\Orchestrating a brighter world NEC

Information Security Report 2020

NEC's Approach to Information Security

NEC positions information security as an important management foundation for business continuity 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*1.

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 resulted from it. Particularly, amid the impact of new coronavirus infection (COVID-19) changing the paradigms of society, we need to brace for the new normal.

In these social circumstances, NEC positions information security as an important management foundation for business continuity. We are driving measures to combat increasingly sophisticated cyberattacks, provide highly secure products, systems and services, and ensure information security for the entire supply chain, among other things, in line with Version 2.0 of the "Cybersecurity Management Guidelines" established by the Ministry of Economy, Trade and Industry of the Government of Japan and the Cyber Security Framework (Version 1.1) of NIST*2.

In implementing these measures, we take a comprehensive approach from multiple aspects, including information security management, information security infrastructure and information security personnel, with the aim of continuing to be a trusted company. We place particular focus on the following:

- Ensuring that NEC Group companies work together to build an information security management framework and risk management mechanisms and to implement the PDCA cycle
- Deploying security management measures that cover the entire supply chain and putting in place a framework for grasping the situation
- Safe and appropriate balance between protection and use of information based on the concept of zero trust
- Providing internally proven security solutions featuring NEC's own AI and automation technologies
- Ensuring accountability and cyber resiliency, and reducing reputation risks by improving the incident response and recovery framework

Under the company's corporate message of "Orchestrating a brighter world," NEC aims to use ICT to solve various social issues to contribute to the realization of a safe, secure, efficient, and equal society where people are able to live prosperous lives. 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.

*1 DX: Digital Transformation. A concept of creating new value and changing living and business conditions for the better by digitizing real-world events, integrating them with the cyber world, and connecting people, things, and events.
*2 NIST: National Institute of Standards and Technology

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 2020"

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 2020.

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

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.

NEC has established an information security promotion framework to fulfill its responsibilities to society as a trusted company. This framework enables us to realize a secure information society and provide value to our customers by protecting the information assets entrusted to us by our customers and business partners.
NEC is implementing cyber attack measures, providing secure products, systems and services, and promoting information security in collaboration with business partners. At the same time, we have positioned information security management, information security infrastructure, and information security personnel as three pillars in achieving thorough information security governance within the NEC Group, thereby maintaining and improving our comprehensive and multi-layered information security.
We are committed to abide by the NEC Information Security Statement and make Group-wide rules in line with it as well as to refine the common information security infrastructure. Our top management sets security goals and determines Group policies, organizational structure and the policy for allocating management resources while 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

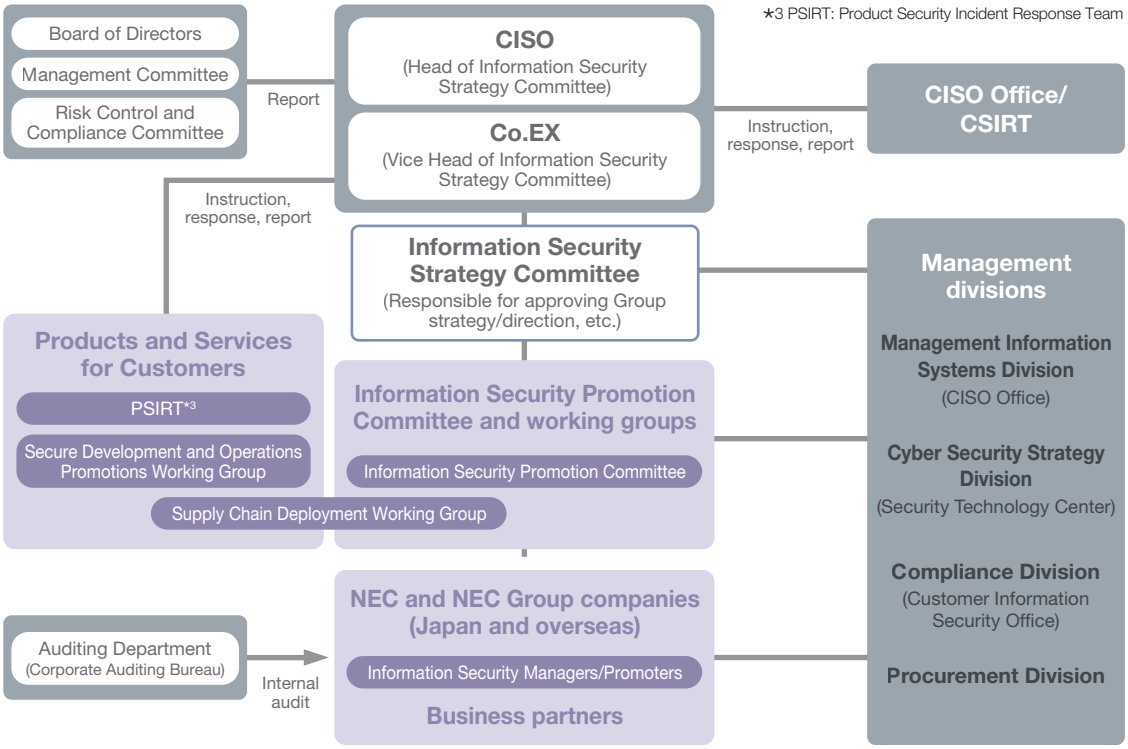
NEC has established the NEC Group Management Policy, setting standardized rules and implementing unified systems, business processes and infrastructure, in order to create a foundation for standard global management.
The top management establishes security goals based on the NEC information security governance scheme, and determines Group policies, organizational structures and the policy for allocating management resources. We are monitoring the progress and achievement status of security measures as well as the occurrence of information security incidents at the organizational level, and leading security to a new direction by evaluating requirement compliance state, giving necessary instructions in order to improve the entire framework.
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 cyber security measures and the CSIRT*2 that monitors for cyber attacks 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 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

3 Information Security Risk Management

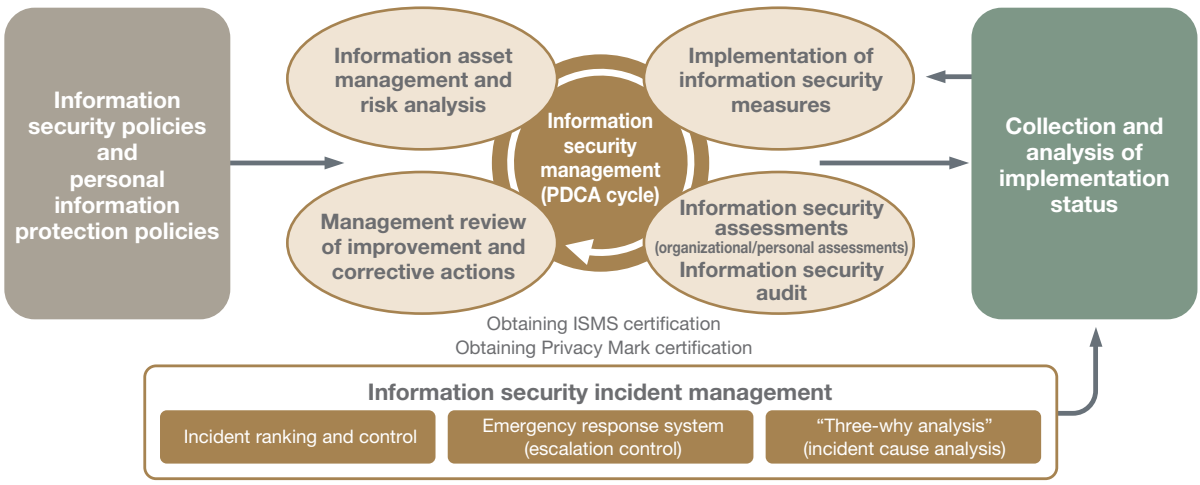
❶ Information Security Risk Assessment

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.

❷ Management of Information Security Incident Risk

It is mandatory in the NEC Group to report security incidents, and we manage risks by utilizing the results of analyzing reported data in the PDCA cycle. We manage incident information centrally on a Group-wide basis, analyze factors such as changes in the number of incident cases as well as trends by organization and incident type. We reflect the results to measures taken across the entire Group and

NEC's Information Security Management



assess their effectiveness as well. In the case of a serious incident, we perform impact analysis with professional advisors to quantify the response cost and possible damage. The results are reported to the top management and shared across the entire Group.

4 Information Security Assessments

❶ Details of Information Security Assessments

Considering the results of information security incidents analysis, we have set our priorities on eliminating information leaks through checking. Surveys are conducted to check whether required security measures are implemented, and if not, what are the obstacles. They help respondents realize what is required to secure their environment and raise their awareness on security. More specifically, assessments are conducted on such subjects as security management of confidential and personal information, management of external contractors, measures against targeted attack emails, and secure development and operations.

❷ Information Security Assessment Methods

NEC implements the following two information security assessments: organizational assessments and personal assessments. In organizational assessments, the information security promoter in each organization checks the status of the entire organization. In personal assessments, individuals respond by indicating the implementation status of measures. Personal assessments are targeted at both employees and managers to identify the situation of the operations and management sides respectively. The gaps between employees and managers are analyzed to improve the accuracy of assessments.

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.

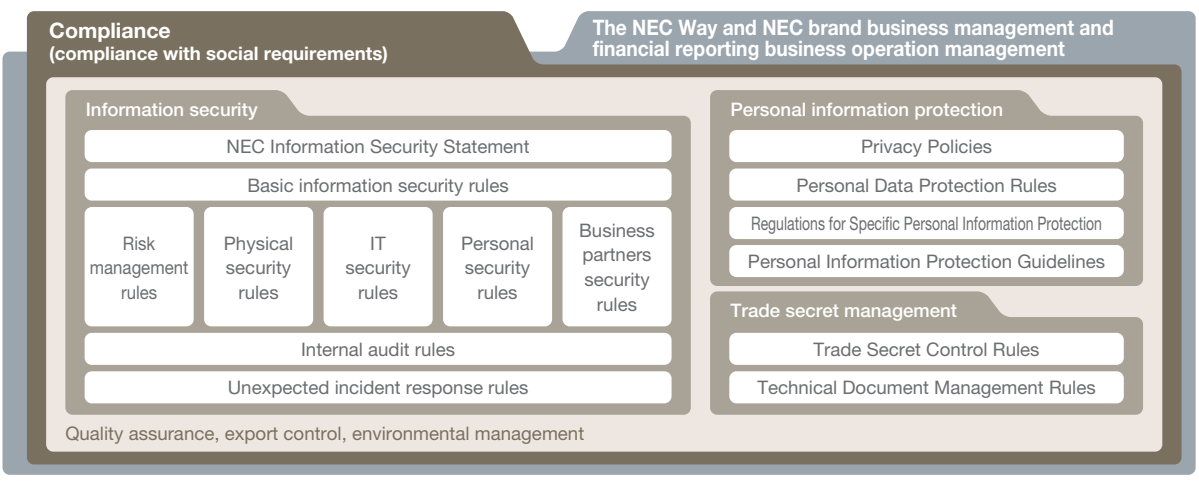
5 Information Security Audits

NEC's Corporate Auditing Bureau plays the main role in conducting audits with regard to information security management and the Privacy Mark. 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

In order to protect the invaluable personal information and confidential information of customers, NEC has information security infrastructure in place that enables safe, secure, and efficient promotion of business activities and projects based on the concept of zero trust.

