Orchestrating a brighter world

NEC

Information Security Report 2024

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.

Noboru Nakatani

NEC Corporation
Corporate EVP and CSO
NEC Security Executive

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

Given these circumstances, NEC is building a zero trust security platform across our group that has robust and flexible security measures, such as password-less authentication, based on CISA’s Zero Trust Maturity Model.*1

We are developing our cybersecurity organizational structure by strengthening our intelligence gathering capabilities (for preventive defense) against increasingly damaging cyberattacks and our resilience capabilities (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 2.0)” that the US National Institute of Standards and Technology (NIST) revised in February 2024 for the first time in 10 years. In addition, with our data-driven cybersecurity initiative, we visualize cybersecurity risks through dashboards to provide all employees with information on these risks. This helps top management make data-driven business decisions quickly and members of the workforce to act autonomously, allowing us to achieve security governance. These initiatives have earned us the “2024 IT Excellence Award (Management Category)" of the Japan Institute of Information Technology and the “Japan DX Grand Prize 2024 Special Award" of the Japan Digital Transformation Promotion Association.

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, which takes security into account from the design phase. In order to nurture security personnel who promote DX, we encourage our employees to acquire internationally recognized information security certification, CISSP.*2 We also work with educational institutions to foster future talents. In recognition of these efforts, the Information Technology Federation of Japan awarded NEC the highest “two star” rating in its Cyber Index Corporate Survey 2023.

Going forward, we will stay focused on enterprise risk management and providing cutting-edge technologies which has been internally implemented. These technologies include walk-through facial recognition for entry/exit gate control using NEC’s face recognition technology that is praised as the best in the world,*3 as well as the use of generative AI for security. Through these efforts, we aim to continuously earn trust within society.

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 multiple 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
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 2024"

The purpose of this report is to introduce stakeholders to NEC Group's information security activities based on "Cybersecurity Management Guidelines Ver. 3.0" by the Ministry of Economy, Trade and Industry, Government of Japan. The report covers our activities conducted up to June 2024.

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

Contents

Information Security Promotion Framework

Direction 1

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 considers information security to be a key management priority. We are committed to protecting the information assets entrusted to us by our customers and business partners, as well as our own information assets, from threats such as cyberattacks. Additionally, we provide secure products, systems, and services to ensure an increasingly safe digital environment. In the face of escalating risks, we strive to create a society that is "Truly Open, Truly Trusted." By realizing this vision, we aim to foster 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 takes a comprehensive multi-layered approach to maintain and enhance information security. We implement cyberattack countermeasures, promote information security through partner collaboration, and provide secure products, systems, and services. Our efforts focus on three pillars: information security management, infrastructure, and personnel. Through robust governance across these areas, we diligently work to maintain comprehensive, multi-layered information security measures for the NEC Group.

The NEC Group has established the NEC Group Information Security Statement and maintains robust information security through comprehensive policies, regulations, and a common security infrastructure across the organization. Our top management sets security goals, determines group-wide initiatives, builds organizational structures, and allocates resources accordingly. We conduct regular monitoring and implement continuous improvement measures to enhance our information security practices.

Information Security Governance

Direction 2

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.

Guided by our information security governance framework, NEC's top management conducts an annual review of security objectives and provides instructions for improvements and corrective actions. This is based on monitoring results across the entire NEC Group, including affiliated companies and overseas subsidiaries.

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

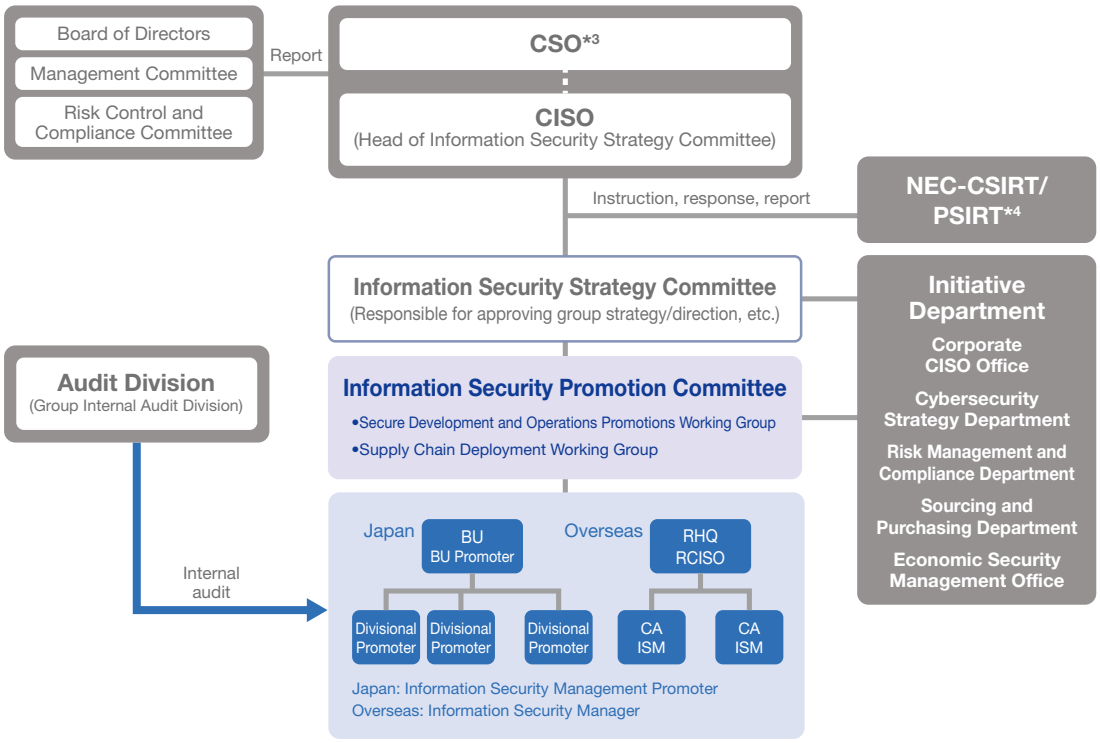
The information security promotion organizational structure of the NEC Group consists of the Information Security Strategy Committee, its subordinate organs, and other relevant organizations. The Information Security Strategy Committee, headed by the CISO, 1) evaluates, discusses, and improves information 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 CISO oversees the Corporate CISO Office, which promotes information security measures, and the CSIRT*1, which monitors for and swiftly responds to cyberattacks.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.

Each department head, acting as the Information Security Manager, is responsible for ensuring information security within their respective organizations, including the group companies under their supervision. They continually raise awareness of security rules, introduce and operate measures, monitor implementation, and drive improvements.

Furthermore, NEC appoints regional CISOs*2 in each region to enhance governance. These regional CISOs are accountable for security management and results within their respective regions.

Information Security Promotion Structure



*1 CSIRT: Computer Security Incident Response Team *2 CISO: Chief Information Security Officer *3 CSO: Chief Security Officer *4 PSIRT: Product Security Incident Response Team

Information Security Management

Direction 2 Direction 6

To firmly establish various information security measures across the entire NEC Group, we have implemented a comprehensive information security management framework and a structured system of security policies, which we continually maintain and enhance.

1 | Information Security Management Framework

Based on our information security and personal information protection policies, NEC implements the PDCA cycle to continuously maintain and improve our information security practices. 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 the My Number (personal identification number) management framework to ensure compliance with the Act on the Use of My Number 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.

