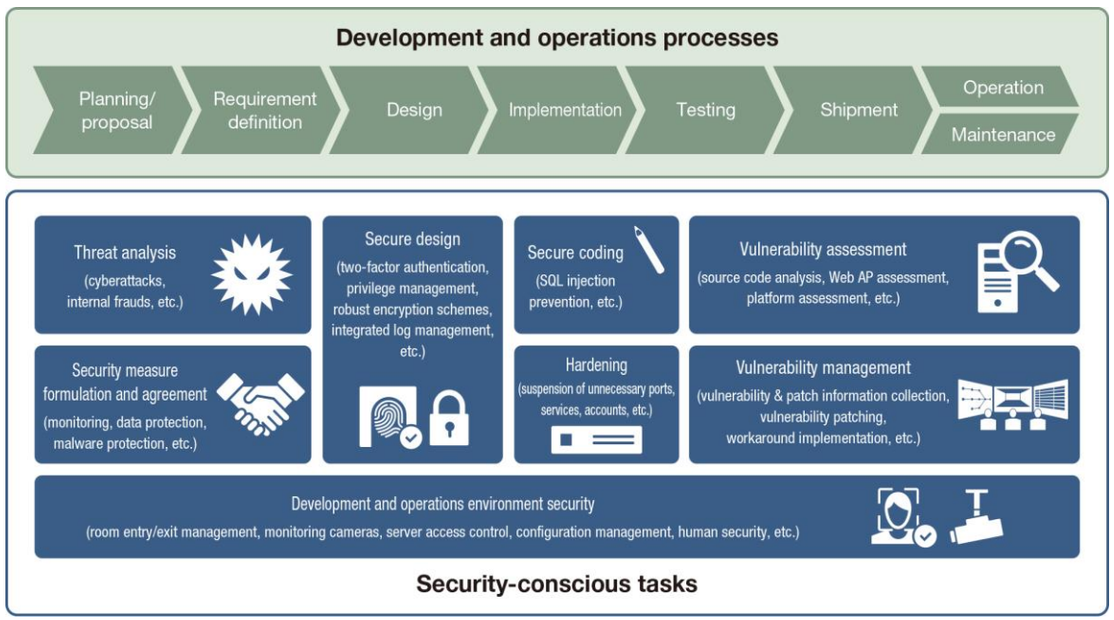
In addition to comprehensive risk analysis using conventional checklists, conducting testing by our risk hunting team in particularly high-risk domains has enabled the development and operation of more robust systems.

Information Security in Collaboration with Business Partners

NEC conducts its business activities in collaboration with business partners. In these collaborations, we believe it is important to ensure that the technology capabilities and information security level of the business partners meet our required standards. To this end, NEC categorizes its business partners by information security level based on the implementation status of their information security measures. In selecting business partners for a project appropriately, we check the information security level to outsource tasks, thus reducing risks of information security incidents occurring at business partners.

NEC requires its business partners to take appropriate information security measures in the following seven critical areas: (1) Contract management, (2) Subcontracting management, (3)Staff management, (4) Information management, (5) Introduction of technological measures, (6) Secure development and operations, and (7) Assessments. In fiscal 2020, we held information security briefings for business partners and provided information about risks and countermeasures against cyber attacks, to minimize the risk of information leaks.

To protect customers' information, NEC works together with its business partners to increase their information security levels by ensuring that information security measures are implemented throughout their organizations and that assessments and improvement actions are carried out.



Secure development and implementation based on the security by design (SBD) concept

Information security countermeasures for business partners