

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.

We recognize 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 positioned security, correctly referring to both information security and cyber security, as one of the critical subjects of "materiality", its priority management them from an ESG perspective—materiality, and has established its "Information Security Statement" as the basis for driving our efforts.

NEC has evaluated risks from various perspectives including the need of countermeasures as well as the possible damage both to corporate business and society, and has selected priority risks that will have huge impact and need to be addressed. With these risks in mind, we are deploying measures to counter cyber attacks which are becoming increasingly sophisticated, while complying with US National Institute of Standards and Technology (NIST) Cybersecurity Framework Version 1.1 and the Cybersecurity Management Guidelines Version 2.0 by Japan's Ministry of Economy, Trade and Industry (METI).


In addition, almost 100% of our business divisions in which information security is particularly important, such as healthcare, finance, government, and cloud computing services, have obtained Information Security Management System (ISMS) certification.

Based on our information security implementation framework (see the figure at right) as well as on our Purpose that shows why as a company we conduct business, NEC is working to realize a secure information society and provide value to our 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

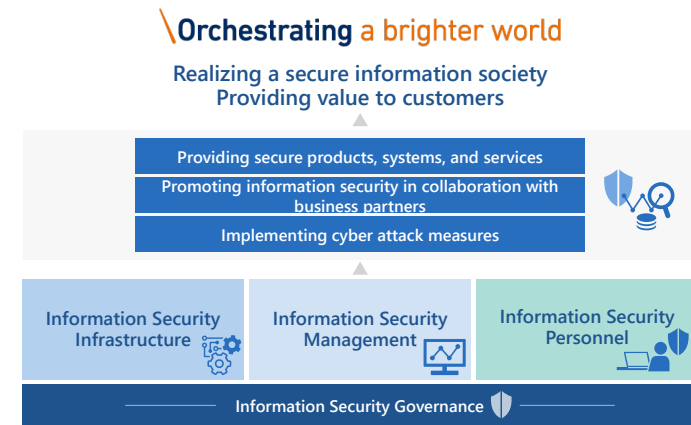
At the same time, we have positioned information security management, information security infrastructure, and information security personnel as the three pillars of the information security governance framework within the NEC Group, thereby maintaining and improving our comprehensive and multilayered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

 NEC Information Security Statement

 Information Security Report

 Priority Management Themes from an ESG Perspective—Materiality

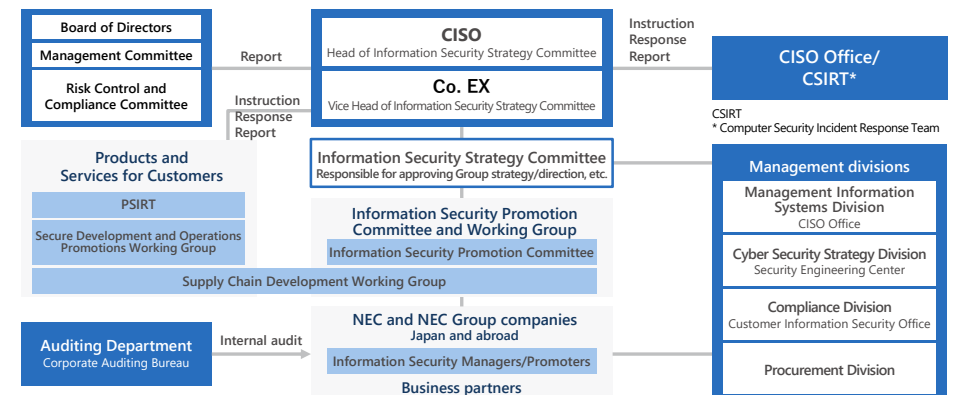
Information Security Implementation Framework



Implementation Framework

The NEC Group's information security implementation framework consists of the Information Security Strategy Committee, its subordinate organizations, and each organization's information security managers and promoters. Under the direction of the Chief Information Security Officer (CISO), NEC Group companies coordinate to advance information security measures.