1 Features and Configuration of Information Security Infrastructure

The three platforms composing the information security infrastructure interact with and complement one another to achieve the information security policies of NEC. These are the IT platform for user management and control, IT platform for PC and network protection and IT platform for information protection.

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

The basis of information security management is the user authentication infrastructure. Using a system to identify individuals enables proper control of access to information assets and prevents spoofing by using digital certificates.

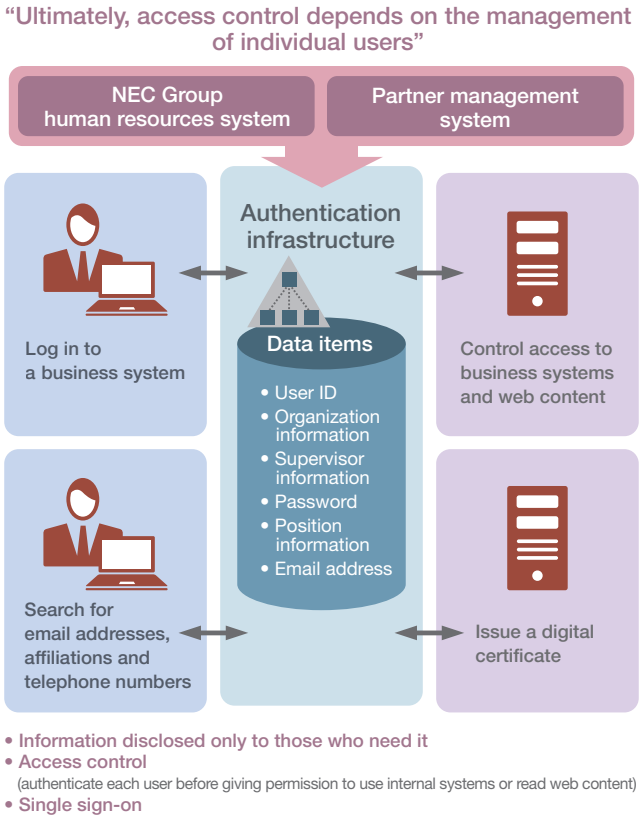
It is important to identify and authenticate users and assign them correct privileges so that information assets can be managed appropriately. NEC has built an authentication platform to centrally manage information used for authenticating users and assigning privileges (authorization), covering not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

The information used for authenticating and authorizing users consists of access control information such as the user's ID and password, as well as information about their organization and position. 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.

With respect to controlling access to systems that handle critical information, besides the use of the user's ID and password (memory-based authentication), we are also promoting the use of certificate-based individual authentication (token-based authentication). In addition, plans are in place to adopt face recognition (biometrics authentication) in the future.

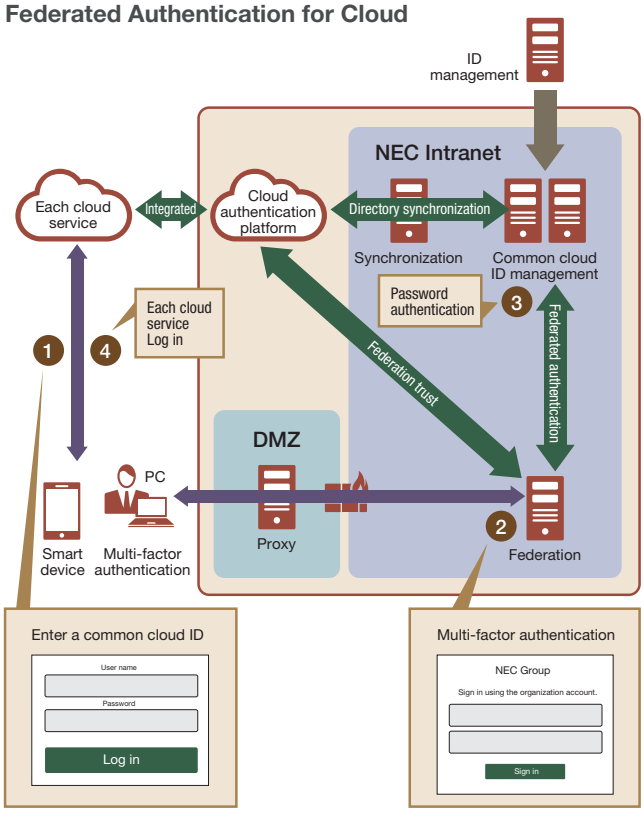
Furthermore, a cloud service authentication system has been connected to the internal authentication platform, enabling a seamless system of authentication for internal and external services. The system ensures that users can safely, securely, and comfortably share information with external parties when using cloud services.

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 IT platform to protect the Group's PCs and networks from viruses, worms, and other attacks and maintain the security of information devices connected to the NEC Intranet. In addition, multi-level measures are required to address risks of recently increasing advanced persistent threat (APT)*1 attacks and it is important to install all necessary security updates and antivirus software on information devices.

*1 Advanced persistent threat (APT): a prolonged and targeted cyberattack

❶ Protecting Our PCs from Viruses and Worms

• Support for user environments

NEC Group employees using the NEC Intranet are required to install software to check the status of their PCs and the network. Being able to visualize the current state allows us to instantly check whether all the necessary security software is installed on all PCs. In addition, there is a system in place to automatically distribute security patches and updates of definition files for antivirus software.
We also define prohibited software and monitor whether users are using software properly.

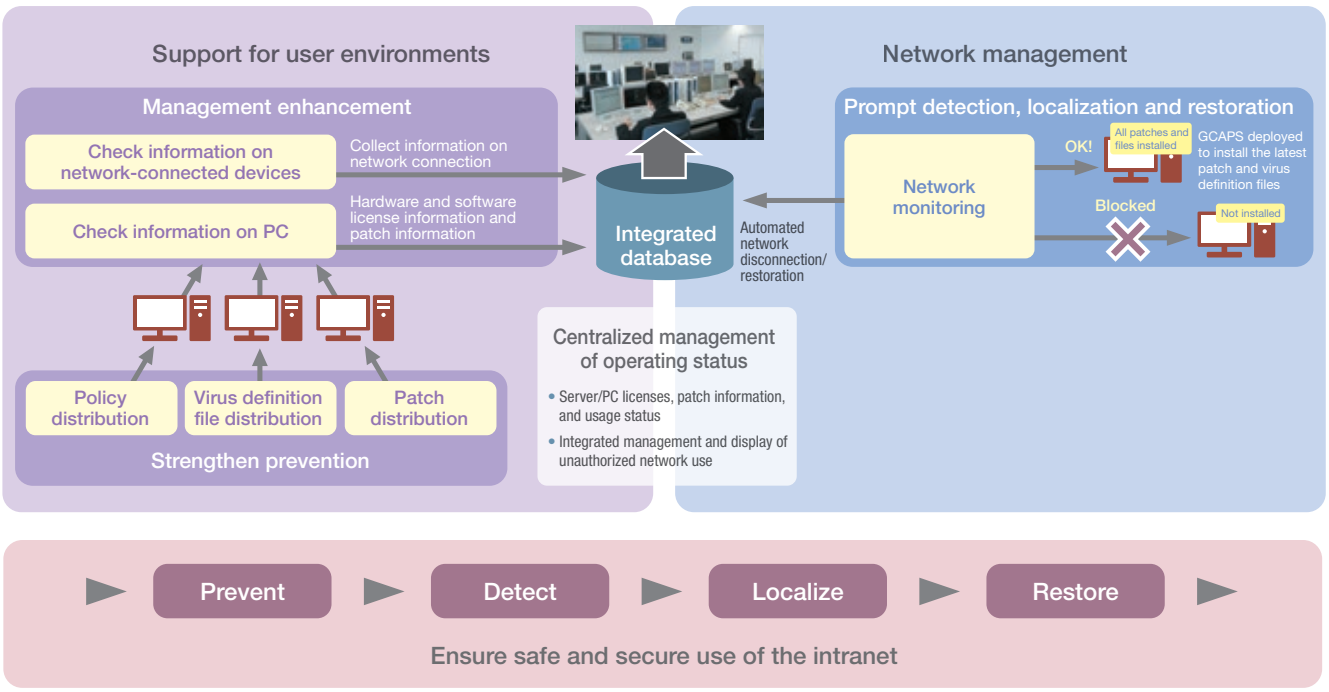
• Network management

In addition to visualizing PC status, when a PC for which security measures are not sufficiently implemented is connected to the NEC Intranet or a worm is detected on the NEC Intranet, that PC or LAN is disconnected from the Intranet. We also control communications to people or organizations outside NEC by web filtering that blocks access to sites of unauthorized categories, prohibiting the use of free email accounts, using SPF authentication to recognize the identity of the sender, and other methods.

• Centralized management of security updating

Data on the implementation status of security measures, including installation of patch programs and antivirus software, is collected into a single management system so that information security managers and security promotion managers can see the implementation status in their department in a timely fashion. This enables the managers to ensure all the required security measures have been implemented and if not, to take immediate actions for improvement.

Protection of PCs and Networks from Viruses and Worms



4 IT Platform for Information Protection

Preventing information leaks requires identifying possible information leakage paths, analyzing the risks involved, and then taking appropriate measures. Since NEC manages the invaluable information of customers and business partners in addition to our own, we have implemented comprehensive and multi-layered measures for blocking possible information leakage paths while taking into account the characteristics and risks of digital devices.

❶ NEC Group Information Leakage Prevention System

NEC's information leakage prevention system implements encryption, device control, and logging in order to counter the risks of information leakage due to external attacks and internal frauds.

We encrypt PC hard disks and files to prevent information leaks due to theft or loss. In encrypting files, we define access privileges and usage periods as group-wide default security. 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.

