\Orchestrating a brighter world NEC

Information Security Report 2021

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

In recent years, our society has been at a major turning point as new business models and schemes are being created as a result of DX*. While the progress of the work style reform has enabled people to choose new work styles and helped companies grow and develop innovations, a number of security issues have arisen from it.

In these social circumstances, NEC is shifting its information security approach from the conventional boundary defense to a security platform based on the concept of zero trust, a protection framework in which no access is granted without verification.

We are driving cybersecurity measures 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 goals include enabling early detection, damage minimization and rapid recovery (cyber resilience) for increasingly sophisticated cyberattacks, while providing highly secure products, systems and services through Security by Design (SBD) concept, and stepping up the information security level of the entire supply chain.

In May 2021, we revised the NEC Group Information Security Statement to declare our commitment to the group-wide security governance and an information management system and framework designed with business risks in mind. Based on this statement, we will drive our security efforts with a comprehensive approach in various information security domains from management to infrastructure and personnel. At the same time, by developing, testing and providing security solutions featuring our unique AI and automation technologies, we aim to continue to be a trusted company.

Under the company's corporate message of "Orchestrating a brighter world," NEC will use ICT to solve various social issues and contribute to the realization of a safe, secure, efficient, and equal society where everyone has the chance to reach their full potential. This report introduces the NEC Group's information security activities related to the ICT business. We hope that you read this report and find it informative.

* DX: Digital Transformation. A concept of creating new value and changing life and business style for the better by digitizing real-world events, integrating them with the cyber world, and connecting people, things, and events.

For inquiries regarding this report, please contact:

CISO Office
Management Information Systems Division
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 2021"

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 2021.

Contents

NEC's Approach to Information Security ····· 2

On the Publication of "Information Security Report 2021" ····· 3

NEC's Information Security Report

Information Security Promotion Framework Direction 1 ····· 4

Information Security Governance Direction 2 ····· 5

Information Security Management Direction 2 Direction 6 ····· 6

Information Security Infrastructure Direction 3 Direction 5 ····· 8

Information Security Personnel Direction 3 ····· 12

Measures Against Cyberattacks Direction 4 Direction 5 Direction 7 Direction 8 Direction 10 ····· 14

Information Security in Cooperation with Business Partners Direction 9 ····· 16

Providing Secure Products, Systems, and Services Direction 2 Direction 4 ···· 18

Leading Edge of NEC's Information Security

Development and Global Deployment of a Zero Trust Security Platform ··· 20

NEC's Cybersecurity Strategy ····· 24

Cases of R&D of the Leading-edge Cybersecurity Technology ····· 28

Third-party Evaluations and Certifications ····· 30

NEC Group Profile ····· 31

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

NEC 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 contribute to realizing a more sustainable world where everyone has the chance to reach their full potential.

NEC is implementing anti-cyberattack measures and providing secure products, systems and services as well as promoting information security 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.

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.

2 Information Security Promotion Organizational Structure of the NEC Group

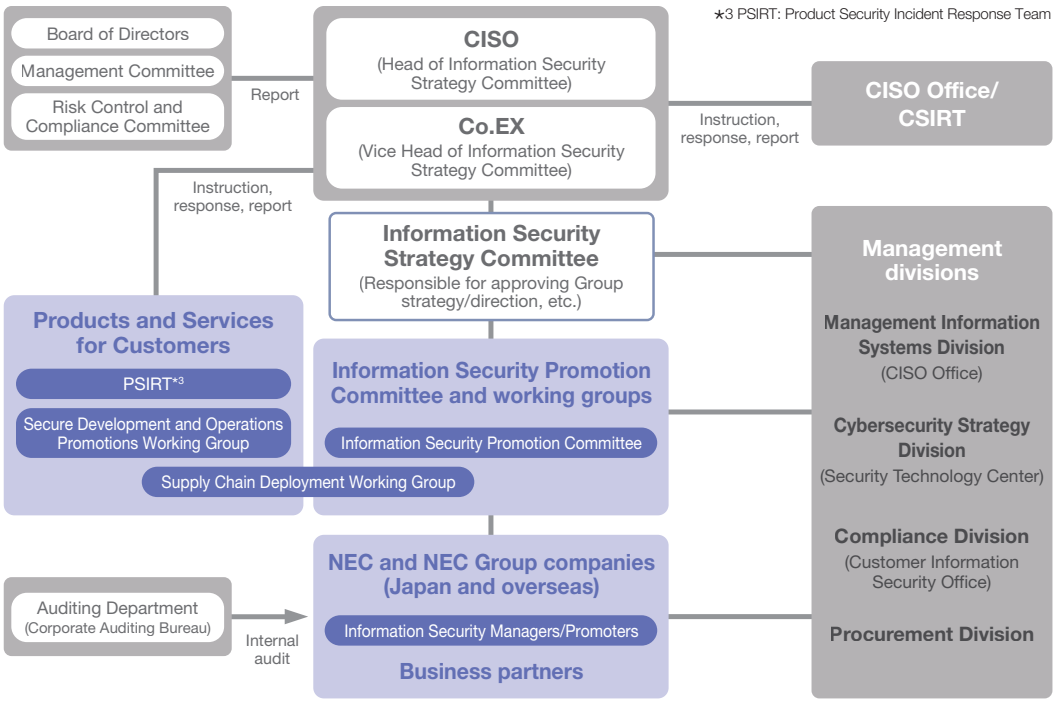
The information security promotion organizational structure of the NEC Group consists of the Information Security Strategy Committee, its subordinate organs, and other relevant organizations. The Information Security Strategy Committee, headed by the CISO*1, 1) evaluates, discusses, and improves information 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 cybersecurity 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 secure development and operations initiative, 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.

*1 CISO: Chief Information Security Officer
*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 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, 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 2017, as well as with revisions made to the JISQ 15001 standards, we have revised the personal information protection rules and manuals, along with the GDPR*1-compliant NEC guidelines.

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 2020, 29 NEC Group companies have acquired Privacy Mark certification.

*1 GDPR: The EU General Data Protection Regulation

NEC Group Information Security Statement

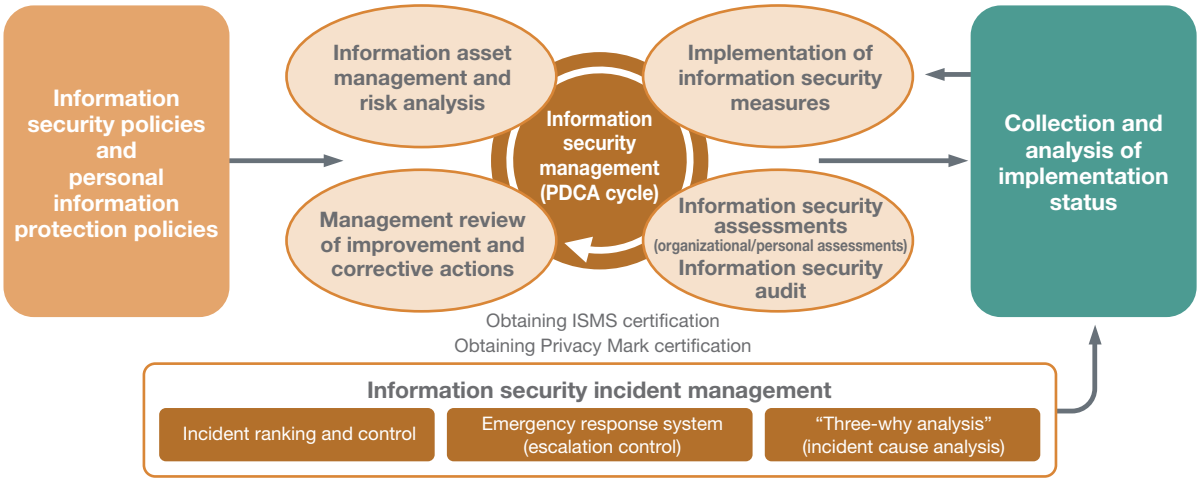
https://www.nec.com/en/global/iss/index.html

3 Information Security Risk Management

❶ Information Security Risk Assessment

The NEC Group assesses risks and takes 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 according to the Information Security Risk Assessment Standards.

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 » Information Security Assessments

❶ Details of Information Security Assessments

Based on the analysis of information security incidents, we set priorities for our assessment to eliminate information leaks. Surveys are conducted to identify whether required security measures are implemented, and if not, what are the obstacles. The assessment is intended to help respondents realize what is required to secure their environment and to raise their awareness for improvement. Specifically, our assessment focuses on such subjects as protection of critical and personal information, external contractor management, and information security awareness.

❷ Information Security Assessment Methods

Our information security assessment is conducted both for individual employees and managers in terms of execution and management of required security measures. The gaps between employees and managers are analyzed to improve the accuracy of the assessment.

❸ Improvements Leveraging Assessment Results

If there is any measure that failed to be sufficiently implemented, we find out the reason for the failure and make improvements. At the same time, we analyze trends in the entire NEC Group and solve the remaining problems. If further enhancements are needed, we continue to enhance our security in the information security promotion plan for the following fiscal year.

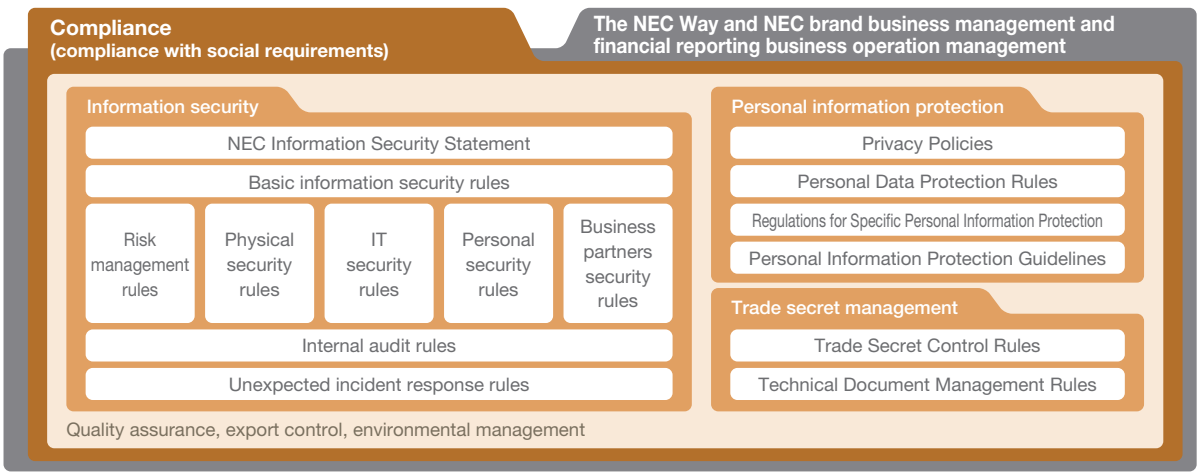
5 » Information Security Audits

NEC's Corporate Auditing Bureau drives internal 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

For protecting personal and confidential information entrusted by customers,
NEC has information security infrastructure in place based on Zero Trust and other security concepts that enables safe, secure and efficient promotion of business activities and projects.