The NEC Group's Information Security Implementation Framework



Measures and Main Fiscal 2021 Activities

● Measures against Cyber Attacks

As cyber attacks grow increasingly complex and sophisticated, the NEC Group focuses on the 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, given that NEC creates and provides social solutions for countries worldwide, a single information security incident caused by a cyber attack or any other factor could diminish the social trust of the entire NEC Group and materially affect its business management. For

this reason, we view a comprehensive and global approach to cyber security risks as essential for our business continuity.

We are strengthening our global measures against increasingly sophisticated cyber attacks based on a multilayered defense approach. In fiscal 2021, our measures focused on the following tasks.

Cyber Risk Assessments by Red Team*1

The NEC Group's Red Team conducts cyber risk assessments to increase the cyber resilience and accountability of the Group. The team creates assessment scenarios from attackers' point of view, conducts pseudo attacks on key systems within organizations to identify lacks and insufficient points in their existing cyber security measures, and takes actions for improvement.

*1 Red Team is a team of experts that launches a cyber attack similar to actual threats to a company or organization, assesses the organization's resilience against the attack, identifies risks involved in terms of policies, CSIRT operations and technologies, and proposes possible improvements and additional measures.

Using Threat Intelligence

NEC uses threat intelligence to identify threats including their early signs and emerging trends. This framework enables us to reduce risks, take rapid response, and minimize the damage of advanced threats that cannot be blocked by conventional measures.

Advanced EDR

NEC has implemented endpoint detection and response (EDR) technologies in all of its Group companies to ensure early detection of threats that break into the intranet as well as efficient incident response. We also use the Global Cyber Attack Protection System (GCAPS) to address vulnerabilities of PCs and servers. Combining EDR and GCAPS with threat intelligence allows us to detect and respond to sophisticated threats that could not be addressed previously.

Critical Information Management

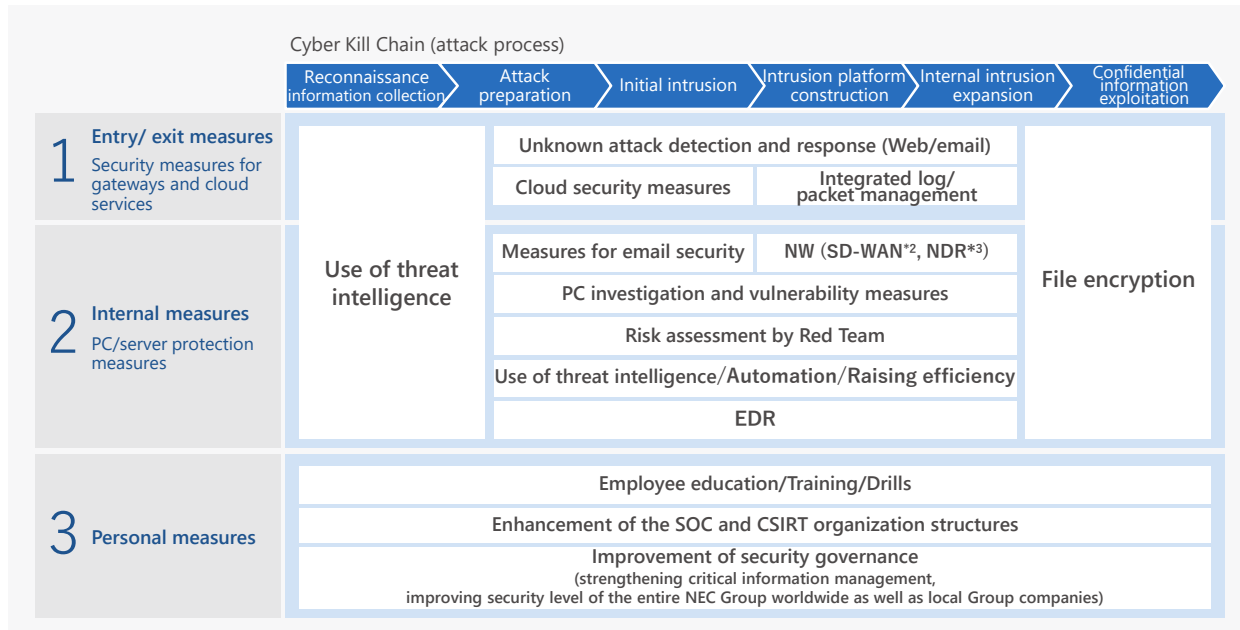
To minimize the impact of information leaks, we have defined "critical information" as information that would have huge impact on our business management and performance if it should be stolen or exposed externally. For critical information, we conduct stringent management and countermeasures including security assessments in all the organizations and internal audits by the Corporate Auditing Bureau.