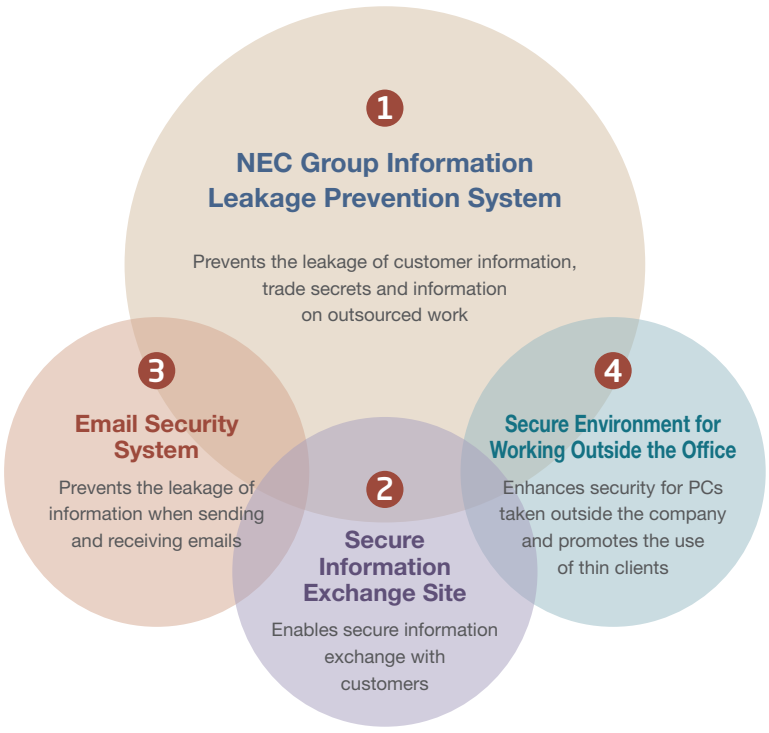
For device control, we set usage restrictions prohibiting any recording of information on external media such as USB flash drives, SD cards, CDs, and DVDs, as well as on communications devices such as smartphones and devices using Bluetooth or infrared. If such devices are needed for work, the types and usage are restricted to the minimum depending on the business of the organization and user.

We record all the operation logs of in-house PCs.

In the event that an information leakage incident occurs, analysis of the logs is a significant aid in identifying the scope of impact of the incident, grasping the current situation, formulating recurrence prevention measures, etc.

In addition, to prevent information leaks due to internal frauds, we have specified internal systems that need focused management considering the impact on business in the event of an incident. The specific measures we implement with regard to these include vulnerability information collection and handling, log management, network protection, authentication, access control, privileges

Overview of IT Platform for Information Protection



management, secure operation and maintenance procedures, operation and maintenance checking, security settings, physical entry controls, and contractor management.

❷ Secure Information Exchange Site

NEC operates a secure information exchange site to exchange important information with customers and business partners in a safe and secure manner. Users can exchange information in an access-restricted area by using one-time URLs and passwords. Each one-time URL has a time limit, after which it becomes invalid. The information is deleted from the site once the URL is expired.
With this exchange site, users do not need to use USB flash drives or other external media, which in turn reduces the risk of information leakage incidents caused by theft or loss.

❸ Email Security System

OMCA*2 prevents information leakage incidents from occurring in sending and receiving emails.
This add-in features the functions to alert the user about a suspicious email that may be an APT attack, to display a popup 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

NEC has built an external secure digital workplace (for details, see “Creation of a Digital Workplace” on page 20) to prevent information security incidents.
When a PC needs to be taken out of the office, a thin client PC 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 fully encrypted HDDs, a pre-boot authentication feature that launches before OS startup, remote data deletion/PC locking, a function to mitigate attacks that exploit unknown vulnerabilities, a feature to block autorun viruses, etc., in order to counter increasingly sophisticated cyberattacks.

Secure Information Exchange Site

Illustration of Data Upload

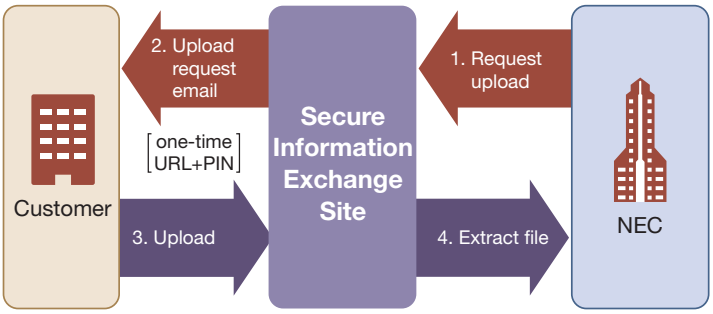
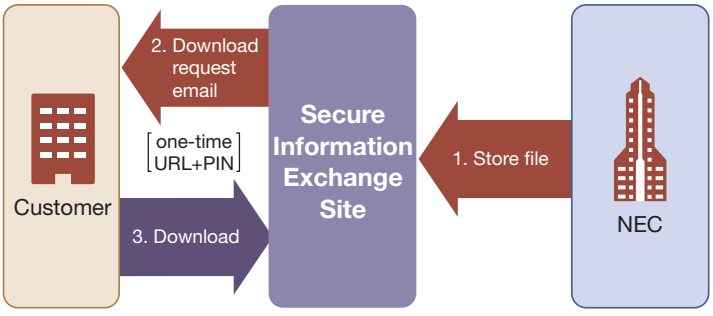


Illustration of Data Download



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 this training is updated every year to reflect trends in security threats and other security-related information. The course aims to raise awareness about new security threats and required responses, and promote understanding in areas including information handling and internal fraud prevention.

*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 Cyber Security Training Site

An EC site-like dedicated virtual environment is used as a site for practical security training, where employees learn about environment hardening techniques in the system construction phase. In fiscal 2019, over 300 engineers used this site and enhanced their security skills to protect customers' systems.

❷ Group-wide CTF

NEC holds an in-house CTF*4 event called "NEC Security Skill Challenge." In fiscal 2019, about 1,000 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 a WBT course for sales personnel and system engineers to acquire the basic security knowledge they need, with the focus on security by design (SBD). The training is aimed at enhancing the security skills across the entire NEC Group.

❹ SBD Specialists

A new program began in fiscal 2019 to develop specialists who 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 Cyber Security Analyst)

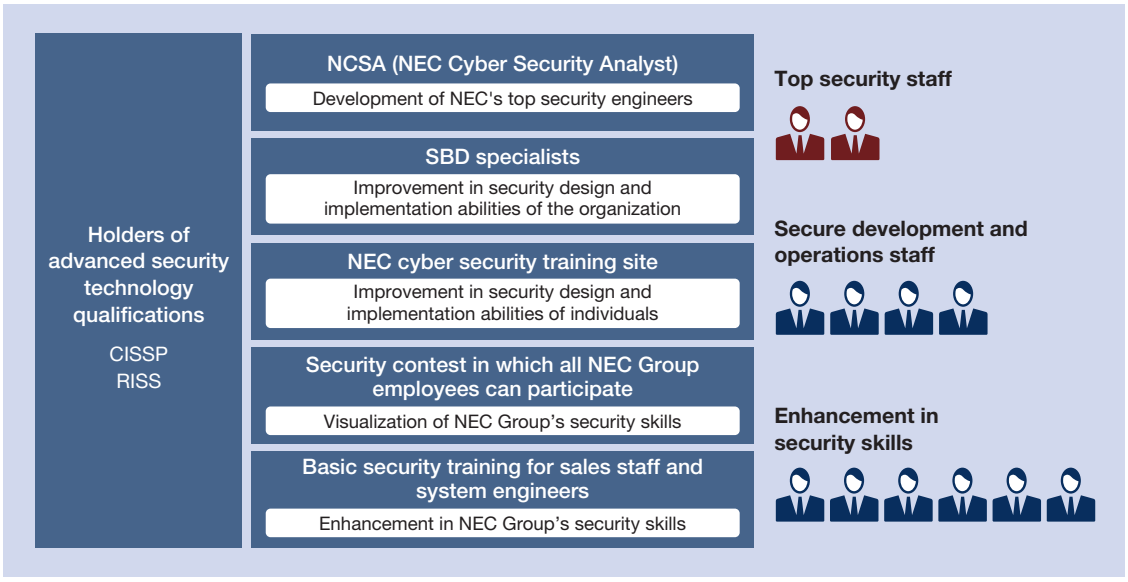
In fiscal 2020, NEC launched an NCSA (NEC Cyber Security Analyst) program improved to better suit practical needs compared to the existing NEC CISO assistant training. The purpose of the program is to enhance the skills of top security staff. Intended for those staff members who have knowledge of security technologies, the six-month intensive program lets trainees master the technical skills required for advanced security services, such as CSIRT*5 work and risk hunting.

*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 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 Cyber Attacks

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 Measures against Cyber Attacks

NEC ensures cyber resiliency by implementing advanced measures based on cybersecurity risk analyses globally while having a CSIRT*1 framework to respond to security incidents. 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: National Institute of Standards and Technology Cyber Security Framework
A framework issued by the NIST to enhance the cybersecurity of critical infrastructure

2 Cyber Security Risk Analysis

NEC performs four types of risk analysis with regard to cyber threats such as APT attacks including BEC*3, ransomware, and indiscriminate email attacks*4, and is developing measures against the cyberattacks based on the analysis results.

⋆3 BEC: Business E-mail Compromise
⋆4 Indiscriminate email attack: Attack targeting an unspecified number of users

❶ Cyber threat analysis

We assess the status and characteristics of cyberattacks on the NEC Group through real-time monitoring, malware analysis, and threat intelligence. We also determine threat risk levels and consider responses in accordance with the threat status.

❷ Monitoring operations analysis

We perform reviews of our current monitoring processes as needed, consider operations that are appropriate for responding to ever-changing cyber threats, and identify operational issues.

❸ Solution and IT analysis

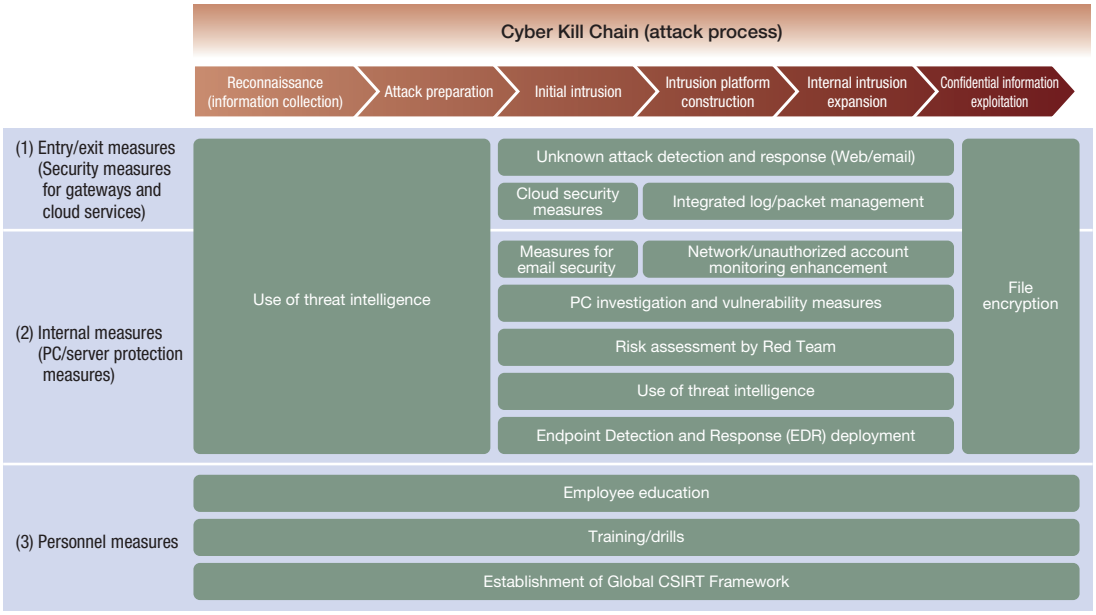
NEC researches security products and services as well as market trends to keep track of the ever-changing technology. Also, through PoC*5 evaluations and internal IT environment research, we analyze if the products and services work well and meet the security requirements in our environment.

