\Orchestrating a brighter world

Information Security Report 2023

To Be “Truly Open, Truly Trusted”

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

Today, when the entire world is openly connected, it is becoming a critical challenge, for nations and businesses alike, how to address increasingly sophisticated AI-based cyberattacks, the growing risk of information leakage stemming from the increasing use of cloud services, and information management issues related to economic security.

Given these circumstances, NEC is building a zero trust security platform and has robust and flexible security measures in place across our group that are based on the Zero Trust Maturity Model of CISA[1].

We are stepping up our intelligence about increasingly damaging cyberattacks (proactive defense) and our resilience (ability to recover from cyberattacks) in line with Version 3.0 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). In addition, as part of our data-driven reform, we provide all employees with information on cybersecurity risks through dashboards, helping management make business decisions quickly and members of the workforce act spontaneously.

Our efforts also include enhancing the information security, including that of the supply chain, to provide high-quality and secure services, based on the concept of Security by Design 3.0, which takes security into account from the design phase. In order to develop security personnel who promote DX, we encourage our employees to acquire international information security certification of CISSP[2]. At the same time, we also work with educational institutions to foster future human resources. In recognition of these efforts, the Information Technology Federation of Japan awarded NEC the top-notch “two star” rating in its Cyber Index Corporate Survey 2022.

Going forward, we will stay focused on enterprise risk management as well as on providing internally implemented cutting-edge technologies. These include password-less authentication and walk-through facial recognition for entry/exit control using NEC’s facial recognition technology that is praised as the best in the world[3]. Through these efforts, we aim to earn sustained social trust.

Citing “Orchestrating a brighter world” as its Purpose, NEC is committed to using ICT to solve social issues and contribute to the realization of a safe, secure, fair and efficient world where everyone has the chance to reach their full potential. This report brings you up to date on the NEC Group’s information security activities. We hope that you read the report and find it informative.

[1] CISA: U.S. Cybersecurity and Infrastructure Security Agency
[2] CISSP: Certified Information Systems Security Professional
[3] NEC ranked first for five times in the facial recognition technology benchmarking testing conducted by the US National Institute of Standards and Technology (NIST).

For inquiries regarding this report, please contact:

Corporate CISO Office
Corporate IT and Digital 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 2023”

The purpose of this report is to introduce stakeholders NEC Group’s information security activities performed based on “Cybersecurity Management Guidelines Ver. 3.0” by the Ministry of Economy, Trade and Industry, Government of Japan. The report covers our activities up to June 2023.

Contents

NEC’s Information Security Report

Cutting Edge of NEC’s Information Security

10 important directions of “Cybersecurity Management Guidelines Ver. 3.0” by the Ministry of Economy, Trade and Industry of Japan

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 improving cybersecurity measures continuously
Direction 7 Develop an emergency response system for cybersecurity incidents
Direction 8 Develop a business continuity and recovery system 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 Promote the collection, sharing, and disclosure of cybersecurity information

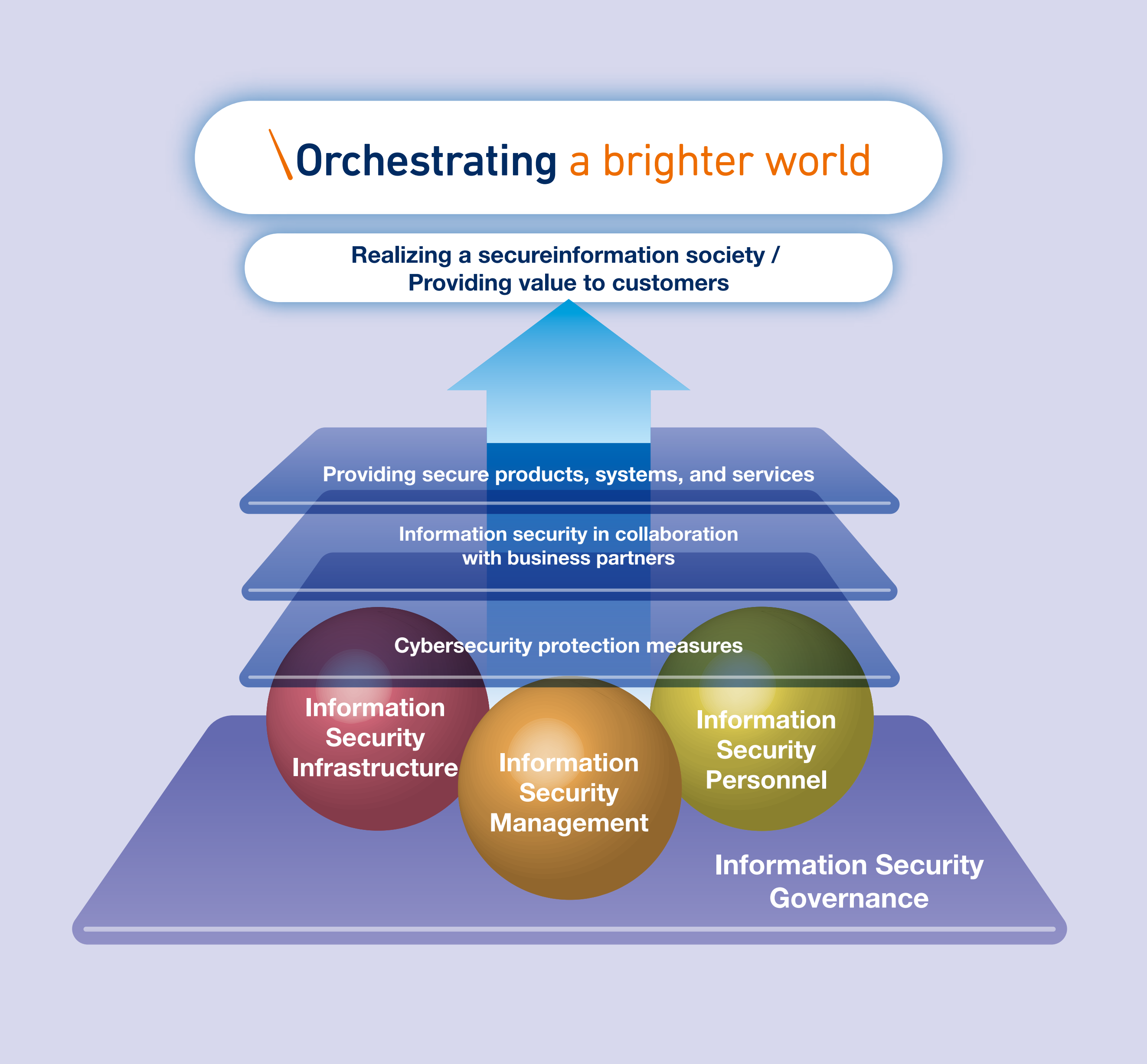
Information Security Promotion Framework

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

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

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

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


\Orchestrating a brighter world
Realizing a secureinformation society /
Providing value to customers
Providing secure products, systems, and services
Information security in collaboration
with business partners
Cybersecurity protection measures
Information Security Infrastructure
Information Security Management
Information Security Personnel
Information Security Governance

Information Security Governance

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

1 Information Security Governance in the NEC Group

With the understanding that ensuring information security is one of the top priority management issues, the NEC Group considers investments in information security indispensable for corporate management. We have established the NEC Group Management Policy, setting standardized rules and implementing unified systems, business processes, and infrastructure in order to create a foundation for standard global management. NEC has a regional CISO*[1] at each of its global operation sites. To enhance security governance, these regional CISOs are in charge of security management for their respective regions and take responsibility for the results of their management.

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

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

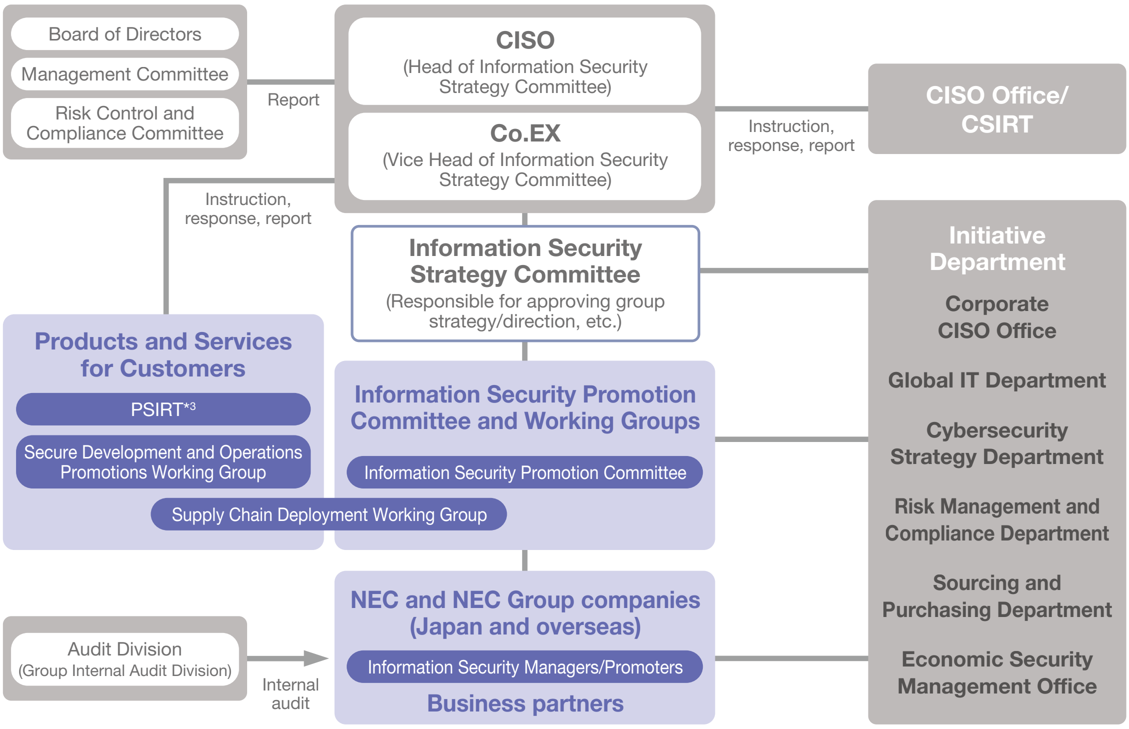
2 Information Security Promotion Organizational Structure of the NEC Group

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

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

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

Information Security Promotion Structure



Board of Directors
Management Committee
Risk Control and Compliance Committee
Report
CISO
(Head of Information Security Strategy Committee)
Co.EX
(Vice Head of Information Security Strategy Committee)
Instruction, response, report
CISO Office/ CSIRT
Instruction, response, report
Information Security Strategy Committee
(Responsible for approving group strategy/direction, etc.)
Initiative Department
Corporate CISO Office
Global IT Department
Cybersecurity Strategy Department
Risk Management and Compliance Department
Sourcing and Purchasing Department
Economic Security Management Office
Products and Services for Customers
PSIRT*3
Secure Development and Operations Promotions Working Group
Information Security Promotion Committee and Working Groups
Information Security Promotion Committee
Supply Chain Deployment Working Group
NEC and NEC Group companies (Japan and overseas)
Information Security Managers/Promoters
Business partners
Audit Division
(Group Internal Audit Division)
Internal audit

*1 CISO: Chief Information Security Officer *2 CSIRT: Computer Security Incident Response Team *3 PSIRT: Product Security Incident Response Team

Information Security Management

Direction 2 Direction 6

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 required information security measures while reviewing 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 first released the NEC Group Information Security Statement[*1] to establish and streamline a variety of rules, including rules concerning information security in general, trade secret control rules, and IT security rules.

Furthermore, after establishing the NEC Privacy Policy[*2], NEC obtained Privacy Mark certification in 2005 with relation to the protection of personal information. Our management system conforms to the Japan Industrial Standards Management System for the Protection of Personal Information (JISQ 15001) and Japan's Act on the Protection of Personal Information.

Also, in 2015, we added a My Number (personal identification number) management framework to ensure compliance with the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure ("My Number Act"). To comply with the Amended Act on the Protection of Personal Information, which was enacted in 2022, we have revised the personal information protection rules and manuals.

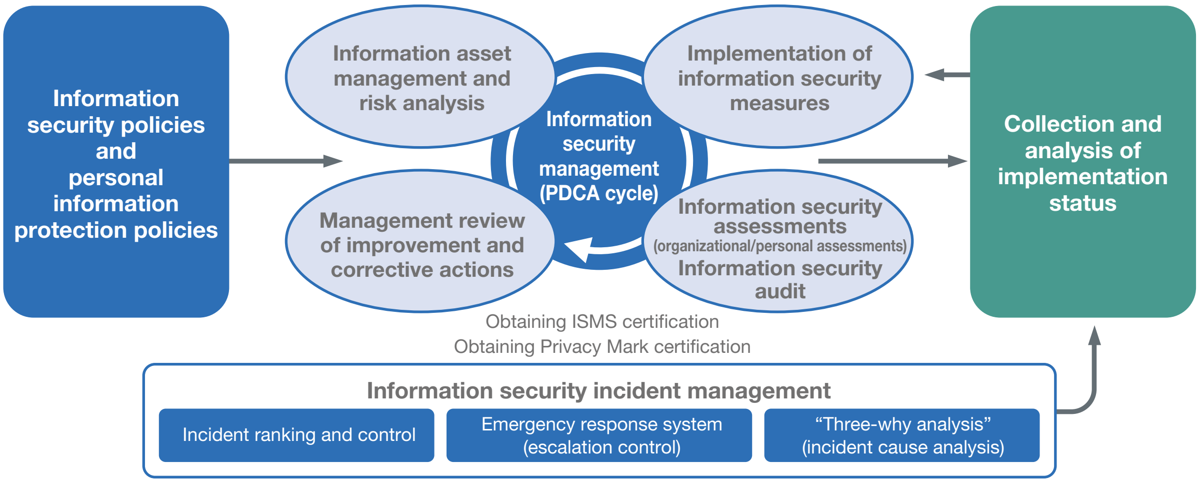
The NEC Group requires its employees to handle personal information at a common protection management level throughout the entire group. As of the end of June 2023, 31 NEC Group companies have acquired Privacy Mark certification.

3 Information Security Risk Management

❶ Information Security Risk Assessment

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

NEC's Information Security Management


Information security policies and personal information protection policies
Information asset management and risk analysis
Implementation of information security measures
Information security management (PDCA cycle)
Management review of improvement and corrective actions
Information security assessments (organizational/personal assessments) Information security audit
Collection and analysis of implementation status
Obtaining ISMS certification
Obtaining Privacy Mark certification
Information security incident management
Incident ranking and control
Emergency response system (escalation control)
"Three-why analysis" (incident cause analysis)

*1: NEC Group Information Security Statement https://www.nec.com/en/global/iss/index.html
*2: NEC Privacy Policy https://jpn.nec.com/site/privacy/en/privacy.html

2 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.

3 Initiatives for Business Continuity

The NEC Group conducts third-party assessments to assess our capability to ensure business continuity when facing cyberattacks on our critical systems. Additionally, we conduct exercises to practice our response and recovery procedures in the event of real incidents.

4 Critical Information Management

1 Three Lines Model

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

2 Strict Management of Critical Information

The NEC Group classifies the trade secrets it handles into several categories based on the secrecy level for management. Each organization checks details of all information they handle, and identifies which information belongs to which category to ensure that all necessary information is properly managed without recognition errors.

We also have rules for handling, storing, and managing critical information according to their importance, as well as thorough measures to prevent information leaks.

5 Information Security Assessments and Audits

1 Information Security Assessments

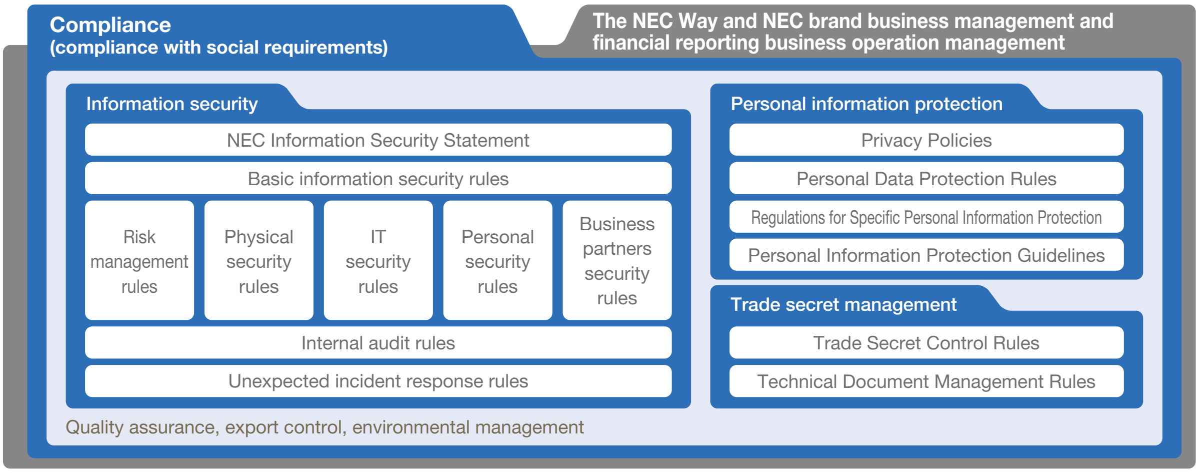
In the light of the analysis results of information security incidents and the recent cyberattack trends, we conduct assessments on an annual basis with priorities set to eliminate information leaks (97% response rate in FY2022). These assessments are intended to grasp the implementation status of security measures by each organization. Surveys on the priority measures help respondents realize what is required to secure their environment and to raise their awareness for improvement.