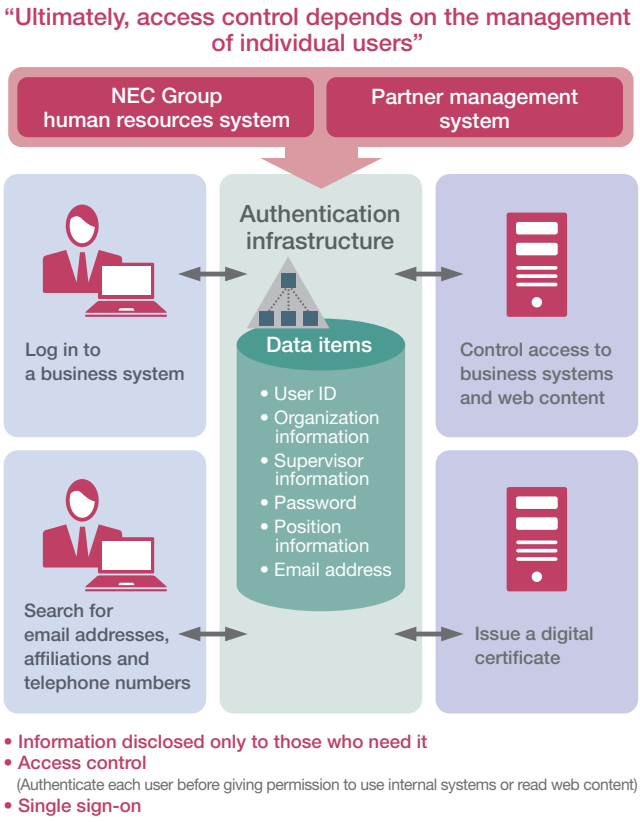
1 ≫ Features and Configuration of Information Security Infrastructure

Three platforms composing the information security infrastructure interact with and complement one another to achieve NEC's information security. These are the information and communications technology (ICT) platform for user management and control, the ICT platform for PC and network protection, and the ICT platform for information protection.

2 ≫ IT Platform for User Management and Control (Authentication Infrastructure)

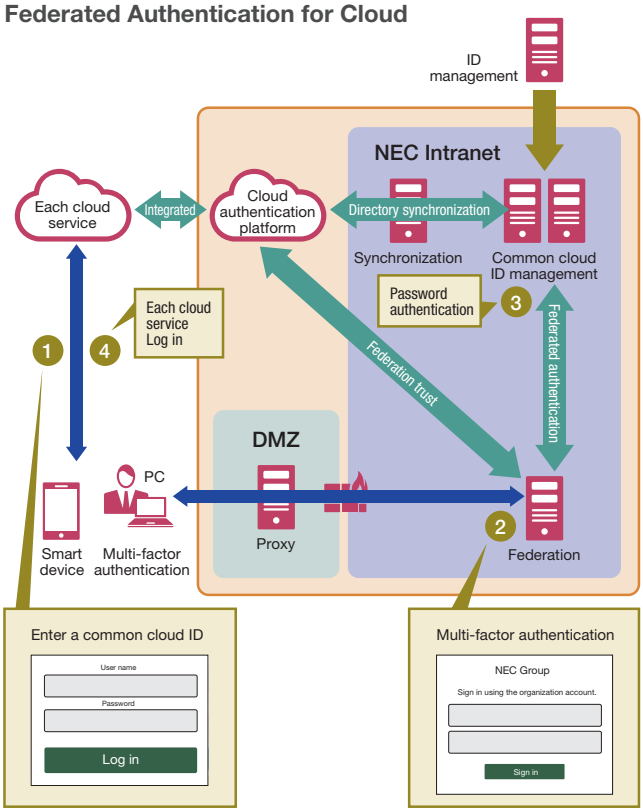
Authentication is the most fundamental and essential part of information security management. Identifying and authenticating individuals enables proper control of access to information assets and prevents spoofing and other fraudulent activities.
It is important to identify and authenticate users and 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 introduction 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.

NEC Group Authentication Infrastructure



- Information disclosed only to those who need it
- Access control
  (Authenticate each user before giving permission to use internal systems or read web content)
- Single sign-on

Federated Authentication for Cloud



3 IT Platform for PC and Network Protection

NEC has constructed a global ICT platform to maintain the security of information devices connected to the NEC Intranet and protect the PCs and networks from viruses and malware. Recently, multi-layered information security measures have become necessary to counter APT attacks*1 toward the NEC Group. As one of such measures, we consider it crucial to install all necessary security updates and virus definition files on information devices.

*1 APT attacks: Advanced Persistent Threat attacks

❶ Protecting PCs from Viruses and Malware

• Support for user environments

NEC Group employees are required to install software to monitor the status 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.

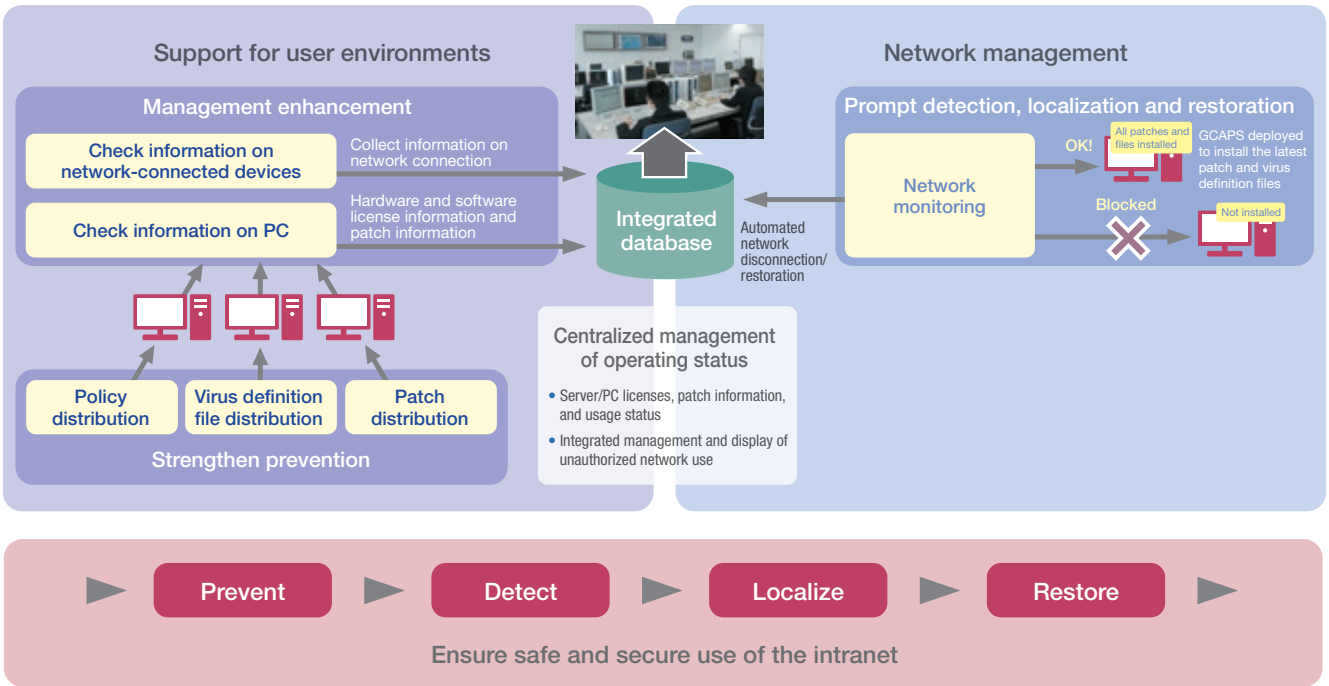
• Network management

In addition to visualizing the PC status, when a PC for which security measures have not sufficiently been implemented is connected to the intranet or malware is detected in a segment of the intranet, that PC or network segment is then 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 SPF authentication to specify domains allowed for sending emails.

• 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.

Protection of PCs and Networks from Viruses and Malware



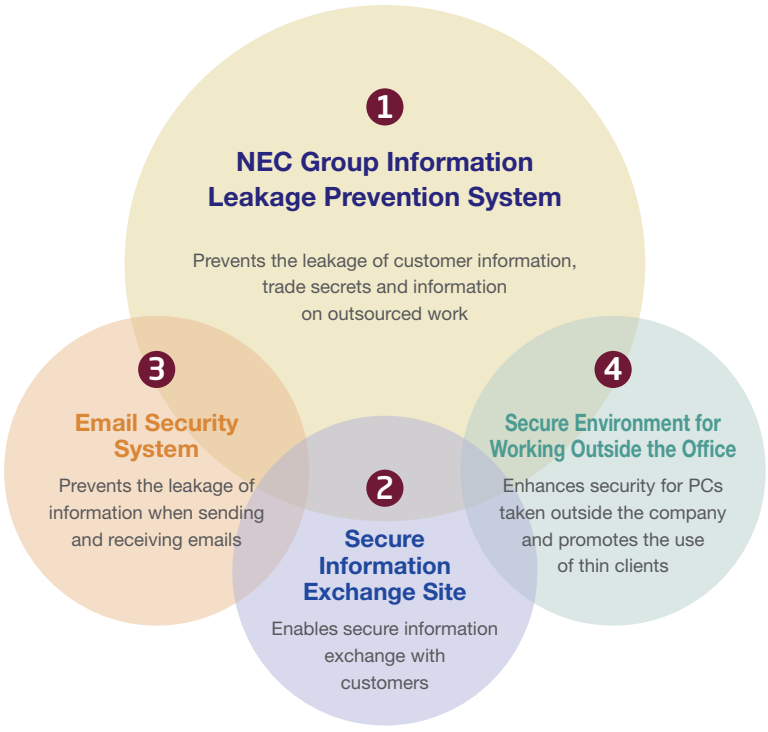
4 IT Platform for Information Protection

Preventing information leaks requires risk analysis to identify possible information leakage paths and take appropriate measures for protection. As NEC manages invaluable information entrusted by the customers and business partners in addition to its own, we are taking a comprehensive and multi-layered approach for blocking possible information leakage paths while considering the risks and characteristics of digital devices.

❶ NEC Group Information Leakage Prevention System

NEC's 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 default to keep a certain security level throughout the 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 as it has been 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. For the case if such devices are needed for work, we have defined 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 incident of 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, security settings, physical entry controls and contractor management.

Overview of IT Platform for Information Protection



❷ Secure Information Exchange Site

NEC developed and operates the “Secure Information Exchange Site” service for exchanging important information with customers and business partners. In the service, users can exchange information securely as access is restricted by one-time URLs and passwords. Each one-time URL has a time limit, after which it becomes invalid. Also, after use, the information is deleted from the site.
The Secure Information Exchange Site reduces the need to exchange information using external media such as USB flash drives or an unauthorized cloud service, which in turn reduces the risk of information leaks resulting from theft or loss.

❸ Email Security System

We have OMCA*2 for preventing information leakage incidents from occurring in sending and receiving emails. This add-in features special functions to alert the user about a suspicious email that may be an APT attack, to display a pop-up window prompting the user to check the destination address and attached file(s) before sending an email, and to delay the transmission of an email for a specified period of time, among other functions. These functions prevent information leaks through emails.