Enhancement of Security and Governance Structure

To strengthen our ability of emergency response and daily operation monitoring, we have revised and enhanced our operation processes as well as the overall structure of our security operation center (SOC) and CSIRT framework.

In addition, we have assigned a regional CISO at each of our global operation sites. To enhance security governance, these regional CISOs are in charge of security management for their respective regions and take responsibility for the results of their management.

Overview of Global Measures against Cyber Attacks



*2 SD-WAN : Software-Defined Wide Area Network

*3 NDR : Network Detection and Response

● 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 the Secure Development and Operations initiative from the planning to operation phases for the products, systems, and services it provides to its 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. Nonetheless, issues remain in relation to the incorporation of security into the development process. These include omissions due to the unique security settings used by each manager and mistakes in settings caused by human error.

To address such issues, NEC has developed tools that automate secure development. For example, we have established an operating system and middleware fortification tool that automatically applies secure settings to servers. Also, we have introduced technologies that realize homogeneous security throughout entire environments used for cloud computing construction, which has been rapidly increasing in

recent years. Specifically, we are advancing an initiative for using technology that describes cloud computing environments in code form, known as “infrastructure as code,” and then distributing and utilizing templates for secure cloud computing environments themselves.

In fiscal 2021, we also created a prototype baseline for privacy evaluation by referring to privacy-related laws and guidelines, such as the NIST Privacy Framework, ISO 29100, and ISO 29134. We are verifying the effectiveness of this baseline with a view to establishing a method for comprehensively inspecting cyber risks and other risks related to business continuity, such as insufficient consideration of privacy.

● Information Security in Collaboration with Business Partners

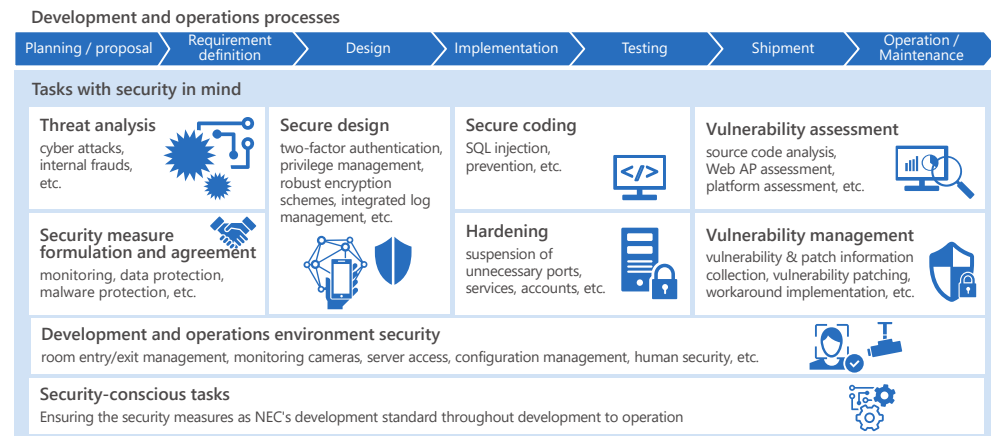
NEC conducts its business activities in collaboration with business partners. In these collaborations, we believe it is important to ensure that the technology capabilities and information security level of the business partners meet our required standards. To this end, NEC categorizes its business partners 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 2021, we held information security briefings (data disclosure method) 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 SBD Concept



Information Security Countermeasures for Business Partners