If there is any measure that failed to be sufficiently implemented, the responsible organization is asked to find out the reason for the failure and make improvements. If the problem cannot be solved by the organization alone, the NEC Group addresses that problem on a continual basis through the information security promotion plan for the following fiscal year.

2 Information Security Audits

NEC's Audit Division drives internal annual audits on information security management, such as critical information handling, as well as on the protection of personal information. 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. We also promote the acquisition of ISMS certification.
(For the companies that have obtained ISMS certification, see page 30.)

NEC Group Management Policy



Compliance
(compliance with social requirements)

The NEC Way and NEC brand business management and financial reporting business operation management

Information security

NEC Information Security Statement

Basic information security rules

Risk management rules

Physical security rules

IT security rules

Personal security rules

Business partners security rules

Internal audit rules

Unexpected incident response rules

Personal information protection

Privacy Policies

Personal Data Protection Rules

Regulations for Specific Personal Information Protection

Personal Information Protection Guidelines

Trade secret management

Trade Secret Control Rules

Technical Document Management Rules

Quality assurance, export control, environmental management

Information Security Infrastructure

Direction 3 Direction 5

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

1 Identity Security

Proper identification and authentication of users is an essential part of information security. Identifying and authenticating individuals enables proper control of access to information assets and prevents spoofing and other fraudulent activities. The information used for identification, authentication, and authorization includes user IDs and attribute information such as information about organizations and roles. Access to business systems and other company infrastructure is controlled on an individual basis.

NEC has built an authentication platform to manage information used for identification, authentication, and authorization on a group-wide basis, which covers not only our employees but also some business partners and other related parties if needed for business. We also centrally manage by which system and for what purpose the information is being used.

For systems that handle critical information, we adopt multi-factor authentication utilizing electronic certificate-based individual authentication (possession-based authentication) and facial recognition (biometric authentication) in addition to passwords (knowledge-based authentication). For using cloud services, we provide an authentication system that is seamlessly integrated with the internal authentication platform, in order to ensure that cloud services can be used safely and securely while meeting business needs quickly.

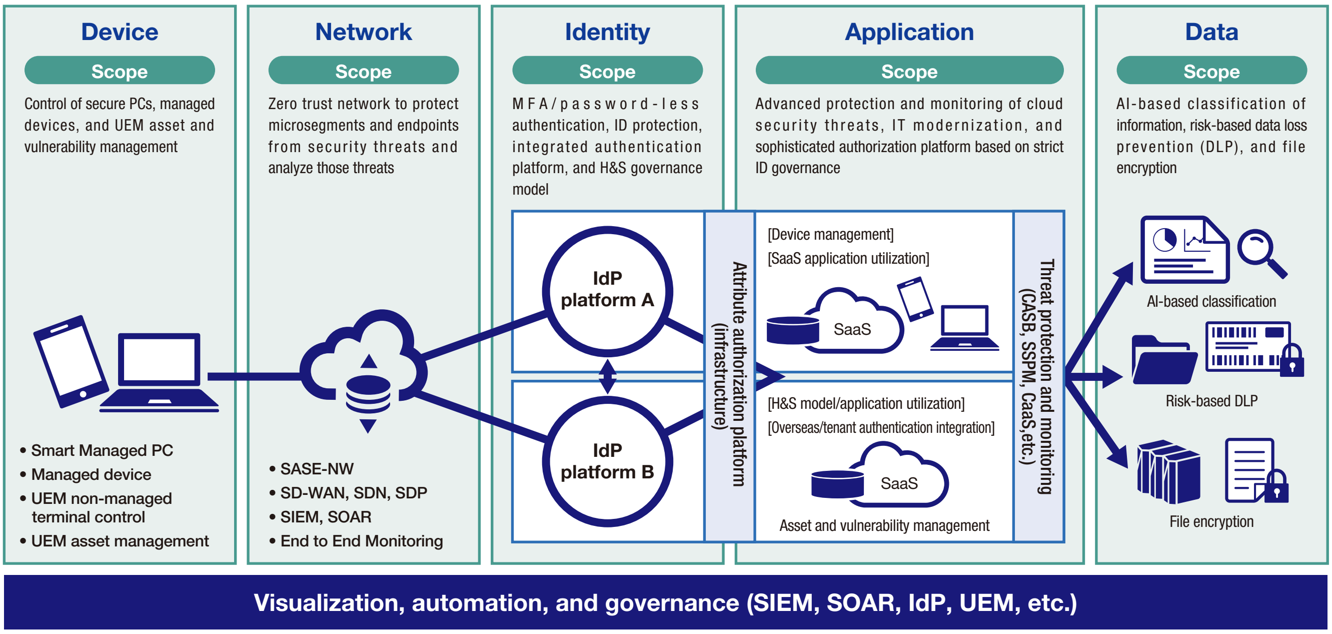
To provide enhanced and advanced authentication capabilities, NEC is deploying multi-factor authentication (MFA) and password-less authentication that satisfies the needs for both security and usability.

2 Device Security

NEC offers its employees various types of endpoint terminals for supporting diverse work styles. In addition to thin clients that do not store any data on the client side, we also use rich client-based PCs (Smart Managed PCs or SMPCs) that are secure and easy to use in a hybrid work environment that recently becomes more common, which allow employees to work both in a physical office and online. SMPCs feature secure facial recognition login, a comfortable operating environment that allows users to opt to go offline using dedicated resources, and simplified application and device setup among other capabilities. This has increased work efficiency and productivity while improving employee engagement.

We also have a unified endpoint management (UEM*2) platform to provide a secure device environment. This is aimed at making the entire NEC Group more resilient, cutting security management costs, promoting our internal DX initiatives, and bolstering risk response capability in order to enhance endpoint security across the NEC Group.

Overview and Scope of the Zero Trust Platform



Device

Scope

Control of secure PCs, managed devices, and UEM asset and vulnerability management

- Smart Managed PC
- Managed device
- UEM non-managed terminal control
- UEM asset management

Network

Scope

Zero trust network to protect microsegments and endpoints from security threats and analyze those threats

- SASE-NW
- SD-WAN, SDN, SDP
- SIEM, SOAR
- End to End Monitoring

Identity

Scope

MFA/password-less authentication, ID protection, integrated authentication platform, and H&S governance model

Application

Scope

Advanced protection and monitoring of cloud security threats, IT modernization, and sophisticated authorization platform based on strict ID governance

Data

Scope

AI-based classification of information, risk-based data loss prevention (DLP), and file encryption

IdP platform A
IdP platform B
Attribute authorization platform (infrastructure)
[Device management]
[SaaS application utilization]
SaaS
[H&S model/application utilization]
[Overseas/tenant authentication integration]
SaaS
Asset and vulnerability management
Threat protection and monitoring (CASB, SSPM, CaaS,etc.)
AI-based classification
Risk-based DLP
File encryption

Visualization, automation, and governance (SIEM, SOAR, IdP, UEM, etc.)

*1 CISA: U.S. Cybersecurity and Infrastructure Security Agency   *2 UEM: Unified Endpoint Management

As an effort to address information leakage risks, we implement various measures, including encryption, device control, and taking log records, so as to prevent information leaks resulting from external attacks, internal fraud, and so forth.

Encryption is done both at the hardware level and information level to prevent information leaks due to theft, loss, email sent to the wrong address, etc.

For the information-level encryption, we have infrastructure in place to make security settings with access privileges and the expiration date defined file by file. This encryption scheme protects information even if the information is transmitted to the outside after malware infection.

For device control, we set restrictions on using external media such as USB flash drives, SD cards, CDs, and DVDs as well as on communications devices such as smartphones and devices using Bluetooth or infrared technology. It is prohibited in principle to export information to these media and devices or to communicate with external devices that may cause information leaks. In cases such devices are needed for work, we allow each organization or employee to use specific devices or functions with minimum necessity.

We record all the operation logs of in-house PCs. In the event that an information leakage occurs, we analyze the logs to identify the impact of the incident, grasp the current situation, and develop measures to prevent a recurrence.

In addition, we define internal systems that require focused management. For these critical internal systems, we perform risk assessment and business impact analysis, and then implement suitable 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.

For the security of infrastructure, we have a global ICT platform in place to protect information devices and networks from various security threats.

❶ Support for User Environments

NEC Group employees are required to install management software to monitor the security status of their PCs, which visualizes if all required measures have been installed on all PCs, thus enabling us to grasp security risks on a real time basis. In addition, there is a system in place to automatically distribute security patches and definition file updates of anti-virus software, ensuring that all of them are properly installed. We also define prohibited software programs and monitor whether every user is using software appropriately.

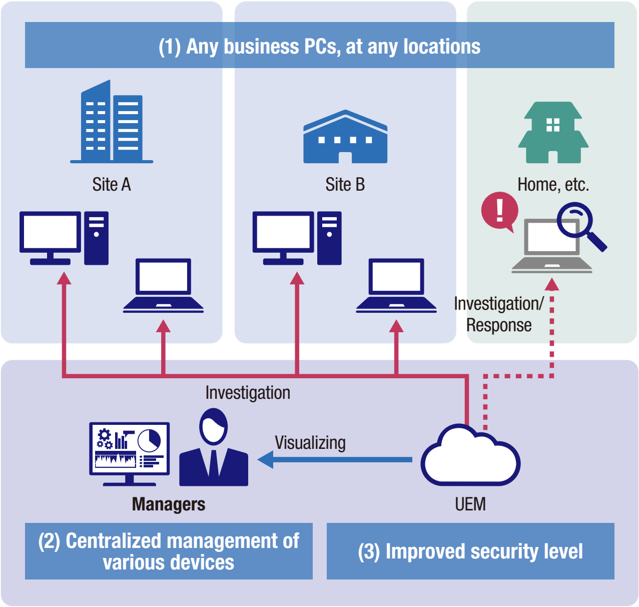
❷ Network Management

In addition to visualizing the PC status, we exercise control so that, if a PC with insufficient security is connected to the intranet or malware is detected on a PC or in a segment of the intranet, the PC or network segment is disconnected from the intranet. We also control outgoing communications by various methods including web access filtering based on an allow list, prohibiting the use of free email accounts, and sender domain authentication.

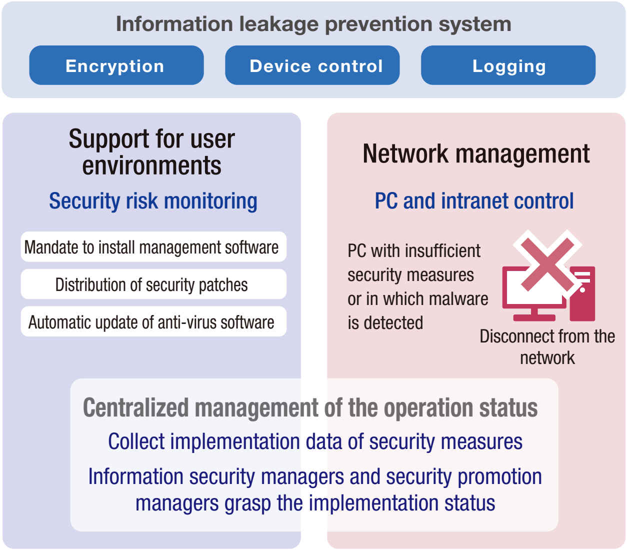
❸ Centralized Management of Security Updating

Data on the implementation status of security measures, including installation of patch programs and anti-virus software, is collected so that Information Security Managers/Promoters can grasp the implementation status in a timely fashion. This ensures rapid and smooth implementation of security measures.

UEM-based Secure Endpoint Management


(1) Any business PCs, at any locations
Site A
Site B
Home, etc.
Investigation/
Response
Investigation
Visualizing
Managers
UEM
(2) Centralized management of various devices
(3) Improved security level

Protect Devices and Networks from External Attacks and Internal Fraud


Information leakage prevention system
Encryption
Device control
Logging
Support for user environments
Security risk monitoring
Mandate to install management software
Distribution of security patches
Automatic update of anti-virus software
Network management
PC and intranet control
PC with insufficient security measures or in which malware is detected
Disconnect from the network
Centralized management of the operation status
Collect implementation data of security measures
Information security managers and security promotion managers grasp the implementation status

Ensure safe and secure use of the intranet

3 Network Security

The NEC Group has a zero trust platform deployed and expanded on a global scale to deliver both robustness and flexibility to system services and user devices.

The SD-WAN supports intranet segmentation and globally centralized control to enable incident prevention, emergency shutdown, and collection of a wider range of log data, thus boosting security, especially in faster damage localization and incident response. It also improves both security and usability by reducing the time it takes to make changes to the network, optimizing the network through Internet local breakouts, and increasing the total network bandwidth by twice.

Also, we upgrade remote connection environments to achieve zero trust security on a global basis. An access platform linking cloud RAS and proxy servers provides efficient access to resources scattered across SaaS, IaaS, and on-premise systems. Moreover, it enhances security through a zero trust model integrated with endpoint security and the next-generation authentication platform.

In addition to the above, NEC adopts Domain-based Message Authentication Reporting and Conformance (DMARC) to prevent email spoofing.

4 Application Security

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

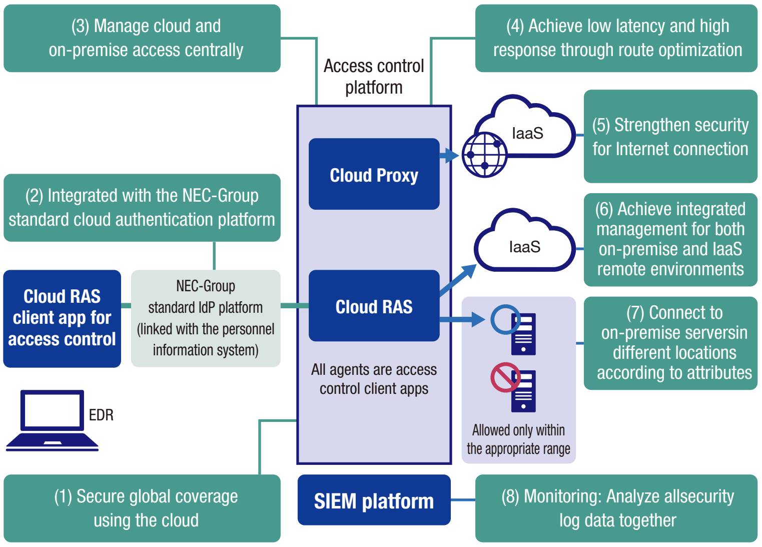
❶ Grasp of the SaaS Usage Status

We monitor and analyze log data and files on cloud services using the CASB*3 to protect the cloud services and critical data handled by them from internal fraud and cyberattacks. We also visualize the usage status of internally used cloud services to check whether any unapproved risky services are in use.

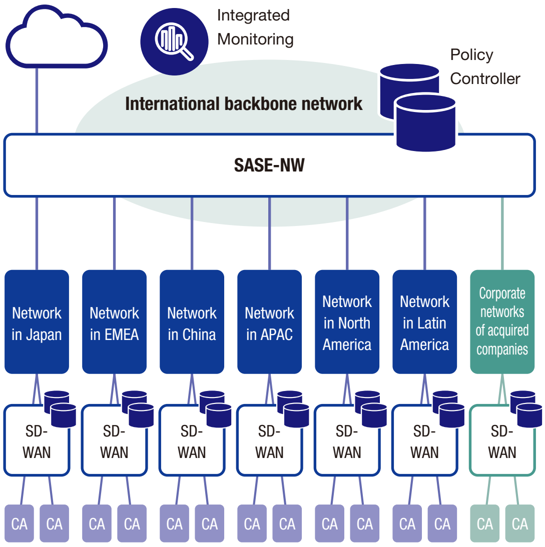
❷ Prevention of Incidents Resulting from Improper Public Cloud Settings

The use of public cloud services, such as AWS, Azure, and GCP, is increasing. While these services are easy to use, there is a risk of information leaking to the outside due to improper settings or for some other reason. The NEC Group employs CSPM*4 to check the settings of the internally used public cloud services according to the security standard and constantly monitor for potential risks.