*2 OMCA: Outlook Mail Check AddIn

❹ Secure Environment for Working Outside the Office

To prevent information security incidents from occurring outside the company, NEC has built a digital workplace environment*3 so that employees can work outside the office in a secure manner.
When a PC needs to be taken out of the office, a thin client or a “Trusted PC” with enhanced PC data protection is used depending on the purpose of the work and the usage environment among other factors. Trusted PCs are equipped with a fully encrypted hard disk drive (HDD), a pre-boot authentication feature that launches before startup of the operating system (OS), remote data deletion/PC locking, a function to mitigate attacks that exploit unknown vulnerabilities, a feature to block autorun viruses, and others in order to counter increasingly sophisticated cyberattacks.

*3 Digital workplace environment:
A workplace environment digitized using various tools. It is a comprehensive platform that allows employees to work and share information anytime, anywhere in the same environment they have inside the company.

Secure Information Exchange Site

Illustration of Data Upload

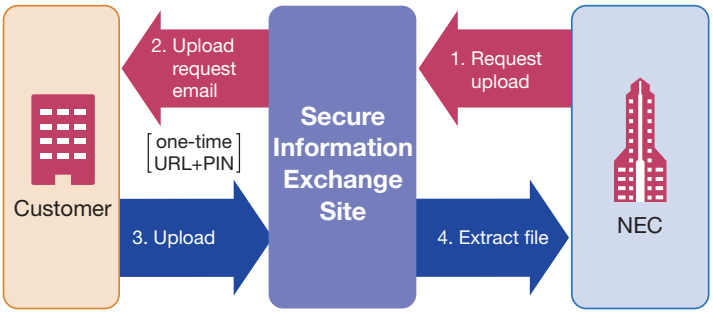
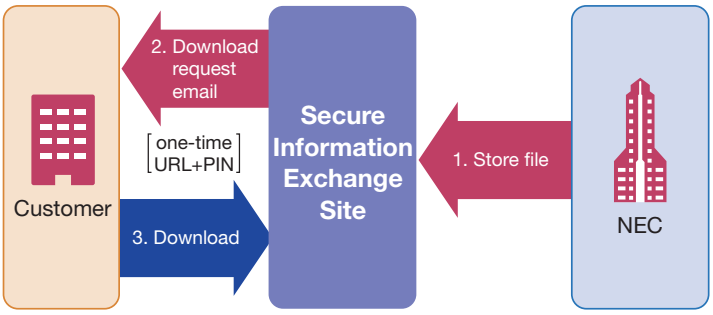


Illustration of Data Download



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) strengthening the knowledge and awareness of information security of all employees; 2) developing personnel who promote security measures; and 3) developing experts who can provide value to customers.

2 Strengthening Literacy and Awareness of Information Security

Knowing how to properly handle information and having a high level of awareness of information security are important to maintain and improve 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 web-based training (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 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

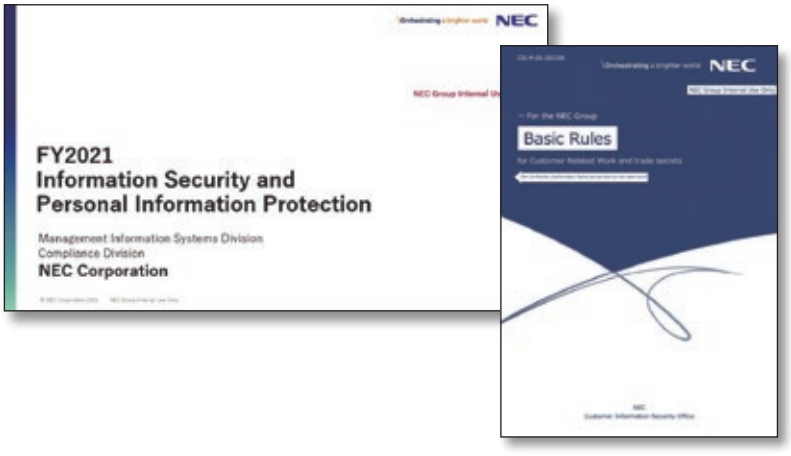
NEC performs awareness-raising activities using videos and other materials so that employees gain a greater sense of crisis concerning information security risks and learn how to think, decide, and act by themselves. Events such as workplace discussions encourage employees to improve their risk analysis and judgment skills.

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. In fiscal year 2020, the site started to provide remote training and, despite the impact of the new coronavirus disease (COVID-19), many engineers stepped up their security skills to protect customers' systems.

❷ Group-wide CTF

Since fiscal year 2015, NEC has held an in-house CTF*4 event called "NEC Security Skill Challenge" for all employees. A total of over 5,000 employees voluntarily participated, helping to expand the breadth of NEC's security personnel.

*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 SBD*5. The training is aimed at enhancing the security skills across the entire NEC Group.

*5 SBD: Security By Design

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. 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.

❺ NCSA (NEC Cybersecurity Analyst)

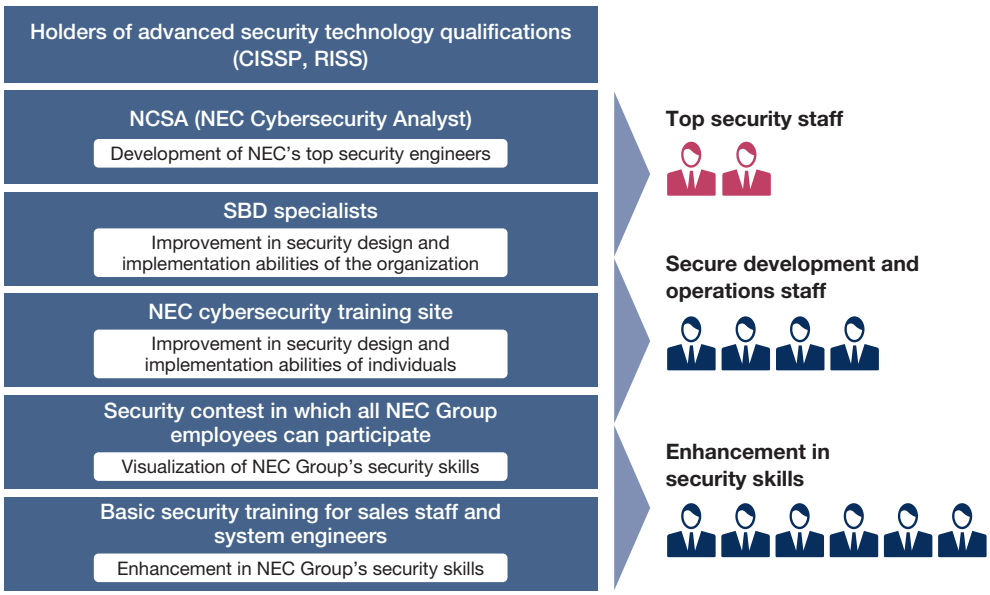
In fiscal 2020, NEC launched an NCSA (NEC Cybersecurity Analyst) program improved to better suit practical needs compared to the existing NEC CISO assistant training. The purpose of the program is to enhance the skills of top security staff. Intended for those staff members who have knowledge of security technologies, the six-month intensive program lets trainees master the technical skills required for advanced security services, such as CSIRT*6 work and risk hunting.

*6 CSIRT: Computer Security Incident Response Team

❻ Holders of Advanced Security Technology Qualifications

NEC strongly encourages its employees to acquire official qualifications for security and is increasing the number of staff who have obtained CISSP, an international certification, and RISS certification. Staff members who have advanced skills and qualifications in the information security field take the lead in providing customers with optimal solutions.

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: Cybersecurity Framework issued by the US National Institute of Standards and Technology (NIST) to enhance the cybersecurity of critical infrastructure.

2 Global Measures against Cyberattacks

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 attacks, 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. With the results of research and analysis, we consider countermeasures that will be needed in the future and determine the targeted scope while analyzing their effects and costs. We create a promotion plan every year based on the above-mentioned activities and, upon approval of the CISO*4, carry out the planned measures.
Our global measures against cyberattacks are being stepped up based on the concept of multilayered defense to counter ever sophisticated cyberattacks. These measures include education to employees such as annual training for targeted email attacks, entry/exit protection of networks, and internal control. We are focused particularly on the following seven points: (1) cyber risk assessment by the Red Team*5, (2) generation and use of threat intelligence, (3) advanced EDR*6, (4) enhancement of the CSIRT structure, (5) development and deployment of CSIRT-NDR*7, (6) enhancement of global security governance, and (7) 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.
*6 EDR: Endpoint Detection and Response
*7 NDR: Network Detection and Response

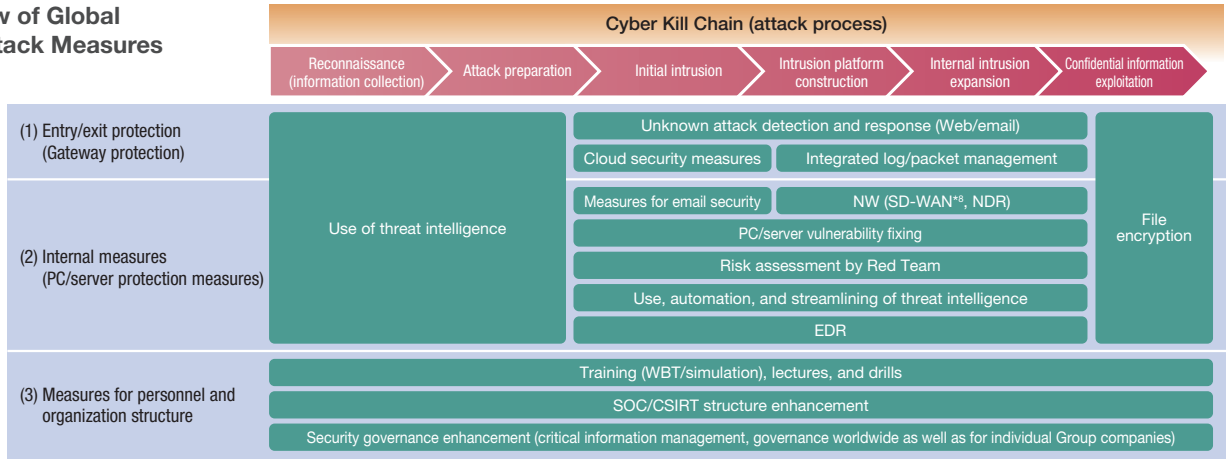
❶ Cyber Risk Assessment by the Red Team

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.

❷ Generation and Use of Threat Intelligence

Threat intelligence is used to identify threats to NEC including their early signs and to implement a proactive defense against advanced threats that cannot be blocked by conventional measures. The Cyber Threat Intelligence (CTI) team formed by high-level experts engages in threat hunting by leveraging external and internally developed custom

Overview of Global Cyberattack Measures



*8 SD-WAN: SoftWare-Defined Wide Area Network

CTI technologies to identify potential threats within the NEC Group. We also have established an advanced research framework for enhancement of our CTI, which enables us to generate intelligence proactively and analyze threats in details on our own.

