Orchestrating a brighter world

NEC

Information Security Report 2022

NEC's Approach to Information Security

NEC positions information security as a key management mission and aims to continue to be a trusted company by complying with national guidelines and international standards.

Hiroshi Kodama

Executive Vice President,
Chief Information Officer (CIO) and
Chief Information Security Officer (CISO)
NEC Corporation

Today, when the entire world is openly connected, it is becoming a critical issue, for nations and businesses alike, how to address increasingly sophisticated and commercialized cyberattacks including ransomware, the growing needs for personal information protection, economic security and other social challenges. Given these circumstances, NEC is shifting from its conventional boundary defense model to "Zero Trust" by deploying a zero trust security platform in which no access is granted without verification. We have also implemented robust and flexible security measures across our group that are based on the Zero Trust Maturity Model of CISA*1.

We are stepping up our intelligence about increasingly damaging cyberattacks (for proactive defense based on attacker trends and other factors) and our resilience (ability to recover from cyberattacks) in line with Version 2.0 of the "Cybersecurity Management Guidelines" established by Japan's Ministry of Economy, Trade and Industry (METI) and the "Cybersecurity Framework (Version 1.1)" issued by the US National Institute of Standards and Technology (NIST). Our efforts also include enhancing the information security in the entire supply chain and providing high-quality total security packages, such as ensuring security with the focus on the data being handled based on the concept of Security by Design 3.0. In recognition of these efforts, the Information Technology Federation of Japan awarded NEC a "star" in 2021 as a model company with outstanding security measures.

In order to become a company that is consistently trusted by customers and society, we will continue to bolster our information security efforts through comprehensive approaches, while providing our internally proofed cutting-edge technologies. These technologies include privacy-preserving biometric authentication, which enables authentication with encrypted facial data, and walk-through facial recognition for entry/exit control.

Under its corporate message of "Orchestrating a brighter world," NEC will use ICT to solve social issues and contribute to the realization of a safe, secure, fair and efficient world where everyone has the chance to reach their full potential. This report brings you up to date on the NEC Group's information security activities. We hope that you read the report and find it informative.

★1 CISA: U.S. Cybersecurity and Infrastructure Security Agency

For inquiries regarding this report, please contact:

Corporate Transformation Division
Corporate CISO Office
NEC Corporation
NEC Headquarters, 7-1 Shiba 5-chome, Minato-ku, Tokyo 108-8001
Phone: 03-3454-1111 (main line)

On the Publication of "Information Security Report 2022"

The purpose of this report is to introduce stakeholders NEC Group's information security activities performed based on "Cybersecurity Management Guidelines Ver. 2.0" by the Ministry of Economy, Trade and Industry, Government of Japan. The report covers our activities up to June 2022.

Contents

10 important directions of "Cybersecurity Management Guidelines Ver. 2.0" by the Ministry of Economy, Trade and Industry

- Direction 1 Recognize cybersecurity risk and develop a company-wide policy
- Direction 2 Build a management system for cybersecurity risk
- Direction 3 Secure resources (budget, workforce etc.) for cybersecurity measures
- Direction 4 Identify cybersecurity risks and develop plans to address them
- Direction 5 Establish systems to effectively address cybersecurity risks
- Direction 6 Implement a PDCA cycle for cybersecurity measures
- Direction 7 Develop a cybersecurity incident response team and relevant procedures
- Direction 8 Develop a recovery team and relevant procedures in preparation for damage due to cyber incidents
- Direction 9 Understand cybersecurity status and measures in the entire supply chain including business partners and outsourcing companies
- Direction 10 Gather, utilize, and provide cyber-threat information through information sharing activities

Information Security Promotion Framework

The NEC Group maintains and enhances information security throughout the NEC Group and contributes to the realization of an information society friendly to humans and the earth by creating a secure information society and providing value to its customers.

The NEC Group positions information security as a key management mission and protects the information assets entrusted to us by our customers and business partners, as well as its own information assets, against cyberattacks and other threats. At the same time, by providing secure products, systems, and services, we create the social values of safety, security, fairness, and efficiency to promote a more sustainable world where everyone has the chance to reach their full potential.

The NEC Group is implementing anti-cyberattack measures, promoting information security, and providing secure products, systems, and services in collaboration with business partners. At the same time, we have positioned management, infrastructure, and personnel as three pillars in achieving thorough information security governance within the NEC Group in order to maintain and improve our comprehensive and multi-layered information security.

We have established the NEC Group Information Security Statement, and streamlined our group-wide rules and common information security infrastructure. Based on the security goals, group strategies, organization structure and resource allocation policy set by our top management, we are monitoring the entire environment to improve it further.

Information Security Governance

In order to effectively control risks stemming from business activities, the NEC Group has information security governance in place to efficiently raise the information security level across the entire Group.

1 Information Security Governance in the NEC Group

With the understanding that ensuring information security is one of the top priority management issues, the NEC Group considers investments in information security indispensable for corporate management. We have established the NEC Group Management Policy, setting standardized rules and implementing unified systems, business processes, and infrastructure in order to create a foundation for standard global management. NEC has a regional CISO*1 at each of its 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.

The top management recognizes risks through our information security governance scheme, sets information security goals and allocates resources to address the risks. The progress security activities is monitored and reported to the top for continuous improvement of our information security.

We pursue total optimization for our Group by cycling these processes at both the top management level and the organizational level and implementing an oversight function. We also disclose information properly to stakeholders and continue to improve our corporate value.

*1 CISO: Chief Information Security Officer

2 Information Security Promotion Organizational Structure of the NEC Group

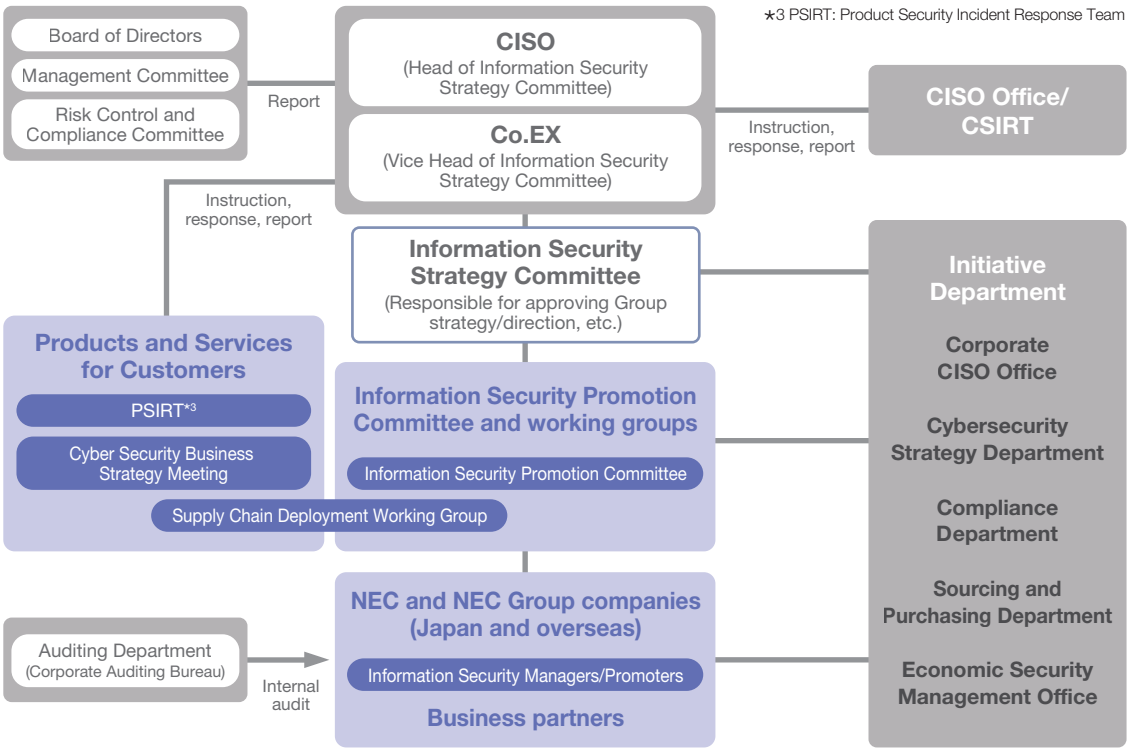
The information security promotion organizational structure of the NEC Group consists of the Information Security Strategy Committee, its subordinate organs, and other relevant organizations. The Information Security Strategy Committee, headed by the CISO, 1) evaluates, discusses, and improves information security measures, 2) identifies the causes of major incidents and defines the direction of recurrence prevention measures, and 3) discusses how to apply the results to NEC's information security business, among other things. We regularly brief the CEO on the status of measures adopted by this committee to obtain his approval.

The Corporate Executive (Co.EX), who assists the CISO, leads the CISO office that implements information security measures and the CSIRT*2 that monitors for cyberattacks and quickly addresses security incidents when they happen. The Information Security Promotion Committee and working groups plan and promote security implementation, discuss and coordinate implementation measures, ensure that all instructions are followed, and manage the progress of measures.

The information security manager in each organization has responsibility for ensuring information security for the relevant organizations including the Group companies under their supervision. They make efforts to ensure that rules are understood within their organizations, introduce and deploy measures, while continuously checking the implementation progress to improve the situation.