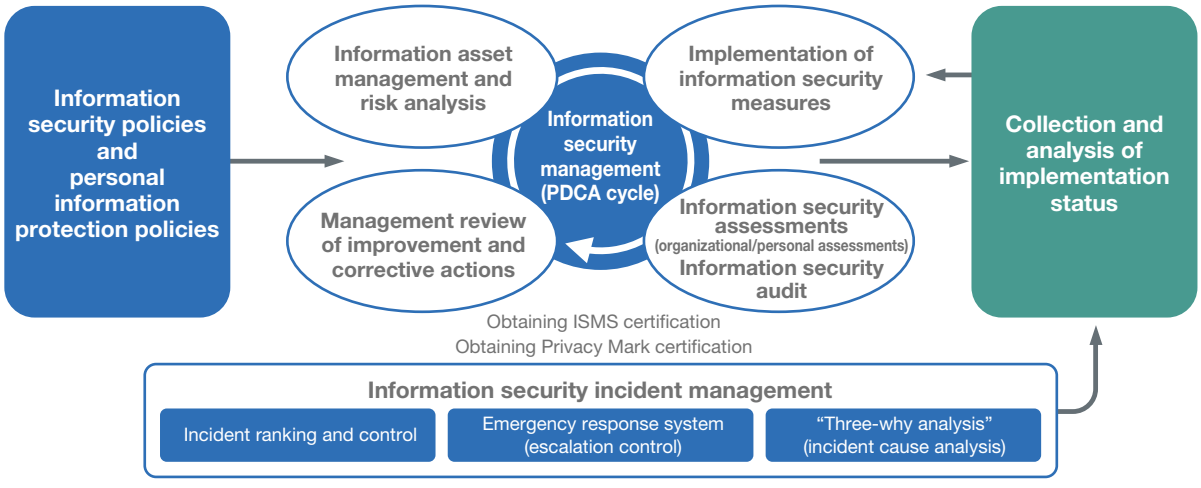
The NEC Group promotes consistent personal information protection and management practices across the organization. As of June 2024, 31 NEC Group companies have acquired Privacy Mark certification.

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



*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

❷ Management of Information Security Incident Risk

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

❸ 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

❶ Three Lines Model

The NEC Group ensures rigorous handling of critical information based on the concept of the Three Lines Model. The risk owner divisions, as the first line, strictly manage information, while the risk management divisions, as the second line, monitor the first line and provide support for their risk management practices. The audit division at the third line checks the status of management.

❷ 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 identifies the specific information they handle and maps it to the appropriate secrecy level. This systematic approach ensures comprehensive information management without any misclassification or oversight.

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 Surveys and Audits

❶ Information Security Surveys

Critical information management assessments were conducted in accordance with NEC trade secret control rules implemented in July 2020. These assessments verified how business divisions manage top secret and strictly confidential information while raising employee awareness about information security. Furthermore, we analyzed trends in awareness and implementation of security measures across the NEC Group, which enabled us to continuously maintain and improve our information security practices.

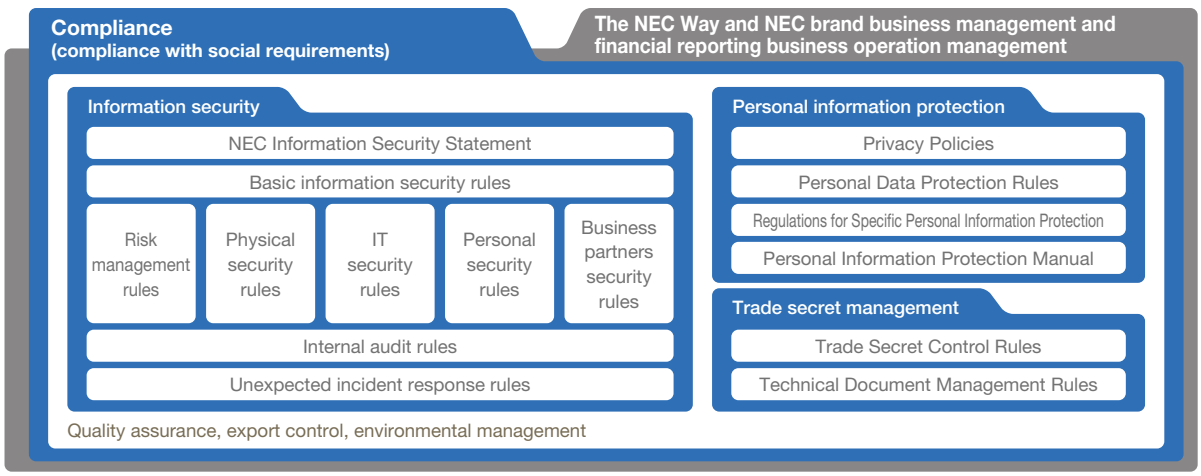
As awareness increases and security operations become well established, we are transitioning towards decentralized management at the divisional level. Starting in fiscal year 2024, we have adopted the Three Lines Model, shifting to information security surveys with a focus on security awareness.

❷ 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 assess each organization's compliance with ISO/IEC 27001 and JISQ 15001 standards. Concurrently, we encourage individual organizations to acquire ISMS certification, taking into account the trends and dynamics within their respective business areas.

(For a list of companies that have obtained ISMS certification, see page 30.)

NEC Group Management Policy



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 consists of five distinctive pillars—identity, device, network, application and data.
We have the following security measures in place covering each of these pillars.

1 | Identity Security

Amid the spread of cloud services and telework and the advent of increasingly sophisticated cyberattacks, NEC is promoting password-less authentication as a vital step to provide enhanced and advanced authentication capabilities in a zero trust environment.

NEC has introduced multi-factor authentication (MFA*2), which combines multiple authentication techniques such as biometric authentication (face recognition, fingerprint recognition, etc.) and device authentication. This allows us to reduce the risks of spoofing and cyberattacks and to promote password-less authentication on a company-wide basis. Last fiscal year, we deployed multi-factor authentication for almost all of our users.

At the same time, we use risk-based authentication, which requires additional authentication only when there is a risk of spoofing or a cyberattack. This reduces the frequency of authentication while satisfying the needs for both improved usability and enhanced security, implementing a user-friendly security measure that is tough on attackers.

NEC also has an authentication platform for managing user authentication and authorization information on a group-wide basis. This IAM platform*3 enables globally integrated authentication and device management, which is crucial in a zero trust architecture.

To enable both security and the effective utilization of enterprise resources through our IAM platform, NEC implements the following four measures.

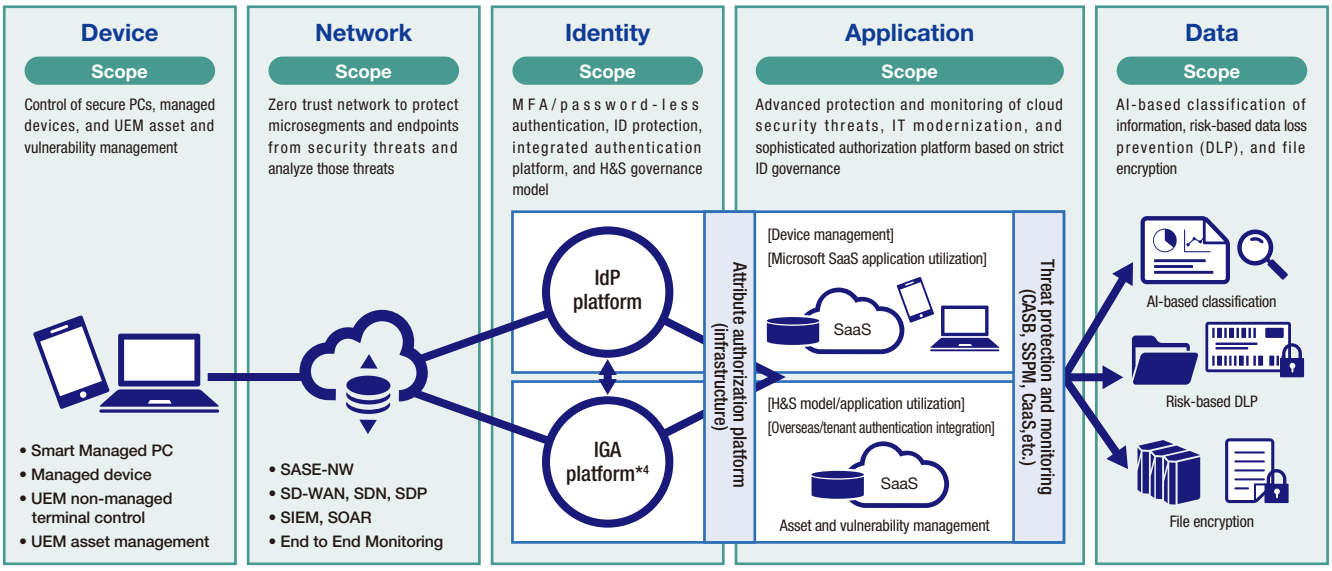
(1) Use of global ID	Identity management (unique account for each user, appropriate lifecycle, and centralized management)
(2) Authentication and device management	Control environment for user authentication (password-less, multi-factor authentication), device authentication, and managed devices
(3) Global app management	Management of access to common systems and services and single sign-on (SSO)
(4) Security governance	Globally centralized management and control of security policies and setting information