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 CSIRT Structure Enhancement

The CISO has a CSIRT structure under its direction. CSIRT members monitor cyberattacks, analyze the characteristics of detected attacks and malware, and share information with related organizations. In the event of a security incident, they protect the internal systems and analyze the attack to identify the cause and resolve the situation.
The CSIRT consists of four teams: the CTI team that exploits threat intelligence, the incident response (IR) team that responds to incidents, the team at the security operations center (SOC) that monitors alerts from security devices 24/7 and the developer team that enhances tools, platforms and operation processes. For the overseas affiliates, we have a team in Singapore that constantly monitors for cyberattacks. This team shares threat intelligence on detection status, unauthorized communication destinations, etc. on a global basis in conjunction with the CSIRT in Japan.
If a security incident occurs, the CSIRT collaborates with the related departments and, upon approval of the CISO, deals with the incident handling process up to recovery, while taking into account the risks involved.

❺ Development and Deployment of CSIRT-NDR

The developer team in the CSIRT is engaged in research, development, and deployment of unique NDR technology to step up the monitoring of internal networks such as the intranet and Infrastructure as a Service (IaaS), to enhance security incident investigations, and to detect suspicious communications through the proactive use of threat intelligence.

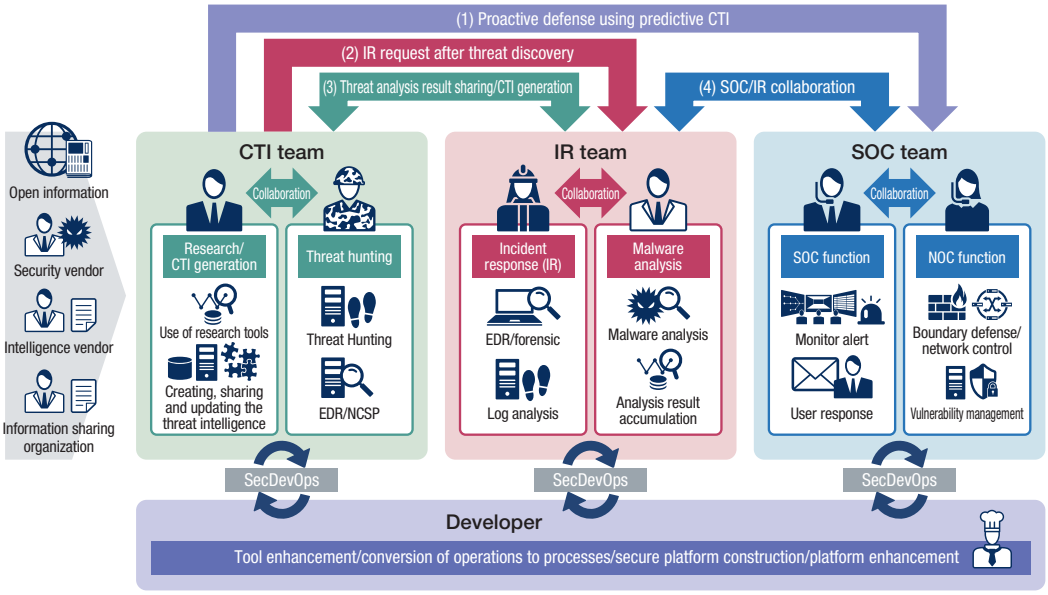
❻ Enhancement of Global Security Governance

NEC has a regional CISO 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.

❼ Critical Information Management

We strictly protect and manage critical business information based on the concept of the “Three Lines of Defense”. The first line of defense is formed by individual business divisions that take responsibility for managing critical information as risk owners. The second line of defense is a function for establishing rules regarding critical information management, checking the implementation status of the rules and providing advice. In the third line of defense, the Corporate Auditing Bureau performs internal audits to ensure that information is managed appropriately through all the applicable measures within the company or organization.
Especially for trade secrets and other critical information that will have huge impact on NEC’s business management or performance if leaked, we have a special secure storage service to protect them in a most stringent environment.

CSIRT System Enhancement



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. These guidelines include conducting development according to secure coding protocols and performing vulnerability diagnoses before releasing products, systems, and services.

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 1,500 companies, including approximately 750 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 Use of Videos to Maintain Awareness

NEC distributes educational videos to business partners and encourages their use for in-house education. The themes of past videos include compliance, confidential information management, cyberattacks, virus infections, loss of data when drunk, secure email distribution, personal information protection, and incident response.

❹ Operation of Examination System

NEC creates and distributes examination sheets to business partners to ensure thorough implementation of the "Basic Rules for Customer Related Work." We encourage them to use these examination sheets for in-house education as well as to see where they rank among all our business partners.

❺ 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.

❻ 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

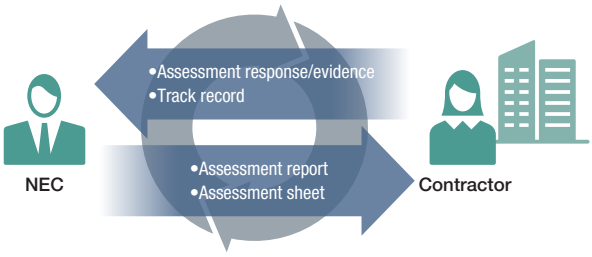
This assessment is conducted every year on about 50 companies that do large volumes of business with NEC. Approximately 100 assessors authorized by NEC visit business partners for on-site assessments or perform remote assessments.

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

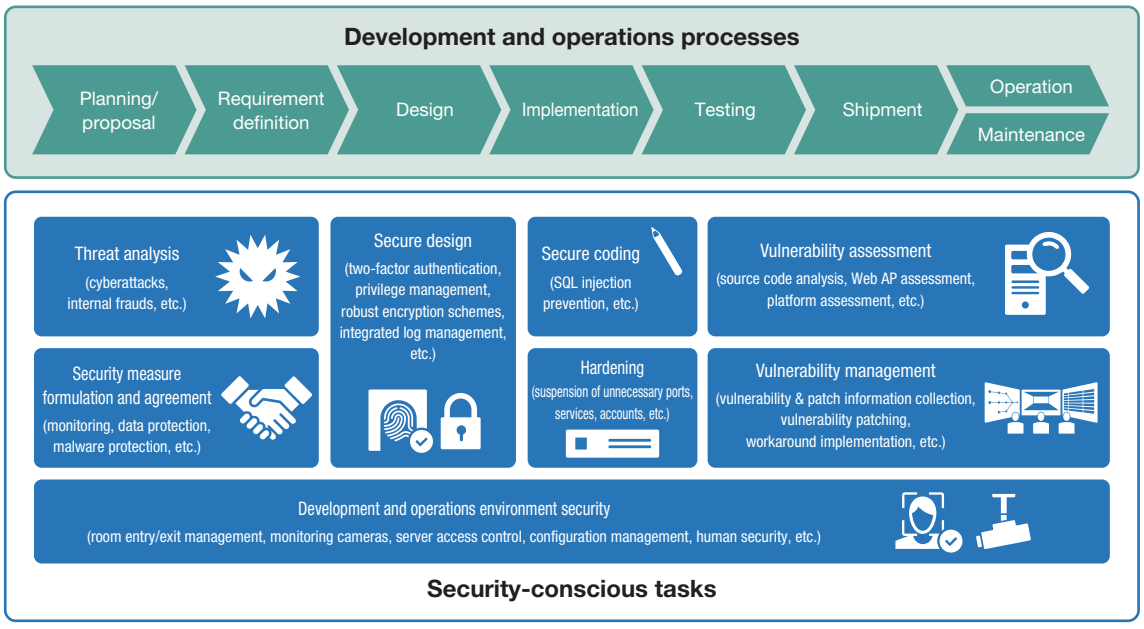
❶ Group-wide Promotion Structure

In order to enable secure development and operations for the products, systems, and services we offer to our customers, the NEC Group has created a secure development and operations promotion structure. This promotion structure consists of security managers appointed in each of the business divisions.
The security managers discuss proposed measures for secure development and operations directed at the eradication of information security incidents caused by product, system, and service vulnerabilities, misconfiguration, and system failures, and share information on the implementation progress of adopted measures. The security managers ensure that the secure development and operations measures are fully disseminated within their respective divisions, carry out implementation status inspections, and continuously work on improvements.

❷ NEC’s Secure Development

Based on the security by design (SBD) concept for ensuring security, NEC implements secure development and operations for 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 in early stages for the customer’s system environment.
NEC has defined the “Standards for Implementing Secure Development and Operations” as the baseline security requirements to be considered during development and operations. 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 guidelines.

Secure Development and Operations Processes



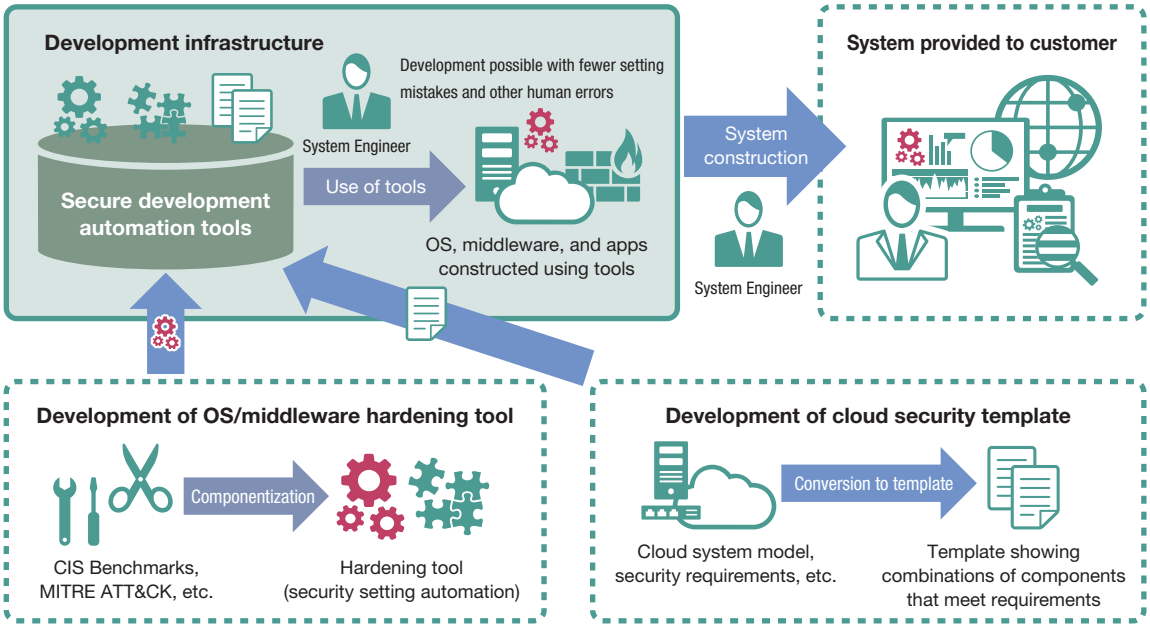
In the development of products, systems, and services, we have created a checklist to ensure that security measures are implemented in each phase. Based on this checklist, business projects are managed and the status of security measures are efficiently assessed and audited using the “Secure Development and Operations Assessment System” developed to visualize the implementation status of security measures.
In fiscal year 2020, we created a prototype baseline for privacy evaluation based on privacy-related laws, regulations, and guidelines (NIST Privacy Framework, ISO 29100/29134, etc.). We are now verifying the effectiveness of this baseline in order to establish a technique for comprehensively checking risks that may affect business continuity, such as lack of privacy considerations in addition to cybersecurity.