*2 CSIRT: Computer Security Incident Response Team

Information Security Promotion Structure



Information Security Management

In order to have information security measures take root across the entire NEC Group, we have an information security management framework and security policy in place and ensure their continued maintenance and improvement.

1 Information Security Management Framework

Based on its information security and personal information protection policies, NEC is making efforts to maintain and improve information security by continuously implementing the PDCA cycle. We track and improve the implementation status of information security measures and review policies by checking the results of information security assessments and audits as well as the situation of information security incidents among other factors. We also encourage the acquisition and maintenance of ISMS and Privacy Mark certifications within the group.

2 Information Security Policies

NEC has laid out the NEC Group Management Policy as a set of comprehensive policies for the entire Group. We have released the NEC Group Information Security Statement*1 and established and streamlined a variety of rules, including basic information security rules, information management rules, and IT security rules.
Furthermore, after establishing the NEC Privacy Policy*2, NEC obtained Privacy Mark certification in 2005. Our management system conforms to the Japan Industrial Standards Management System for the Protection of Personal Information (JISQ 15001) and Japan's Act on the Protection of Personal Information. Also, in 2015, we added a My Number (personal identification number) management framework to ensure compliance with the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure ("My Number Act"). To comply with the Amended Act on the Protection of Personal Information, which was enacted in 2022, we have revised the personal information protection rules and manuals.
The NEC Group requires its employees to handle personal information at a common protection management level throughout the entire Group. As of the end of June 2022, 31 NEC Group companies have acquired Privacy Mark certification.

*1: NEC Group Information Security Statement
https://www.nec.com/en/global/iss/index.html

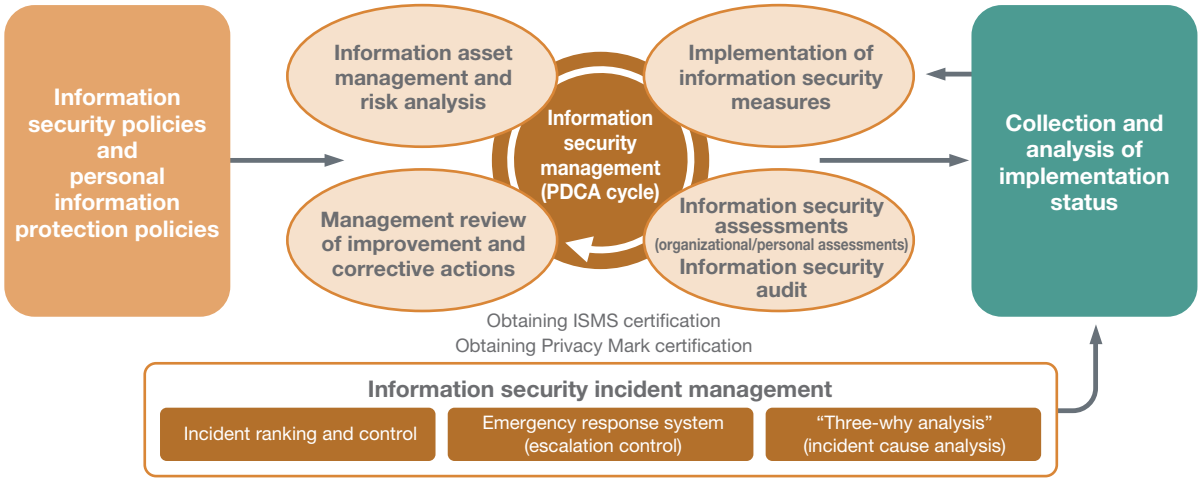
*2: NEC Privacy Policy
https://jpn.nec.com/site/privacy/en/privacy.html

3 Information Security Risk Management

❶ Information Security Risk Assessment

The NEC Group assesses risks and takes appropriate measures either by identifying differences from a baseline or by analyzing risks in detail on a case-by-case basis. Basically, we maintain security by using an information security baseline defined to keep the fundamental security level implemented across the Group. If advanced management is required, we perform detailed risk analysis and take more refined measures.

NEC's Information Security Management



❷ Management of Information Security Incident Risk

It is mandatory in the NEC Group to report information security incidents, and we manage risks by utilizing the analysis results of reported data in the Plan-Do-Check-Act (PDCA) cycle. We centrally manage incident information on a group-wide basis, analyze factors such as changes in the number of incidents and trends for each organization and incident type, and reflect the analysis results in measures taken across the entire group. We also assess the effectiveness of these measures.

4 Critical Information Management

❶ Three Lines Model

The NEC Group manages critical information based on the concept of the Three Lines Model. The information owner division at the first line strictly manages information, and the risk management division at the second line monitors the first line and assists in management. The auditing division at the third line checks the status of management.

❷ Thorough Management of Critical Information

The NEC Group has set a framework to classify the trade secrets it handles into several categories for management based on the severity. Each organization checks details of all information they handle, and identifies which information belongs to which secret category to ensure that all necessary information is properly managed. We also have rules for handling, storing, and managing critical information according to their importance, as well as thorough measures to prevent information leaks.

5 Information Security Assessments and Audits

❶ Information Security Assessments

In the light of the analysis results of information security incidents and the recent cyberattack trends, we conduct assessments on an annual basis with priorities set to eliminate information leaks. These assessments are intended to grasp the implementation status of security measures by each organization. Surveys on the priority measures help respondents realize what is required to secure their environment and to raise their awareness for improvement.
If there is any measure that failed to be sufficiently implemented, the responsible organization is asked to find out the reason for the failure and make improvements. If the problem cannot be solved by the organization alone, the NEC Group addresses that problem on a continual basis through the information security promotion plan for the following fiscal year.

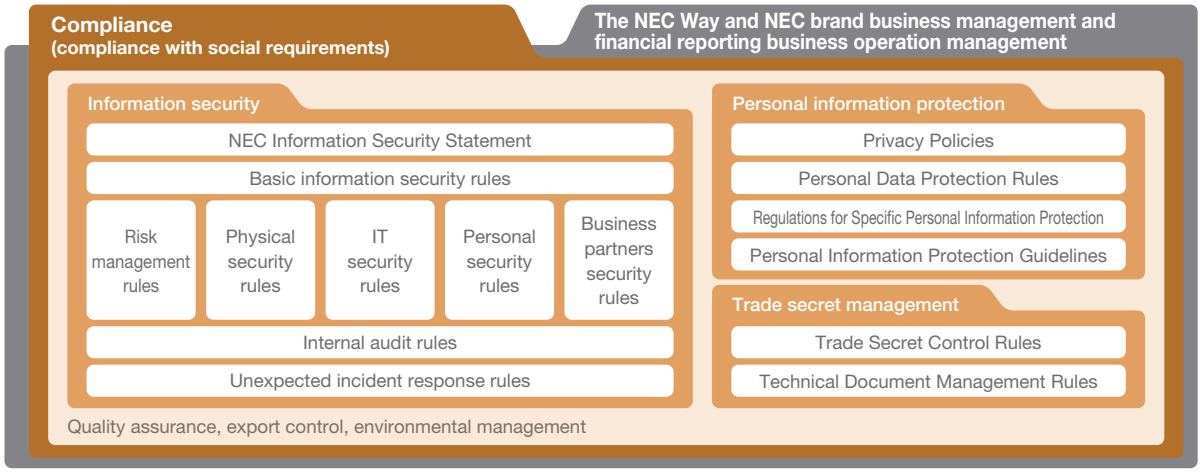
❷ Information Security Audits

NEC's Corporate Auditing Bureau drives internal annual audits on information security management, such as critical information handling, as well as on qualification for the PrivacyMark certification. These audits are performed regularly based on the ISO/IEC 27001 and JISQ 15001 standards to check how information security is managed in each organization.

6 Acquiring the ISMS Certification

To support organizations seeking to acquire ISMS certification, NEC provides the "NetSociety for ISMS" services based on the "Standard Content" showing what is required for getting the certification.

NEC Group Management Policy



Information Security Infrastructure

The NEC Group aims to realize zero trust for digital transformation (DX), using the Zero Trust Maturity Model of CISA*1 as a benchmark. This model uses five distinctive pillars – identity, device, network/environment, application workload, and data – to represent the degree of implementation. We have the following security measures in place covering each of these pillars.

*1 CISA: U.S. Cybersecurity and Infrastructure Security Agency

1 Identity Security

Authentication is an essential part of information security management. Identifying and authenticating individuals enables proper control of access to information assets and prevents spoofing and other fraudulent activities.

It is important to identify and authenticate users and assign them correct privileges so that information assets can be managed appropriately. NEC has built an authentication platform to centrally manage information used for identification, authentication, and authorization, covering not only our employees but also some business partners and other related parties if needed for business.

The information used for authentication and authorization includes user IDs and passwords as well as other access control information such as information about their organizations and roles. This information is used to control access to business systems and other company infrastructure on an individual basis. We also centrally manage which system and for what purpose the information for authenticating and/or authorizing users managed by each group company is being used. For systems that handle critical information, we are also promoting the adoption of multi-factor authentication utilizing electronic certificate-based individual authentication (possession-based authentication) and facial recognition (biometric authentication) in addition to user IDs and passwords (knowledge-based authentication).