2 | Device Security

NEC provides its employees various types of secure standard endpoint devices (SmartPC series) to support diverse work styles.

The SmartPC series consists of thin clients that do not store any data on the client side (Smart Connect PCs or SCPCs), rich client-based PCs (Smart Managed PCs or SMPCs) that are suited for use in a real and online hybrid work environment, and devices that

Overview and Scope of the Zero Trust Platform



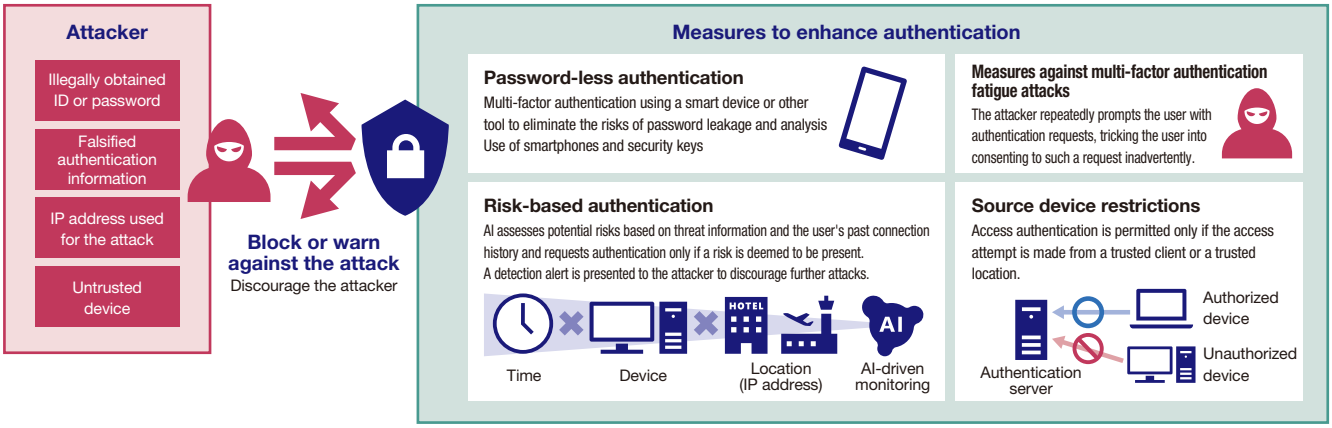
*1 CISA: U.S. Cybersecurity and Infrastructure Security Agency *2 MFA: Multi-Factor Authentication *3 IAM: Identity and Access Management
*4 IGA(Identity Governance and Administration): Framework for identity governance including lifecycle management, access privilege management, provisioning, and qualification information management for users and others

support high-spec resources (Smart Engineer PCs or SEPCs). The SmartPC series devices support face recognition, password-less authentication, device authentication, device management (use of Intune), and integrated in-house authentication among other features.

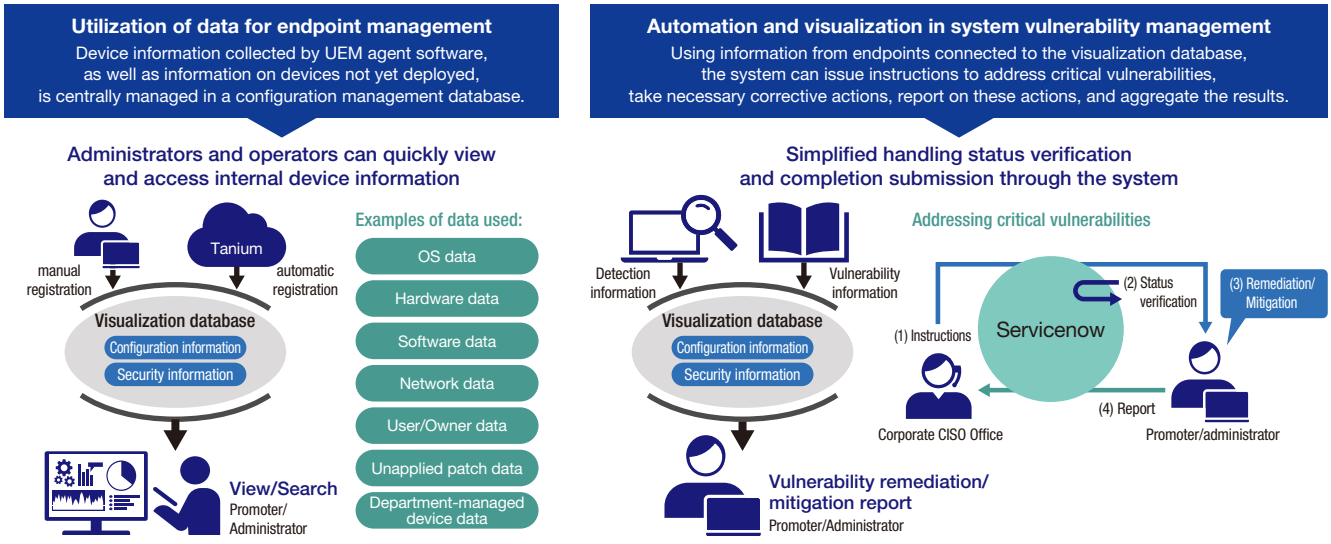
Furthermore, NEC has a Unified Endpoint Management (UEM*5) platform to cope with endpoint vulnerabilities. By mandating the installation of UEM agent software, we manage the information on all our IT assets globally, in a centralized manner using the cloud. This makes us better able to address security risks and helps us increase our management work efficiency.

For endpoint management, we use UEM to monitor and visualize the environments of individual information devices, grasping the status of security measures and IT asset management. The security measures include distributing security patches, keeping anti-virus software updated, and ensuring the appropriate use of EDR software, and we also monitor for the use of prohibited software programs. In addition, we perform vulnerability scans on business servers, public servers, etc. to detect problems, which are automatically reported to system operators to prompt improvements. Moreover, unaddressed vulnerabilities are also automatically tracked and their information is collected and visualized to enable quick responses and save costs. For network site management, we have a mechanism in place whereby UEM-based monitoring grasps the installation status of agent software and, if not installed, employees are prompted to install it. Any device with insufficient security or found to be infected with malware or other malicious software is disconnected from the business network. External communications are currently managed through a whitelist-based web access control system, and moving forward, we plan to strengthen security by implementing controls on an individual ID basis as well. We also support sender domain authentication (DMARC), one of the requirements specified in the Email Sender Guidelines*6 put into effect by Google in February 2024.