⋆5 PoC: Proof Of Concept

❹ Countermeasure analysis

Working based on the three types of analysis on cyber threat, monitoring operations, and solution and IT, we seek countermeasures required for NEC, and determine the targeted scope while analyzing their effects and costs.

Overview of Global Cyberattack Measures



3 Global Measures against Cyber Attacks

NEC creates a security promotion plan every year based on the cybersecurity risk analysis and, upon approval of the CISO*6, carries out the planned measures. In the Solutions for Society business in particular, implementing global comprehensive measures to eliminate cybersecurity risks is indispensable for business continuity.

Our global measures against cyberattacks are being stepped up based on the concept of multilayered defense to counter increasingly sophisticated cyberattacks. We are focused particularly on the following four points: (1) unknown attack detection and response, (2) risk assessment by the Red Team*7, (3) use of threat intelligence, and (4) enhancement of the CSIRT framework.

★6 CISO: Chief Information Security Officer

★7 Red Team: A team of experts that launches a dummy attack similar to an actual threat to a company or organization, assesses the organization's resistance against the attack and risks involved, and proposes possible improvements and additional measures

❶ Unknown attack detection and response

NEC monitors Web traffic and in-coming emails using an unknown malware detection system as an entry/exit measure. Unauthorized communication is filtered out based on the information obtained through analyzing behaviors of suspected unknown malware that has been detected and other data, and measures are taken for those PCs and servers suspected to be infected. We have EDR*8 deployed in all the PCs and servers within the NEC Group and detect unknown attacks rapidly by collecting and analyzing detailed information of terminal behavior. With remote forensics and other capabilities, the CSIRT effectively responds to incidents. Also, to address PC and server vulnerabilities, we provide the GCAPS*9 (marketed under the solution name of NCSP*10).

★8 EDR: Endpoint Detection and Response

★9 GCAPS: Global Cyber Attack Protection System ★10 NCSP: NEC Cyber Security Platform

❷ Risk assessment by the Red Team

The NEC Group has a cyber risk assessment conducted by its Red Team on a regular basis to improve its cyber resiliency and accountability. The team conducts a cyber risk assessment with three activities combined into a package: examination of confidential information management scheme, investigation of vulnerabilities, leaks, and other risks of public servers, and an intranet intrusion test from the attacker's point of view. They check the existing security measures for loopholes and missing steps and implement improvement measures.

❸ Use of threat intelligence

Threat intelligence is used to identify threats to NEC including their signs in the early stage, avoid risks of advanced threats that elude the existing measures, minimize their damage, and reduce the time it takes to contain such threats. NEC has a high-level expert system for leveraging the threat intelligence provided from internal and external sources.

❹ Enhancement of the CSIRT framework

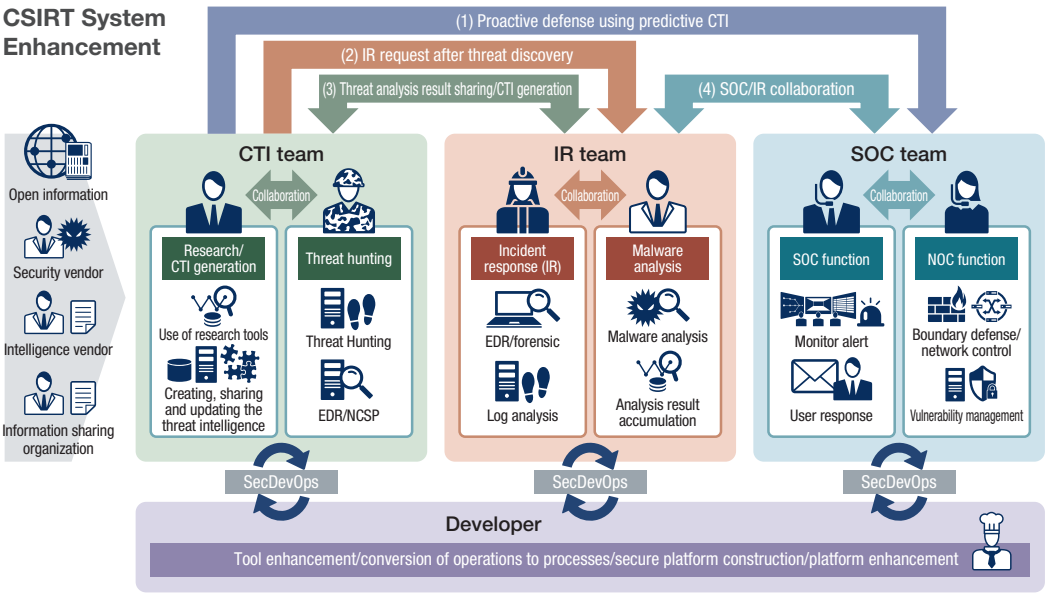
The CISO has a CSIRT organization under his direction; its members monitor cyberattacks, analyze the characteristics of detected attacks and malware, and share information with related organizations. In the event of a security incident, they protect the internal systems and analyze the attack to identify the cause and resolve the situation.

The CSIRT consists of four teams: the CTI*11 team that exploits threat intelligence, the IR*12 team that responds to incidents, the SOC*13 team that monitors alerts from security devices, and the Developer team that enhances tools, platforms, and operation processes. Alerts issued in Japan are monitored by Infosec Corporation. For the overseas group companies, 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.

★11 CTI: Cyber Threat Intelligence ★12 IR: Incident Response

★13 SOC: Security Operation Center



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.

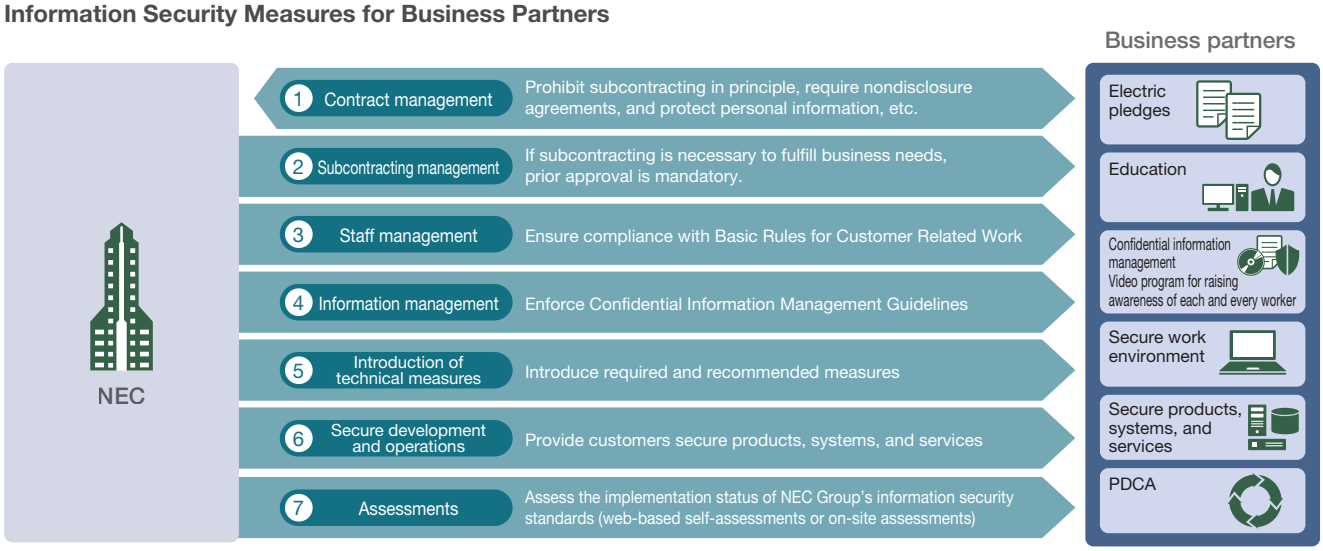
❻ Secure Development and Operations

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 1,400 companies, including approximately 700 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 1,400 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

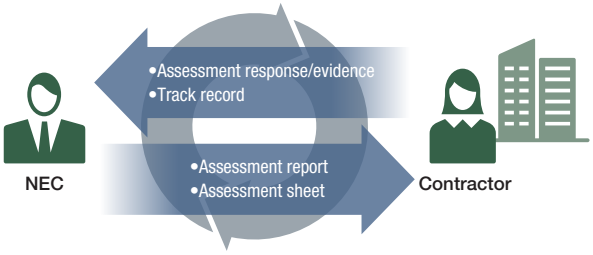
This assessment is conducted every year on about 50 companies that do large volumes of business with NEC. Approximately 100 assessors authorized by NEC visit the business partners for on-site assessments.