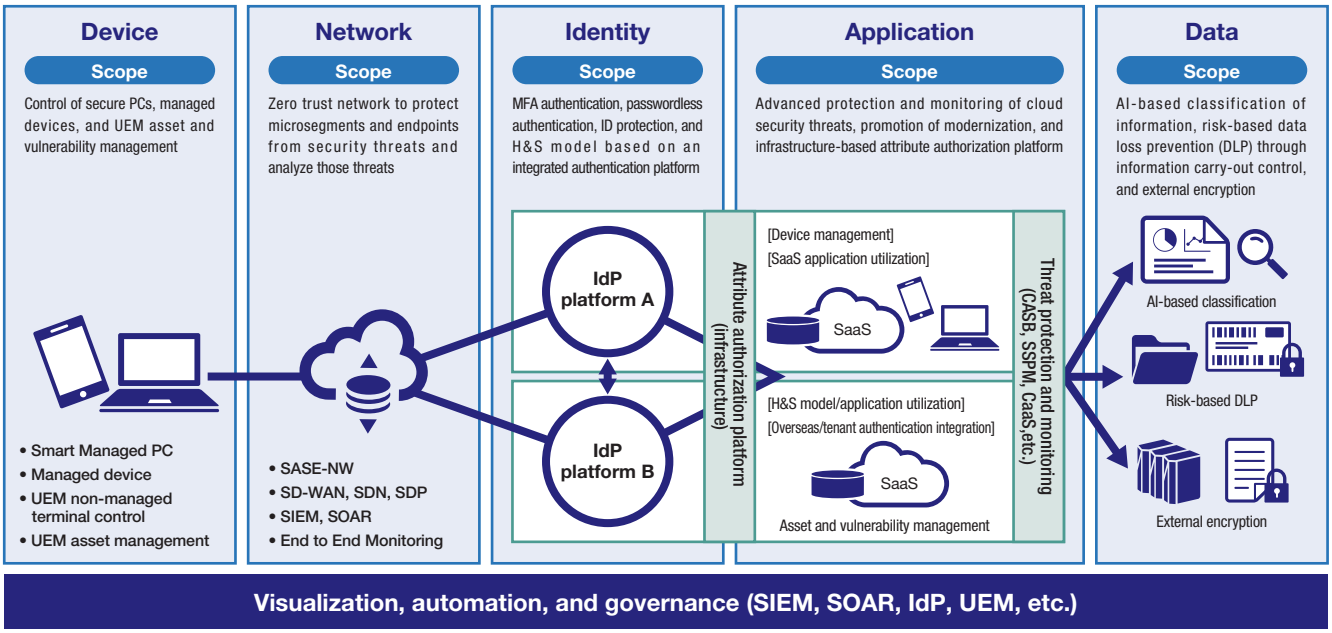
The cloud service authentication system is connected to the internal authentication platform, enabling seamless authentication for internal and external services. This system ensures that cloud services can be used safely and securely.

2 Device Security

As endpoint terminals, we use rich client-based PCs (“Smart Managed PCs”) that are secure and easy to use to support diverse work styles. Designed to ensure both security and usability, these terminals feature simple and secure facial recognition login, a comfortable operating environment that allows users to opt to go offline using dedicated resources, and simplified extended application and device settings among other capabilities. This has increased work efficiency and productivity while at the same time driving greater employee engagement.

We also have a unified endpoint management (UEM) platform to provide a secure device environment. This is aimed at making the entire NEC Group more resilient, cutting security management costs, promoting our internal DX initiatives, and bolstering risk response capability in order to enhance endpoint security across the NEC

Overview and Scope of the Zero Trust Platform



Group.
Our information leakage prevention system implements encryption, device control, and logging to address the risks of information leakage resulting from external attacks and internal fraud.
We encrypt storage devices and files to prevent information leaks due to theft or loss. In encrypting files, we define access privileges and usage periods as defaults to maintain a certain security level throughout the NEC Group. Therefore, even if information is transmitted to a third party because of malware infection or sent to the wrong address by email, the information is not leaked since it is encrypted.
For device control, we set restrictions prohibiting any recording of information on external media such as USB flash drives, SD cards, CDs, and DVDs as well as on communications devices such as smartphones and devices using Bluetooth or infrared technology. In cases such devices are needed for work, we define devices and functional restrictions for each organization and user to minimize their use.
We record all the operation logs of in-house PCs. In the event that an information leakage occurs, we analyze the logs to identify the scope of impact of the incident, grasp the current situation, and formulate measures to prevent a recurrence. In addition, to prevent information leaks caused by internal fraud, we have specified internal systems that require focused management, considering the impact on the business in the event of an incident. For these critical internal systems, we implement strict security measures including vulnerability information collection and handling, log management, network protection, authentication, access control, privileges management, secure operation and maintenance procedures, operation and maintenance checking, stringent security settings, physical entry controls and contractor management.
We also have a global ICT platform in place to maintain the security of information devices connected to the intranet and protect the PCs and networks from viruses and malware, as described below.

★2 UEM: Unified Endpoint Management

❶ Support for User Environments

NEC Group employees are required to install management software to monitor the security environment of their PCs. This software checks whether all PCs have all necessary security measures implemented, thus instantly visualizing existing security risks. Also, there is a system in place to automatically distribute security patches and definition file updates of anti-virus software, ensuring that they are properly installed. We also define prohibited software programs and monitor whether every user is using software appropriately.

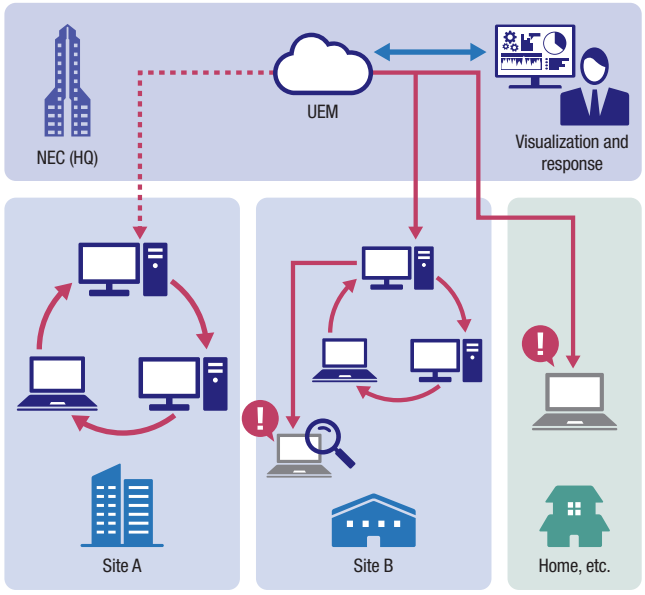
❷ Network Management

In addition to visualizing the PC status, if a PC with insufficient security measures is connected to the intranet or malware is detected in a segment of the intranet, that PC or network segment is disconnected from the intranet. We also control outgoing communications by various methods including web access filtering based on an allow list, prohibiting the use of free email accounts, and sender policy framework (SPF) authentication to specify domains allowed for sending emails.

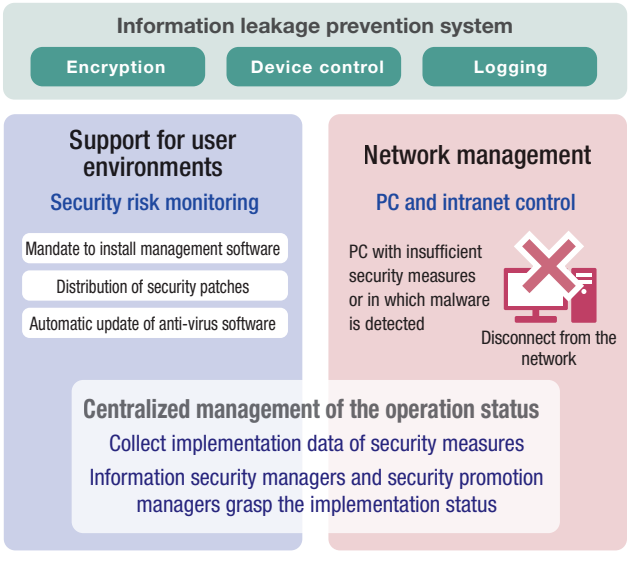
❸ Centralized Management of Security Updating

Data on the implementation status of security measures, including installation of patch programs and anti-virus software, is collected so that information security managers and security promotion managers can grasp the implementation status in their respective departments in a timely fashion. This ensures rapid and smooth implementation of security measures.

UEM-based Secure Endpoint Management



Protect Devices and Networks from External Attacks and Internal Fraud



Ensure safe and secure use of the intranet

3 Network Security

The NEC Group has a zero trust platform deployed and expanded on a global scale to deliver flexibility and robustness to system services and user devices.
The SD-WAN supports intranet segmentation and global centralized control to enable incident prevention, emergency shutdown, and collection of a wider range of log data, thus boosting security (damage localization and faster incident response). It also offers both security and improved user convenience by reducing the time it takes to make changes to the network, optimizing the network through local breakouts, and increasing the total network bandwidth by twice.
Also, we upgrade remote environments on a global basis in a zero trust-oriented fashion. An access platform linking cloud RAS and proxy servers provides efficient access to resources scattered across SaaS, IaaS, and on-premise systems. Moreover, it enhances security in a zero trust-oriented manner in conjunction with endpoint security and the next-generation authentication platform.