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


(3) Manage cloud and on-premise access centrally
Access control platform
(4) Achieve low latency and high response through route optimization
IaaS
(5) Strengthen security for Internet connection
Cloud Proxy
(2) Integrated with the NEC-Group standard cloud authentication platform
IaaS
(6) Achieve integrated management for both on-premise and IaaS remote environments
Cloud RAS client app for access control
NEC-Group standard IdP platform (linked with the personnel information system)
Cloud RAS
(7) Connect to on-premise serversin different locations according to attributes
All agents are access control client apps
EDR
Allowed only within the appropriate range
(1) Secure global coverage using the cloud
SIEM platform
(8) Monitoring: Analyze allsecurity log data together

Global Deployment of SD-WAN



⭑3 CASB: Cloud Access Security Broker ⭑4 CSPM: Cloud Security Posture Management

❸ Prevention of Incidents Resulting from Improper SaaS Settings

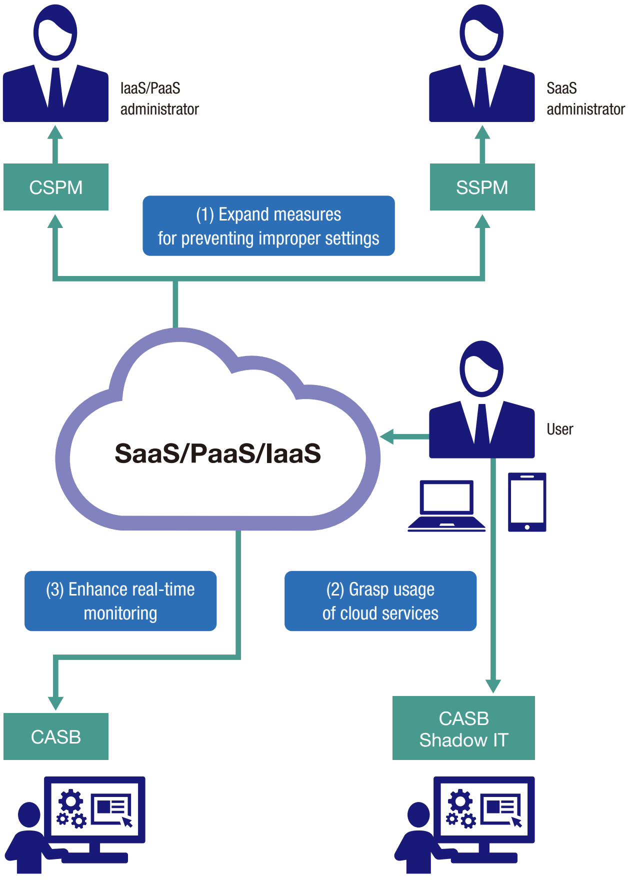
Cloud services such as Microsoft 365, Box, and Salesforce often require complicated setup before use, which tends to result in a risk of information leaking due to improper settings. The NEC Group has implemented a global strategy leveraging SSPM*5 to visualize and correct any misconfigurations in our internally used cloud services.

5 Data Security

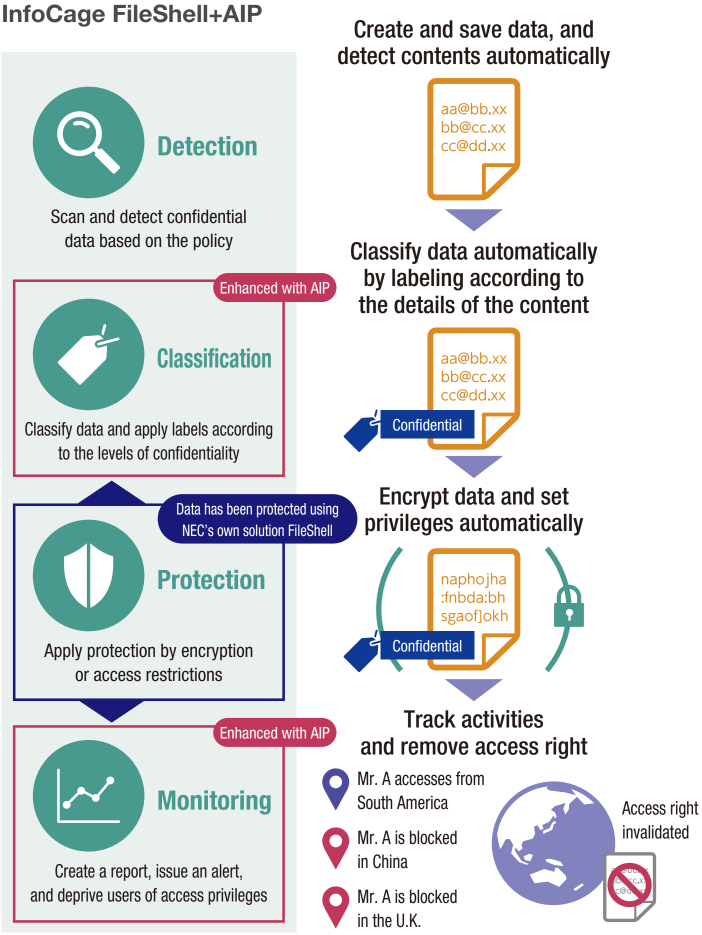
With an eye on security in the era of zero trust, the NEC Group protects data using its own solution "InfoCage FileShell." We achieve file-by-file automatic classification, encryption, tracking, access privileges management, and so forth through the use of AIP*6 unified labeling that supports a cloud environment. This allows accurate data management in a zero trust environment.

Also, to accomplish thorough information management, we have implemented the Secure Storage service as infrastructure to securely manage critical information. The service meets the requirements for critical information management such as access control, encryption, trail management, intrusion investigation, and ISMS management while reducing the operational burden of the personnel.

Security Measures for Using Cloud Services


IaaS/PaaS administrator
SaaS administrator
CSPM
SSPM
(1) Expand measures for preventing improper settings
SaaS/PaaS/IaaS
User
(3) Enhance real-time monitoring
(2) Grasp usage of cloud services
CASB
CASB Shadow IT

InfoCage FileShell+AIP


Detection
Scan and detect confidential data based on the policy
Enhanced with AIP
Classification
Classify data and apply labels according to the levels of confidentiality
Data has been protected using NEC's own solution FileShell
Protection
Apply protection by encryption or access restrictions
Enhanced with AIP
Monitoring
Create a report, issue an alert, and deprive users of access privileges
Create and save data, and detect contents automatically
aa@bb.xx
bb@cc.xx
cc@dd.xx
Classify data automatically by labeling according to the details of the content
Confidential
Encrypt data and set privileges automatically
naphojha
:fnbda:bh
sgaofJokh
Track activities and remove access right
Mr. A accesses from South America
Mr. A is blocked in China
Mr. A is blocked in the U.K.
Access right invalidated

*5 SSPM: SaaS Security Posture Management *6 AIP: Azure Information Protection

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 Personnel and Expanding the Scope of Their Expertise

NEC is training all its employees to develop information security personnel from three points of view: 1) raising awareness of information security; 2) developing personnel to promote information security measures; and 3) developing personnel capable of practicing Security by Design (SBD).

2 Raising Awareness of Information Security

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

❶ Training on Information Security and Personal Information Protection

NEC provides a WBT*[1] course on information security and personal information protection (including protection of people's personal identification numbers [“My Numbers” in Japan]) for all NEC Group employees to increase knowledge and skills in the information security field. (In fiscal year 2022, 97% of employees completed the course, which is available in seven foreign languages.) The content of the training is updated every year to reflect the trends of information security, such as emerging threats, appropriate ways of handling information, and security measures required in remote work.

❷ Commitment to Following Information Security Rules

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

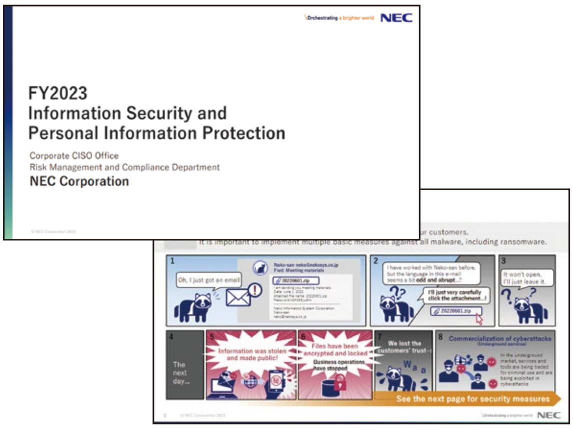
❸ Activities to Raise Awareness of Information Security

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

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 Registered Information Security Specialist (RISS) qualification are assigned to the role.

Training for All Employees



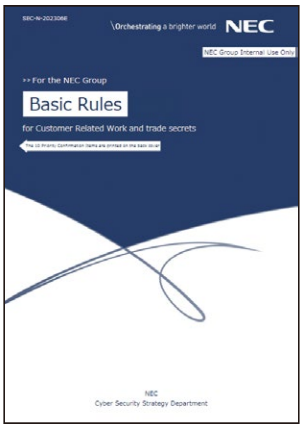
\Orchestrating a brighter world NEC

FY2023
Information Security and
Personal Information Protection

Corporate CISO Office
Risk Management and Compliance Department
NEC Corporation

...ur customers.
It is important to implement multiple basic measures against all malware, including ransomware.

1
Oh, I just got an email
Neko-san neko@nekosys.co.jp
Fwd: Meeting materials
20220601.zip
2
I have worked with Neko-san before, but the language in this e-mail seems a bit odd and abrupt...?
I'll just very carefully click the attachment...!
20220601.zip
3
It won't open. I'll just leave it.
4
The next day...
5
Information was stolen and made public!
6
Files have been encrypted and locked
Business operations have stopped
7
We lost the customers' trust...
Waa
8
Commercialization of cyberattacks
(Underground services)
In the underground market, services and tools are being traded for criminal use and are being exploited in cyberattacks
See the next page for security measures



SEC-N-2023066

\Orchestrating a brighter world NEC

NEC Group Internal Use Only

>> For the NEC Group

Basic Rules

for Customer Related Work and trade secrets

NEC
Cyber Security Strategy Department

[1] WBT: Web Based Training [2] CISSP: Certified Information Systems Security Professional

4 Developing Personnel Capable of Practicing Security by Design (SBD)

We are committed to developing security personnel to implement appropriate security in products, systems, and services provided by the NEC Group and to help customers reduce business risks.

❶ NEC Cybersecurity Training Site

This training site is provided for all employees involved in customer systems to acquire the knowledge necessary to speak to customers about security and to learn adequate risk assessment techniques. A dedicated virtual environment that emulates an e-commerce (EC) site is used for practical security training, and employees learn about environment hardening techniques in the system construction phase. The training course that supports remote learning was attended by more than 1,900 employees, mainly sales personnel and system engineers, in fiscal year 2022. Since March 2019, a total of 6,000 employees have received the course.

❷ Group-wide CTF

To expand the breadth of NEC's security personnel, NEC has held an in-house CTF*3 event called "NEC Security Skill Challenge," which is aimed to step up the employees' security skills and raise their security awareness. Since the event began in 2015, a total of over 7,200 employees have participated, with more than 800 employees voluntarily taking part in fiscal year 2022.

❸ Basic Security Training for Sales Personnel and System Engineers

NEC provides e-learning courses for sales personnel and system engineers to acquire the basic security knowledge they need, with the focus on Security by Design (SBD). In fiscal year 2022, a total of more than 35,000 employees participated in these courses. The training is aimed at enhancing the security skills across the entire NEC Group.

❹ SBD Specialist Training

A program has been underway since fiscal year 2019 to develop specialists who assist security managers and implement SBD in the individual business divisions. A new course for salespeople started in fiscal year 2021 to help them acquire the skills required to present appropriate security proposals, including incident case studies and offerings of countermeasures. A total of over 55 employees have attended the program as of fiscal year 2022. 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.

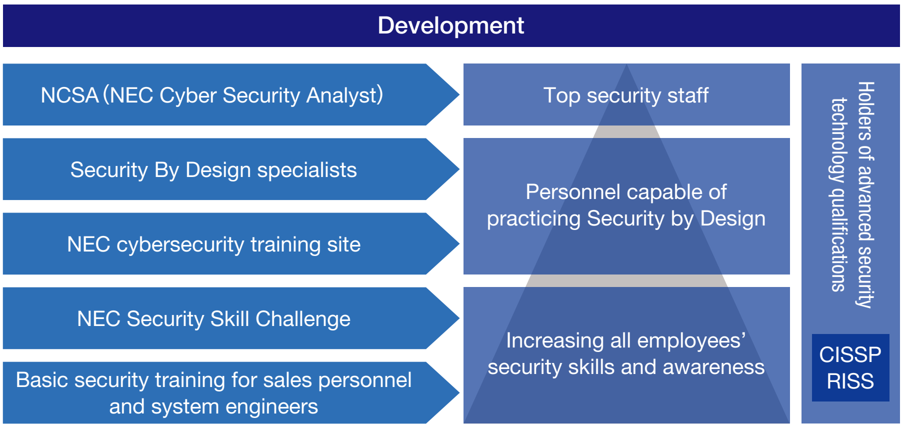
❺ NCSA (NEC Cybersecurity Analyst) Training

The purpose of this program is to enhance the skills of top security staff. Intended for those staff members who have knowledge of security technologies, the six-month intensive program lets attendees master the practical technical skills required for advanced security services, such as CSIRT*4 work and risk hunting. When combined with those who attended the NEC CISO Assistant Training (NCAT) program that lasted until fiscal year 2019, a total of 65 staff members have participated in these programs. They now engage in providing professional services.

❻ Holders of Advanced Security Technology Qualifications

NEC encourages its employees who directly serve customers, such as salespeople and system engineers, to acquire official qualifications for security as proof that they have high-level information security skills to deliver the most suitable solutions to customers. We hold internal seminars, workshops, and other events to increase the number of staff who acquire the CISSP international certification and Registered Information Security Specialist (RISS) certification. With regard to CISSP in particular, we have a strategic partnership with (ISC)², the governing body of the certification, and encourage our staff to get certified, in order to develop personnel who not only have advanced technical skills but are also capable of assessing risks from a business perspective. The NEC Group now has a total of more than 300 CISSP certification holders, up about 100 holders from fiscal year 2021.

Developing Personnel Capable of Practicing Security by Design (SBD)


Development
NCSA (NEC Cyber Security Analyst)
Security By Design specialists
NEC cybersecurity training site
NEC Security Skill Challenge
Basic security training for sales personnel and system engineers
Top security staff
Personnel capable of practicing Security by Design
Increasing all employees' security skills and awareness
Holders of advanced security technology qualifications
CISSP
RISS

*3 CTF: Capture the Flag   *4 CSIRT: Computer Security Incident Response Team

Measures Against Cyberattacks

Direction 4 Direction 5 Direction 7 Direction 8 Direction 10

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 Global Cyberattacks

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.

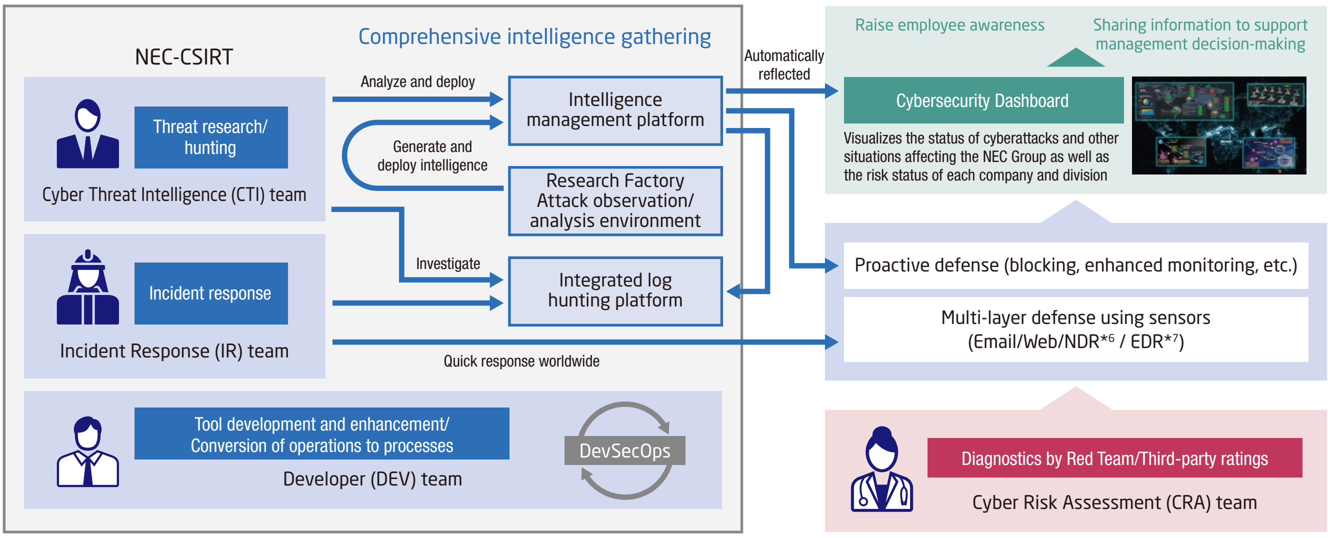
Specifically, with the belief that taking a globally standardized approach toward cybersecurity risks is vital for business continuity, we use AI and other technologies to continuously monitor for possible cyberattacks and analyze and grasp the situation, and review our monitoring and operation processes whenever needed.