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

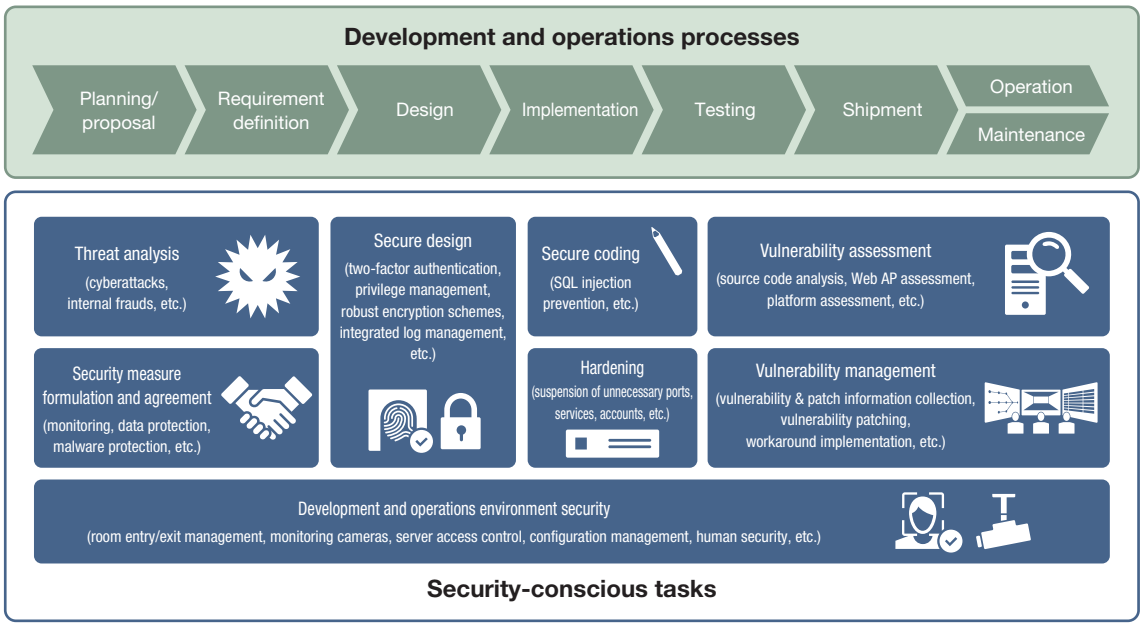
❶ Group-wide Promotion Structure

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.
In the past, security requirements were defined according to the confidentiality of information assets. With the diversification of cyberattack methods, such as ransomware and denial of service (DoS*1), and attack targets, it has become necessary to consider

Secure Development and Operations Processes



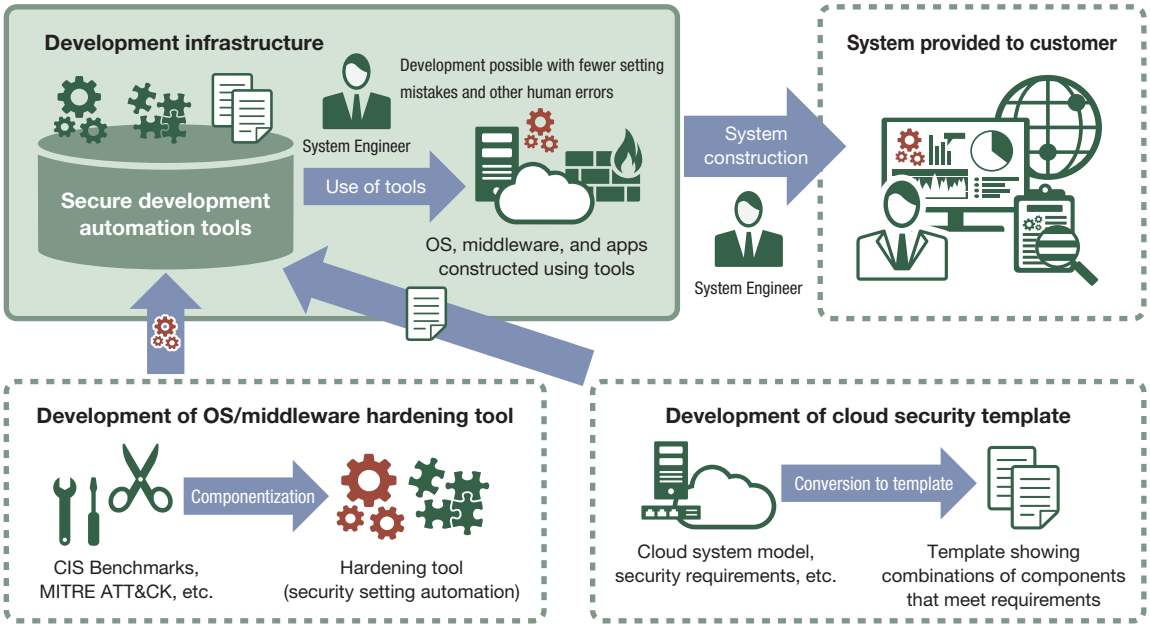
not just confidentiality but integrity and availability as well. In line with this trend, we have revised the Operation to better suit the current situation, by adding NIST SP800-53 and other new requirements.
In the development of products, systems, and services, we create and use a checklist to ensure that security tasks are implemented in each phase. Based on this checklist, approximately 7,000 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 tasks.
We have also set up Risk Hunting team made up of members who are skilled at identifying risks that are difficult to find by checklist- or tool-based routine checks based on system analyses from the attacker’s point of view. In addition to conventional checklist-based comprehensive assessments, Risk Hunting team assesses particularly high-risk areas, thus making our system development and operations framework even more robust.

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*2 technology to describe the cloud environment as code.

*1 DoS: Denial of Service attack
*2 IaC: Infrastructure as Code

Secure Development Automation Tools



Creation of a Digital Workplace

NEC promotes business continuity through the use of a digital workplace without stopping business operations while ensuring user convenience and information security under any circumstances.

1 Work Style Reform and Digital Workplace

For over 30 years, NEC has been committed to creating a conducive digital workplace environment in which each and every employee can bring the best out of themselves. After opening satellite offices as early as 1987, the company introduced teleworking for employees in research positions in 1993. In 2018, all employees of the entire NEC Group became eligible to telework.

Building on this abundant experience, NEC began to prepare ICT infrastructure early on and drove work style reform from three aspects: review of internal systems, optimization of business processes, and awareness raising among employees.

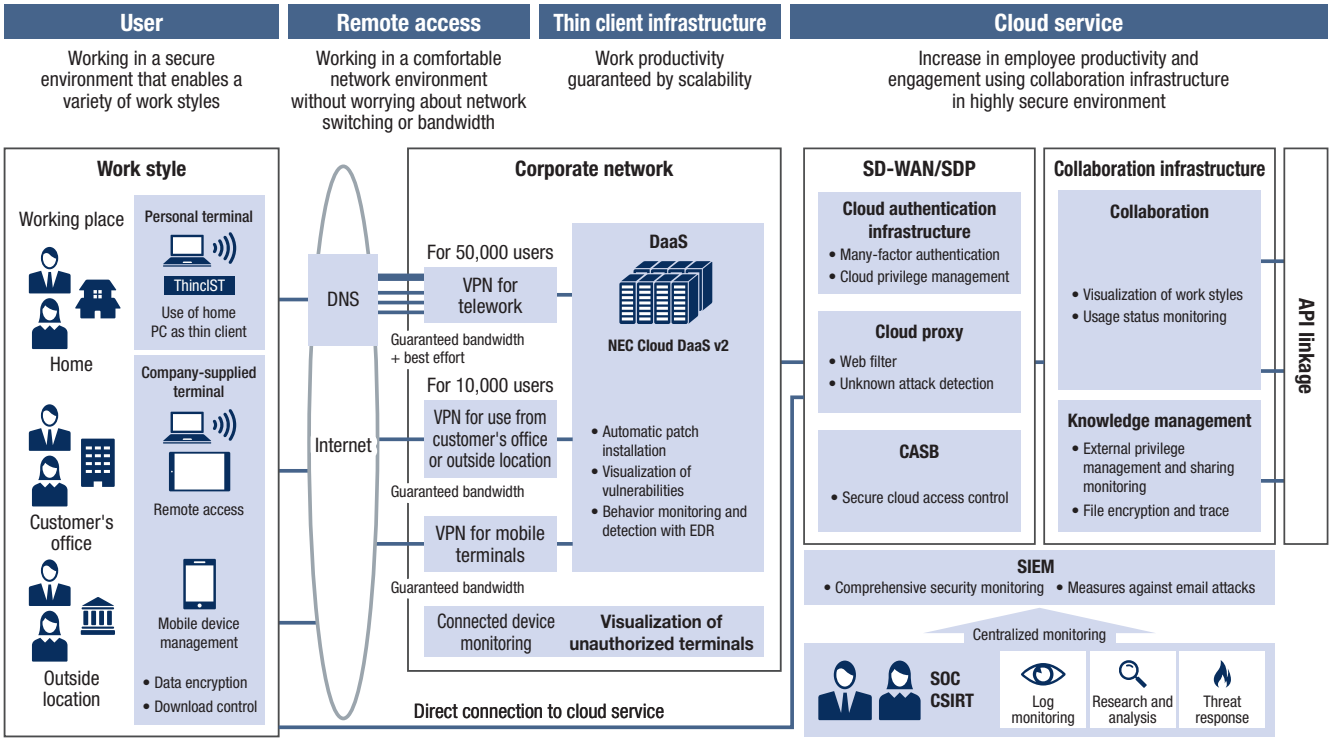
In preparing ICT infrastructure, NEC upgraded its business systems to a cloud-based platform, thus bolstering its communication infrastructure to promote collaboration among internal and external stakeholders. With mobile devices distributed to all employees, the company now has a digital workplace environment in place that allows individuals to work with anyone anytime, anywhere (e.g., through teleworking). These efforts have gained social recognition. In 2019, NEC received the 20th Chairman's Award of the Japan Telework Association, the best of all awards it gives to organizations that have established an advanced teleworking framework.

2 Deployment of the Digital Workplace

NEC aims to evolve its digital workplace from a Group-wide information sharing infrastructure to a business collaboration foundation. Accelerating smart work by making PCs, tablets, smartphones, and other mobile terminals more convenient to use, we build a platform that facilitates collaboration between the NEC Group and its customers and business partners.

The account domains of the digital workplace are integrated so that anyone can use multiple terminals anywhere, anytime. This requires the "protection of information assets." It includes establishing an environment in which users can use any type of terminal safely and securely and exchange files in a secure manner, as well as providing powerful encryption to prevent confidential information from leaking. By putting these technologies in place, we intend to enable smooth communication not just within the NEC Group but with customers and business partners as well no matter when and where they work, with the goal of brushing up our co-creation capabilities.

Digital Workplace Realized by NEC



3 Use of the Digital Workplace

In the spring of 2020, COVID-19*1 became a global pandemic in just a few months. In Japan, too, citizens are asked to avoid “3 Cs” (Closed space, Crowded places, Close-contact settings) and change behavior in all kinds of situations in order to prevent the spread of the infection. Under these circumstances, NEC is making the most of the digital workplace to ensure business continuity.
The basic concept of the digital workplace is to allow employees to choose the terminal model that is best suited for the place they work and the task they perform. While ensuring thorough information security, three different types of terminals - thin client PCs, “Trusted PCs”, and smart devices on the mobile infrastructure - are used for a wide variety of jobs.

*1 COVID-19: New coronavirus infectious disease

❶ Thin Client PC

Since 2006, NEC has used thin clients PCs across the entire Group to prevent information leaks and reduce TCO. With about 60,000 virtual desktop PCs (VPCs) in use as of April 2020, we have a secure work environment in place that enables employees to work anywhere they want. This has been made possible by introducing SS10 software thin clients that leave no data in hardware terminals to prevent information leaks in case of theft or loss. Some employees are using their VPCs even at their desks in the office.