4 Application Security

The NEC Group uses many cloud services as it drives its DX initiatives. While DX increases user convenience, thorough security measures become necessary since critical data is stored in the cloud and more easily accessed from outside the company. Taking into account the risks involved in using cloud services, we have put in place security measures that underpin the convenience of those services, like the ones described below.

❶ Grasp of the SaaS Usage Status

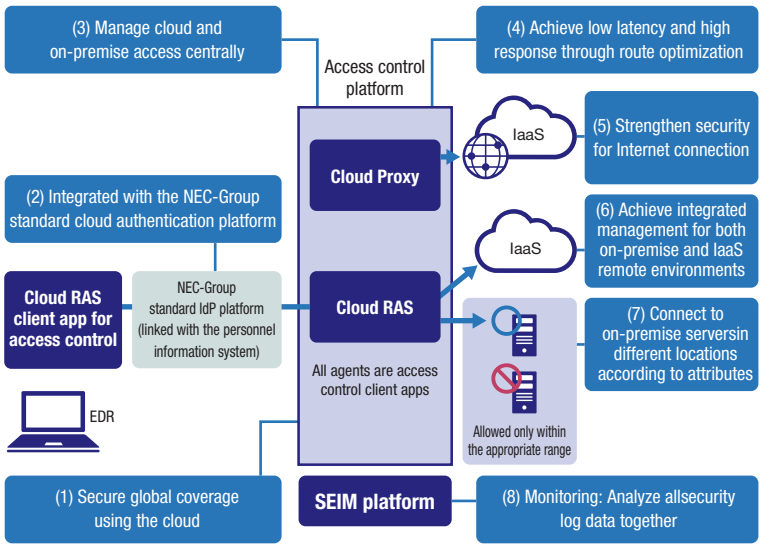
We monitor and analyze cloud service log data using the CASB*2 to protect cloud services that handle critical data from internal fraud and cyberattacks. We also visualize the usage status of internally used cloud services to check whether any unapproved services are in use.

*2 CASB: Cloud Access Security Broker

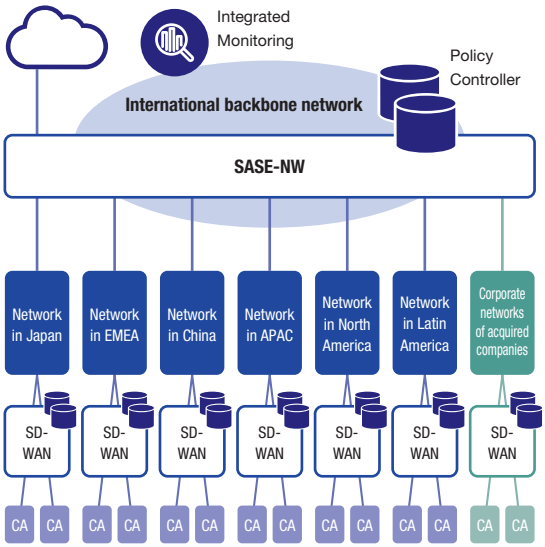
❷ Prevention of Incidents Resulting from Improper Public Cloud Settings

The use of public cloud services, such as AWS, Azure, and GCP, is increasing. While these services are easy to use, there is a risk of information leaking to the outside due to improper settings or for some other reason. The NEC Group employs CSPM*3 to check the

Upgrading Remote Environments on a Global Basis in a Zero Trust-oriented Fashion



Global Deployment of SD-WAN



settings of the internally used public cloud services according to the security standard and constantly monitor for potential risks.

*3 CSPM: Cloud Security Posture Management

❸ Prevention of Incidents Resulting from Improper SaaS Settings

Cloud services such as Microsoft 365, Box, and Salesforce often require complicated setup before use, which tends to result in a risk of information leaking due to improper settings. The NEC Group utilizes SSPM*4 to visualize and correct improper settings of the internally used cloud services.

*4 SSPM: SaaS Security Posture Management

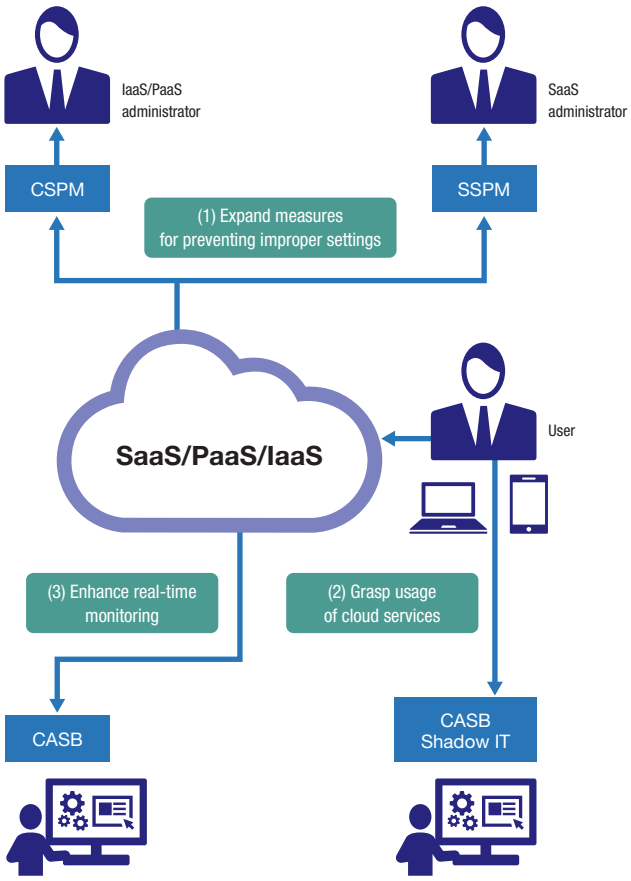
5 Data Security

With an eye on security in the era of zero trust, the NEC Group is promoting data protection using its own solution "InfoCage FileShell." In addition, we achieve file-by-file automatic classification, encryption, tracking, access privileges management, and so forth through the use of AIP*5 unified labeling that supports a cloud environment. Tracking enables the usage status to be traced, allowing accurate data management in a zero trust environment.

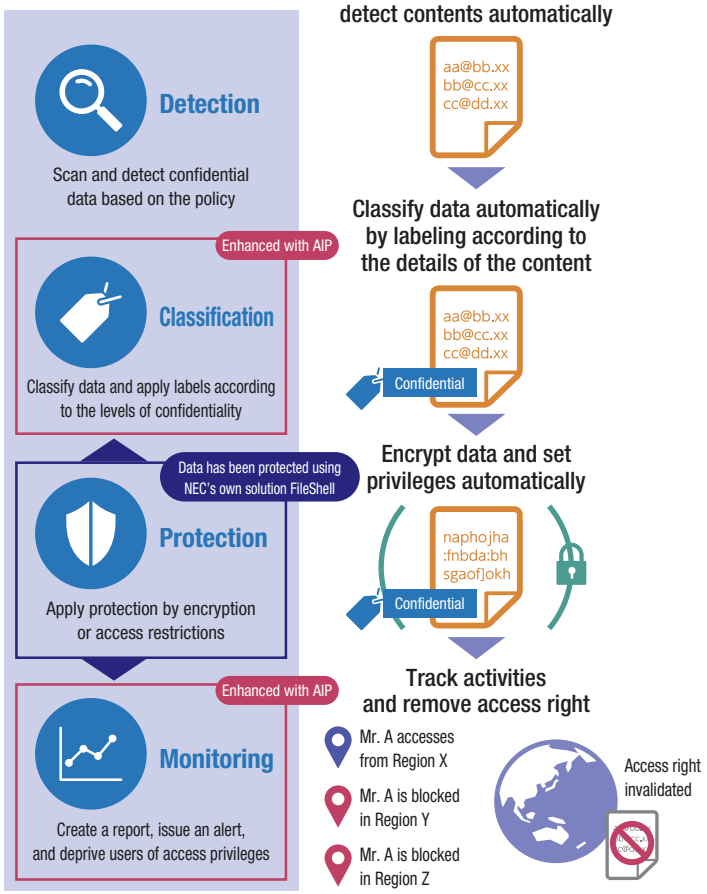
Also, to accomplish thorough management of critical information, we use secure storage as infrastructure to securely manage confidential information. The secure storage meets the requirements for confidential information management – access control, encryption, trail management, intrusion investigation, and ISMS management. This helps reduce the workload of the personnel striving to attain conformity with these requirements, thus achieving secure information management.

*5 AIP: Azure Information Protection

Security Measures for Using Cloud Services



InfoCage FileShell+AIP



Information Security Personnel

In addition to increasing employees' awareness of information security,
NEC promotes measures to enhance security skills and develop security experts in order to maintain its abundant human resources in the information security field.

1 Developing Information Security Expertise

NEC develops information security expertise from three points of view: 1) raising awareness of information security among all employees; 2) developing personnel who promote security measures; and 3) developing experts who can provide value to customers.