NEC researches security products and services as well as market trends to keep track of the ever-changing technology. Also, through PoC[*3] evaluations and internal IT environment research, we analyze if the products and services work well and meet the security requirements in our environment. Based on the results of research and analysis, we consider countermeasures that will be needed in the future and determine the targeted scope while finding out their effects and costs.

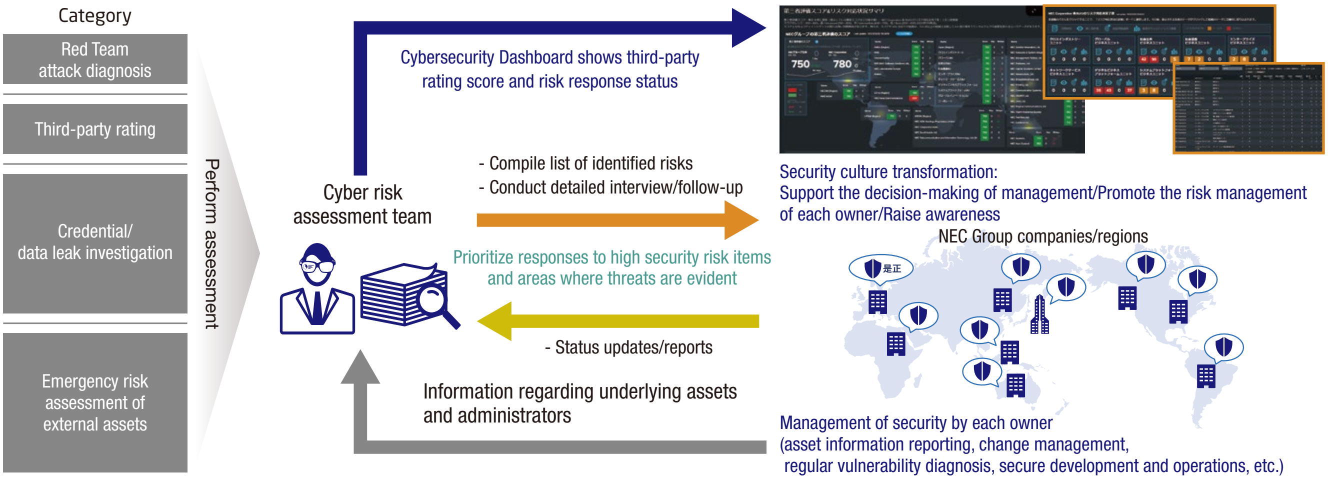
We create an action plan every year based on the above-mentioned activities and, upon approval of the CISO[*4], carry out the planned measures.

The NEC Group implements measures against ever sophisticated cyberattacks based on the concept of multilayered defense. We are focused particularly on: 1) cyber risk assessment by the Red Team[*5], 2) generation and use of threat intelligence, 3) enhancement of the CSIRT structure, and 4) enhancement of systematic security resilience.

Overview of Our Cybersecurity Measures


NEC-CSIRT
Comprehensive intelligence gathering
Threat research/ hunting
Cyber Threat Intelligence (CTI) team
Analyze and deploy
Generate and deploy intelligence
Intelligence management platform
Research Factory Attack observation/ analysis environment
Investigate
Integrated log hunting platform
Incident response
Incident Response (IR) team
Quick response worldwide
Tool development and enhancement/ Conversion of operations to processes
Developer (DEV) team
DevSecOps
Automatically reflected
Raise employee awareness
Sharing information to support management decision-making
Cybersecurity Dashboard
Visualizes the status of cyberattacks and other situations affecting the NEC Group as well as the risk status of each company and division
Proactive defense (blocking, enhanced monitoring, etc.)
Multi-layer defense using sensors (Email/Web/NDR*6 / EDR*7)
Diagnostics by Red Team/Third-party ratings
Cyber Risk Assessment (CRA) team

Cyber Risk Assessment


Category
Red Team attack diagnosis
Third-party rating
Credential/ data leak investigation
Emergency risk assessment of external assets
Perform assessment
Cyber risk assessment team
Cybersecurity Dashboard shows third-party rating score and risk response status
- Compile list of identified risks
- Conduct detailed interview/follow-up
Prioritize responses to high security risk items and areas where threats are evident
- Status updates/reports
Information regarding underlying assets and administrators
750
780
Security culture transformation:
Support the decision-making of management/Promote the risk management of each owner/Raise awareness
NEC Group companies/regions
是正
Management of security by each owner
(asset information reporting, change management,
regular vulnerability diagnosis, secure development and operations, etc.)

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

[*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] NDR: Network Detection and Response [*7] EDR: Endpoint 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 for improving cyber resilience and accountability of the group as well as for attack surface management (ASM).

Working with auditing firms and security companies, the team assesses cyber risks on a global scale through third-party evaluations of intrusion probability from outside and inside the company from the attacker's point of view, examination of critical information management, investigation of asset risks such as public server vulnerabilities, investigation of credential information and data leaks, and third-party security ratings by BitSight and other organizations. They check the existing security measures and operations, identify what is lacking or insufficient, and take actions for improvement in collaboration with server administrators, managers of overseas affiliates, and so forth.

❷ Generation and Use of Threat Intelligence

The Cyber Threat Intelligence (CTI*8) team identifies threats to NEC including their early signs and implements proactive high-level defense. Using a group-wide EDR platform, a unique CSIRT-developed NDR platform, and an integrated log analysis platform, the team hunts unknown threats.

We also have a research environment (Research Factory) in place for enhancing our ability to generate unique CTI proactively and analyze threats in detail.

❸ Enhancement of the CSIRT Structure

We have a CSIRT under the direction of the CISO. This team monitors for cyberattacks, analyzes the characteristics of attacks and malware programs, and shares information with relevant organizations. In the event of a security incident, they protect systems and other assets and analyze the attack to identify the cause and recover from the incident.

The CSIRT consists of four teams: the CTI team that utilizes threat intelligence, the IR team that responds to incidents, the SOC team that monitors for alerts from security devices 24/7, and the Developer team that enhances tools, platforms, and operation processes. For overseas group companies, we have another CSIRT in Singapore, which works with the CSIRT in Japan to share threat information such as detected incidents and unauthorized communication sources on a global scale.

If a security incident occurs, the CSIRT works upon approval of the CISO to achieve recovery from the incident in cooperation with the related divisions while taking risks into account.

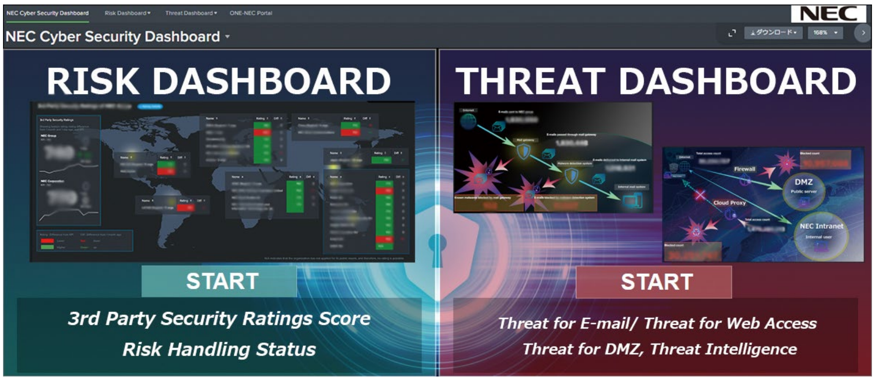
❹ Enhancement of Systematic Security Resilience

To make ourselves better prepared for global cyber threats such as ransomware, we train our employees on targeted email attacks and provide manuals and guidelines to enable a rapid response to a security incident. We also conduct contingency drills at least once every six months attended by staff of the related divisions and experts.

2 Security Culture Transformation Using Cybersecurity Dashboards

We release cybersecurity dashboards that visualize the cyberattacks targeting the NEC Group, the threat intelligence gathered by the CTI team, and the security risks of the individual companies and divisions found by the cyber risk assessment. These dashboards are available to all employees. Having each employee understand the actual situation and risks helps raise their security awareness. The dashboards are used at executive meetings, as well as at meetings attended by overseas group companies, to check how each individual organization is responding to security risks. Through these meetings, we identify the organizations at high risk that are exposed to threats and take immediate actions, such as requesting improvements. This enables quick business decisions and helps promote the management of security managers.

NEC Cybersecurity Dashboard


NEC Cyber Security Dashboard
Risk Dashboard
Threat Dashboard
ONE-NEC Portal
NEC
NEC Cyber Security Dashboard
ダウンロード
RISK DASHBOARD
THREAT DASHBOARD
Firewall
DMZ
Cloud Proxy
NEC Intranet
START
START
3rd Party Security Ratings Score
Risk Handling Status
Threat for E-mail/ Threat for Web Access
Threat for DMZ, Threat Intelligence

[*8] CTI: Cyber Threat Intelligence

Information Security in Cooperation with Business Partners

Direction 9

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) technology deployment , 6) security implementation, 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. Additionally, submitting documentation to verify the subcontractor is required in order to clearly define the organizational roles within each individual project.

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 classified and labeled, that the taking of information outside the company is controlled, and that confidential information is appropriately disposed of or returned.

❺ Technology Deployment

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.

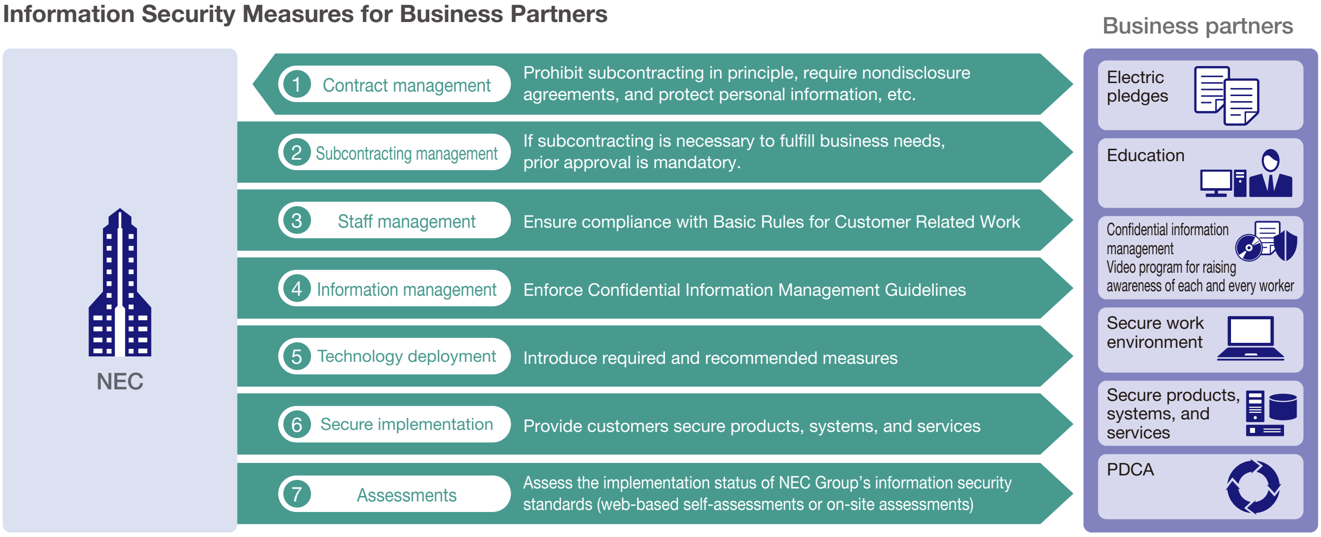
❻ Security Implementation

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

❼ Assessments

NEC assesses the implementation status of information security measures at each business partner and gives instructions for improvement as needed, based on the "Information Security Standards for Business Partners," which defines the security levels required by NEC. Taking into account recent circumstances in cybersecurity, NEC has updated the "Information Security Standards for Business Partners" to prepare for potential incidents and has further strengthened collaborative efforts with business partners.

Information Security Measures for Business Partners



NEC

1 Contract management: Prohibit subcontracting in principle, require nondisclosure agreements, and protect personal information, etc.

2 Subcontracting management: If subcontracting is necessary to fulfill business needs, prior approval is mandatory.

3 Staff management: Ensure compliance with Basic Rules for Customer Related Work

4 Information management: Enforce Confidential Information Management Guidelines

5 Technology deployment: Introduce required and recommended measures

6 Secure implementation: Provide customers secure products, systems, and services

7 Assessments: Assess the implementation status of NEC Group's information security standards (web-based self-assessments or on-site assessments)

Business partners

- Electric pledges
- Education
- Confidential information management Video program for raising awareness of each and every worker
- Secure work environment
- Secure products, systems, and services
- PDCA

2 Promotion of Security Measures for Business Partners

❶ Information Security Seminars

NEC organizes information security seminars every year for business partners in Japan (approximately 1,800 companies, including approximately 900 ISMS certified companies) to ensure that they understand and implement NEC's information security measures. We also hold seminars for overseas business partners and workshops on cybersecurity measures as needed.

❷ Skill Improvement Activities for Core Business Partners

NEC works closely with core business partners that conduct a particularly high volume of business with NEC (about 100 software firms) to encourage them to thoroughly implement security measures and improve their skills.

❸ Distribution of Measure Implementation Guidebooks

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

❹ Standardization of Contractor Management Process

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

3 Assessments and Improvement Actions for Business Partners

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

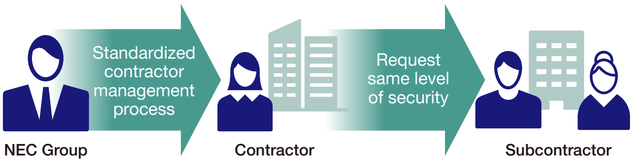
❶ Document-based assessment/on-site assessment

We conduct document-based assessment on about 1,800 selected companies that deal with NEC. The selected business partners assess the implementation status of security measures by themselves and feed back the assessment results to our Web system in real time. As for those business partners with whom we conduct a high volume of business, we carry out on-site assessment by visiting them directly or remotely. The number of companies we visit increases every year (we visited approximately 200 companies in fiscal year 2022). This activity is done by approximately 100 assessors of NEC.

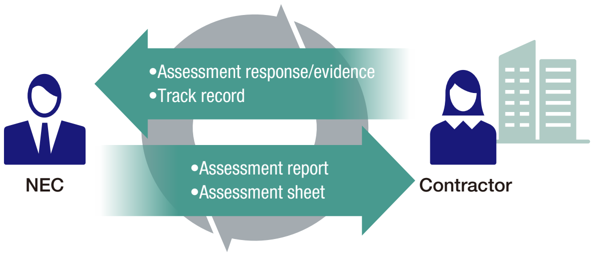
❷ Information security assessment sheet

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


Standardized contractor management process
Request same level of security
NEC Group
Contractor
Subcontractor

Assessments and Improvement Actions for Business Partners



4 Enhancement of Cybersecurity Measures

To enhance cybersecurity measures, premised on the occurrence of security incidents, we revised our information security standard in April 2022, based on the NIST SP 800-171 standard that requires establishing an incident-handling capability that includes preparation, detection, analysis, containment, recovery, and user response activities. Also, we use a third-party rating service (BitSight) to support core business partners in reducing security risks.

5 Enhancement of Global Supply Chain Management

With the aim of enhancing global supply chain management, we hold information security seminars for overseas group companies to raise awareness among their employees about information security management at outsourcing companies. We will continue to organize these seminars to improve the security level of the entire global supply chain.

Providing Secure Products, Systems, and Services

Direction 2 Direction 4

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

1 Promotion of Secure Development and Operations

❶ Group-wide Promotion Structure and Rules

In order to enable secure development and operations for the products, systems, and services we offer to our customers, the NEC Group has a security implementation promotion structure in place. This promotion structure consists of cybersecurity management divisions and security officers assigned to each business division of the group. To eradicate information security incidents caused by product, system, and service vulnerabilities, security misconfigurations, and system failures, the security managers serve as a bridge between cybersecurity management division and business divisions, ensuring that security measures are fully disseminated within their respective divisions and supporting employees in implementing security measures. The roles of the security managers and the security implementation processes in the individual divisions are defined in the “Cybersecurity Management Rules.” We upgrade these rules to cope with increasing cybersecurity risks.

In recent years, we have seen an increasing number of business partners and outsourcing companies targeted by cyberattacks, resulting in leaks of critical information or delays in product manufacturing and supply.

To address the risk of these attacks, we have reviewed and reinforced security measures, including those of business partners, so that we can continue to provide products, systems, and services to customers.