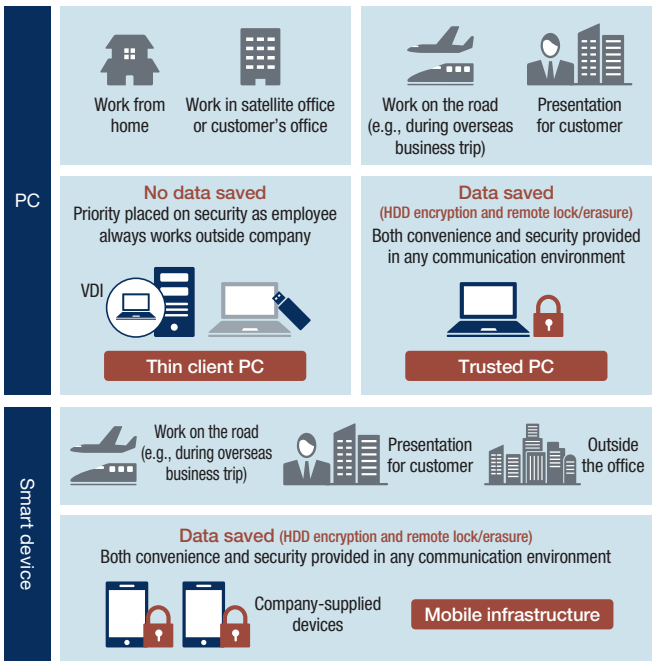
❷ Trusted PC (Fat client PC for taking out only)

In some cases, NEC supplies its employees with trusted PCs, which enable them to work even in an environment with poor network access, thus achieving both convenience and security. Trusted PCs were introduced in 2012 and, as of April 2020, about 20,000 units are in use. Even if a trusted PC is stolen or lost, data cannot be read from it. In addition, these PCs are protected by thorough security features, including countermeasures against cyberattacks and information leaks. No major security incident has been reported since we began to use trusted PCs.

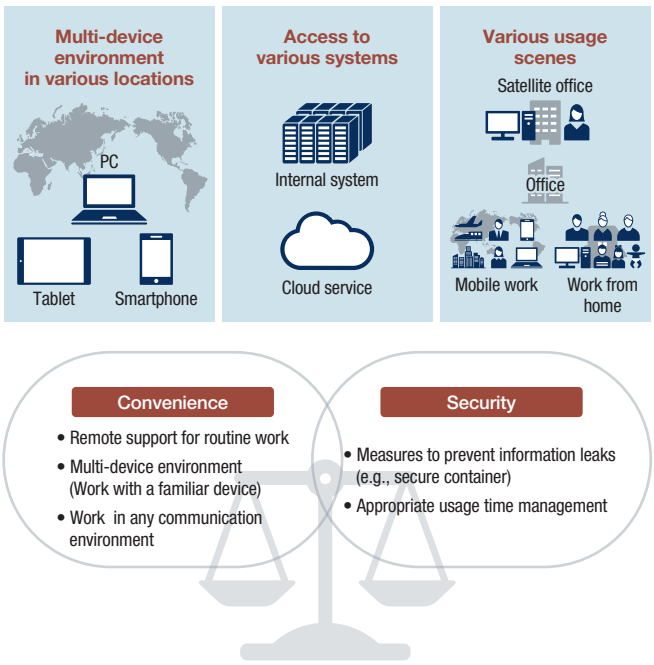
❸ Renewal of the Mobile Infrastructure

NEC has established a mobile workplace that provides both convenience and information security so that it can flexibly support increasingly diversifying needs for terminals, systems, and work locations. Particularly, now that changes in the work style and behavior are required, renewing the mobile infrastructure while ensuring sufficient information security is a major theme to address for business continuity and the creation of a sustainable business environment.

Basic Concept of Terminal Use



Concept of the Mobile Infrastructure



4 Digital Workplace Products, Systems, and Services

NEC has been promoting a digital workplace for the work style reform and better work-life balance. Recently, implementing a digital workplace has become more and more important from the perspective of ensuring business continuity amid the COVID-19 pandemic. NEC provides products, systems, and services that address the diverse issues and needs of customers. These customers wish to build or add a teleworking environment rapidly, establish an ICT infrastructure suitable for a digital workplace as a corporate strategy, make the teleworking environment perfectly secure, achieve proper management of teleworking employees, introduce chatbots for call center work, and train employees remotely at their homes, among other things.

The key point in implementing a digital workplace environment is the protection of information assets. As more employees start working from home, it is becoming increasingly crucial to mitigate the associated risks. This report outlines some of the products, systems, and services tailored to telework security protection.

Telework Security Assessment Tool (Free)

Visualizing security risks and promoting efficient and effective measures

Damage from information leaks and cyberattacks is a major problem that could shake the business of a company. As a company sets up a teleworking environment, implementing socially accountable measures is essential. This tool allows customers to do a comprehensive check on their existing security measures from five perspectives based on the “Telework Security Guidelines” (Version 4) of the Ministry of Internal Affairs and Communications. Just by answering 20 questions, customers will be able to find out whether their security measures are sufficient for teleworking, as well as what to improve.

This is a free service whereby we provide questionnaire forms to customers, visualize security risks based on returned questionnaires, and feed findings back to customers.

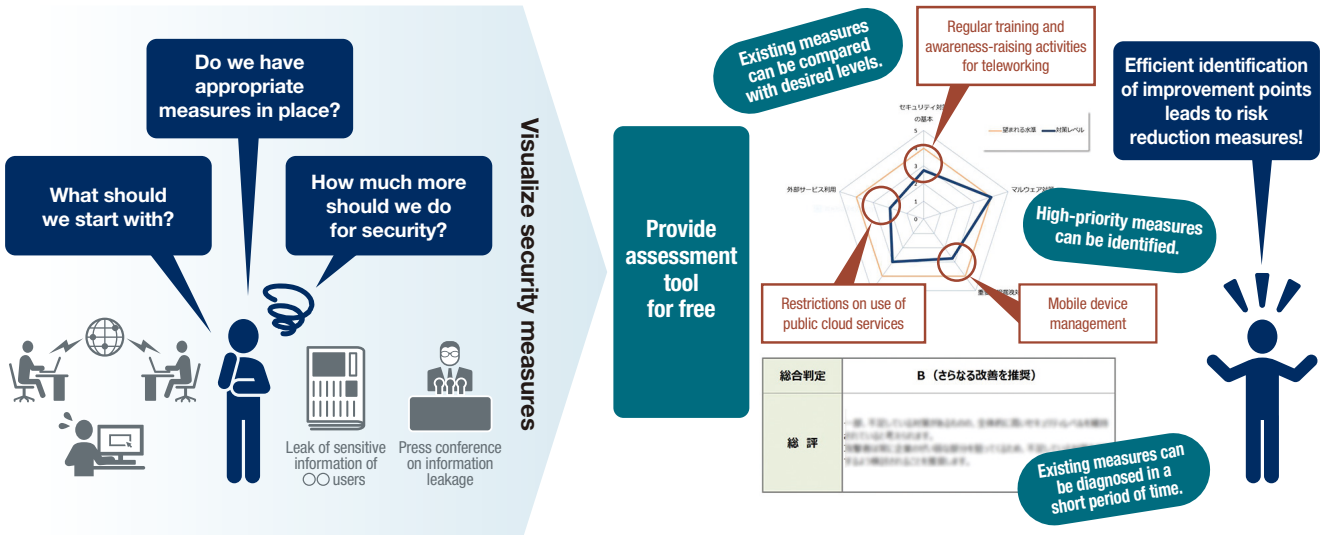
Telework Security Risk Assessment

Pre-introduction assessment to prioritize security measures

NEC provides an assessment service for security consultants to assist in the introduction of teleworking. A team of consultants assesses the corporate organization, internal systems and equipment, etc., based on the Cybersecurity Management Guidelines, Telework Security Guidelines (the Ministry of Internal Affairs and Communications), NIST SP800-171, and other relevant standards, and offers assistance in formulating necessary measures. Visualizing security risks and analyzing their costs and impacts helps determine the priorities of those risks.

- Use of the NEC Group’s unique contents created on the basis of the standards and guidelines appropriate for the target customer
- Efficient assessment by using hearing and assessment sheets in combination
- Assessment result report to explain identified problems and propose possible measures based on their impacts and root causes
- Mitigation of security risks by prioritizing identified problems and taking appropriate measures
- Assessment conducted on a regular basis to maintain and improve the security level

Promoting Security Measures by Visualizing Risks



Telework Security Consulting

Multifaceted analysis to offer proposals on a range of topics from work improvement to organization building from the management perspective

NEC provides a consulting service to assist in formulating security measures for the introduction of teleworking from the cybersecurity management perspective. Leveraging our internal hands-on experiences, we help customers review the security policies of their organizations and establish security management systems in order to introduce teleworking across the board including suppliers in the supply chain.

Security Measure Support Service

Total security measure support for the introduction of teleworking

This service helps customers enhance security for the entire process from measure formulation to system integration with regard to the risks visualized through the security assessment tool (free), security risk assessment, security consulting, etc. as they prepare to introduce teleworking for various jobs.

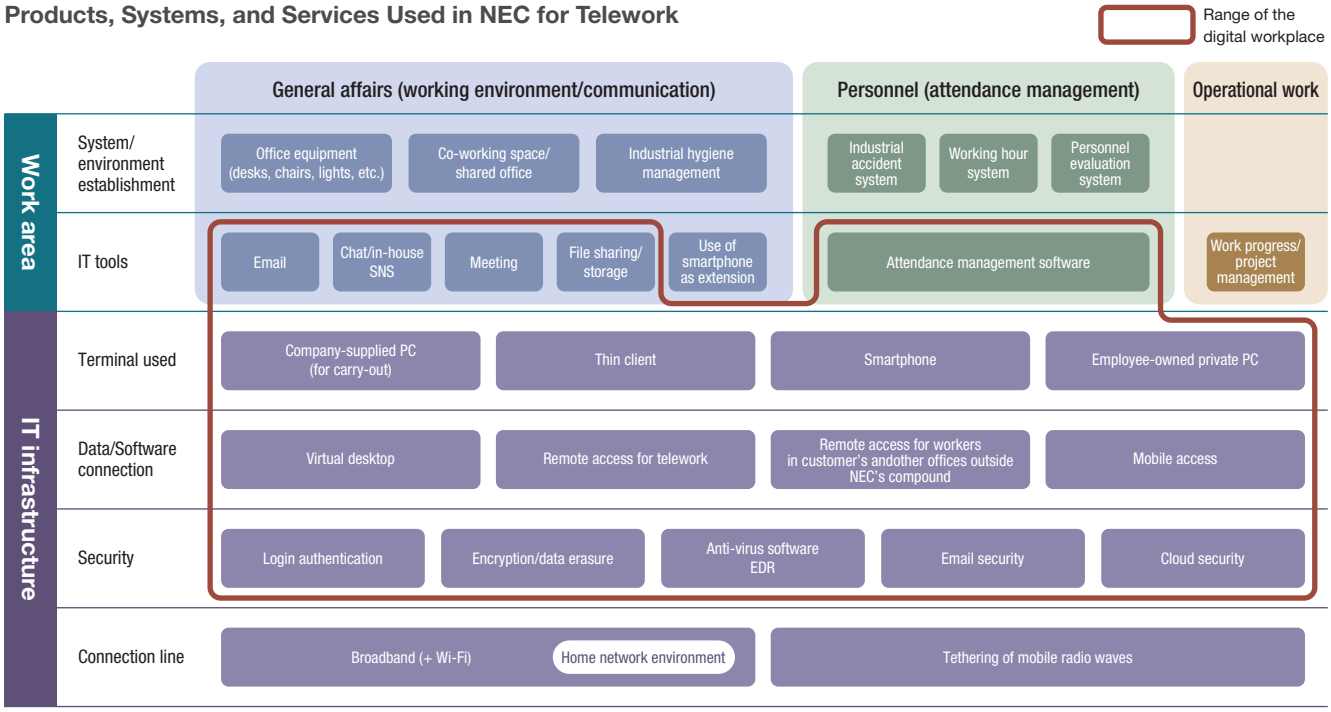
While making use of the existing security measures in which customers have invested, we offer total support for the deployment of new security measures so that customers can implement a teleworking environment and address cyberattacks and information leaks.