2 Raising Awareness of Information Security

Being sensitive to security risks, knowing how to properly handle information, and having an information security risk culture are important to raise awareness of information security. The NEC Group provides training and awareness-raising events in these fields.

❶ Training on Information Security and Personal Information Protection

NEC provides a WBT*1 course on information security and personal information protection (including protection of people's personal identification numbers ["My Numbers" in Japan]) for all NEC Group employees to increase knowledge and skills in the information security field.
The content of the training is updated every year to reflect the trends of information security including emerging threats and how to respond to them, security measures required in remote work, appropriate ways of handling information, as well as to raise information security awareness of employees.

*1 WBT: Web Based Training

❷ Commitment to Following Information Security Rules

NEC has established the Basic Rules for Customer Related Work and Trade Secrets, a set of basic rules that must be followed when handling customer information, personal information (including personal identification numbers), and trade secrets. All NEC Group employees have pledged to observe these rules.

❸ Activities to Raise Awareness of Information Security

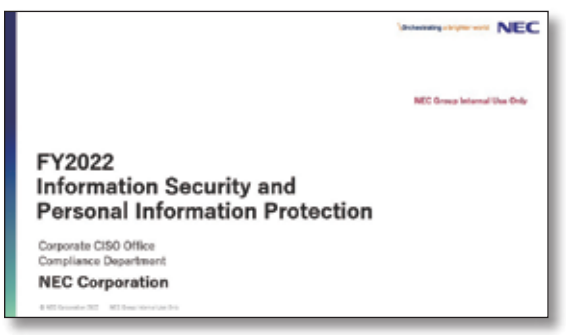
NEC carries out awareness-raising activities using videos and other material to raise a sense of urgency about information security risks and to develop employees capable of thinking, judging, and acting on their own. NEC also holds roundtable discussions called "Theme-based Talks" in the workplace to enhance the ability of each employee to analyze and judge risks and to foster a culture where information security risk management is an important and valued aspect in the organization. According to the results of a questionnaire, information security awareness has improved by 40 points since the implementation of theme-based talks, indicating that the activity is starting to produce intended results.

3 Developing Personnel to Promote Information Security Measures

Within our information security promotion framework, NEC deploys a variety of measures internally to develop dedicated staff having the skills necessary for promoters who drive those measures. As promoters are required to have high-level expertise in critical information management, personal information protection, secure development and operations, incident response, etc., managers who have acquired CISSP*2 or RISS*3 qualification are assigned to the role. NEC develops an information security promoter for each business unit (BU) and business division to enhance its ability to address security threats.

*2 CISSP: Certified Information Systems Security Professional
*3 RISS: Registered Information Security Specialist

Training for All Employees



4 Developing Experts

NEC is actively developing security experts to enhance our security response capabilities in products, systems, and services, and to help customers reduce risks.

❶ NEC Cybersecurity Training Site

A dedicated virtual environment that mimics an e-commerce (EC) site is used for practical security training, and employees learn about environment hardening techniques in the system construction phase. The training course that supports e-learning has been attended by a total of 4,000 employees since March 2019 despite the COVID-19 pandemic. This has helped the trainees enhance their security knowledge and skills to develop and operate systems for customers.

❷ Group-wide CTF

To expand the breadth of NEC's security personnel, NEC has held an in-house CTF*4 event called "NEC Security Skill Challenge" for all employees. Since the event began in 2015, a total of over 6,000 employees have voluntarily participated and stepped up their security skills.

*4 CTF: Capture the Flag

❸ Basic Security Training for Sales Personnel and System Engineers

NEC provides e-learning courses for sales personnel and system engineers to acquire the basic security knowledge they need, with the focus on Security by Design (SBD). In fiscal year 2021, a total of more than 30,000 employees participated in these courses. The training is aimed at enhancing the security skills across the entire NEC Group.

❹ SBD Specialists

A program has been underway since fiscal year 2019 to develop specialists who assist security managers and implement SBD in the individual business divisions. A total of 40 employees have attended the program so far. These specialists play a pivotal role in overseeing all the system development processes as a whole and implementing complete and adequate security, which enables us to deliver safe and secure systems to our customers. A new course for salespeople started in fiscal year 2021 to help trainees acquire the skills they need to present appropriate security proposals, including incident case studies and offerings of countermeasures.

❺ NCSA (NEC Cybersecurity Analyst)

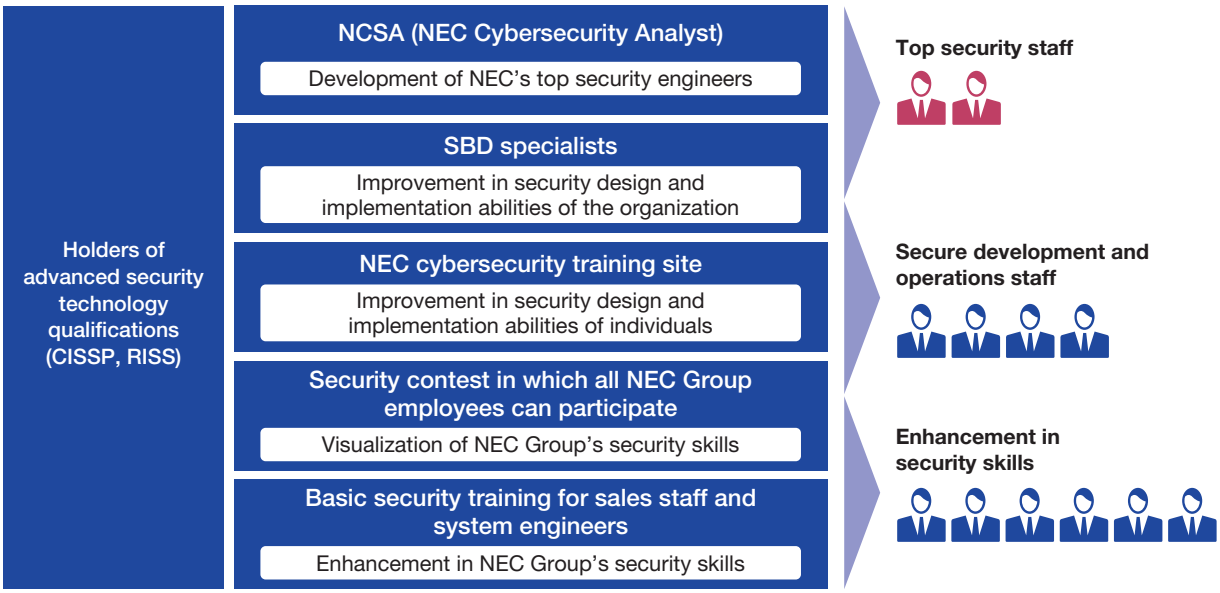
The purpose of this program is to enhance the skills of top security staff. Intended for those staff members who have knowledge of security technologies, the six-month intensive program lets trainees master the practical technical skills required for advanced security services, such as CSIRT*5 work and risk hunting. When combined with those who attended the NEC CISO Assistant Training (NCAT) program that lasted until fiscal year 2019, a total of 60 staff members have participated in these programs. They now engage in providing professional services.

*5 CSIRT: Computer Security Incident Response Team

❻ Holders of Advanced Security Technology Qualifications

NEC strongly encourages its employees to acquire official qualifications for security as proof that they have high-level information security skills to deliver the most suitable solutions to each customer. We hold internal seminars, workshops, and other events to increase the number of staff who acquire the CISSP international certification and RISS certification. The NEC Group has more than 200 holders of the CISSP certification.

Developing Experts



Measures Against Cyberattacks

As cyberattacks are becoming increasingly advanced and sophisticated,
NEC accomplishes cybersecurity management by implementing cutting-edge protection measures on a global scale while having a CSIRT framework that enables rapid incident response.

1 Ensuring Cyber Resilience

NEC ensures cyber resilience by implementing advanced and standardized measures worldwide based on cybersecurity risk analyses while having a CSIRT*1 structure responsible for rapid incident response. We also conduct third-party assessments based on NIST CSF*2 to enhance our security.

★1 CSIRT: Computer Security Incident Response Team
★2 NIST CSF: The Cyber Security Framework issued by the US National Institute of Standards and Technology (NIST) to enhance the cybersecurity of critical infrastructure

Specifically, with the belief that taking a globally standardized approach toward cybersecurity risks is vital for business continuity, we are monitoring our networks 24/7 for possible cyberattacks, analyze the situation, and review our monitoring and operation processes whenever needed. NEC researches security products and services as well as market trends to keep track of the ever-changing technology. Also, through PoC*3 evaluations and internal IT environment research, we analyze if the products and services work well and meet the security requirements in our environment. Based on the results of research and analysis, we consider countermeasures that will be needed in the future and determine the targeted scope while finding out their effects and costs. We create an action plan every year based on the above-mentioned activities and, upon approval of the CISO*4, carry out the planned measures.
The NEC Group implements measures against ever sophisticated cyberattacks based on the concept of multilayered defense. We are focused particularly on: 1) cyber risk assessment by the Red Team*5, 2) generation and use of threat intelligence, 3) enhancement of the CSIRT structure, 4) enhancement of systematic security resilience, and 5) management of critical information.