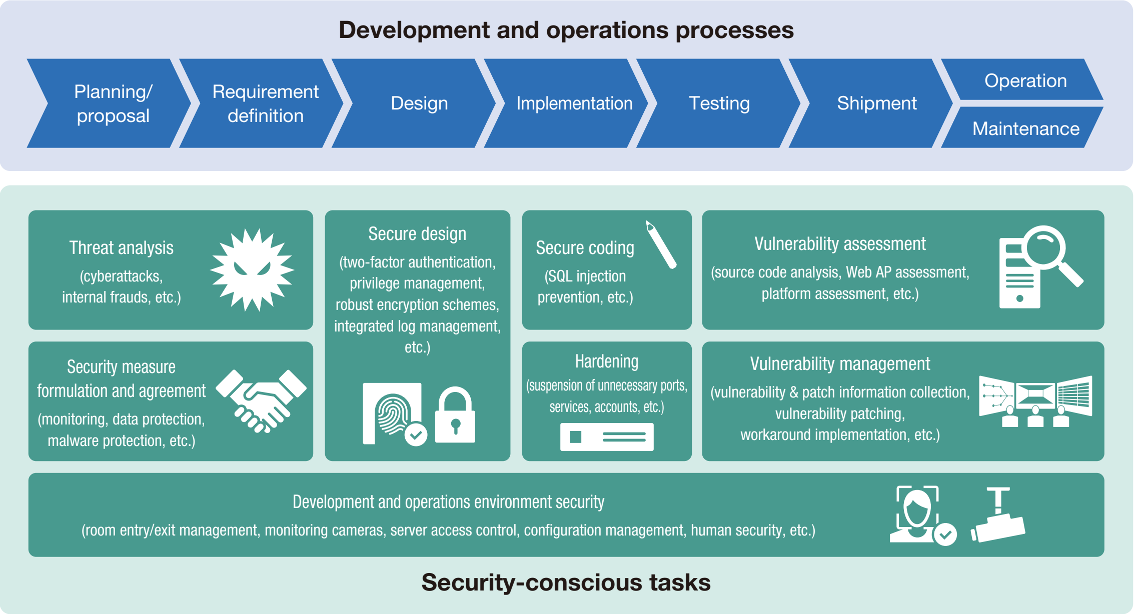
In fiscal year 2022, we stepped up security measures further by checking security management systems and measures of business partners, based on the “Information Security Standards for Business Partners” revised in the previous year.

❷ Key Security Implementation Efforts

Based on the security by design (SBD) concept for ensuring security, NEC implements security throughout the entire process from the planning and proposal phases to the implementation, operation, and maintenance phases. Ensuring security in early stages of system development directly leads to various benefits, including cost reductions, on-time deliveries, and development of easy-to-maintain systems. Particularly, we focus on risk assessments in the requirement definition phase to discuss and implement optimal security for the customer’s system environment in early stages.

NEC has defined the “Cybersecurity Implementation Standard” as the baseline security requirements to be considered at the time of proposal presentation and implementation. This standard specifies strict security requirements, taking into account not only the international security standards such as ISO/IEC 15408 and ISO/IEC 27001 but also the security standards of government agencies and industry guidelines. Moreover, we issue and deploy guidelines as needed to implement security measures for the latest technologies, ensuring that the measures can be introduced securely to the systems, products, and services we develop and operate.

Secure Development and Operations Processes


Development and operations processes
Planning/ proposal
Requirement definition
Design
Implementation
Testing
Shipment
Operation
Maintenance
Threat analysis
(cyberattacks, internal frauds, etc.)
Secure design
(two-factor authentication, privilege management, robust encryption schemes, integrated log management, etc.)
Secure coding
(SQL injection prevention, etc.)
Vulnerability assessment
(source code analysis, Web AP assessment, platform assessment, etc.)
Security measure formulation and agreement
(monitoring, data protection, malware protection, etc.)
Hardening
(suspension of unnecessary ports, services, accounts, etc.)
Vulnerability management
(vulnerability & patch information collection, vulnerability patching, workaround implementation, etc.)
Development and operations environment security
(room entry/exit management, monitoring cameras, server access control, configuration management, human security, etc.)
Security-conscious tasks

In the development of products, systems, and services, we have created a checklist to ensure that security tasks are performed in each phase. Based on this checklist, business projects are managed and the status of security measures is efficiently assessed and audited using the "security implementation assessment system" developed to visualize the implementation status of security tasks.

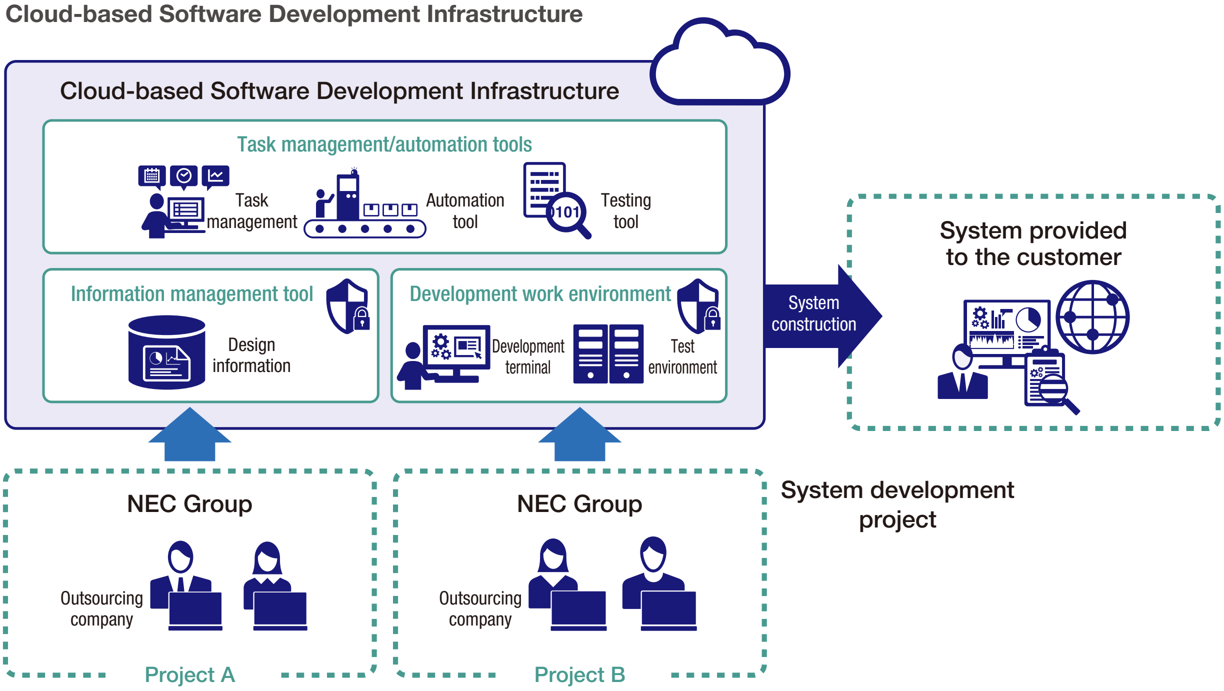
In the operation and maintenance phases of products, systems, and services, we ensure security by using the "vulnerability management system," which collects and distributes vulnerability information in a centralized manner, along with the "cyber intelligence sharing platform." The cyber intelligence sharing platform features a function to distribute the cybersecurity threat information (cyberattack tactics and techniques, cases of incidents, indicators for security measures, etc.) quickly with the business divisions. Distributing cybersecurity intelligence to the business divisions in a timely fashion enables us to have thorough security measures against emerging threats, helping build a secure business environment less prone to security incidents in the operation and maintenance phases of products, systems, and services. In addition, NEC has the PSIRT function for vulnerability information collection and handling. We have a point of contact in place to receive queries and other information from outside the company and publish our vulnerability disclosure policy. Acting as a CNA[*1] organization, NEC addresses vulnerabilities by appropriately handling undisclosed vulnerability information of its products and vulnerability information of customer systems.

❸ Software Development Infrastructure for Security Implementation

NEC has cloud-based software development infrastructure in place as an internal standard environment for system development. This development infrastructure is an integrated development environment that provides an information management tool for managing design information such as source code and specifications, tools for managing and automating various tasks, and a development work environment for implementation and testing, among other features. It also offers tools for streamlining and automating security implementation, such as a security vulnerability testing tool, leading to increased productivity, quality, and security in system development.

Consolidating the development environments of the supply chain, including business projects and outsourcing companies, as cloud-based development infrastructure enables the security of those development environments to be managed in a centralized manner. This makes it possible to ensure that the security measures that the individual business projects use for their development environments comply with the Cybersecurity Implementation Standard, which allows us to securely manage the design information of the customer's system that we use during development.

Cloud-based Software Development Infrastructure



[*1] CNA (CVE[*2] Numbering Authority): An organization authorized to assign CVE numbers to vulnerabilities
[*2] CVE (Common Vulnerabilities and Exposures): A database of publicly available vulnerability information in which CVE numbers are assigned to uniquely identify individual registered vulnerabilities

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 Policy

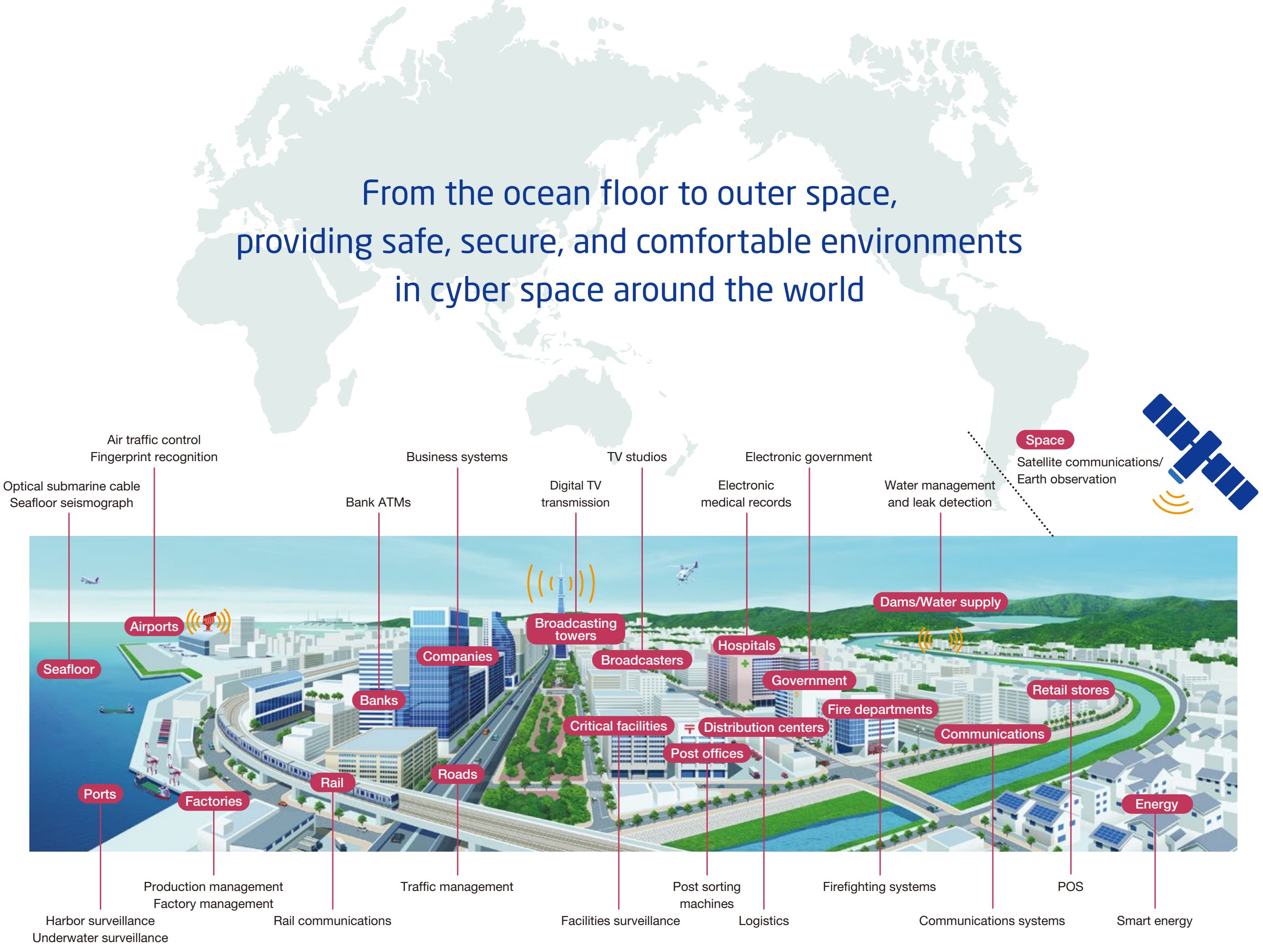
In a keynote speech entitled, "Shaping the Communications Industry to Meet the Ever-Changing Needs of Society" in October 1977, NEC put forth the concept of “C&C (Computer & Communication)” as its slogan for achieving the integration of computers and communications. In line with this declaration, we 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.

Amidst the recent advances in DX*1, there has been a drastic change in the way people work, such as an increasing number of people choosing to telework. This has led to a convergence between physical space (real-world) and cyberspace, where nearly everything is interconnected. In a world like this, the potential for security risks exists everywhere requiring proactive responses to emerging threats. To do business safely while adapting to the rapidly changing business environment, cybersecurity is crucial more than ever.

NEC has accumulated and makes use of numerous technologies that support essential social infrastructures, ranging from domestic traffic control systems, disaster prevention and firefighting systems to production management systems, water management systems, ATMs, logistic systems, and even those systems used on the ocean floor and in outer space. By leveraging these technologies, we provide total security solutions that integrate the physical space and cyberspace to the global market. Moreover, to address ever-evolving cyber risks, we put emphasis on creating secure products and maintaining security of products, as well as on protecting against attacks. Instead of retrofitting security measures, we promote the implementation of security in all the stages from design to construction and operation, including the execution framework.

Based on these achievements and know-how, NEC contributes to the realization of a safe and secure information society through cybersecurity.

NEC’s Business Domains to Support Social Infrastructure



*1 DX: Digital Transformation

2 Contribution to Society

❶ Collaboration with Relevant Organizations

NEC collaborates with relevant organizations at home and abroad to step up its ability to cope with the increasing cyber risks.

NEC has long been a member of the Japan Cybercrime Control Center (JC3[*2]), promoting industry-academia-government collaboration among domestic and foreign research institutions, industry circles, and law enforcement agencies and making progress in the prevention of cybercrimes. We are also taking part in the ICT-ISAC and Cyber Threat Alliance (CTA), among other organizations, to promote the use of information on cyber threats.

Additionally, we began developing an international standard on the organizational framework for cyber risk response in 2021. The developed standard has been published as the ITU-T recommendation. By returning the results we obtained from these activities to society, we contribute to creating a safe, secure, and comfortable environment.

❷ Contribution to National Projects

Nobuhiro Endo, Special Advisor, serves as a member of the Cybersecurity Strategic Headquarters (of the Cabinet), Director General of the Industrial Cyber Security Center of Excellence (of the IPA[*3]), and the President of the Supply Chain Cybersecurity Consortium (SC3). Kazuhiro Sakai, Corporate SEVP and Co-COO (Chief Operating Officer), is the Chief Director of the Japan Cybercrime Control Center (JC3). In this way, NEC is actively contributing to national security projects. Also, by making recommendations to government ministries and agencies through industry groups such as the Japan Business Federation, SC3, and JDTF[*4], we are contributing to the creation of a safe and secure society in which the government and private sector work as one.

Collaboration with Relevant Organizations

Membership

Joined the Japan Cybercrime Control Center (JC3) (November 2014)

JC3 gathers, analyzes, and shares experience in dealing with threats in cyberspace across industry, academia, and public (law enforcement) sectors. Its aim is to identify, mitigate, and neutralize the root causes of threats. Kazuhiro Sakai, Corporate SEVP and Co-COO (Chief Operating Officer), is the Chief Director of this organization.

Participation in ICT-ISAC launch (March 2017)

NEC is a member of the ICT-ISAC, which was established for telecom carriers, broadcasters, software vendors, information service providers, information equipment manufacturers, and many other business operators to share information on cyberattacks and other threats and to work together across industrial boundaries in order to counter those threats. NEC's engagement began from the Telecom-ISAC, the predecessor of the ICT-ISAC.

Joined the Cross Sector Forum for Cybersecurity Workforce Development (January 2016) (April 2017)

NEC set up a study group with NTT Corp. and Hitachi Ltd. for the development of cybersecurity personnel. In 2017, the study group was transferred to Cyber Risk Information Center (CRIC) to further bolster its information sharing efforts.

Joined the 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. Ever since gaining membership, we have been providing the CTA with threat information on a continuous basis.

Interorganizational Collaboration

Formed an alliance with INTERPOL on cybersecurity measures (October 2012) (March 2017) (October 2022)

With the aim of strengthening security at an international level, NEC formed an alliance with INTERPOL on global cybersecurity measures to investigate and analyze increasingly sophisticated and complex cybercrimes and other threats. In 2017, we started contributing to the INTERPOL Digital Security Challenge, a virtual cybercrime investigation training event hosted by INTERPOL, supporting the development of training scenarios and data to be analyzed, etc. We also cooperated in holding the 5th Digital Security Challenge in October 2022.