Examples of measures

- Remote access
- Cloud security measures
- Authentication enhancement
- Information leak prevention measures
- Endpoint security measures

Lastly, the COVID-19 pandemic is said to continue for several years, and there is an urgent need to establish a digital workplace environment that allows employees to work anywhere, anytime. The following figure shows the products, systems, and services that NEC has deployed within the Group to implement teleworking. Enclosed in the bold-line frame is the range of the digital workplace. We hope that our customers and business partners find it informative.

Products, Systems, and Services Used in NEC for Telework



NEC's Cyber Security 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

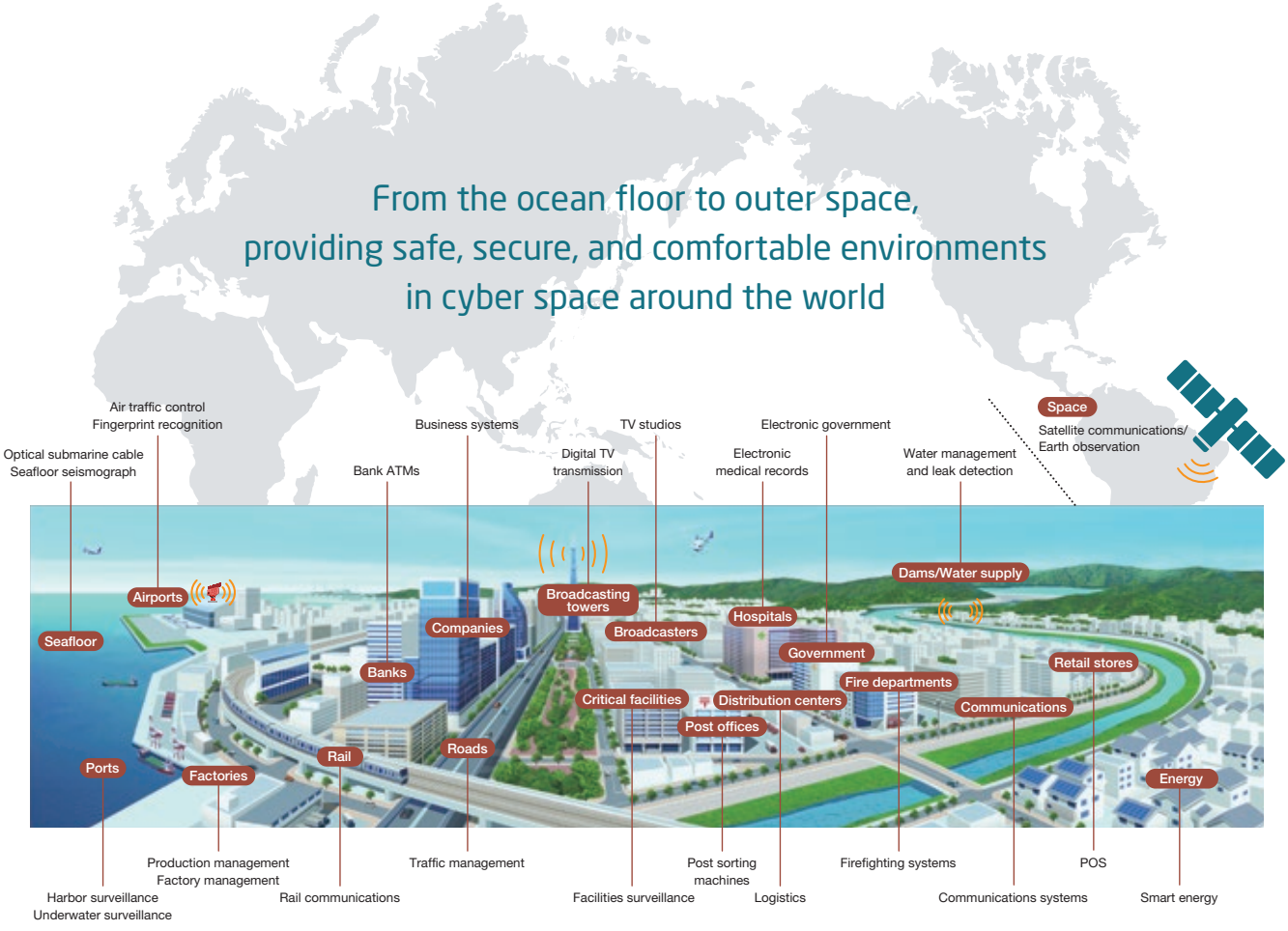
In a keynote speech titled "Shaping the Communications Industry to Meet the Ever-Changing Needs of Society" in October 1977, the NEC Group put forth the concept of "C&C (Computer & Communication)" as its slogan for achieving the integration of computers and communications. In line with this declaration, 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 government-industry-academia collaboration among domestic academic research organizations, industries, and legal enforcement bodies and enhancing cybercrime measures. 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 Cyber Security 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.

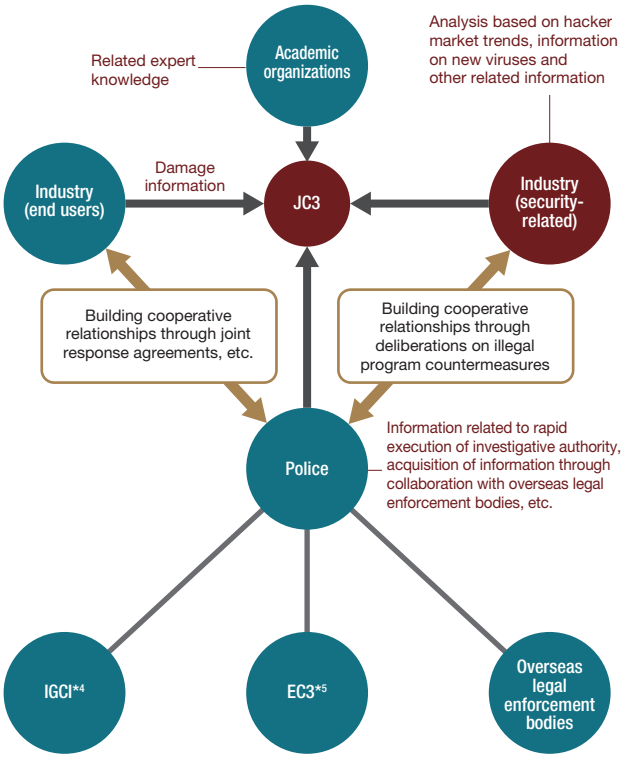
Participation in AIS* initiative of the U.S. Department of Homeland Security (DHS) for public-private sector intelligence sharing (March 2017)
NEC became the first Japanese company to join the AIS initiative of the U.S. Department of Homeland Security (DHS) for swiftly sharing intelligence on cyber threats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

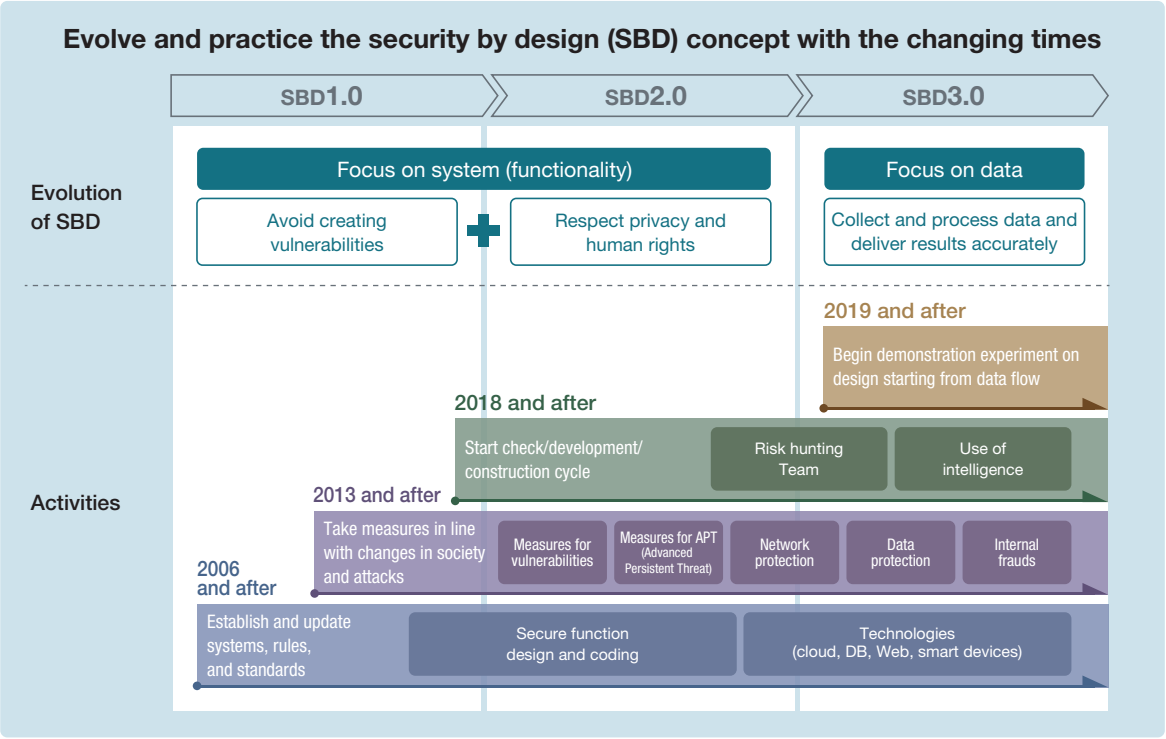
❸ Investments in the Development of Domestic Security Human Resources

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)

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

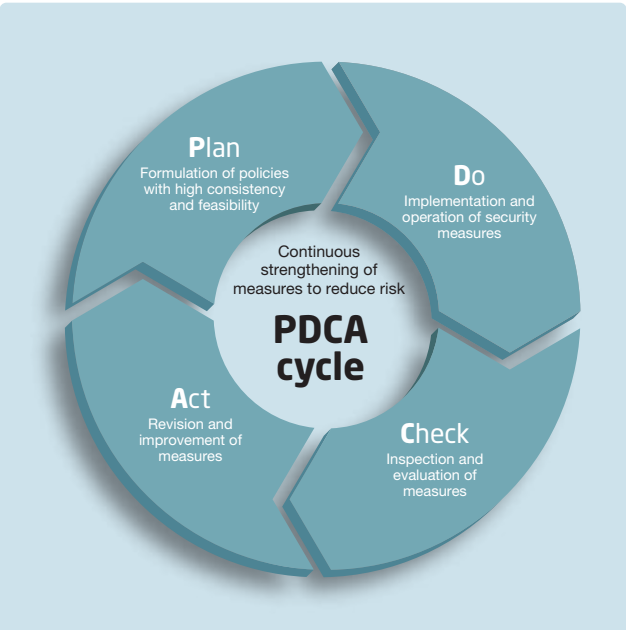
5 Support for Strengthening Security Based on In-House Operational Expertise

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.