★3 PoC: Proof of Concept. A demonstration to prove the feasibility of a new concept.
★4 CISO: Chief Information Security Officer
★5 Red Team: A team of experts that launches a pseudo cyberattack similar to actual threats to a company or organization, assesses the organization's resistance against the attack and risks involved, and proposes possible improvements and additional measures.

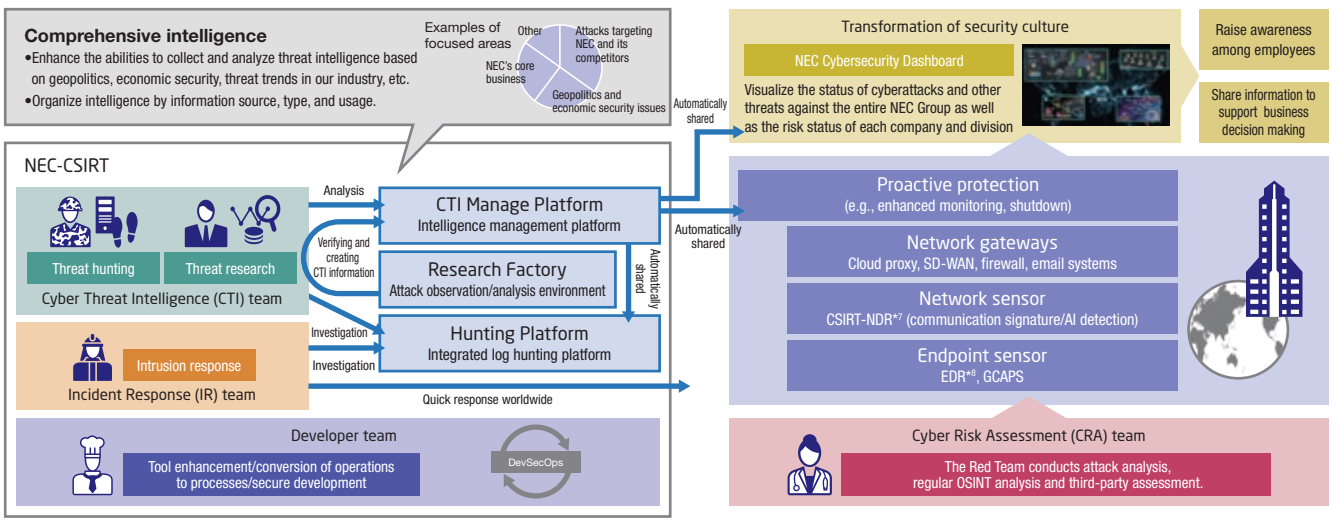
❶ Cyber Risk Assessment by the Red Team

The NEC Group's Red Team conducts cyber risk assessment on a regular basis to continuously improve cyber resilience and accountability of the Group. The cyber risk assessment is implemented on a global scale with three activities combined into a package: examination of critical information management, investigation of vulnerabilities, data leaks and other risks of servers open to the public, and evaluation of intrusion probability from outside and inside the company from the attacker's point of view. The team checks all the existing security measures and operations, identifies what is lacking or insufficient, and takes actions for improvement.
We also undergo third-party evaluations by auditing firms and security companies.

❷ Generation and Use of Threat Intelligence

The Cyber Threat Intelligence (CTI*6) team identifies threats to NEC

Overview of Our Cybersecurity Measures



★7 NDR: Network Detection and Response
★8 EDR: Endpoint Detection and Response

including their early signs and implements proactive high-level defense. Exploiting the NEC Group's integrated EDR and log analysis platform, the team hunts unknown threats.
We also have a research environment (Research Factory) in place for enhancing our ability to generate unique CTI proactively and analyze threats in detail.

*6 CTI: Cyber Threat Intelligence

❸ 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. In addition, we use Global Cyberattack Protection System (GCAPS) to address vulnerabilities of PCs and servers. Combining EDR and GCAPS with threat intelligence allows us to detect and respond to more advanced threats.

❹ Enhancement of Systematic Security Resilience

To make ourselves better prepared for global cyber threats such as ransomware, we train our employees on targeted email attacks and have improved documentation to enable a rapid response to a ransomware incident. We also conduct drills at least once every six months attended by staff of the related divisions and experts. Furthermore, we have a third party evaluate the resilience of our critical systems to ensure high-level business continuity.

❺ Critical Information Management

We strictly protect and manage critical business information based on the concept of the Three Lines Model, with risk owners clearly identified. Especially for trade secrets and other critical information that will have huge impact on NEC's business management or performance if leaked, we store them in highly secure storage for stringent protection.

2 NEC Group's Cyber Defense in the Tokyo 2020 Olympic and Paralympic Games

We built an organizational structure dedicated to cyber threat intelligence in 2018, and collected and utilized intelligence, including early signs of threats, for proactive defense. Before the start of the Tokyo 2020 Olympic and Paralympic Games, our Red Team conducted cyber risk assessments (CRA) on all NEC Group companies around the world to identify and mitigate security risks and our CSIRT underwent training to prepare for emergencies.
During the Games, we had a special surveillance system in place, with the CSIRT bolstering its monitoring activities, managing critical information thoroughly, and quickly grasping incidents of internal systems in a centralized manner. This helped us go through this international event without any problem.
The know-how we gained through these experiences will be inherited as NEC's legacy in the field of security defense. We share this know-how on cybersecurity dashboards to raise awareness of all employees, which helps us transform our security culture.

NEC Cybersecurity Dashboard

Information Security in Cooperation with Business Partners

In order to protect the invaluable information of customers, NEC promotes the dissemination of information security measures and improvement actions in coordination with business partners to improve the level of information security for the entire supply chain.

1 Framework

NEC believes that, in collaborating with business partners, it is important that their level of information security, along with technical capabilities, meet NEC's standard. We classify business partners into different security levels according to their information security implementation status and have a mechanism in place whereby we can outsource work to business partners of appropriate levels. This reduces the risk of information security incidents occurring at our business partners.
NEC requires business partners to implement information security measures classified into seven categories: 1) contract management, 2) subcontracting management, 3) staff management, 4) information management, 5) introduction of technical measures, 6) secure development and operations, and 7) assessments.

❶ Contract Management

NEC and business partners to which we entrust work must sign comprehensive agreements that include nondisclosure obligations (basic agreement).

❷ Subcontracting Management

The basic agreement stipulates that business partners may not subcontract work to other companies unless they obtain written permission in advance from the organization that outsourced the work to them.

❸ Staff Management

NEC has compiled security measures to be implemented by people engaging in work outsourced from NEC in the "Basic Rules for Customer Related Work." We promote thorough implementation of these measures by asking workers to promise the company for which they work that they will take these measures.

❹ Information Management

NEC has guidelines in place concerning the management of confidential information handled when carrying out work. This ensures that confidential information is properly labeled, that the taking of information outside the company is controlled, and that confidential information is appropriately disposed of or returned after the work is complete.

❺ Introduction of Technical Measures

We categorize technical measures into required measures (e.g., encryption of all mobile electronic devices and external storage media) and recommended measures (e.g., an information leakage prevention system) and ask business partners to implement them.

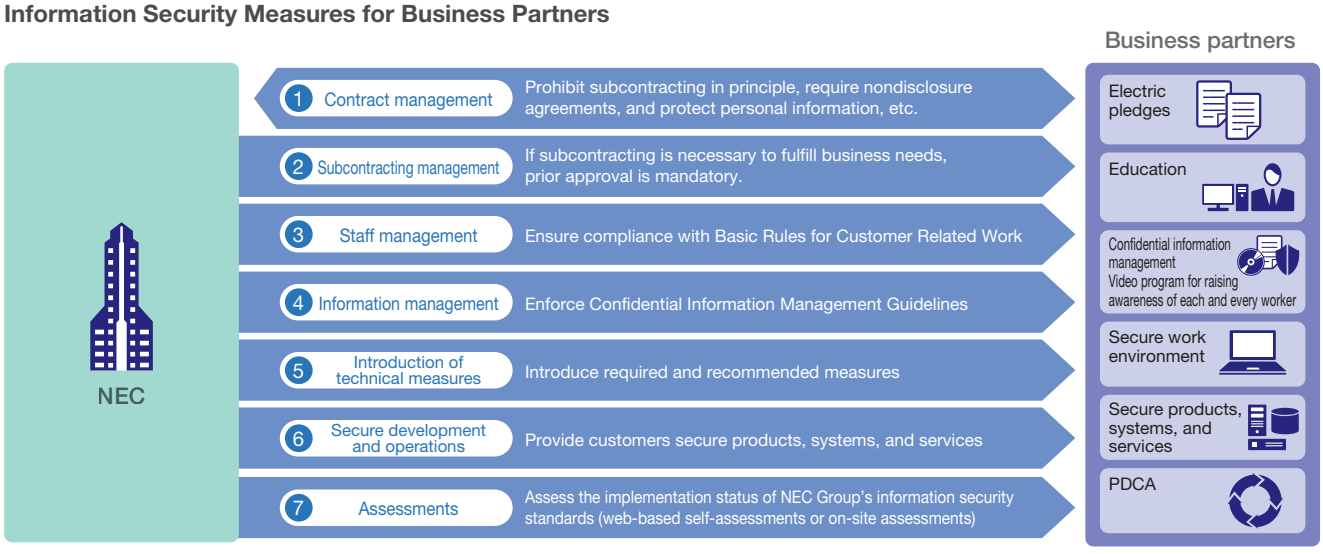
❻ Secure Development and Operations

NEC has guidelines in place concerning the development and operation of products, systems, and services for customers and asks business partners to consider security during development and operation.