Advanced Authentication Using Password-less Authentication and Risk-based Authentication



UEM-based Secure Endpoint Management



★5 UEM: Unified Endpoint Management

★6 Guidelines for email senders
https://support.google.com/a/answer/81126?hl=ja-jp#zippy=%2C%E6%97%A5%E3%81%82%E3%81%9F%E3%82%8A-%E4%BB%B6%E4%BB%A5%E4%B8%8A%E3%81%AE%E3%83%A1%E3%83%BC%E3%83%AB%E3%82%92%E9%80%81%E4%BF%A1%E3%81%99%E3%82%8B%E5%A0%B4%E5%90%88%E3%81%AE%E8%A6%81%E4%BB%B6

For information leaks risk measures, we use a multi-faceted approach that includes encryption, device control, and log recording to prevent leaks resulting from external attacks and internal fraud. For encryption, we protect both hardware and data, establishing an infrastructure that assigns access rights and usage periods for each file. This helps prevent information leaks caused by theft, loss, or email misdelivery, and ensures data protection in case of malware infection. In terms of device control, we restrict the use of external devices such as USB drives and SD cards to only essential business needs, minimizing the risk of information leaks from external sources. For log recording, we maintain detailed operation logs for all PCs. In the event of an incident, these logs are analyzed to understand the extent and circumstances of the issue and to develop measures to prevent recurrence.

3 | Network Security

The NEC Group has implemented a global zero trust network platform deployed to ensure end-to-end security and availability, from the connection source (endpoints) to the destination (systems and services).

The SD-WAN enhances security across all 297 of our global locations through segmentation and centralized control. Additionally, by reducing network change lead times and doubling total network bandwidth, it not only ensures robust security but also delivers high availability. We plan to complete the expansion to the remaining three regions—North America, Latin America, and EU—by the end of the first half of fiscal year 2024.

We are also globally upgrading our remote connection environment with a zero-trust architecture. By integrating secure web gateway and remote gateway into a cloud-based access control framework, we ensure efficient access to decentralized resources. This framework not only bolsters endpoint security but also interoperates with next-generation authentication systems, adding further value. Our goal is to complete deployment across all five international regions by the end of the first half of fiscal year 2024.

4 | Application Security

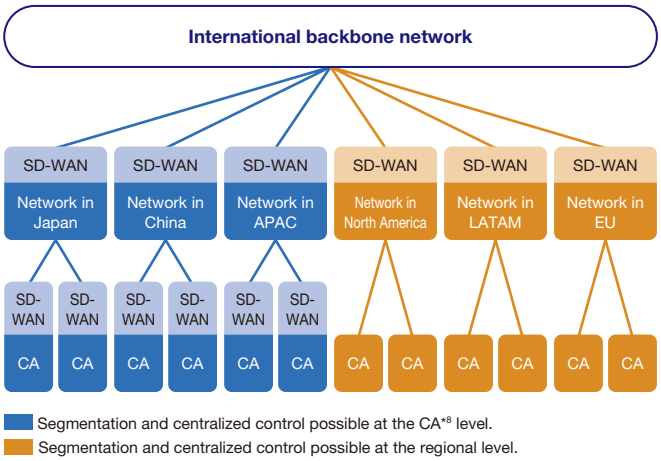
The NEC Group uses many cloud services as it drives its DX initiatives. While DX increases user convenience, thorough security measures become necessary since critical data is stored in the cloud and more easily accessed from outside the company. Taking into account the risks involved in using cloud 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

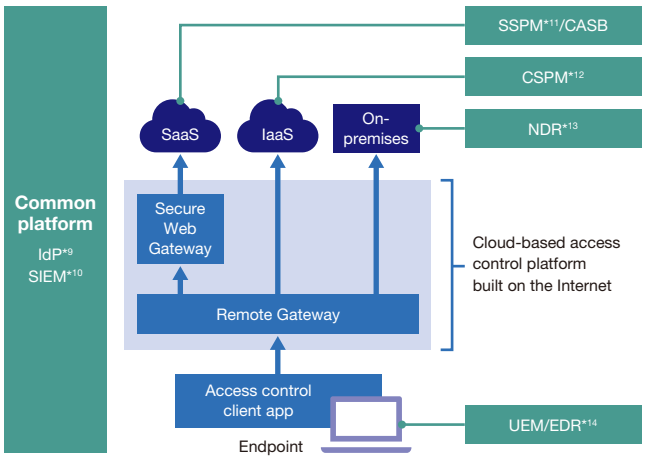
We are implementing measures to counter internal fraud and cyberattacks targeting critical data within cloud services by monitoring and analyzing logs data and stored files through a CASB.*7

We also visualize the usage status of internally used cloud services to check whether any unapproved risky services are in use.

Global Deployment of SD-WAN



Zero Trust Remote Connection Environment



★7 CASB: Cloud Access Security Broker ★8 CA: Corporate Affiliate ★9 IdP: Identify Provider ★10 SIEM: Security Information and Event Management
★11 SSPM: SaaS Security Posture Management ★12 CSPM: Cloud Security Posture Management ★13 NDR: Network Detection and Response
★14 EDR: Endpoint Detection and Response

❷ Prevention of Incidents Resulting from Improper Public Cloud Settings

The use of public cloud services like AWS, Azure, and GCP, is on the rise. While these services are easy to use, they also come with the risk of information leaks due to configuration errors. The NEC Group employs CSPM to continuously verify that the configurations of public cloud services used within the group adhere to any security standards, ensuring that any potential risks are identified.

❸ Prevention of Incidents Resulting from Improper SaaS Settings

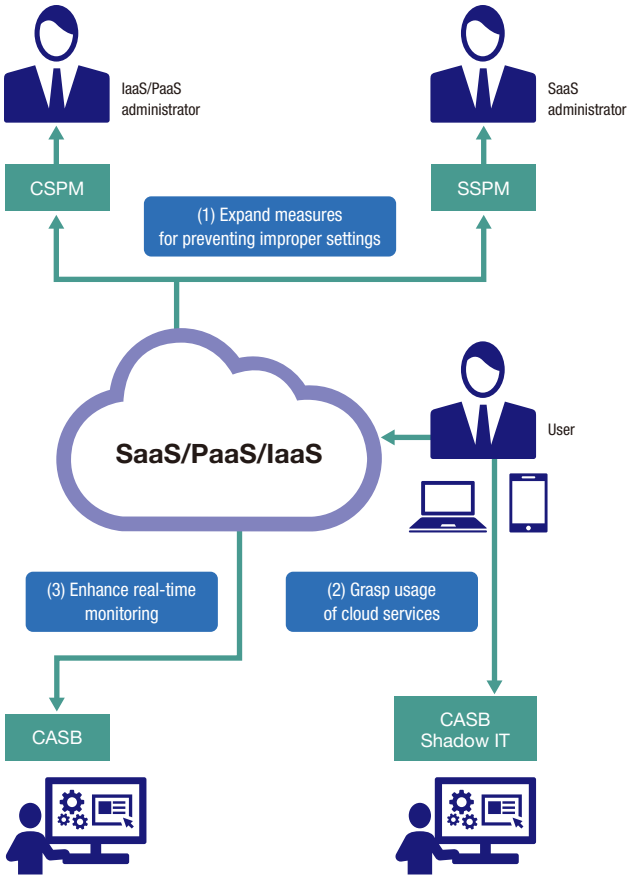
Cloud services like Microsoft 365, Box, and Salesforce have numerous configuration options, which can lead to the risk of information leaks if improperly set up. The NEC Group uses SSPM to globally identify and correct configuration errors in the cloud services we use internally.