❸ Secure Development Automation Tools

As stated earlier, NEC conducts system development in accordance with the Standards for Implementing Secure Development and Operations. However, there still remain problems, such as staff members failing to include necessary security items because of their unique security settings or misconfiguration due to human error when building security into the development process.
To solve these problems, NEC has built secure development automation tools. One of them, for example, is the OS/middleware hardening tool, which automatically configures secure settings in a server. Also, for the building of cloud environments that have been increasing rapidly in recent years, we have a technology to implement homogeneous security across the entire environment. Specifically, we are driving efforts to distribute a secure cloud environment as a template, by using the IaC*1 technology to describe the cloud environment as code.

*1 IaC: Infrastructure as Code

Secure Development Automation Tools



Development and Global Deployment of a Zero Trust Security Platform

A rapid increase in the number of people who work remotely is making zero trust security more important than ever. NEC has expanded the scope of zero trust security to cover not just its internal and external business environments but its global operation sites as well in pursuit of thorough risk mitigation and security.

1 Increase of Remote Workers and Security Risks

The year 2021 has witnessed a drastic change in both the internal and external business environments due to the new coronavirus disease (COVID-19). At NEC, roughly twice as many employees as before now work remotely, with the number of remote access users increased by about 2.3 times. The volume of network traffic, the number of devices connected remotely and the use of remote tools are also increasing sharply. In these circumstances, risks like the following ones that may lead to security incidents have emerged.

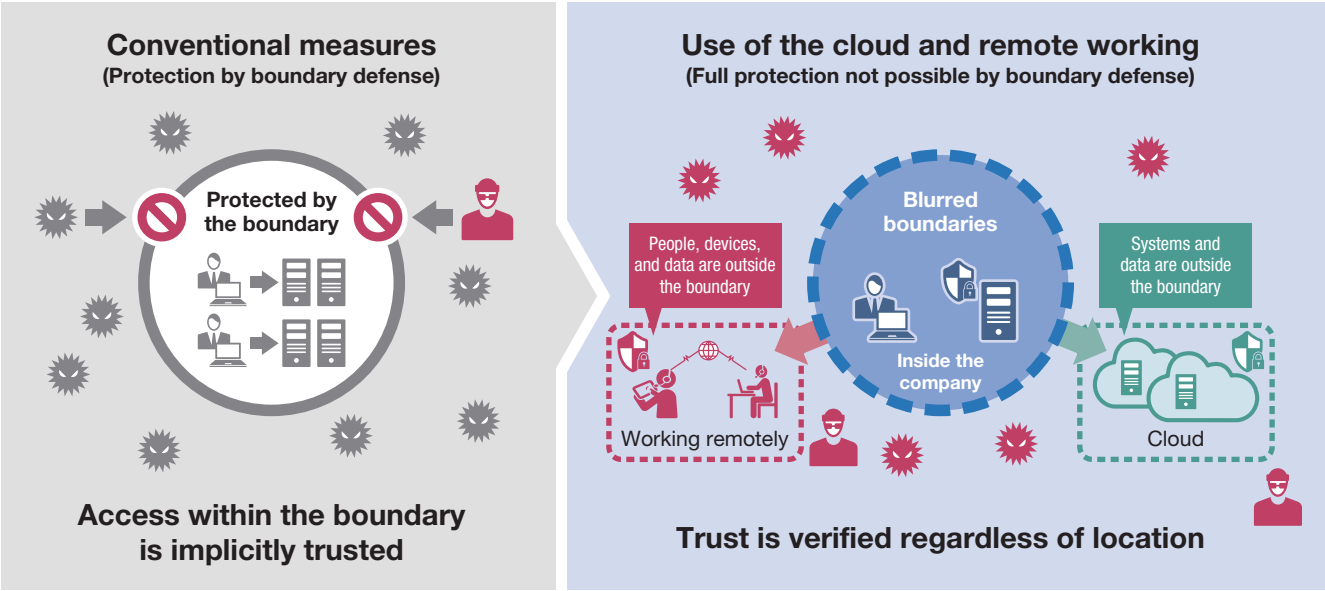
Device risks	As more employees work from home or a satellite office, risks increase such as data leaks from their devices, uninstalled software security patches, insufficient malware protection, and screen peeking.
Cloud risks	These risks include the use of a vulnerable or unsecured cloud services, access to an improperly configured cloud system, and unauthorized service access by spoofing.
System risks	These risks refer to unauthorized access to a remote access server (RAS) in the company's system, attacks against the RAS, and system outage or a business continuity failure in the case of a disaster.

NEC has a robust security framework in place to counter these risks and is implementing various security measures both inside and outside the company.

2 New Reforms in Line with Social and Business Issues

For over 30 years, NEC has been committed to creating DX environments that are easy to work in which individual employees can bring out the best of themselves. After opening satellite offices as early as 1987, the company introduced remote working for R&D members in 1993. In 2018, in line with the work style reform in progress, all employees of the entire NEC Group became eligible to remote work. In fiscal year 2019, just before the COVID-19 pandemic occurred, NEC received the 20th Telework Promotion Award and the Chairman's Award from the Japan Telework Association.
Building on these achievements, NEC is now engaged in a new reform of its security measures, taking into consideration the current social circumstances and business environment. Our conventional approach to security has been to rely on implicit trust with a particular focus on the use of internal systems and networks. With the aforementioned risks emerging as a result of the rapid increase in remote working, we are shifting toward the use of a more secure and safer network of constantly verifying trust. This is the "zero trust" approach whereby security risks are reduced by checking and verifying every access without blindly trusting specific network traffic.

Limitations of Boundary Defense Exposed by Increases in Remote Working and Use of the Cloud



3 Efforts to Eliminate Information Security Risks

NEC has taken up its security measures to another level, implementing a method whereby access is always verified on a zero trust security platform – that is, zero trust-oriented network infrastructure. We conduct a security assessment regularly on our internal digital workplace in accordance with the "Telework Security Guidelines" of Japan's Ministry of Internal Affairs and Communications (MIC). As for remote access systems (RAS), we perform emergency inspections and penetration tests not just in Japan but on a global scale as well.

To reduce the security risks of cloud services, we visualize the usage of the services by means of a CASB*1 and constantly monitor and control the services by tracking down internal fraud, detecting and preventing cyberattacks, and evaluating safety. In addition, we provide a training program to our employees every year on information security rules and measures, personal information protection and other issues to ensure they understand all that is required. As described above, NEC is taking a multifaceted security approach to the risks that have emerged with the sudden increase of remote working in order to keep our business operations secure.

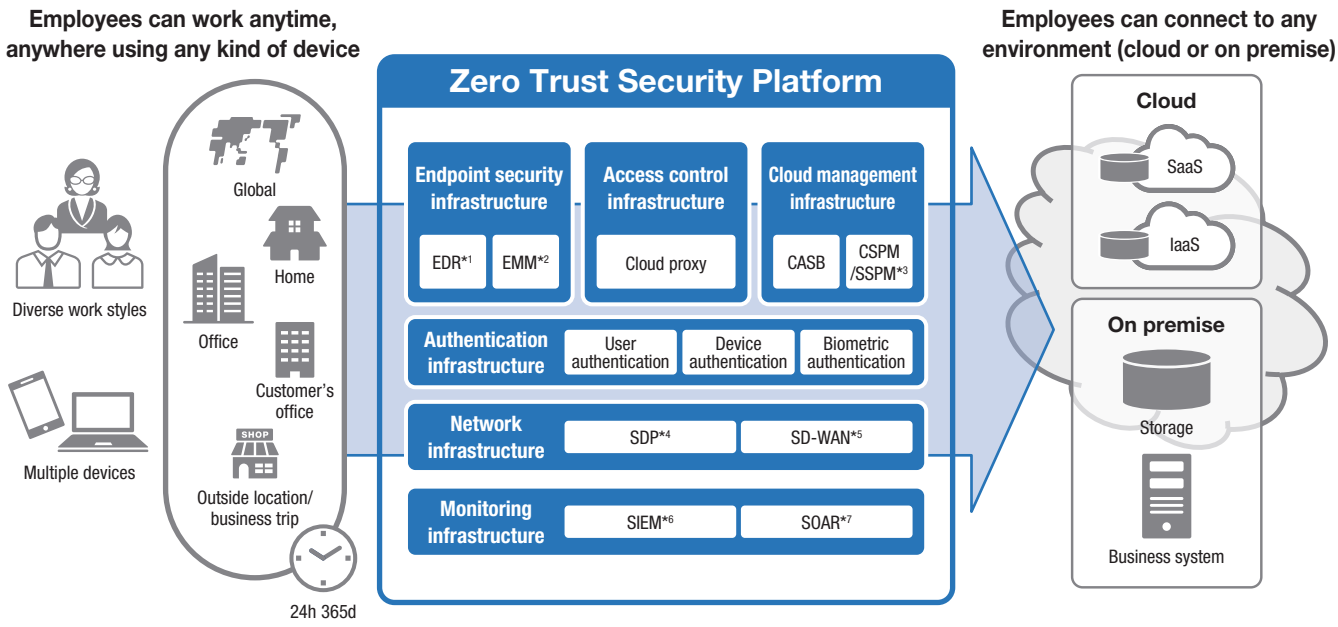
★1 CASB (Cloud Access Security Broker):
A tool to visualize and control the usage of cloud services.

4 Global Deployment of a Zero Trust Security Platform

NEC is expanding its zero trust security platform to its overseas operation sites. As of 2021, the Internet access infrastructure including proxy and RAS servers of the overseas operation sites is operated and managed in accordance with a globally standardized policy by using cloud infrastructure. We design individual cloud security features as an integrated platform rather than running those features separately to achieve zero trust.

While deploying the zero trust security platform on a global scale, NEC is centralizing management for risk blocking, implementing security detection capabilities and adopting an allow list for operations management. We plan to continue enhancing security features on this platform in a step-by-step manner.

Overview of the Zero Trust Security Platform



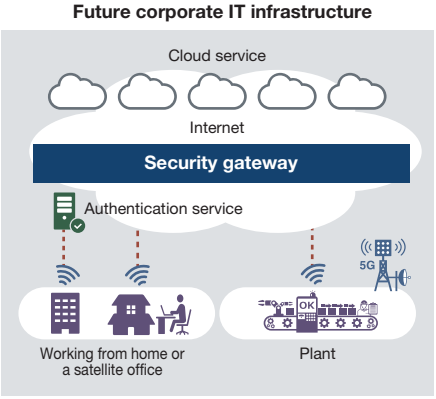
★1 EDR: Endpoint Detection and Response ★2 EMM: Enterprise Mobility Management ★3 CSPM/SSPM: Cloud/SaaS Security Posture Management ★4 SDP: Software Defined Perimeter
★5 SD-WAN: Software Defined WAN ★6 SIEM: Security Information and Event Management ★7 SOAR: Security Orchestration, Automation and Response

5 Products, Systems, and Services to Achieve Zero Trust

While NEC has been promoting a digital workplace through a work style reform, the COVID-19 pandemic has rapidly entrenched remote working into our society as well as in the business community. On the other hand, new risks and issues regarding information security have become noticeable (see page 20). Customers are concerned about the security of PCs taken off the premises as well as the security of virtual private networks (VPN) used for remote working. They also want to boost defense against targeted attacks, visualize the configurations of internal and external terminals, enable faster distribution of software patches, and have encryption to prevent data leaks. We provide products, systems, and services that meet the various needs of these customers seeking to implement zero trust.