❼ Assessments

NEC assesses the implementation status of information security measures at each business partner and gives instructions for improvement as needed, based on the "Information Security Standards for Business Partners," which defines the security levels required by NEC.

Information Security Measures for Business Partners



2 Promotion of Security Measures for Business Partners

❶ Information Security Seminars

NEC organizes information security seminars every year for business partners across the country (approximately 1,800 companies, including approximately 850 ISMS certified companies) to ensure that they understand and implement NEC's information security measures.

❷ Skill Improvement Activities for Core Business Partners

NEC works closely with about 100 core software business partners that frequently deal with NEC to encourage them to thoroughly implement measures and improve their skills.

❸ Distribution of Measure Implementation Guidebooks

NEC provides measure implementation guidebooks so that business partners can implement the information security measures more smoothly. We have issued a variety of guidebooks for achieving required standards, such as a guidebook for antivirus measures and a guidebook for development environment security measures.

❹ Standardization of Contractor Management Process

In addition to encouraging business partners to implement information security measures, NEC—the outsourcing organization—has also standardized the contractor management process to ensure that a standard set of information security measures are applied across the entire supply chain.

3 Assessments and Improvement Actions for Business Partners

NEC assesses our business partners through document-based assessment and on-site assessment. We review assessment items every year, taking into account the status of security incidents and other factors, and feed back reports of the assessment results to the business partners. We offer follow-up support on issues that need improvement to step up the security levels of our business partners.

❶ Document-based assessment

We conduct this assessment on about 1,500 selected companies that deal with NEC. The selected business partners assess the implementation status of security measures by themselves. They can input assessment results to our Web system and update the registered data anytime.

❷ On-site assessment

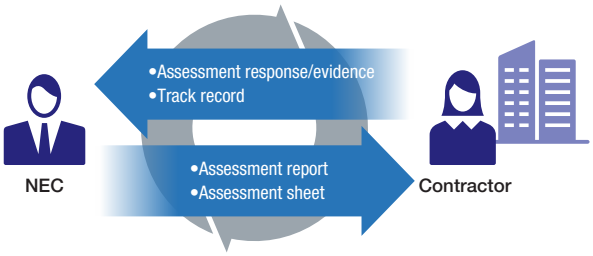
This assessment is conducted every year on about 200 companies that do large volumes of business with NEC. Approximately 100 assessors authorized by NEC visit business partners for on-site assessments or perform remote assessments.

❸ Information security assessment sheet

The information on the implementation status of information security measures, along with assessment results, are compiled into an assessment sheet, which is published on our system. Business partners can always check their latest status.

Standardized Contractor Management Process

Assessments and Improvement Actions for Business Partners



Providing Secure Products, Systems, and Services

To offer “better products, better services” to customers,
NEC carries out a variety of activities to ensure high-quality security in its products, systems, and services.

1 Promotion of Secure Development and Operations

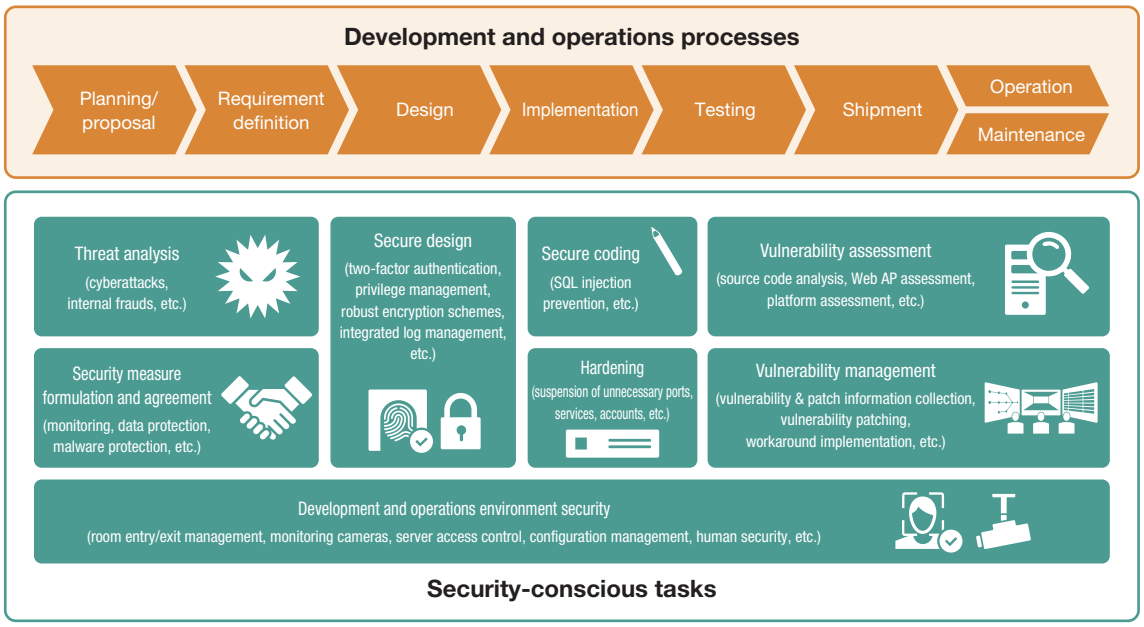
❶ Group-wide Promotion Structure and Rules

In order to enable secure development and operations for the products, systems, and services we offer to our customers, the NEC Group has a security implementation promotion structure in place. This promotion structure consists of security managers appointed in each of the cybersecurity management divisions and business divisions of the group. To eradicate information security incidents caused by product, system, and service vulnerabilities, security misconfigurations, and system failures, the security managers serve as a bridge between the cybersecurity management divisions and business divisions, ensuring that security measures are fully disseminated within their respective divisions and supporting employees in implementing security measures. The roles of the security managers and the security implementation processes in the individual divisions are defined in the “Cybersecurity Management Rules.” We upgrade these rules to cope with increasing cybersecurity risks.
In fiscal year 2021, we revised the security standard for outsourcing companies by reference to the Security Guidelines of the NIST (US National Institute of Standards and Technology). In recent years, we have seen an increasing number of business partners and outsourcing companies targeted by cyberattacks, resulting in leaks of critical information provided by NEC or delays in product manufacturing and supply. To address these attacks on the supply chain, we have reviewed and reinforced security measures, including those for business partners, so that we can continue to provide products, systems, and services to customers. In fiscal year 2022, we are stepping up security measures further by checking security management systems and measures of business partners based on the revised standard mentioned above.

❷ Key Security Implementation Efforts

Based on the security by design (SBD) concept for ensuring security, NEC implements security throughout the entire process from the planning and design phases to the construction and operation management phases. Ensuring security in early stages of system development directly leads to various benefits, including cost reductions, on-time deliveries, and development of easy-to-maintain systems. Particularly, we focus on risk assessments in the requirement definition phase to discuss and implement optimal security for the customer’s system environment in early stages.
NEC has defined the “Cybersecurity Implementation Standard” as the baseline security requirements to be considered at the time of proposal presentation and implementation. This standard specifies strict security requirements, taking into account not only the international security standards such as ISO/IEC 15408 and ISO/IEC 27001 but also the standards of government agencies and industry

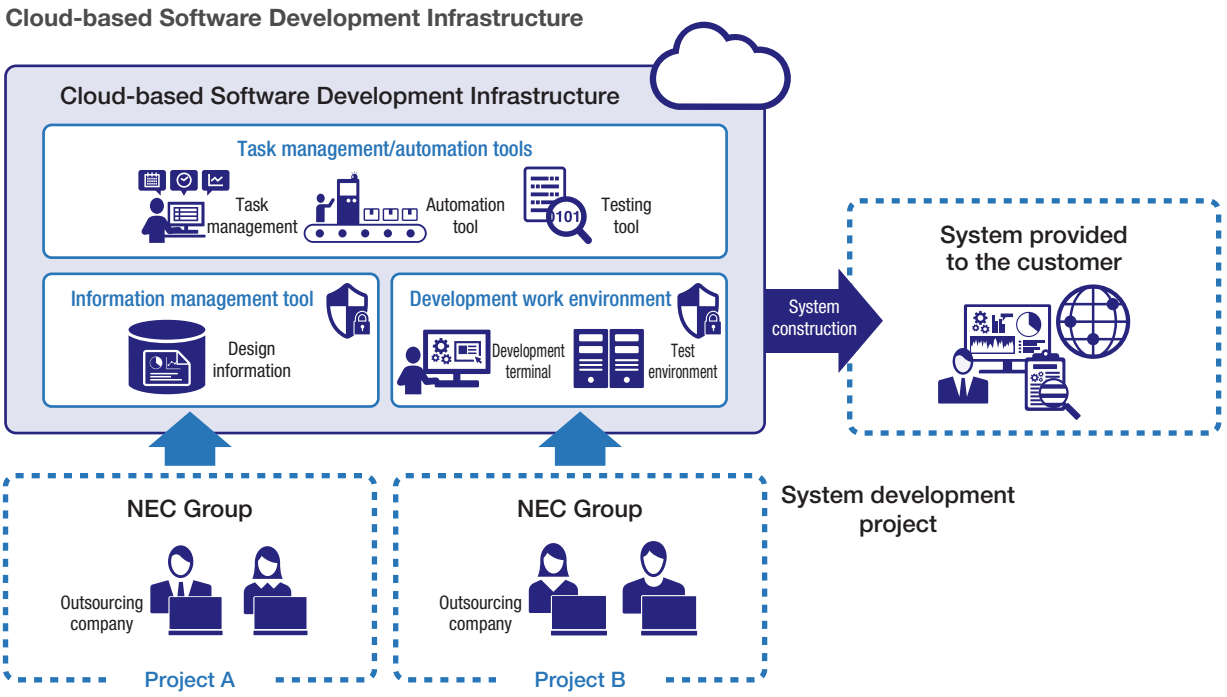
Secure Development and Operations Processes