Developed technologies to reduce supply chain security risks in information and telecommunication infrastructure (October 2021) (November 2022)

NEC developed security transparency assurance technology with NTT Corp. to reduce supply chain security risks drastically by assuring security transparency for information and telecommunication infrastructure systems.
Field experiments began in November 2022.

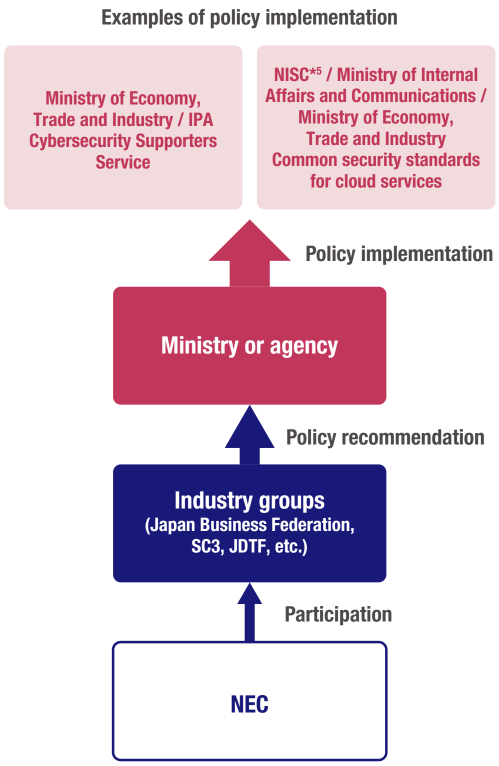
Released an ITU-T recommendation on the organizational framework for cyber risk response (November 2021)

NEC worked with NTT Corp., NTT Security Holdings, and NTT TechnoCross Corp. to develop an international standard for the concept of a cyber defense center to enable strategic and systematic cyber risk response, as well as on its construction, management, and evaluation processes. ITU-T published this standard as the ITU-T Recommendation X.1060.

NEC signed a comprehensive partnership agreement with the National Institute of Technology in the field of cybersecurity (July 2022)

NEC has been engaged in industry-academia joint education assistance by providing 51 national technical colleges across the country with its latest security technologies and knowledge. This activity has contributed to the development of human resources with practical abilities to show greater job performance than ever.

Policy Recommendations Made Through Industry Groups


Examples of policy implementation
Ministry of Economy, Trade and Industry / IPA Cybersecurity Supporters Service
NISC*5 / Ministry of Internal Affairs and Communications / Ministry of Economy, Trade and Industry Common security standards for cloud services
Policy implementation
Ministry or agency
Policy recommendation
Industry groups (Japan Business Federation, SC3, JDTF, etc.)
Participation
NEC

[*2] JC3: Japan Cybercrime Control Center [*3] IPA: Information-technology Promotion Agency, Japan
[*4] JDTF: Japan Digital Trust Forum [*5] NISC: National center of Incident readiness and Strategy for Cybersecurity

3 World-Leading Human Resources and Technologies

① Organizational Structure for Offering Advanced Services

The NEC Group includes companies that offer advanced services like Cyber Defense Institute, Inc. and NEC Security Ltd. Particularly, security operation centers in charge of security surveillance are located not only in Japan but also in North America, Singapore, and other overseas sites. Our overseas presence allows us to continue security surveillance 24 hours a day based on cyberattack information collected not just domestically but from overseas sources as well, thereby enabling us to provide customers with safety and security.

② Development of In-House Human Resources

The NEC Group is also committed to developing security personnel (for details, see “Information Security Personnel” on page 12) and has employees who have won top prizes at international security skill competitions.

③ Development of Security Human Resources in Japan

NEC signed a comprehensive partnership agreement with the National Institute of Technology (NIT) to develop highly skilled engineers through practical education initiatives in society and promote industry-academia joint education support by providing NEC’s latest security technologies and expertise. Under the agreement, NIT’s instructors and NEC’s professional engineers exchange information to share the latest trends, NEC’s top security engineers visit technical colleges to teach students, NEC provides a cybersecurity exercise environment for students, and NIT and NEC jointly create educational materials for systematic security knowledge acquisition. Through these initiatives, NEC is contributing to the development of human resources who possess practical skills and can thrive in the corporate environment.

This is the first time that the National Institute of Technology has engaged in an initiative to develop human resources utilizing the teaching materials and exercise environment that are actually used at a private company.

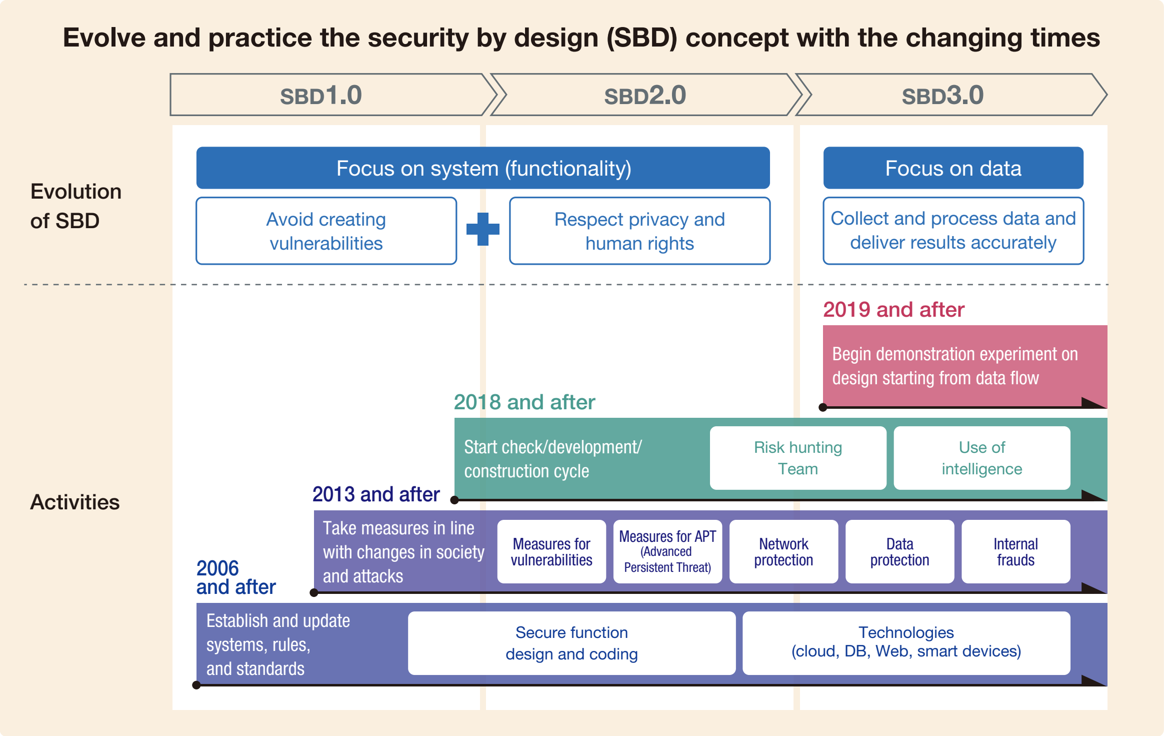
④ Providing Training Programs for Customers

Through the NEC Academy for DX service, NEC provides human resources development programs aimed to promote DX that comply with the Digital Skill Standard released by the Ministry of Economy, Trade and Industry and the Information-technology Promotion

Lecture by Hiroshi Kodama, Corporate EVP, CIO, and CISO of NEC (at the time)

External lectures delivered by NEC employees

Concept of SBD 3.0-Based Security Implementation



Evolve and practice the security by design (SBD) concept with the changing times

SBD1.0 | SBD2.0 | SBD3.0

Evolution of SBD

Focus on system (functionality)

Avoid creating vulnerabilities + Respect privacy and human rights

Focus on data

Collect and process data and deliver results accurately

Activities

2019 and after: Begin demonstration experiment on design starting from data flow

2018 and after: Start check/development/construction cycle; Risk hunting Team; Use of intelligence

2013 and after: Take measures in line with changes in society and attacks; Measures for vulnerabilities; Measures for APT (Advanced Persistent Threat); Network protection; Data protection; Internal frauds

2006 and after: Establish and update systems, rules, and standards; Secure function design and coding; Technologies (cloud, DB, Web, smart devices)

Agency, Japan (IPA) in December 2022.

NEC Academy for DX offers programs to develop DX promoters tasked with ensuring the stable provision of business services with high customer value while reducing the impact of cybersecurity risks, as well as programs to develop experts responsible for addressing actual cybersecurity risks.

4 Thorough Security Implementation

In order to provide customers with safe and secure products, systems, and services, NEC has a framework in place to promote security implementation. Also, in an effort to address the risk of cyberattacks to the supply chain, we review the business partners' security management systems and the measures they have taken, based on the Information Security Standards for Business Partners that we revised last year, so that we can continue to provide products, systems and services to customers (for details, see "Providing Secure Products, Systems, and Services" on page 18).

Moreover, to ensure security in an environment where data, systems, and others become increasingly entwined as DX accelerates, NEC adopts Security by Design (SBD) 3.0 as a concept for ensuring security with a focus on data. Our aim is to implement security in ways that allow us to deal quickly with the latest threats.

■ **Cybersecurity in the Era of DX (NEC)(Japanese only)**

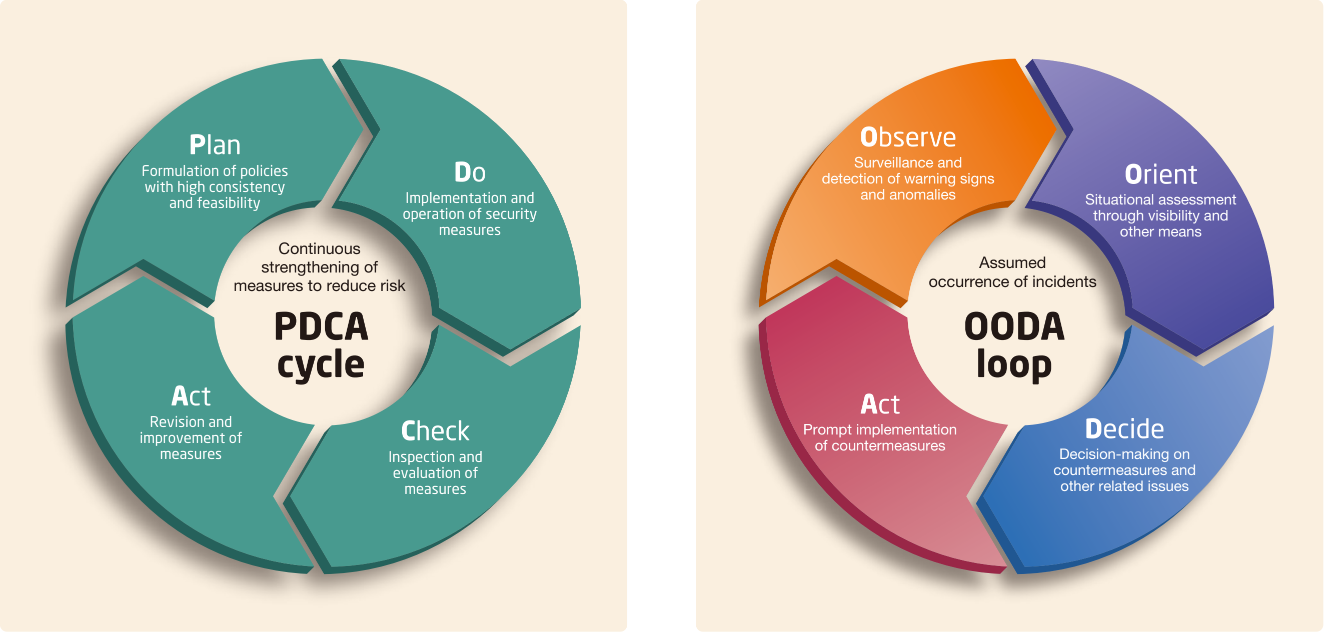
https://jpn.nec.com/cybersecurity/nec_cybersecuritywhitepaper202004.pdf

5 Supporting the Enhancement of Security Based on In-House Operational Expertise

Cybersecurity measures do not end with the introduction of relevant products and services. In order to counter increasingly sophisticated cyberattacks, it is crucial to apply cybersecurity measures appropriately and keep them in proper condition. This requires continuous efforts to eliminate vulnerabilities by implementing the PDCA cycle for a series of processes from formulating cybersecurity policy to taking actions, checking their effects, and making improvements. It is also important to prepare for cyber incidents such as intrusion and malware infection.

Based on expertise in operating the systems used by about 110,000 NEC Group employees across the world, we offer cybersecurity measures that customers can use for their system operation. We also adopt the concept of the OODA loop, a cycle of observe, orient, decide, and act, which facilitates appropriate and speedy incident response.

PDCA Cycle-Based Continuous Security Measures and OODA Loop-Based Speedy Incident Response


Plan
Formulation of policies with high consistency and feasibility
Do
Implementation and operation of security measures
Continuous strengthening of measures to reduce risk
PDCA cycle
Act
Revision and improvement of measures
Check
Inspection and evaluation of measures
Observe
Surveillance and detection of warning signs and anomalies
Orient
Situational assessment through visibility and other means
Assumed occurrence of incidents
OODA loop
Act
Prompt implementation of countermeasures
Decide
Decision-making on countermeasures and other related issues

Response to New DX-Related Security Risks

As DX becomes more prevalent, there is a growing social demand for security.
This section introduces the NEC Group's support framework for responding to security risks in the DX era and for ensuring customers advance DX safely.

1 Changes in Risks Brought About by DX

❶ Changes in Security Risks

As the geopolitical situation changes, private companies are also becoming targets of national cyberattacks and companies that possess critical information such as advanced technological information are facing increasing security risks. Also, while DX is advancing rapidly, cyberattacks for economic purposes are intensifying, all kinds of systems and data are targeted, threatening the business continuity of enterprises. One of the recent trends in security risks is that DX has more systems interconnected, and the damage is not limited to single organization. Under this situation, the Economic Security Promotion Act, which was passed to address economic security risks, also mentions response to cyberattacks. The "Cybersecurity Policy for Critical Infrastructure Protection", issued by NISC, makes it obligatory to ensure security for critical equipment that supports the backbone infrastructure. It also states that management will be held liable for damages suffered by a company due to an inappropriate cybersecurity system.

❷ Security Risks in the Cloud Environment

The conventional perimeter-based network security measures are now reaching their limits for several reasons, including because the information to protect has moved from on-premise systems to the cloud systems and remote connections from outside the company have increased.

In addition, data is scattered across multiple locations, and in some cases, there is a risk that data on the cloud will not be operated correctly Therefore, it is important to select a cloud service that considers not only technical safety but also data governance that considers user peace of mind, and data importance and confidentiality.

2 The Concepts of Security Changing with the Architecture

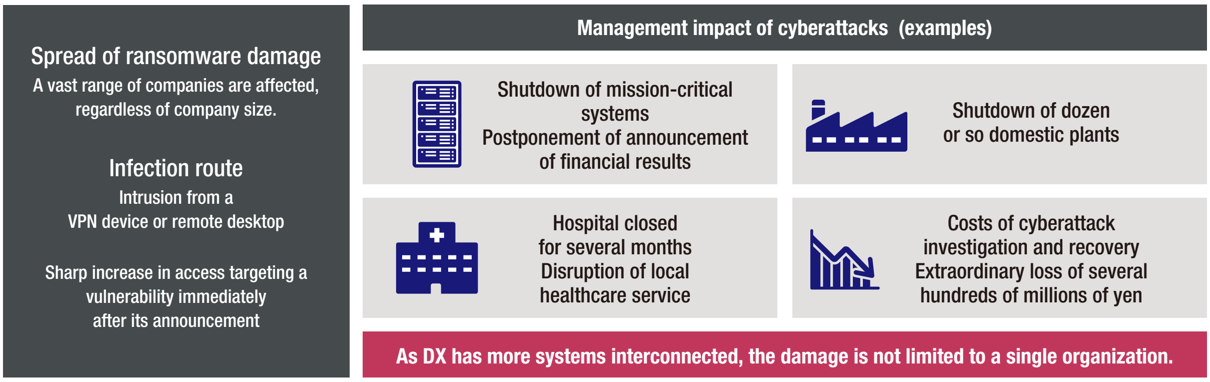
❶ Trusted Cyberspace Supporting DX

The conventional perimeter model, where "threats come from the outside and the data assets to be protected inside the perimeter, has been considered safe in a closed world. In the world of DX, however, threats are everywhere and the hygiene of all IT resources needs to be managed thoroughly. So, the concepts of "zero trust" and "cyber hygiene" are essential for security.

❷ Achieving Total Optimization

The problem is that security measures have been partially optimized and that people are not aware of this. For example, if it is difficult to tell what is really happening just by looking at the results of individual security measures, the risks that should be identified often go unnoticed. If you look at newly added measures individually, they may seem optimal. If you look at these measures from the company-wide

Changes in Security Risks



Spread of ransomware damage
A vast range of companies are affected, regardless of company size.