5 | Data Security

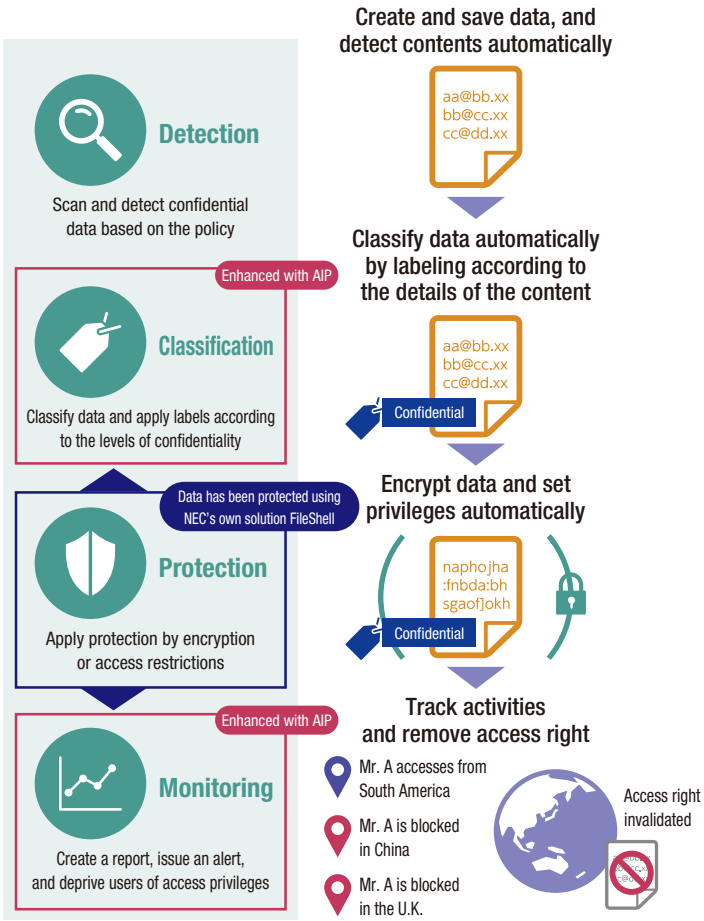
The NEC Group takes a zero-trust security approach by using cloud-compatible AIP*15 unified labels and our proprietary solution, InfoCage FileShell. This enables us to automatically classify, encrypt, track, and manage access permissions for various files, not just Office documents. These measures help prevent information leaks caused by malware infections and other threats.

To ensure the secure management of critical information, we have implemented secure storage solutions that encompass access control, encryption, audit trail management, intrusion investigation, and ISMS compliance. This approach helps reduce operational workload while maintaining secure management of critical information. For high-priority internal systems, we deploy robust security measures based on risk analysis and business impact analysis. These measures include vulnerability management, log management, network protection, authentication, access control, and privileged access management.

Security Measures for Using Cloud Services



Data Security through File Encryption



*15 AIP: Azure Information Protection

Information Security Personnel

Direction 3

NEC focuses on developing all our employees in three key areas:
1) raising awareness of information security; 2) developing personnel to promote information security measures;
and 3) developing professionals capable of providing exceptional value to customers.

1 | Developing Information Security Personnel

NEC focuses on developing all our employees in three key areas: raising awareness of information security, developing personnel to promote information security measures, and developing professionals capable of providing exceptional value to customers.

2 | Raising Awareness of Information Security

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

❶ Training on Information Security and Personal Information Protection

The NEC Group offers web-based training (WBT*1) on information security and personal information protection (including My Number compliance in Japan), to all employees. This training aims to enhance knowledge and awareness of these critical areas. In fiscal year 2024, the training achieved a 93% completion rate and was offered in seven languages. We update the training content annually to address evolving security threats, covering topics such as information management, external security measures, and contractor management.

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 Measures to Raise Awareness of Information Security

To heighten awareness of information security risks and empower employees to think critically, make informed decisions, and take effective action, we have implemented several initiatives, including the use of videos on information security. Additionally, we hold quarterly workplace discussions, known as “Theme-based Talks.” These sessions aim to strengthen individual risk analysis and decision-making skills while nurturing a strong culture of information security awareness within our organization. Surveys indicate a notable improvement in both information security awareness and sensitivity to risks, demonstrating the success of these initiatives.

3 | Developing Personnel to Promote Information Security Measures

Within our information security promotion framework, we implement various internal measures to develop employees with essential skills. By appointing qualified individuals—such as CISSPs,*2 registered information security specialists, and personal information protection professionals—we enhance our ability to manage critical information, protect personal information, ensure secure development and operations, and respond to incidents effectively.

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

4 | The initiatives for fostering Security by Design practitioners and the activities for expanding our Talent Base.

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 NCSA (NEC Cyber Security Analyst) Training

To increase top-tier security talent, we offer a six-month intensive program for employees who have security technology knowledge. This program helps participants acquire the practical technical skills necessary for providing advanced security services, such as CSIRT*3 or risk hunting operations. Including the NEC CISO Assistant Training (NCAT) program conducted until the fiscal year 2020, a total of 75 employees have completed these programs and are now contributing to providing professional services.

❷ SBD Specialist Training

Since fiscal year 2020, we have been running a program to develop specialists who assist security managers and implement SBD in each business division. We introduced a new course for sales representatives from the fiscal year 2022 to develop their skills necessary to offer appropriate security proposals including cyber incident case studies and security countermeasures. The total number of participants has reached 82 and more than 20 employees participated in this program in the fiscal year 2023. These specialists play a pivotal role in overseeing the entire system development process and implementing comprehensive security measures. All these efforts enable us to deliver safe and secure systems to our customers.

❸ NEC Cybersecurity Training Site

We offer training for all our employees involved with our customers' systems. This training focuses on acquiring the necessary knowledge, as well as skills such as risk assessment, for appropriate communication with customers about security. Additionally, we provide practical security exercises in a dedicated virtual environment that simulates an e-commerce (EC) site, allowing participants to learn hardening techniques in the system construction phase. With this remotely-accessible training environment, more than 1,600 employees, primarily sales representatives and systems engineers, completed the program in the fiscal year 2024.

❹ Group-wide CTF

We host an inhouse Capture The Flag (CTF*4) contest called the "NEC Security Skill Challenge" to expand our security talent, enhance participants' security skills, and raise security awareness. More than 850 employees voluntarily participated in the fiscal year 2024, bringing the total number of participants to over 8,000 since the contest began in 2015.

❺ Basic Security Training for Sales Representatives and Systems Engineers

We offer e-learning courses for our sales representatives and systems engineers to acquire essential and foundational knowledge in the security area, with Security by Design (SBD) set as the core concept. In the fiscal year 2024, 36,000 employees completed the course. Additionally, we organized themed discussions to gain practical insights based on videos about real incidents that occurred in our customers' systems. These initiatives aim to bolster the overall security implementation capabilities across the NEC Group.

❻ Holders of Advanced Security Technology Qualifications

To provide our customers with optimal solutions, NEC encourages our employees who communicate with customers, such as sales representatives and systems engineers, to obtain recognized security certifications as proof of their advanced skills in information security. We are expanding the number of certified professionals through inhouse seminars and study sessions, focusing on international certifications like CISSP and Registered Information Security Specialist (RISS). We have strategically partnered with ISC2, the certifying body, to promote employees' obtaining the CISSP certification. Earning this certification helps our employees develop not only advanced technical skills but also risk assessment skills from a business perspective. As a result, the NEC groups now boasts 450 CISSP-certified professionals.

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

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.