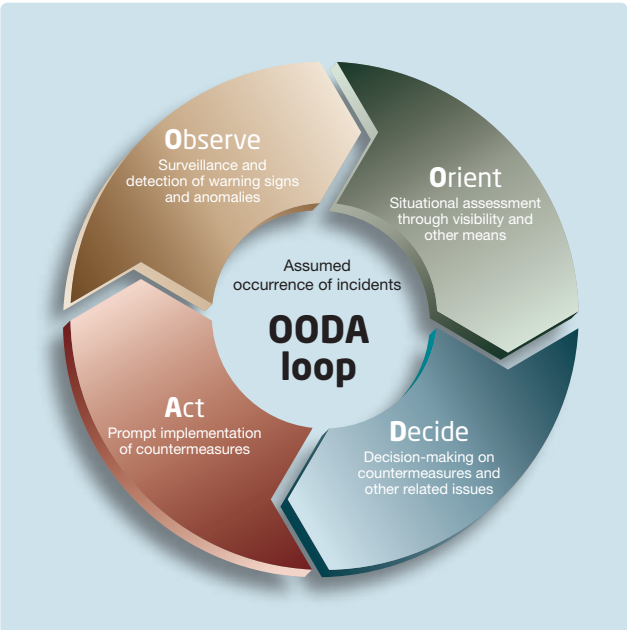
It is essential to implement the PDCA cycle of creating cybersecurity policy, taking measures, checking effects, and making improvements, as well as to have continuous measures in place to eliminate vulnerabilities. Building on its experience in operating the systems used by about 110,000 NEC Group employees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

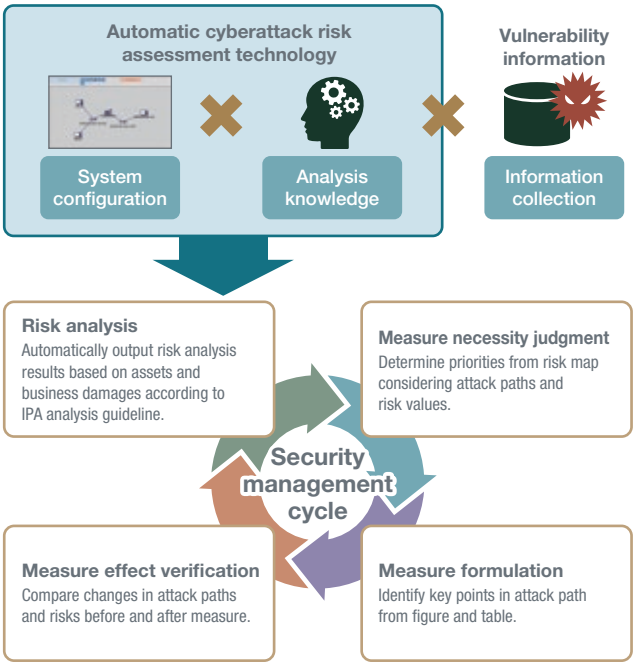
In order to realize a society in which anyone can use digital technology with a sense of security, the NEC Group is conducting R&D activities on both system security and data security, based on the Security by Design (SBD) concept whereby security is taken into consideration from the planning and design stages.
In the field of system security, we have developed some leading-edge technologies. These include the automatic cyberattack risk assessmenttechnology to visualize security risks from increasingly sophisticated and advanced cyberattacks and the lightweight tamperdetection 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

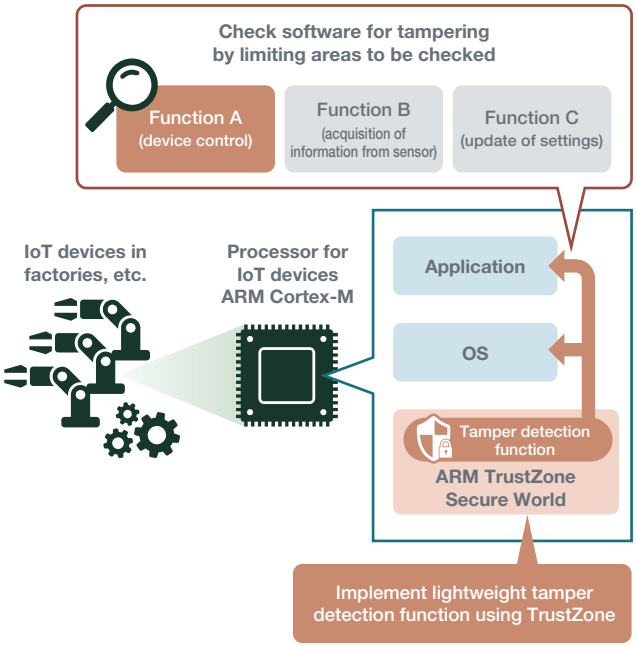
In order to prepare for ever-increasing cyberattacks, it is crucial to keep collecting the latest information, identify the system's potential risks for new threats and vulnerabilities, and take actions beforehand. However, analyzing risks, judging whether to respond, and considering measures to take require numerous 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 TamperDetection Technology



3 Lightweight TamperDetection 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

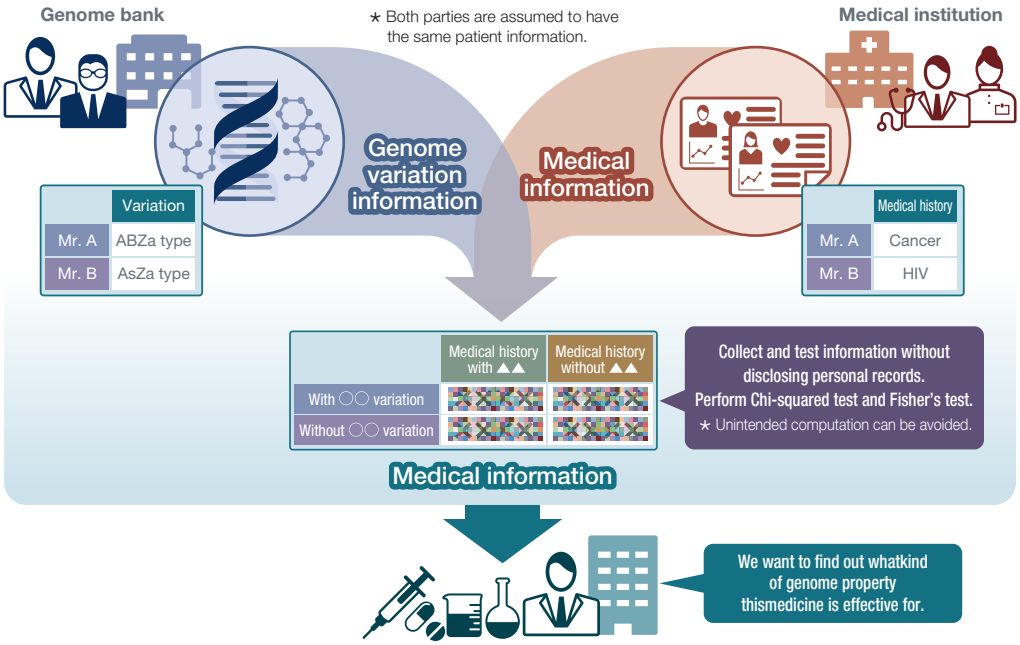
Lightweight cryptography runs smoothly even on IoT devices with limited resources. NEC has the world's top-level lightweight cryptography technology and has proposed it for consideration in the lightweight cryptography standardization process in the U.S., where screening is underway. The use of lightweight 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 VALWAY, 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 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
- YEC Solutions Inc.
- Q&A Corporation
- Q&A WORKS Co., Ltd.
- 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

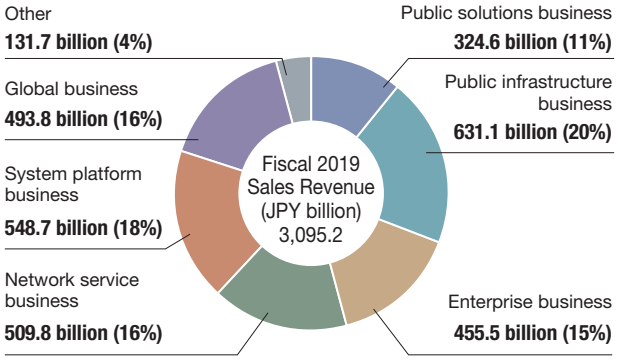
Corporate Profile

Company name	NEC Corporation
Address	7-1, Shiba 5-chome, Minato-ku, Tokyo, Japan
Established	July 17, 1899
Capital	¥397.2 billion*
Number of employees (Consolidated)	112,638*
Consolidated subsidiaries	300 companies*

*As of March 31, 2020

Segment Information

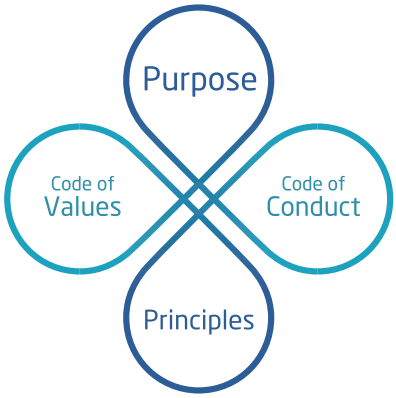
Sales Revenue by Segment (Percentage)



*As of March 31, 2020

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 2020