Infection route
Intrusion from a VPN device or remote desktop

Sharp increase in access targeting a vulnerability immediately after its announcement

Management impact of cyberattacks (examples)

Shutdown of mission-critical systems
Postponement of announcement of financial results

Shutdown of dozen or so domestic plants

Hospital closed for several months
Disruption of local healthcare service

Costs of cyberattack investigation and recovery
Extraordinary loss of several hundreds of millions of yen

As DX has more systems interconnected, the damage is not limited to a single organization.

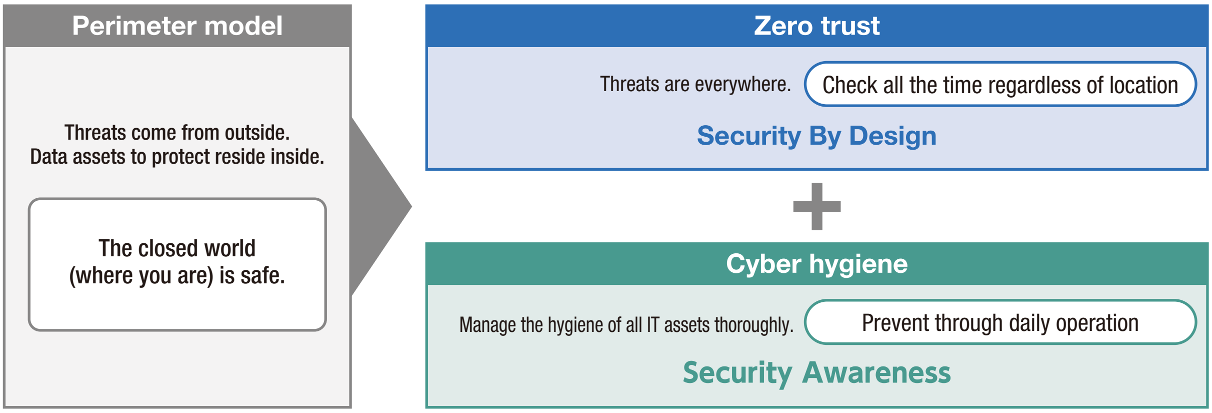
perspective, however, you may find them insufficient or overlapping. And they may be linked with various problems in management, investment decisions, and governance. From the aspect of security, NEC believes that revising partial optimization and aiming for total optimization is an important theme in today's security.

3 What NEC Can Do to Help Customers Promote DX Safely

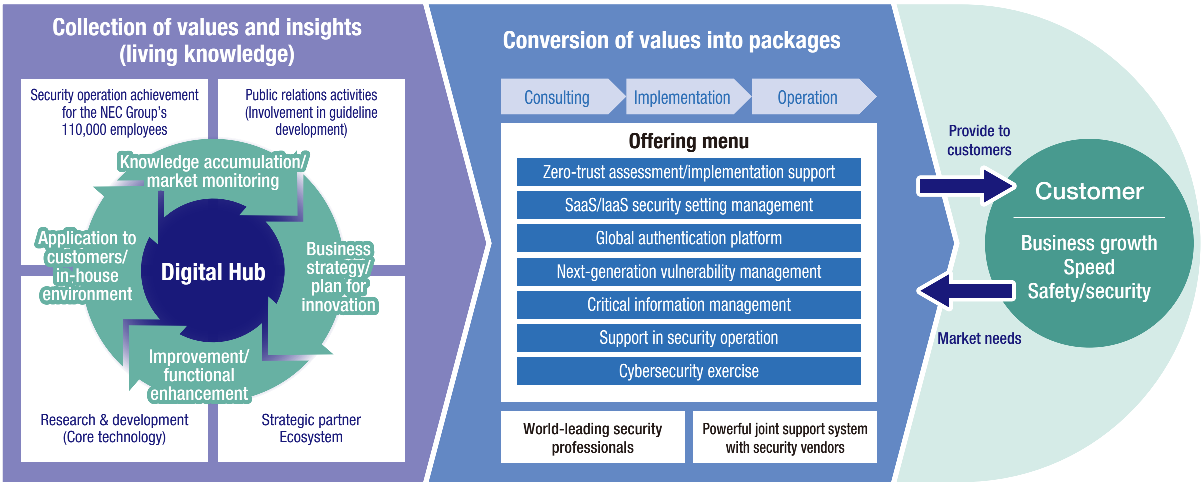
❶ Turning In-House expertise into Solutions

R&D efforts and partnerships with major security vendors have given NEC an aggregated and accumulated base of "living knowledge" made up of values and insights backed by the security measures that 110,000 NEC Group employees have implemented. And our "offering menu" provides total support covering the entire process from consulting to implementation and operation for each individual theme or challenge that a customer faces, such as zero-trust assessment and implementation support, critical information management, and support in security operation. All these offerings are packaged solutions that we have created by extracting values from the security enhancement measures we have implemented as well as from our experience in customer support. They offer very practical support based on methodologies and expertise developed and proven in the field.

Security Base That Supports DX


Perimeter model
Threats come from outside.
Data assets to protect reside inside.
The closed world
(where you are) is safe.
Zero trust
Threats are everywhere.
Check all the time regardless of location
Security By Design
Cyber hygiene
Manage the hygiene of all IT assets thoroughly.
Prevent through daily operation
Security Awareness

Provision of Offerings for Promoting DX Safely



* The offering menu includes planned offerings.

❷ Security Solutions Required for the DX/Cloud Shift

The following table shows the four security issues that are related to the DX/cloud shift and outlines what should be done for those issues going forward.

Issue	What to do	Solution examples
ID management: Zero trust	•Identify users, applications, devices, etc. by monitoring the ID management of the cloud service in use. •Achieve integrated ID management for on-premise systems and cloud services to enable seamless and secure service implementation.	•SSO •Multifactor authentication •Context-based authentication
Information management: Critical information management/ data governance	•Protect critical information by labeling information according to the sensitivity level and taking multi-layered defense measures including encryption. •Create rules and framework for critical information management.	•AIP integrated labels •InfoCage FileShell
Setting management: Cyber hygiene	•Use a cloud setting audit tool to visualize invalid cloud settings and other errors continuously and correct those errors automatically.	•CSPM[*2] •SSPM[*3]
Operation management: Security Operation By Design	•Implement SOBD[*1] for the lifecycle of security operation taking into account all the stages from design to security monitoring.	•Professional services

❸ Professional Services

NEC provides customers with planning and technical advisory from the upstream process. In addition, we achieve high-quality security operation and monitoring by sharing information on new threats and issues with customers and proposing countermeasures and improvements on a continuous basis.

Professional Services

	I. Current situation analysis/ measure discussion	II. Construction	III. Operation
	Diagnosis/evaluation → Measure discussion/roadmap	Design → Deployment	Prevention → Monitoring → Analysis → Response
Technology	Risk hunting Attack route diagnosis Active Directory assessment Simple risk assessment Vulnerability assessment Support in security requirements definition	•Design and deployment of security solutions •Risk analysis for cloud and remote access networks Risk hunting Attack route diagnosis Active Directory assessment Simple risk assessment Vulnerability assessment	Managed service (ActSecure Ｘ) Support in security operation
Organization Process	Security assessment concerning management, organization, and rules Security audits Support in certification acquisition	Support in security policy formulation Secure development and operation framework Support in process development Security incident response framework Support in process development Support in product and system security design	NEC can provide total support tailored to the customer's security lifecycle, including ActSecure Ｘ.
Human resources development	Security education/cyber exercise and training Security awareness training		

4 What NEC Can Do to Help Customers Achieve Total Optimization

Recently, NEC has launched data-driven cybersecurity business. Through this business, we implement DX for security work in two cycles: "operation monitoring/ response" cycle and "management decisions/process reform" cycle using operation monitoring data.

In the operation monitoring/response cycle, security operation monitoring data and vulnerability/threat information are collected to a data lake for integrated management. We support the daily incident response activities of monitoring, detection, and correction, using visualization through dashboard and high-level knowledge and data.

If an incident occurs, we send an alert, identify the cause and the

⋆1 SOBD (Security Operation By Design): To implement security in the upstream stage of the system design process taking operation monitoring into account
⋆2 CSPM: Cloud Security Posture Management ⋆3 SSPM: SaaS Security Posture Management

scope of impact, and propose possible countermeasures.

Moreover, in the management decisions/process reform cycle, we analyze the various kinds of data obtained through the operation monitoring/response cycle to understand the situation of attacks and the security work issues facing the customer. Based on this, we will make proposals that lead to the overall optimization of security measures, such as the optimal architecture and operation processes.

The data-driven cybersecurity business involves repeating operation monitoring in short-term cycles on a daily basis and making improvements continuously in medium-to-long term-cycle. Using these two cycles in combination, we support the implementation of total optimization while working together with the customer. From the perspective of management, this support provides values of enhanced security governance and support in appropriate investment decisions and accountability. In terms of operation monitoring and incident response, we minimize damage through rapid incident detection, identification, and recovery.

And, in the aspect of security measures, we make it possible to achieve total optimization for the customer's existing measures as well as for measures tailored to the attacks being received.

❶ Security Dashboard

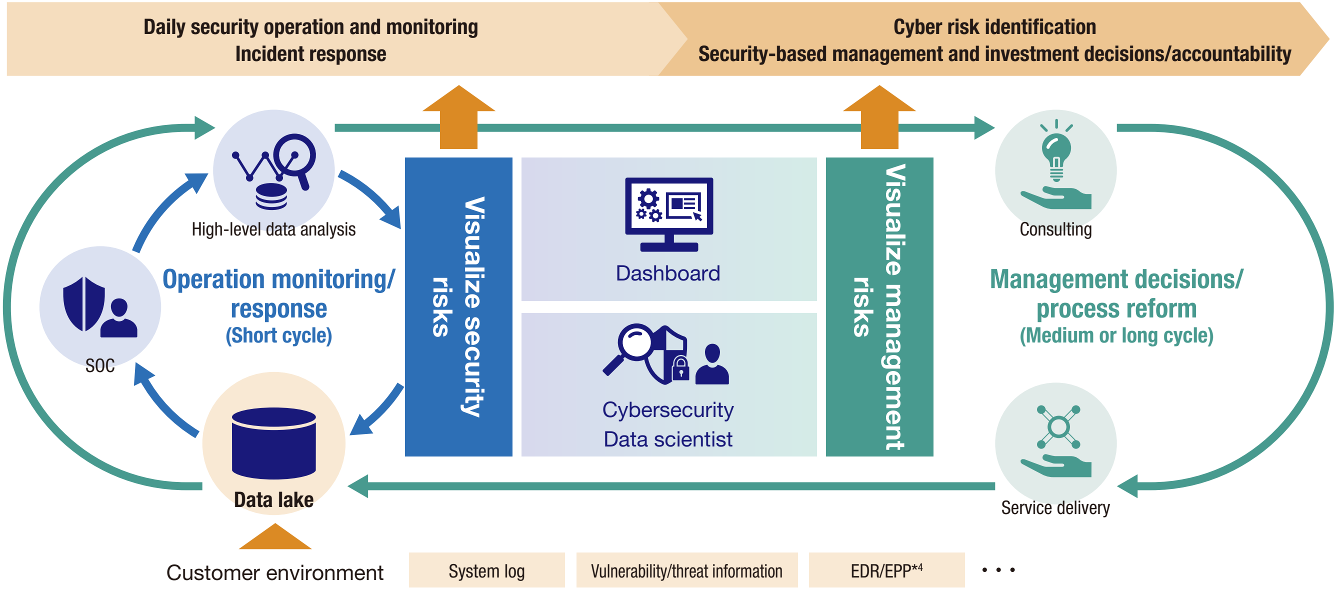
The dashboard is key to visualization and monitoring. We offer dashboards best suited for two purposes: operation monitoring/response and management decisions/process reform. Regarding the former, the dashboard is optimized for information security monitoring, such as the checking of the status of individual security measures, understanding of the incident situation, and log analysis and investigation. As for the latter, the dashboard is designed to make it easy to visualize management risks in such forms as the number and ratio of unapplied patches and countermeasures and the number of suspected cyberattacks. These two dashboards allow customers to understand their own security measures and risks and improve the partial optimization of their existing solutions.

❷ Security Monitoring and Analysis

Experts called cybersecurity data scientists, who have abundant experience in security monitoring and analysis, analyze a huge amount of operation monitoring data to find out what is happening and identify the security work issues facing the customer. Based on the results of this analysis, we work with technical consultants who have extensive knowledge of security implementation to propose the optimal architecture and operational processes for our customers.

While the cloud shift has advanced with the spread of DX and telework, security risks are on the rise. Companies are now required not only to prepare for economic losses but also to address economic security demands, and it is vital for them to adapt to the rapidly changing ICT environment and implement effective security measures. Through its new data-driven cybersecurity business, NEC does all this for customers, helping them protect their valued assets and businesses. Please feel free to contact NEC if you would like to know more about security solutions in DX and data-driven cybersecurity.

Total Optimization Process Through Data-Driven Cybersecurity


Daily security operation and monitoring
Incident response
Cyber risk identification
Security-based management and investment decisions/accountability
High-level data analysis
SOC
Operation monitoring/response
(Short cycle)
Data lake
Visualize security risks
Dashboard
Cybersecurity
Data scientist
Visualize management risks
Consulting
Management decisions/process reform
(Medium or long cycle)
Service delivery
Customer environment
System log
Vulnerability/threat information
EDR/EPP*4
• • •

*4 EDR/EPP: Endpoint Detective and Response, Endpoint Protection

Examples of Cutting-Edge Research and Development of Cybersecurity Technologies

NEC protects social infrastructure and organizations from the threats of cyberattacks through research and development activities for both system security and data security based on the Security by Design (SBD) concept.

1 Concept of the Research Theme

To realize a society in which everyone can use digital technology with peace in mind, the NEC Group is conducting cutting-edge research and development activities from both aspects of system security and data security based on the Security by Design (SBD) concept, which factors in security from the planning and design stages.

This chapter presents examples of our research activities. The example of system security research is "automated secure system design" aimed to automate the design of secure ICT systems. The examples of data security research are "privacy-preserving biometric authentication" that accomplishes facial recognition while keeping the amount of biometric features encrypted and "privacy-preserving federated learning" that builds an AI model without the need for organizations to disclose their data to each other.

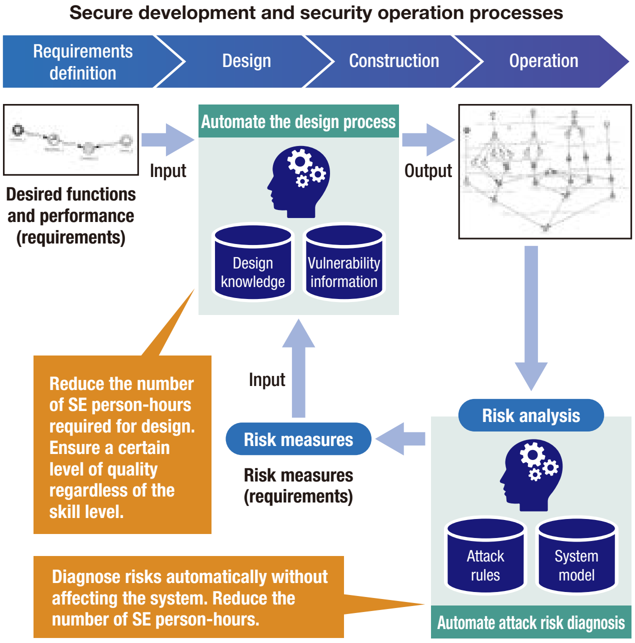
2 Automation of Secure Development and Security Operation

Advances in DX in corporate and social systems have made ICT systems more complex, resulting in an increased risk of cyberattacks. Enhancing the security of ICT systems when the risk of cyberattacks is growing requires factoring in security from the system planning and design stages (Security by Design).

However, ensuring security for complex ICT systems is becoming difficult with the conventional method of manually designing and developing systems, which also requires an enormous number of person-hours. NEC is developing technology that automates the design of complex ICT systems. Based on the functions and performance required for an ICT system (requirements), including security, AI automatically combines and evaluates the components of the ICT system to figure out a secure system configuration that meets the requirements. [1]

Even after you have built a secure ICT system, however, the risk of cyberattacks will increase over time as new vulnerabilities and other problems are found. This makes it necessary to diagnose security risks periodically and respond to those risks during the system operation as well. Typically, human personnel check the system to assess risks, but this manual approach takes considerable time and labor and presents some other problems as well, including the system check causing the system to shut down.