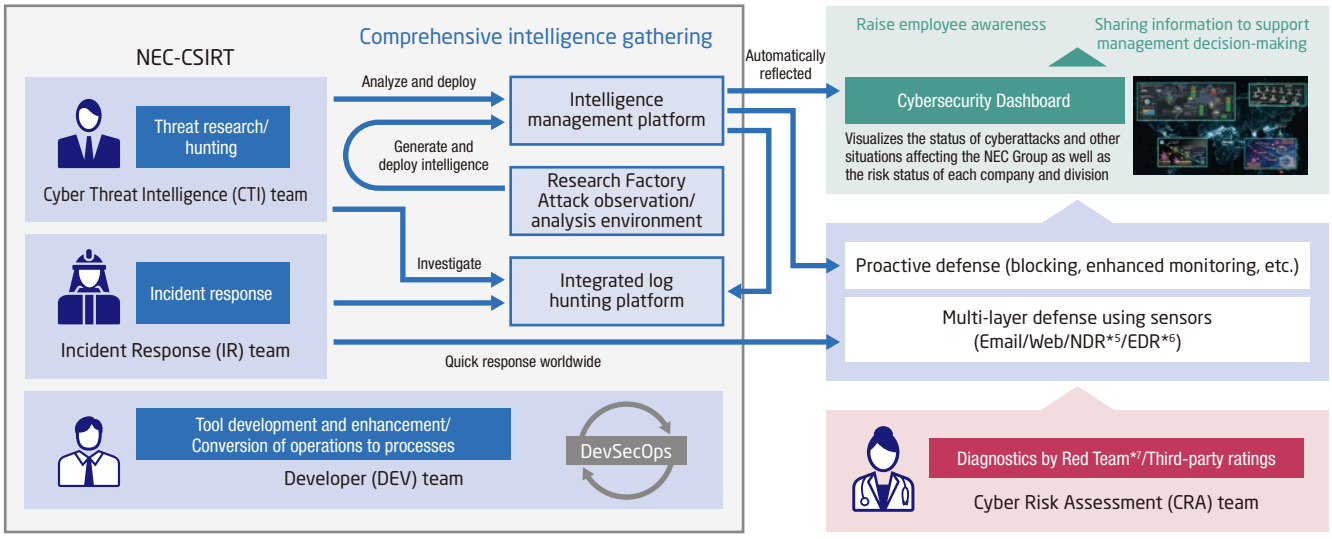
1 | Measures Against Global Cyberattacks

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. To strengthen our measures, we also have third-parties evaluate new components, focusing primarily on the GOVERN function of NIST CSF*1 versions 1.1 and 2.0.

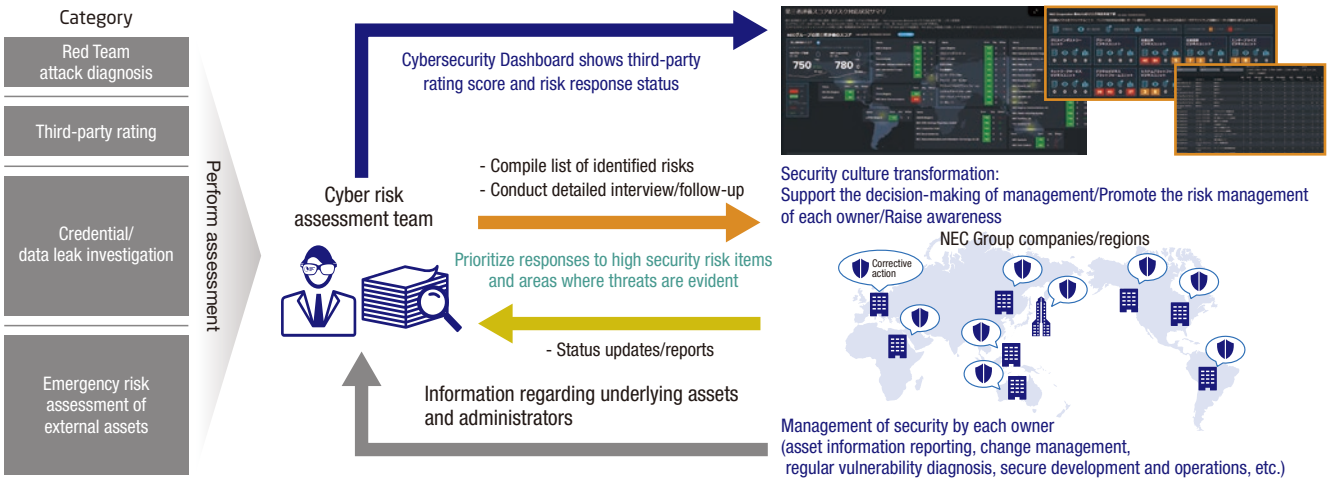
Specifically, we recognize that a unified global approach to cybersecurity risks is crucial for business continuity. Utilizing AI, we continuously monitor, understand, and analyze daily cyberattacks, revising our monitoring and operational processes accordingly. We stay updated on the latest developments in security products, services, and market trends. Through PoC*2 evaluations and internal IT environment assessments, we determine the compatibility of these products and services with our IT infrastructure. From these assessments, we identify necessary future measures and calculate their scope, effectiveness, and costs. Each year, we draft an action plan based on these activities and implement the measures with the approval of the CISO.*3

The NEC Group implements measures based on a comprehensive cyber defense strategy, such as the CDC.*4 Our primary focus areas are outlined in points 1 through 5 below.

Overview of Our Cybersecurity Measures



Cyber Risk Assessment



★1 NIST CSF: The NIST Cybersecurity Framework; issued by the US National Institute of Standards and Technology (NIST) aimed at improving cybersecurity for critical infrastructure
★2 PoC: Proof of Concept; A pilot project conducted to demonstrate the feasibility and potential of a new concept ★3 CISO: Chief Information Security Officer
★4 CDC: Cyber Defense Centre ★5 NDR: Network Detection and Response ★6 EDR: Endpoint Detection and Response
★7 Red Team: A group that performs simulated attacks on a company or organization to emulate real-world threats. Their goal is to assess the organization's ability to withstand attacks, evaluate associated risks, and provide recommendations for improvements and additional security measures.

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) 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 integrated drills involving top management, relevant departments, and experts at least twice a year, and hold mock press conferences led by our CEO.

❺ AI-based Advanced Cybersecurity Measures

We are leveraging AI, including generative AI, to enhance, automate, and streamline a wide range of cybersecurity tasks. These include cyber risk assessments, threat intelligence generation and utilization, network detection and response (NDR), incident research, and phishing email training.

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.

The innovative nature of this initiative has been recognized externally, earning us the "IT Excellence Award (Management Category)" at the 41st IT Awards in 2024, organized by the Japan Institute of Information Technology, and the "Special Award" at the Japan DX Awards 2024, organized by the Japan Digital Transformation Promotion Association.

NEC Cybersecurity Dashboard

IT Excellence Award Presentation Ceremony

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 that meet the appropriate security level. 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.

1 Contract Management

NEC establishes comprehensive intercompany agreements (basic agreements) with business partners, which include confidentiality obligations, as well as a memoranda of understanding (MOUs) for specific customer-related projects.

2 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, we require the submission of a subcontractor verification and organizational structure confirmation form to clearly outline the project's organizational framework and management structure for each individual project.

3 Staff Management

NEC has established a set of guidelines titled "Basic Rules for Customer Related Work," which outlines the measures that workers undertaking outsourced tasks must follow. To ensure these measures are strictly implemented, we require the workers to formally pledge their adherence to these guidelines within their own companies.

4 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.