guidelines.
In the development of products, systems, and services, we have created a checklist to ensure that security tasks are performed in each phase. Based on this checklist, business projects are managed and the status of security measures is efficiently assessed and audited using the “security implementation assessment system” developed to visualize the implementation status of security tasks.
In the operation and maintenance phases of products, systems, and services, we ensure security by using the “vulnerability management system,” which collects and distributes vulnerability information in a centralized manner, along with the “cyber intelligence sharing platform.” The cyber intelligence sharing platform features a tool that automatically collects information about various cybersecurity threats, a work environment for analyzing the collected information, and a function to distribute the collected and analyzed information in order to share the cybersecurity threat information (cyberattack tactics, cases of incidents, indicators for security measures, etc.) quickly with the business divisions. Distributing cybersecurity intelligence to the business divisions in a timely fashion enables us to have thorough security measures against emerging threats. It also helps build a secure business environment less prone to security incidents in the operation and maintenance phases of products, systems, and services.

❸ Software Development Infrastructure for Security Implementation

NEC has cloud-based software development infrastructure in place as an internal standard environment for system development. This development infrastructure is an integrated development environment that provides an information management tool for managing design information such as source code and specifications, tools for managing and automating various tasks, and a development work environment for implementation and testing, among other features. It also offers tools for streamlining and automating security implementation, such as a security vulnerability testing tool, leading to increased productivity, quality, and security in system development.
Consolidating the development environments of the supply chain, including business projects and outsourcing companies, as cloud-based development infrastructure enables the security of those development environments to be managed in a centralized manner. This makes it possible to ensure that the security measures that the individual business projects use for their development environments comply with the Cybersecurity Implementation Standard, which allows us to securely manage the design information of the customer’s system that we use during development.



Third-party Evaluations and Certifications

NEC proactively promotes third-party evaluations and certifications related to information security.

1 ISMS Certification

The following companies have units that have obtained ISMS (ISO/IEC 27001) certification, an international standard for information security management systems.

NEC Group Companies with ISMS Certified Units

- NEC Corporation
- ABeam Consulting Ltd.
- ABeam Systems Ltd.
- NEC Space Technologies, Ltd.
- NEC Solution Innovators, Ltd.
- NEC China Soft (Japan), Ltd.
- NEC Nexsolutions, Ltd.
- NEC Networks & System Integration Corporation
- NEC Network and Sensor Systems, Ltd.
- NEC Fielding, Ltd.
- NEC Fielding System Technology, Ltd.
- NEC Platforms, Ltd.
- Infosec Corporation
- KIS Co., Ltd.
- Cyber Defense Institute, Inc.
- Sunnet Corporation
- YEC Solutions Inc.
- Q&A Corporation
- NEC Shizuoka Business, Ltd.
- NEC Aerospace Systems, Ltd.
- NEC Communication Systems, Ltd.
- Forward Integration System Service Co., Ltd.
- LanguageOne Corporation

2 Privacy Mark Certification

The following companies have been licensed by the Japan Information Processing Development Corporation (JIPDEC) to use the Privacy Mark.

NEC Group Companies with Privacy Mark

- NEC Corporation
- ABeam Consulting Ltd.
- ABeam Systems Ltd.
- NEC VALWAY, Ltd.
- NEC Solution Innovators, Ltd.
- NEC Nexsolutions, Ltd.
- NEC Networks & System Integration Corporation
- NEC Networks & System Integration Services, Ltd.
- NEC Net Innovation, Ltd.
- NEC Facilities, Ltd.
- NEC Fielding, Ltd.
- NEC Fielding System Technology, Ltd.
- NEC Platforms, Ltd.
- NEC Magnus Communications, Ltd.
- NEC Management Partner, Ltd.
- NEC Livex, Ltd.
- KIS Co., Ltd.
- Sunnet Corporation
- Nichiwa
- brees corporation
- Bestcom Solutions Inc.
- YEC Solutions Inc.
- Q&A Corporation
- KIS Dot_i Co., Ltd.
- K&N System Integrations Corporation
- NEC Shizuoka Business, Ltd.
- NEC Communication Systems, Ltd.
- D-Cubic Corporation
- Forward Integration System Service Co., Ltd.
- LanguageOne Corporation
- LIVANCE-NET, Ltd.

3 IT Security Evaluations and Certifications

The following lists major products and systems that have obtained ISO/IEC 15408 certification, an international standard for IT security evaluations. (The list includes products on certified product archive lists.)

NEC products and systems with ISO/IEC 15408 certification

- DeviceProtector AE
  (information leak prevention software product)
- InfoCage PC Security
  (information leak prevention software product)
- NEC Group Information Leakage Prevention System
  (information leak prevention software product)
- NEC Group Secure Information Exchange Site
  (secure information exchange system)
- NEC Firewall SG
  (firewall)
- PROCENTER
  (document management software product)
- StarOffice X
  (groupware product)
- WebOTX Application Server
  (application server software product)
- WebSAM SystemManager
  (server management software product)

NEC Group Profile

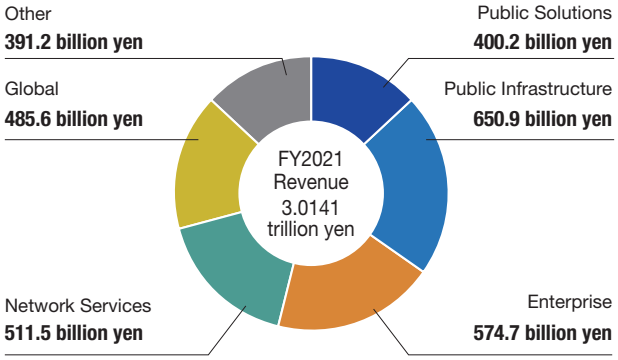
Corporate Profile

Company name	NEC Corporation
Address	7-1, Shiba 5-chome, Minato-ku, Tokyo, Japan
Established	July 17, 1899
Capital	427.8 billion yen*
Number of employees (Consolidated)	117,418*
Consolidated subsidiaries	289*

*As of March 31, 2022

Segment Information

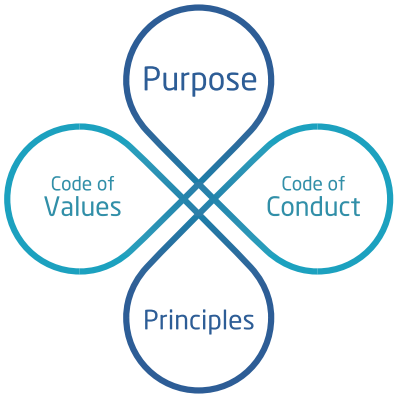
Sales Revenue by Segment (Percentage)



*As of March 31, 2022

NEC Way [Management Policy]

NEC Way



The NEC Way is a common set of values that form the basis for how the entire NEC Group conducts itself.
Within the NEC Way, the "Purpose" and "Principles" represents why and how as a company we conduct business, whilst the "Code of Values" and "Code of Conduct" embodies the values and behaviors that all members of the NEC Group must demonstrate.
Putting the NEC Way into practice we will create social value.

Purpose

\Orchestrating a brighter world

NEC creates the social values of
safety, security,
fairness and efficiency to promote a
more sustainable world
where everyone has the chance to
reach their full potential.

Code of Values

Look Outward. See the Future.
Think Simply. Display Clear Strategy.
Be Passionate. Follow through to the End.
Move Fast. Never Miss an Opportunity.
Encourage Openness. Stimulate
the Growth of All.

Principles

The Founding Spirit of "Better Products, Better Services"
Uncompromising Integrity and Respect for Human Rights
Relentless Pursuit of Innovation

Code of Conduct

1. Basic Position
2. Respect for Human Rights
3. Environmental Preservation
4. Business Activities with Integrity
5. Management of the Company's Assets and Information

Consultation and Report on Doubts and Concerns about Compliance

Information Security Report 2022

NEC Corporation

7-1, Shiba 5-chome, Minato-ku, Tokyo 108-8001, Japan
Tel: 03-3454-1111
https://www.nec.com/

Issued July 2022