In order to quickly deliver the zero trust security platform to customers, NEC is offering a suite of security solutions in collaboration with internationally renowned vendors. This section presents NEC's services that are indispensable for zero trust migration along with some of the deployment successes.

Overview of Zero Trust Security Measures



Layer	Concrete measure
Concept planning	Creation of plans to enhance cloud security
Cloud	Creation of security rules regarding cloud usage
	System development based on security by design
	Visualization of cloud usage, security assessment, and access control (CASB) *CASB: Cloud Access Security Broker
Gateway	Cloud firewall service, cloud proxy service, remote access service, and secure mail service
ID management	ID management for cloud users & authentication and authorization for cloud usage
Network	SD-WAN (Software Defined-WAN)
Device	Enhanced anti-malware measures (EPP/EDR), enhanced mobile device management (MDM/MAM) and data protection (encryption)

Solution Example: Palo Alto Networks Prisma Access

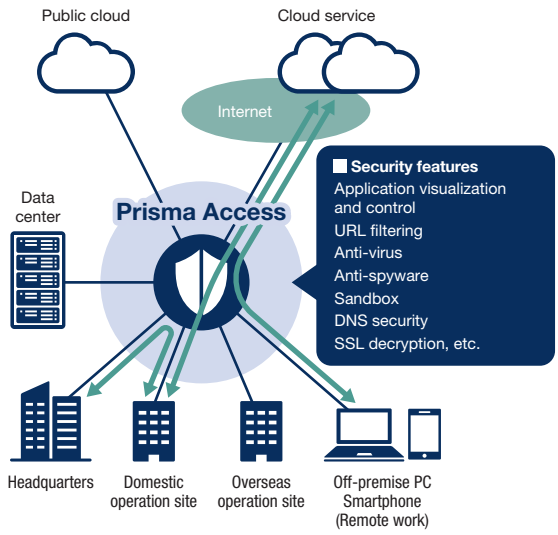
Crisis

- Concern exists about the security levels of PCs and smart devices that are connected from outside the company during remote working.
- Unstandardized security policies of overseas operation sites pose security risks.
- Increases in cloud usage and remote working have resulted in data center congestion and increased loads on network equipment.

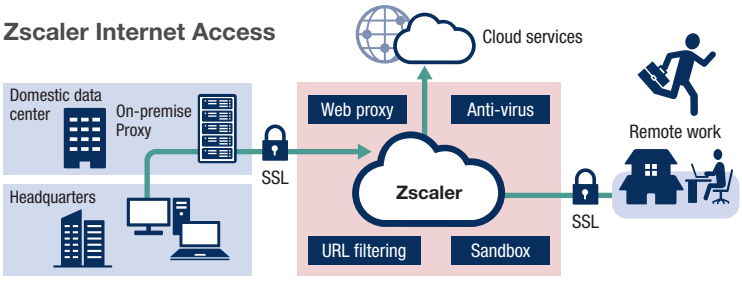
Solution

- Perform a security check based on device information and restrict communications from terminals with low security levels to the internal network.
- Manage security policies in a centralized manner to step up the security of overseas operation sites.
- Move the firewall capability to the cloud and let Internet communications go directly via Prisma Access, thus reducing traffic concentration to the data center.
- Integrate the firewall, proxy, and VPN capabilities into one to reduce the operation management costs.
- Routing internal communications (e.g. between the headquarters and an operation site) through Prisma Access makes it possible to protect and monitor the security of all these communications.

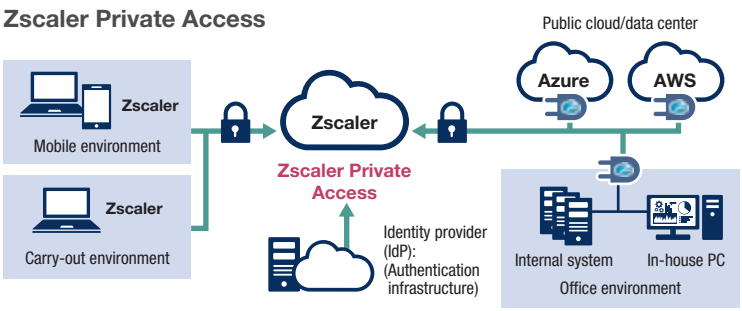
Prisma Access



Zscaler Internet Access



Zscaler Private Access



Solution Example: Zscaler Internet Access

Crisis

- Standardized Web security measures are not in place for the remote work environment, overseas affiliated companies, group companies, etc.
- In-house PCs directly connect to the Internet, leading to an increased risk of malware infection.

Solution

- Routing Web communications from remote workers via a Web proxy enables company-wide Web security measures to take effect regardless of the access location.
- Reduce risks significantly by providing strong protection against malware infection from the Web.
- Cloud services allow the solution to be deployed for operation in a relatively short time, quickly implementing terminal security.
- Integrate the capabilities of multiple existing devices (firewalls, proxy servers, etc.) to reduce the operation costs.

Solution Example: Zscaler Private Access

Crisis

- VPN equipment is used for access during remote working, but the security measures for the equipment are problematic.
- Standardized access control is not available for resources scattered inside the company and in the cloud, leading to high operation loads.

Solution

- Establish secure remote access infrastructure for the cloud without the need for vulnerability handling and sizing for the on-premise VPN equipment.
- Implement advanced security measures while at the same time reducing security operation loads.
- Manage remote access to scattered resources in an integrated manner, and exercise control using a standardized access policy.
- Use cloud services to cut deployment and operation costs.

Solution Example: ActSecure Security Risk Management Service

Crisis

- Since distributing software patches puts a load on the network, patch distribution during the daytime has an enormous impact on routine business.
- Conventional on-premise management is no longer sufficient because of the need to manage terminals outside the intranet.

Solution

- A unique communication system reduces the network load when Windows patches are distributed. (It only takes two days to apply a patch to 10,000 terminals running Windows 10.)
- The service is provided as SaaS (software as a service), enabling centralized management of the terminals regardless of the location.
- The solution ensures that the latest software patches are applied to all terminals, reducing infection risks from attacks exploiting software vulnerabilities.

Solution Example: ActSecure Cloud Secure File Service

Crisis

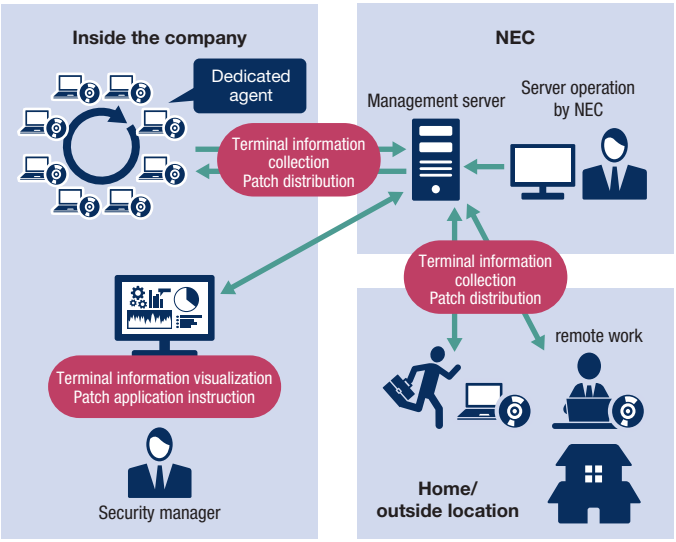
- A data leak due to unauthorized access or other types of attack can directly damage the credibility of a company, and such data leaks need to be prevented.
- It is desirable to introduce encryption software to protect confidential information, but there is concern about users forgetting to encrypt data or making human errors.

Solution

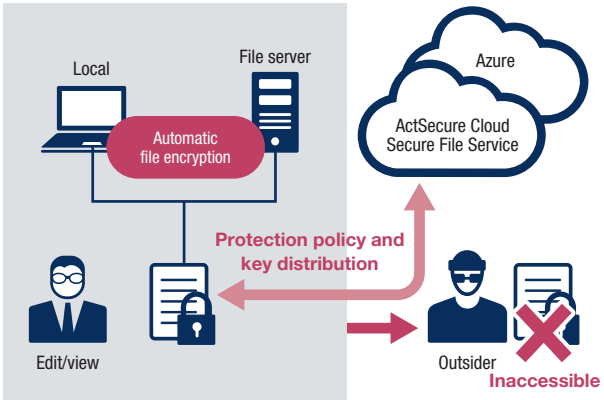
- Even if files are leaked due to unauthorized access, they are encrypted and their contents are inaccessible. This alleviates the risk of confidential information being leaked.
- The solution is based on the premise that files may get leaked and provides a method whereby files are automatically encrypted without depending on users to do so.
- The technique of automatically encrypting all files prevents data leaks resulting from unauthorized access.

In conclusion, it should be stressed that there is an urgent need to implement zero trust security so that employees can work securely anytime, anywhere. If you are concerned about your remote working environment or want to learn more about robust zero trust solutions, please feel free to contact us.

ActSecure Security Risk Management Service



ActSecure Cloud Secure File Service



NEC's Cybersecurity Strategy

By leveraging the collective strength of the entire Group to provide safe, secure, and comfortable social infrastructure and combat cyberattacks, which are a growing problem for the global community, NEC will help achieve an information society that is friendly to humans and the earth.

1 Basic Policies

In a keynote speech titled "Shaping the Communications Industry to Meet the Ever-Changing Needs of Society" in October 1977, the NEC Group put forth the concept of "C&C (Computer & Communication)" as its slogan for achieving the integration of computers and communications. In line with this declaration, we have been committed to connecting computers around the world. By connecting people with things and things with things, we have met diverse social needs and contributed to societal development.

With recent advances in DX*1 spurring drastic changes in the way people work, such as an increasing number of people choosing to telework, almost all things are getting connected to one another. In a world like this, it is possible that security risks are everywhere. To do business safely, cybersecurity is crucial more than ever.

NEC has accumulated and makes use of many technologies that have supported those parts of infrastructure that are vital to society, from domestic traffic control systems, disaster management and firefighting systems, production management and water management systems, ATMs, and logistics systems to those systems used on the ocean floor and in outer space. By doing so, we deliver total security solutions that fuse the physical and cyber worlds to the global market. Building on these achievements and know-how, NEC will contribute to the realization of a safe and secure society through cybersecurity.

*1 DX: Digital Transformation

NEC's Business Domains That Support Social Infrastructure

2 Contribution to Society

❶ Collaboration with Related Organizations

To strengthen information infrastructures against increasing cybercrimes, NEC is collaborating with related organizations in Japan and overseas.
In addition to participating in the Control System Security Center, we joined the Japan Cybercrime Control Center (JC3*2) in 2014. We have since been promoting collaboration among domestic academic research organizations, industries, and law enforcement bodies against cybercrimes. By returning the gains from these activities to society, we are contributing to the creation of a safe, secure, and comfortable environment.

*2 JC3: Japan Cybercrime Control Center

❷ Contribution to the Government's Initiatives

Nobuhiro Endo, Chairman of the Board, is a member of the Cybersecurity Strategic Headquarters (of the Cabinet) and heads the Industrial Cybersecurity Center of Excellence (of the IPA*3). With other officials also serving as members of a number of panels hosted by the government, NEC is actively contributing to national security projects. Through these activities, NEC aims to create a safe and secure society in which the government and the private sector work as one.