5 Technology Deployment

We have divided our technical measures into two categories: mandatory measures, which include full encryption of portable electronic devices and external storage media, and recommended measures, such as systems to prevent information leakage. We request our business partners to implement these measures accordingly.

6 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.

7 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. In light of the evolving cybersecurity landscape, we have updated these standards to better prepare for potential incidents and are enhancing our collaborative efforts with business partners.

Information Security Measures for Business Partners

2 | Promotion of Security Measures for Business Partners

❶ Information Security Seminars

NEC organizes information security seminars every year for business partners 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. Moreover, our CISO gives lectures on cybersecurity to raise awareness about information security.

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. We increase the number of these visits each year, reaching around 300 companies in fiscal year 2024, facilitated by about 100 NEC inspectors.

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

Assessments and Improvement Actions for Business Partners

4 | Enhancement of Cybersecurity Measures

To enhance our cybersecurity measures, we revised our information security standard in April 2022. The new standards are based on NIST SP 800-171, which focuses on incident response capabilities, including preparation, detection, analysis, containment, recovery, and user response activities. Each year we conduct a system security plan (SSP) review to monitor progress against these standards. For areas where our business partners face challenges, we hold cybersecurity training sessions.

Furthermore, for our core business partners, we aim to reduce attack risks and improve security levels by sharing third-party evaluation results and collaborating on risk mitigation efforts. This approach helps our business partners reduce their security risks effectively.

5 | Enhancement of Global Supply Chain Management

To strengthen global supply chain management, we host information security seminars for employees at our overseas subsidiaries. In fiscal year 2022, we held these seminars in China, and in fiscal year 2023, we conducted them in India and Vietnam. We will continue these initiatives to raise awareness about information security among our global workforce and enhance the security level across our entire 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 cybersecurity managers 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 cybersecurity 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. in fiscal year 2024 (ended March 31, 2024), we assigned 400 cybersecurity managers across all the divisions and have strengthened cooperation between the cybersecurity management department and each division through bi-weekly meetings and community forums.

The “Cybersecurity Management Rules,” which is a part of the NEC Group Management Policy, defines the roles of cybersecurity managers and specifies the cybersecurity implementation processes that each division must adhere to. Similar to NEC Corporation, its group companies are also proceeding to establish their security implementation promotion structure and developing their own cybersecurity management rules.

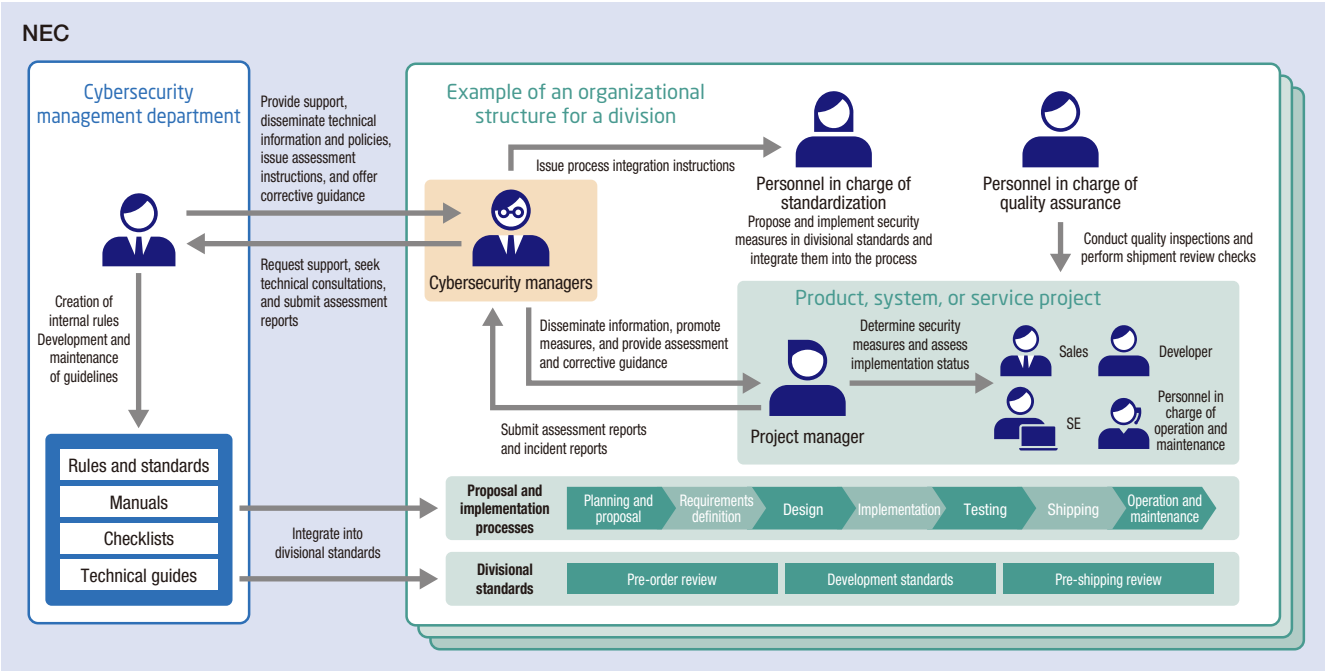
❷ Key Security Implementation Efforts

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 also established the “Cybersecurity Implementation Standard” to serve as the baseline for cybersecurity requirements that must be considered when enforcing security implementations. 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.

In the development of products, systems, and services, we have created a checklist to ensure that security tasks are performed in each phase. Using this checklist, business projects are managed through the “security implementation assessment system,” which was

Security Implementation Process



developed to visualize and centrally manage security tasks. This system allows us to efficiently assess and monitor our current security status. The cybersecurity management department utilizes the integrated information to deploy more effective measures across all divisions and strengthen corporate security implementation governance.

In the operation and maintenance phases of our products, systems, and services, we ensure cybersecurity by using the "vulnerability management system" and the "cyber intelligence sharing platform" to centrally collect and distribute vulnerability information. The vulnerability management system has been revamped through agile development, allowing for flexible extensions of functions and more efficient vulnerability management. The collected vulnerability information is shared not only with each division but also with our customers who use our products, systems, and services to inform them of the risks related to the vulnerabilities. The cyber intelligence sharing platform is equipped with functionalities to swiftly share cybersecurity threat information, such as attack methods, incident cases, vulnerability information, and security measure indicators, to all divisions.

In addition, NEC has established a Product Security Incident Response Team (PSIRT) to collect and respond to vulnerability information related to NEC Group products. We have set up a contact point for receiving external vulnerability reports, announced a vulnerability disclosure policy, and have operated as a CNA.*1 These activities enable us to effectively manage unknown vulnerabilities in our products and in our customers' systems.