Automation of Secure Development and Security Operation Processes

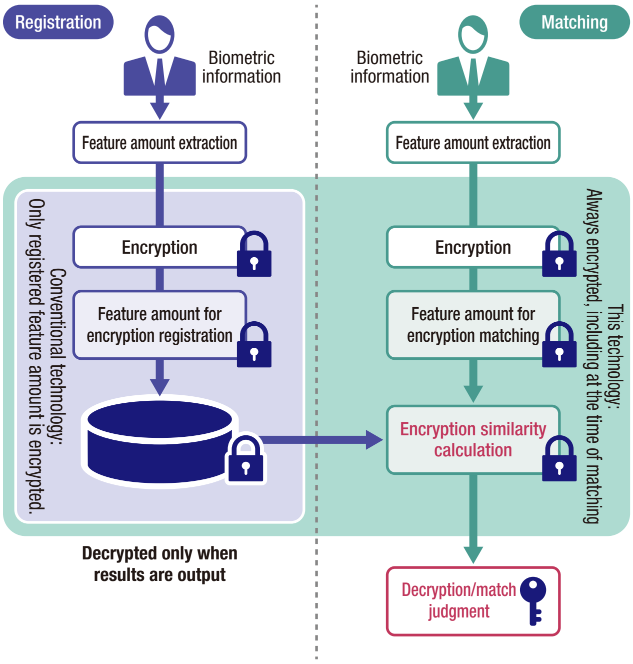


Secure development and security operation processes
Requirements definition
Design
Construction
Operation
Automate the design process
Input
Output
Desired functions and performance (requirements)
Design knowledge
Vulnerability information
Input
Risk measures
Risk measures (requirements)
Risk analysis
Attack rules
System model
Automate attack risk diagnosis

Reduce the number of SE person-hours required for design. Ensure a certain level of quality regardless of the skill level.

Diagnose risks automatically without affecting the system. Reduce the number of SE person-hours.

Protection of the Amount of Biometric Features Using Privacy-Preserving Biometric Authentication



Registration
Biometric information
Feature amount extraction
Encryption
Feature amount for encryption registration
Conventional technology: Only registered feature amount is encrypted.
Decrypted only when results are output
Matching
Biometric information
Feature amount extraction
Encryption
Feature amount for encryption matching
Encryption similarity calculation
Decryption/match judgment
This technology: Always encrypted, including at the time of matching

[1] S. E. Ooi, R. Beuran, T. Kuroda, T. Kuwahara, R. Hotchi, N. Fujita, Y. Tan, "Intent-Driven Secure System Design: Methodology and Implementation", Elsevier Computers & Security, vol. 124, January 2023, 102955. https://www.sciencedirect.com/science/article/pii/S0167404822003479

[2] The Support Center for Advanced Telecommunications Technology Research gave the FY2022 SCAT Award (Chairman Award) to Tomohiko Yagyu, Hirofumi Ueda, Masaki Inokuchi, Shunichi Kinoshita, and Ryo Mizushima for "Research, Development, and Practical Application of Cyberattack Risk Assessment Technology." https://jpn.nec.com/rd/awards/2022/2022-06.html https://www.scat.or.jp/cms/wp-content/uploads/2022/12/award-press2022.pdf

[3] The Promotion Foundation for Electrical Science and Engineering gave the 69th Electrical Science and Engineering Promotion Award to Masaki Inokuchi, Shunichi Kinoshita, and Tomohiko Yagyu for "Development and Practical Application of Automatic Risk Assessment Technology for Identifying Cyberattack Risks." https://jpn.nec.com/rd/awards/2021/2021-06.html http://shoureikai.or.jp/img/awards/past/award_69.pdf

NEC's cyberattack risk assessment technology allows automatic diagnosis of cyberattack risks that an ICT system may face. Using the system data obtained through automatic design, this technology runs computer simulations to comprehensively check possible attack patterns, thereby assessing security risks automatically without affecting the system in operation. Moreover, it automatically derives a secure system configuration based on diagnosis results, helping to maintain the system security. *2*3

NEC automates the processes of secure system development and security operation, which previously required a large number of person-hours, in order to support system design, development, and operation.

3 Privacy-Preserving Biometric Authentication

Facial recognition is coming into wide use as a means of identity check. If registered biometric information is leaked, however, there is a risk of impersonation or other misuse. To address such a risk, we are driving R&D efforts on privacy-preserving biometric authentication. This technology keeps the amount of biometric features that are obtained from biometric information encrypted not only at the time of registration but throughout the whole process, including at the time of matching, in facial recognition and other biometric authentication services. *4*5

To perform the matching process for facial recognition with the feature amount encrypted, privacy-preserving biometric authentication employs secure computation technology based on (1) multi-party computation and (2) homomorphic encryption. The multi-party computation method is suitable for large-scale usage scenes, allowing the matching process for facial recognition to be completed in one second or less when the number of registered users is a million or so. The homomorphic encryption method, which requires no more than one server to provide the authentication service, is suitable for small- and medium-scale usage scenes. This method completes the matching process for facial recognition in one second or less when there are about 10,000 registered users. *6

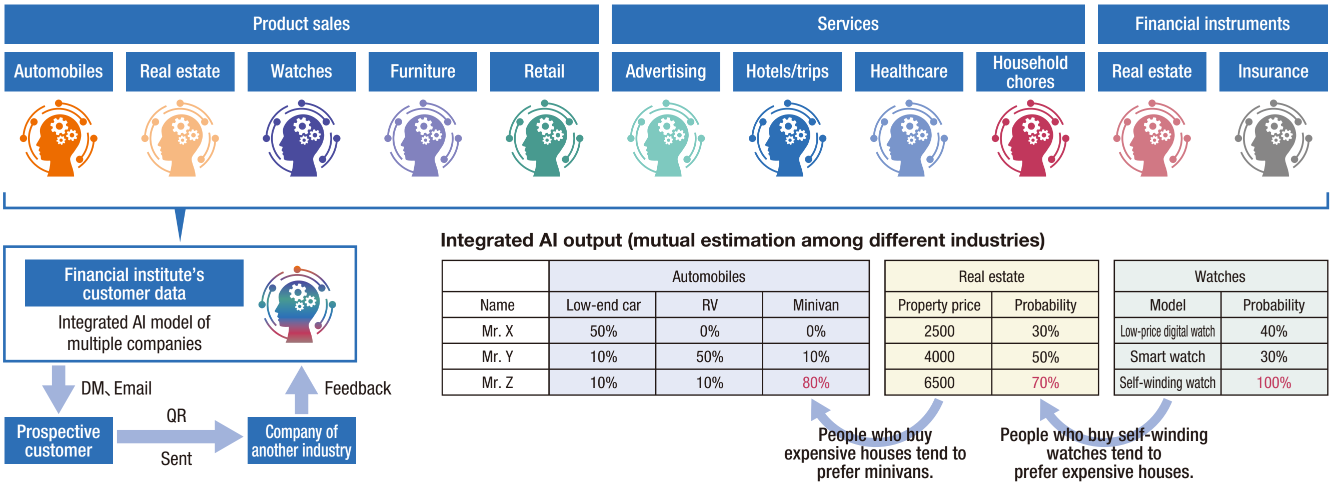
This technology contributes to the safe and secure use of facial recognition and other biometric authentication services.

4 Highly Confidential Hybrid Federated Learning

Many companies collect data and use AI models built with the collected data for their sales activities. Such an AI model is capable of identifying prospective customers, among other things. However, expanding this AI model across industries is difficult. For example, it is difficult to build an AI model that predicts the appropriate purchase price range for real estate by using the purchase data of the auto industry. Of course, an AI model like this can be readily built if the data of the two industries can be gathered in a single location. However, aggregating the data possessed by different industries is problematic in terms of confidentiality since companies give their trade secrets to other companies. Besides, it may also cause legal problems concerning the protection of personal information. For these reasons, aggregating data from multiple industries is not easy. By contrast, highly confidential hybrid federated learning does not gather data directly. Instead, it achieves attribute estimation across industries. By utilizing this technology, we aim to integrate AI models of diverse industries and provide an integrated AI platform that enables mutual estimation of attributes. *7

Collaboration Among Different Industries Through Highly Confidential Hybrid Federated Learning

The local AI models of different industries (automobiles, real estate, watches, etc.) are integrated among multiple companies to provide an integrated AI platform that enables mutual estimation of attributes.


Product sales
Services
Financial instruments
Automobiles
Real estate
Watches
Furniture
Retail
Advertising
Hotels/trips
Healthcare
Household chores
Real estate
Insurance
Financial institute's customer data
Integrated AI model of multiple companies
DM、Email
Feedback
QR
Prospective customer
Sent
Company of another industry
People who buy expensive houses tend to prefer minivans.
People who buy self-winding watches tend to prefer expensive houses.

Integrated AI output (mutual estimation among different industries)

	Automobiles			Real estate		Watches	
Name	Low-end car	RV	Minivan	Property price	Probability	Model	Probability
Mr. X	50%	0%	0%	2500	30%	Low-price digital watch	40%
Mr. Y	10%	50%	10%	4000	50%	Smart watch	30%
Mr. Z	10%	10%	80%	6500	70%	Self-winding watch	100%

*4 Use of Facial Recognition - NEC's Human Rights-Oriented Activities -

*5 Hitoshi Imaoka, Kazuyuki Sakurai, Masato Tsukada, Nobuya Miyagawa, Ryoma Otsuna, Toshiyuki Isshiki, "Future To Be Opened Up by Biometric Authentication," NEC Technical Journal, Vol. 74, No. 2 (2022).

*6 Hiroto Tamiya, Toshiyuki Isshiki, Kengo Mori, Satoshi Obana, Tetsushi Ohki, "Improved Post-quantum-secure Face Template Protection System Based on Packed Homomorphic Encryption", BIOSIG2021(2021).

*7 "Privacy-Preserving Federated Learning: Supporting Both the Protection of Privacy and Confidential Information and the Use of AI," NEC R&D special feature article, https://jpn.nec.com/rd/special/202103/index.html

Third-party Evaluations and Certifications

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

Dow Jones Sustainability Indices (DJSI) World, Global Indices on ESG Investment

NEC earned the top scores in "Information Security/Cyber Security & System Availability" of the IT service sector for three consecutive years (2020, 2021, and 2022).

In 2022, we achieved a perfect score of 100 points.

Member of
Dow Jones
Sustainability Indices
Powered by the S&P Global CSA

Rating by a Domestic Industry Group Cyber Index Company Survey by the Information Technology Federation of Japan

The Information Technology Federation of Japan awarded us the top-notch "two star" rating, citing that NEC was confirmed as implementing outstanding security measures and continuous information disclosure.
(A total of 11 companies were chosen from among the Nikkei 500 Average constituents.)

IT連
日本IT団体連盟

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.
- NEC Security, Ltd.
- KIS Co., Ltd.
- Cyber Defense Institute, Inc.
- Sunnet Corporation
- YEC Solutions Inc.
- Q&A Corporation
- NEC Shizuoka Business, Ltd.
- NEC Aerospace Systems, Ltd.
- NEC Communication Systems, Ltd.
- Forward Integration System Service Co., Ltd.
- LanguageOne Corporation
- Bestcom Solutions Inc.
- NEC Capital Solutions Limited

2 Privacy Mark Certification

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

NEC Group Companies with Privacy Mark

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

3 IT Security Evaluations and Certifications

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

NEC products and systems with ISO/IEC 15408 certification

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

NEC Group Profile

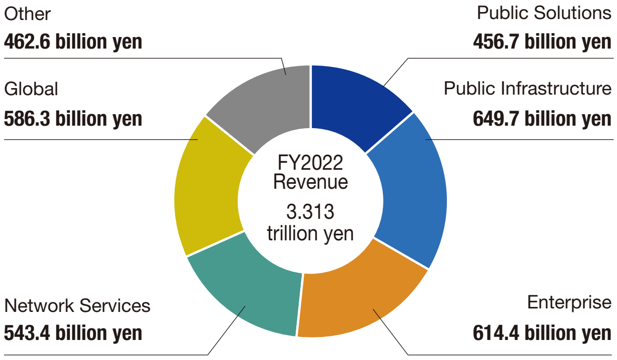
Corporate Profile

Company name	NEC Corporation
Address	7-1, Shiba 5-chome, Minato-ku, Tokyo, Japan
Established	July 17, 1899
Capital	427.8 billion yen*
Number of employees (Consolidated)	118,527*
Consolidated subsidiaries	284*

★As of March 31, 2023

Segment Information

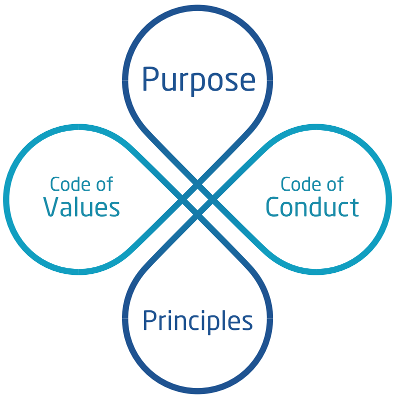
Sales Revenue by Segment (Percentage)



★As of March 31, 2023

NEC Way [Management Policy]

NEC Way



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

Purpose

\Orchestrating a brighter world

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

Code of Values

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

Principles

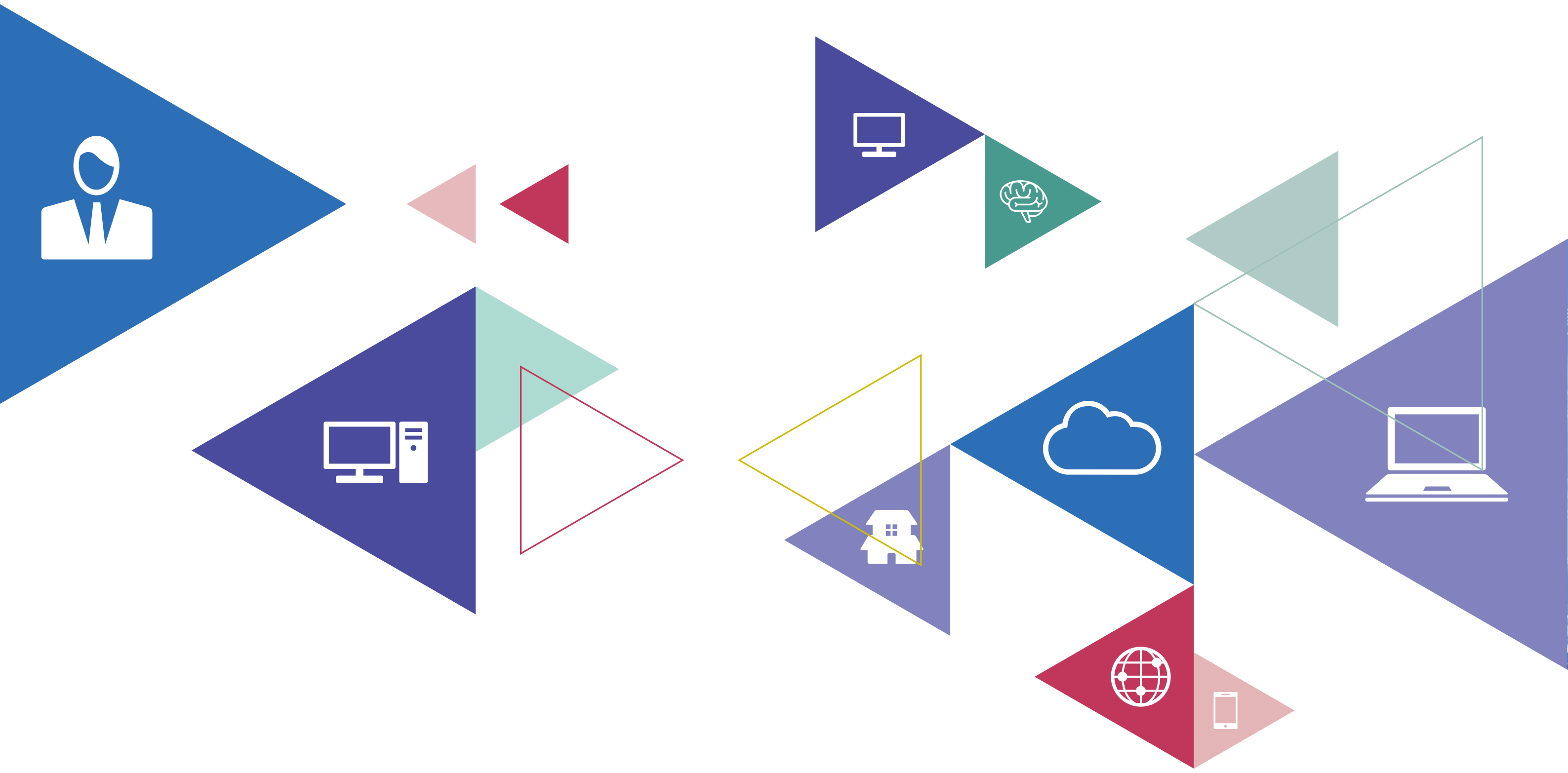
The Founding Spirit of "Better Products,
Better Services"
Uncompromising Integrity and Respect
for Human Rights
Relentless Pursuit of Innovation

Code of Conduct

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

Consultation and Report on Doubts and Concerns
about Compliance

Information Security Report 2023



NEC Corporation

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

Issued September 2023