*3 IPA: Information-technology Promotion Agency

Collaboration with Related Organizations

Strengthening information infrastructures

Participation in Control System Security Center (CSSC) (November 2013)
CSSC is a public-private partnership project of the Ministry of Economy, Trade and Industry for ensuring the security of critical infrastructure equipment and control systems.

Participation in Japan Cybercrime Control Center (JC3) (November 2014)
This is an organization that gathers experience in dealing with threats in cyberspace across industry, academia, and law enforcement agencies.
It aims to neutralize the root of cyber threats and mitigate damage.
NEC Executive Vice President Kazuhiro Sakai serves as representative director.

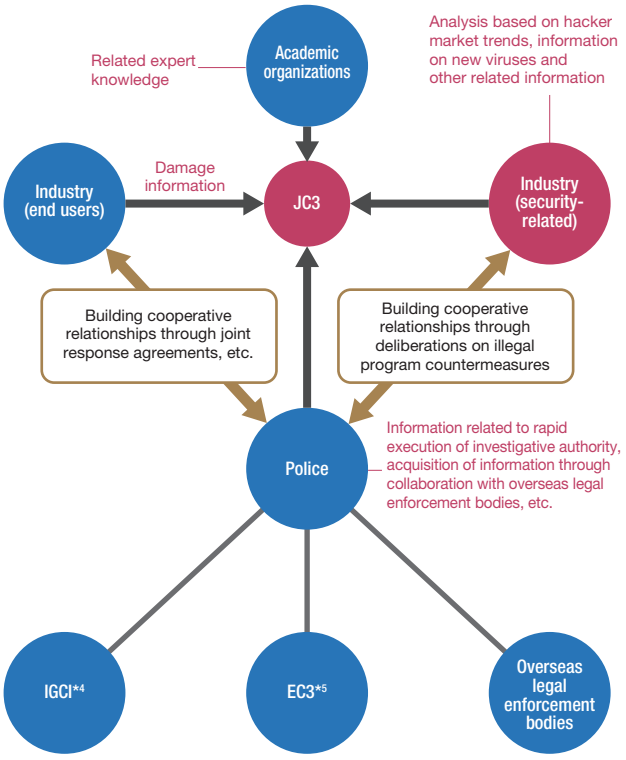
Participation in AIS* initiative of the U.S. Department of Homeland Security (DHS) for public-private sector intelligence sharing (March 2017)
NEC became the first Japanese company to join the AIS initiative of the U.S. Department of Homeland Security (DHS) for swiftly sharing intelligence on cyber threats between the government and the private sectors.
* Automated Indicator Sharing

Participation in ICT-ISAC launch (March 2017)
NEC participates in ICT-ISAC, which was established to enable a diverse group of operators to share information regarding the collection and analysis of information on cyberattack, etc. and countermeasures, and to counter threats as a collaborative and concerted organization, transcending the boundaries of the industry.
(NEC had been a participant of Telecom-ISAC, the predecessor of ICT-ISAC.)

Participation in the Cross Sector Forum for Cybersecurity Workforce Development (January 2016) (April 2017)
Together with NTT and Hitachi, Ltd., we established a study group for the development of cybersecurity personnel. In 2017, this study group was transferred to Cyber Risk Information Center (CRIC) to further step up efforts for information sharing.

Participation in CTA for information sharing among security firms (October 2018)
NEC joined the Cyber Threat Alliance (CTA), a U.S. NPO promoting the sharing of information on cyber threats among security firms.

Framework Centered on the Japan Cybercrime Control Center



*4 IGCI: The INTERPOL Global Complex for Innovation
*5 EC3: European Cybercrime Centre

3 World's Top-level Personnel and Technology

❶ Framework Enhancement for the Provision of Advanced Services

NEC continues to make investments not only in Japan but around the globe. We welcomed the Cyber Defense Institute, Inc. into our Group in 2013, followed by Infosec Corporation in 2014 and NEC Solucoes de Seguranca Cibernetica Brasil S.A in 2016 to promote the framework enhancement for enabling the provision of advanced services.

❷ Development of In-House Human Resources

The NEC Group is also directing its efforts to the development of security experts (for details, see "Information Security Personnel" on page 12). Some members of our taskforce won top prizes at international security skills competitions.

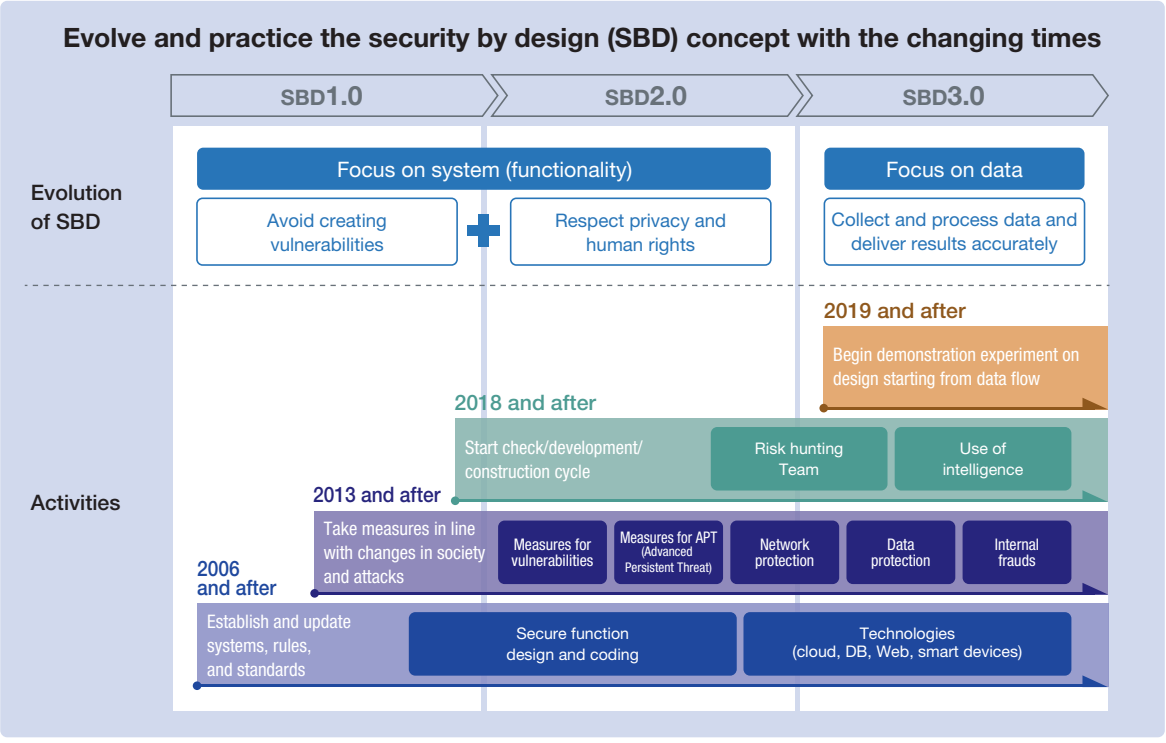
❸ Investments in the Development of Domestic Security Human Resources

By actively developing human resources through the endowed lecture series set up at the Japan Advanced Institute of Science and Technology, NEC is contributing to bolstering the base of security experts in Japan.

❹ Provision of Education Programs for Customers

The education programs offered by NEC include a variety of courses such as training for targeted email attacks. Our cyberattack training program in particular allows participants to learn the flow of actions in incident handling through actual experiences. We hope that these hands-on experiences offer a venue of realization for customers to improve their technical capabilities and to assess the sufficiency of the cybersecurity measures for the ICT platforms that support their business.

Concept of Secure Development and Operations Based on SBD 3.0



4 Thoroughly Secure Development and Operations

NEC has a framework for thoroughly secure development and operations in place to provide customers with safe and secure products, systems, and services. The company has also established a framework in which a group of engineers with the world's top-level skills (risk hunting team) checks developed products, systems, and services for vulnerabilities, as well as whether sufficient security measures are in place. (For details, see “Providing Secure Products, Systems, and Services” on page 18.)

In order to ensure security in an environment where data, systems, and other elements are intricately intertwined as a result of advances in DX, NEC has adopted SBD3.0*6 as a concept for data-centered secure development and operations and aims to meet security needs ahead of the times.

*6 SBD3.0: Security By Design 3.0

Cybersecurity in the era of DX (NEC) (Japanese only)

https://jpn.nec.com/cybersecurity/nec_cybersecuritywhitepaper202004.pdf

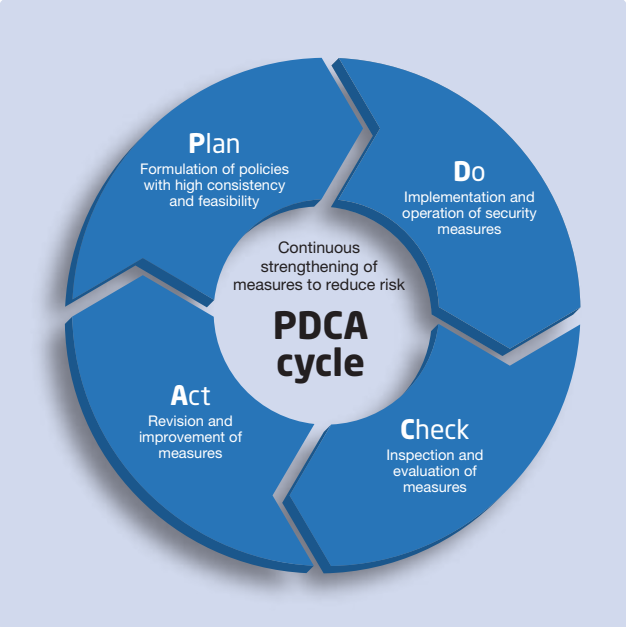
5 Support for Strengthening Security Based on In-House Operational Expertise

Cybersecurity does not end with putting relevant measures in place. In order to fend off increasingly advanced and sophisticated cyberattacks, it is vital to execute cybersecurity measures appropriately and keep them in good shape.

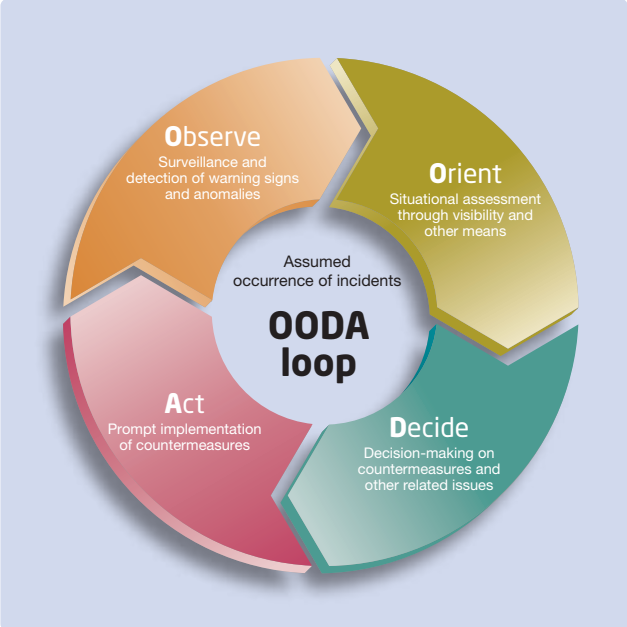
It is essential to implement the PDCA cycle of creating cybersecurity policy, taking measures, checking effects, and making improvements, as well as to have continuous measures in place to eliminate vulnerabilities. Building on its experience in operating the systems used by about 110,000 NEC Group employees around the globe, NEC provides cybersecurity measures designed from the user's point of view.

Preparing for security incidents, such as hacking and malware infection, is important as well. NEC has adopted the concept of “OODA Loop,” a cycle of observe, orient, decide, and act, to support appropriate and speedy incident handling.

Continuous Security Measures Based on the PDCA Cycle



Speedy Incident Handling Based on the OODA Loop



Cases of R&D of the Leading-edge Cybersecurity Technology

NEC protects the social infrastructure and organizations from cyber threats by driving its R&D efforts on both system security and data security based on the Security by Design (SBD) concept.

1 Concepts for Research Themes

In order to realize a society in which anyone can use digital technology with a sense of security, the NEC Group is conducting R&D activities on both system security and data security, based on the Security by Design (SBD) concept whereby security is taken into consideration from the planning and design stages.

In the field of system security, we have developed some leading-edge technologies. These include the automatic cyberattack risk assessment technology to visualize security risks from increasingly sophisticated and advanced cyberattacks and the lightweight tamper detection technology designed for IoT devices that cannot have antivirus software installed in them.

The technologies we have developed for data security are lightweight cryptography for implementing cryptographic functionality in IoT devices to eradicate information leaks and the secure computation technology to process data in encrypted form.

2 Automatic Cyberattack Risk Assessment Technology

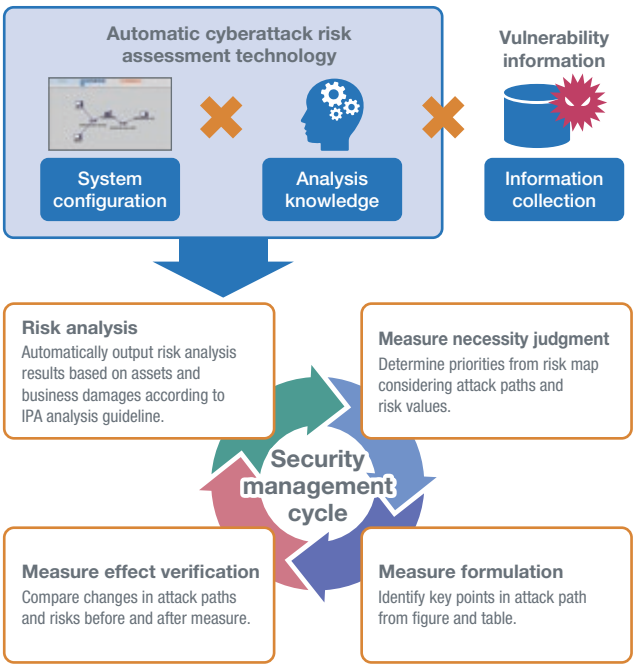
In order to prepare for ever-increasing cyberattacks, it is crucial to identify a system's potential risks for new threats and vulnerabilities and to take actions in advance by collecting the latest information. However, analyzing risks, judging whether to respond and considering what measures to take require many labor hours and security expertise.

The automatic cyberattack risk assessment technology automatically identifies the potential risks of a system by using the latest vulnerability information, based on the analysis logic of security experts provided as a set of rules. Asset-based and business damage-based risk analysis results are output in the sheet format of the security risk analysis guideline for control systems of the IPA*1 and as an attack path diagram for the topology.

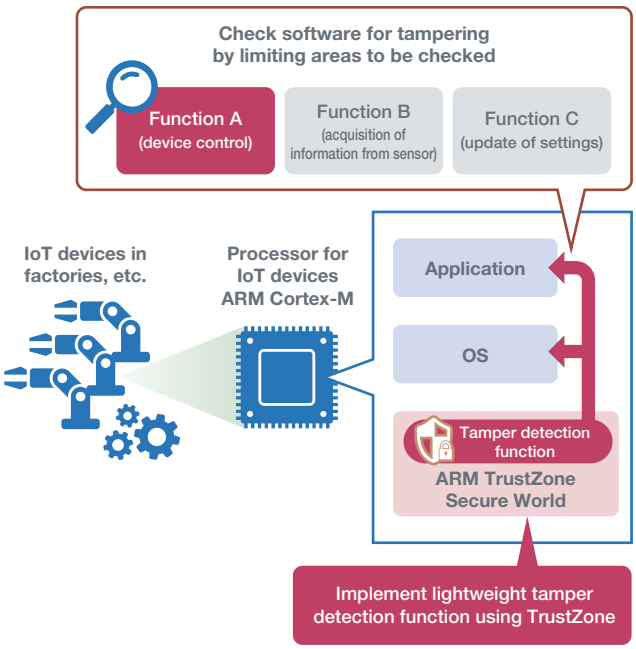
Risk indicators of individual attack paths are automatically calculated according to the attack method used and the type of vulnerability, helping to identify the attack paths that should receive priority response. It is also possible to narrow down effective points and types of measures based on the attack path structure. The function to compare analysis results before and after a measure is taken allows the effect of that measure to be assessed easily in advance.

*1 IPA: Information-technology Promotion Agency

Overview of Automatic Cyberattack Risk Assessment Technology



Mechanism of Lightweight Tamper Detection Technology



3 Lightweight Tamper Detection Technology

In recent years, the use of IoT has increased to ensure the efficient operation of social infrastructure systems and others. IoT-connected devices (IoT devices), however, do not have enough CPU performance and/or memory capacity and have been unable to have existing security measures implemented on them.

The lightweight tamper detection technology can be introduced to these IoT devices and detects tampering in the software of the IoT devices in operation. Since it adopts a lightweight architecture whereby the tamper detection function is implemented by means of TrustZone*2 of the ARM Cortex-M processor for IoT devices, the technology can be deployed in IoT devices with limited memory capacity as well.

Also, this technology identifies the memory areas storing the code to be executed based on the software structure and checks only those areas for tampering. This minimizes the impact on the operation of the IoT device and enables a smooth check even when the device is in operation.

*2 TrustZone: Function to create a protected zone in memory

4 Data Security

❶ Lightweight Cryptography

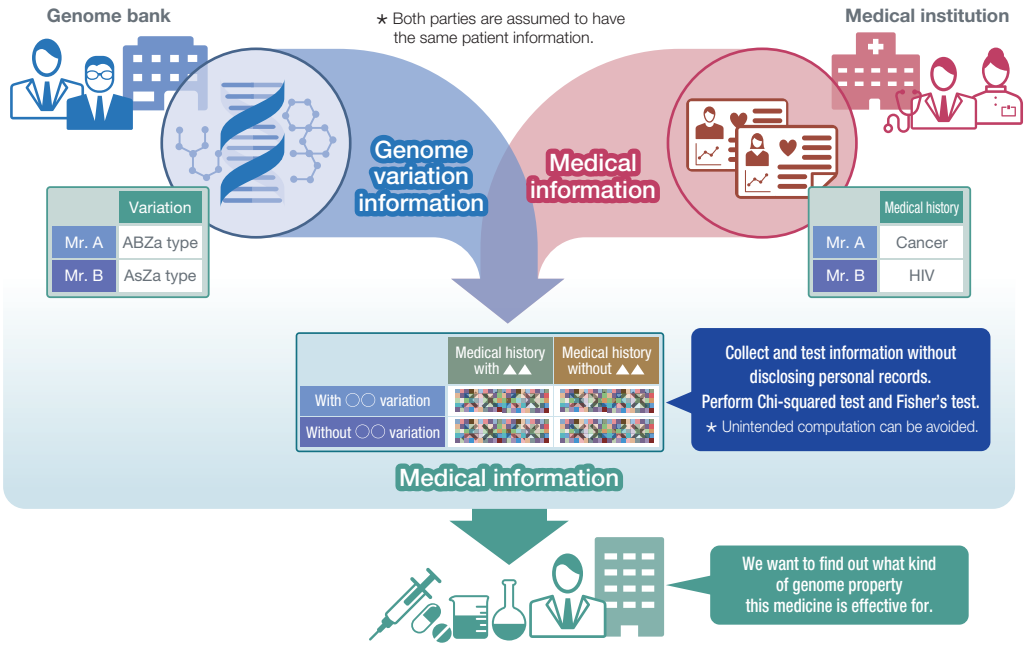
Lightweight cryptography runs smoothly even on IoT devices with limited resources. NEC has the world's top-level lightweight cryptography technology and has proposed it for consideration in the lightweight cryptography standardization process in the U.S., where screening is underway. The use of lightweight cryptography allows various IoT devices to be connected safely to cyberspace.

❷ Secure Computation

Secure computation is a technology to process data in encrypted form. It provides powerful protection against malware attacks and information leaks resulting from fraudulent acts inside the organization. Multiple organizations can use one another's data while keeping their secret information hidden.

Conventional secure computation methods were problematic in terms of performance. By refining the method that processes data while keeping the data secretly distributed across multiple servers, NEC achieved the highest performance in 2016. We also developed a technology to facilitate secure computation-based development and demonstrated in 2019 that secure computation could be applied to a unique analysis algorithm developed by a genome researcher in several days.

Cases of Secure Computation Application in Genome Research



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 Shizuokabusiness, 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 Shizuokabusiness, 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

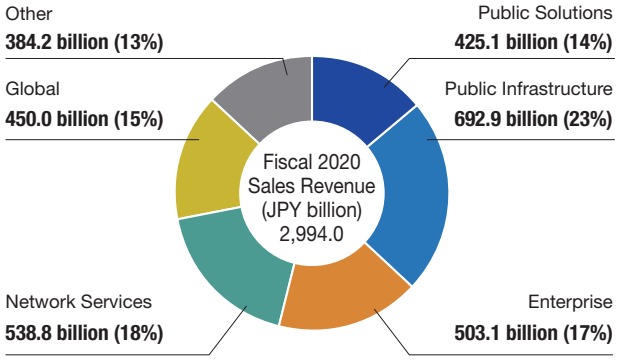
Corporate Profile

Company name	NEC Corporation
Address	7-1, Shiba 5-chome, Minato-ku, Tokyo, Japan
Established	July 17, 1899
Capital	¥427.8 billion*
Number of employees (Consolidated)	114,714*
Consolidated subsidiaries	301 companies*

*As of March 31, 2021

Segment Information

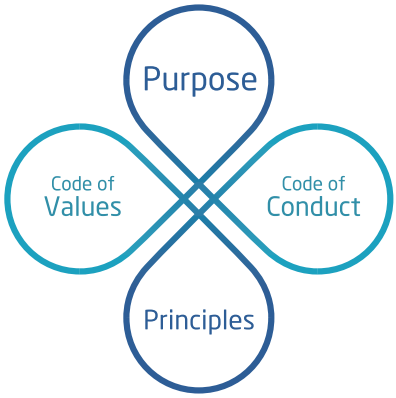
Sales Revenue by Segment (Percentage)



*As of March 31, 2021

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

NEC Corporation

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

Issued July 2021