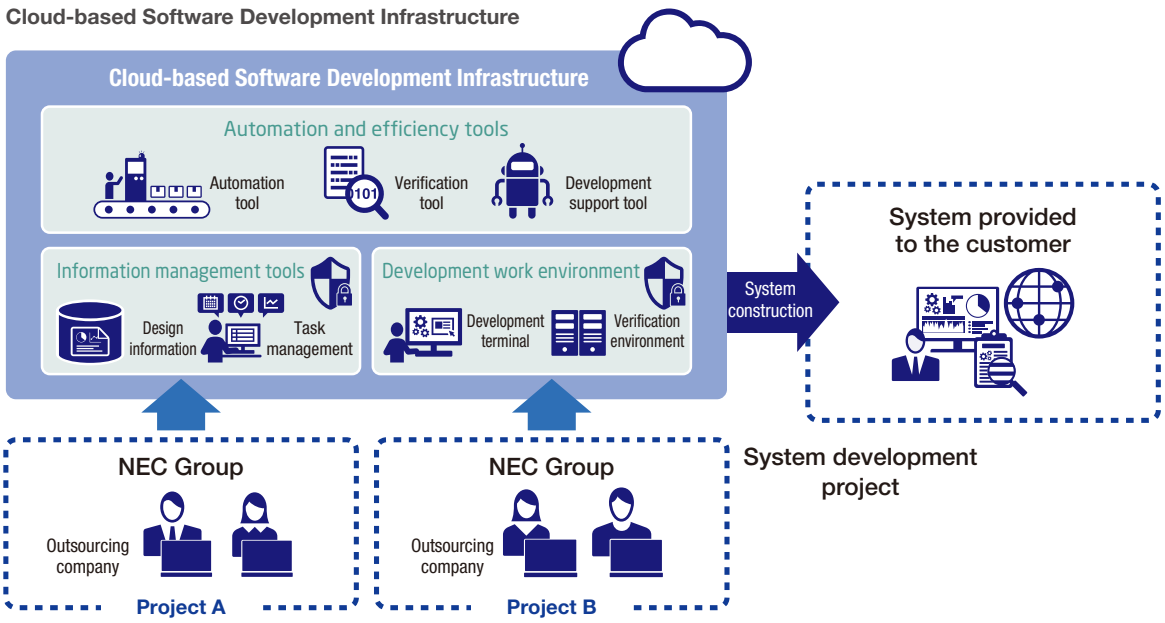
❸ Software Development Infrastructure for Security Implementation

NEC has cloud-based software development infrastructure in place as an internal standard environment for system development. This integrated development environment includes a tool for information management to organize tasks and design information such as source code and specification documents, an automation and efficiency tool that enables the automation of build and test processes, AI-driven software development support, and a development work environment for software implementation and testing. 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.

❹ Security Enhancement in Our Hardware Production Facilities

NEC's factories conduct third-party risk assessments and implement measures tailored to specific risks, such as business continuity planning (BCP) exercises based on cyberattack scenarios.



*1 CNA(CVE Numbering Authority): An organization that assigns CVE*2 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

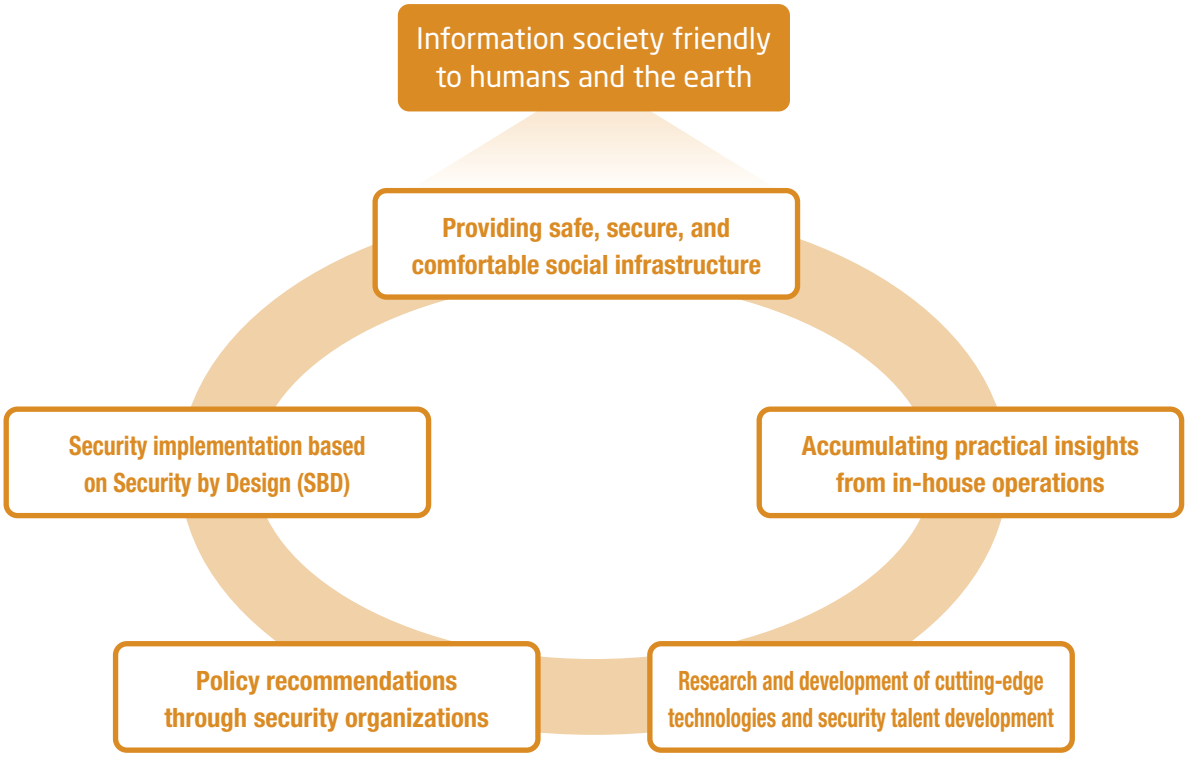
In October 1977, during a keynote speech titled, "Shaping the Communications Industry to Meet the Ever-Changing Needs of Society," NEC proposed the concept of C&C*1 as a vision for integrating computers and communications. In line with this declaration, we have been committed to connecting computers around the world. By connecting people with things and things with things, we have met diverse social needs and contributed to societal development.

With the recent popularization of DX*2, our work styles have undergone significant changes, such as an increase in opportunities for remote work. This has led to a greater integration of physical (real-world) and cyber spaces, connecting everything more closely. In such an interconnected world, security risks can arise anywhere, and we need to address these emerging risks. In the face of rapid changes in the business environment, cybersecurity has become more crucial than ever to ensure safe business operations.

NEC has various initiatives in place to address this challenge. We actively collaborate with domestic and international security organizations , and input policy proposals to the Japanese Cabinet Secretariat, ministries, and agencies through our partners and industry associations. Moreover, not only we offer advanced security services but also we contribute to nurturing skilled security professionals through our research and development activities and capacity building programs for external and internal talent. Based on the Security by Design (SBD) approach, we have introduced security measures at every stage of the system lifecycle, from design through construction and operation, including implementation framework to tackle emerging cyber risks. Additionally, we are driving the "Client Zero" approach in cybersecurity, using our own organization as the initial user to gain practical insights. We gather knowledge from the security measures operating across our 110,000 NEC Group employees.

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

NEC's Cybersecurity Initiatives for Contributing to Safety and Security



*1 C&C: Computer & Communication *2 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.

We have been actively involved with the Japan Cybercrime Control Center (JC3) since its foundation, aiming to solve cybercrime issues and promote collaboration among academic institutions, industry, and law enforcement agencies in Japan. Additionally, we have participated in ICT-ISAC*3 and Cyber Threat Alliance (CTA) to promote the use of cyber threat intelligence. We also contributed to the international standardization of organizational frameworks for managing cyber risks in 2021, which resulted in the ITU-T*4 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, Executive Advisor at NEC, serves as a member of the Cybersecurity Strategic Headquarters of the Cabinet, the Chair of the Committee on Cyber Security at Keidanren (Japan Business Federation), and President of the Supply Chain Cybersecurity Consortium (SC3). Additionally, Kazuhiro Sakai, Corporate SEVP and Co-COO*5 at NEC, serves as the Chief Director of JC3. In this way, NEC is actively contributing to national security projects. Through these roles, NEC actively contributes to national security projects. Furthermore, by advocating and proposing policies to government ministries and agencies through industry associations, such as Keidanren, SC3 and JDTF*6, NEC contributes to the creation of a safe and secure society in solidarity with public and private sectors.

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)

ICT-ISAC was established to enable diverse business entities, such as telecom carriers, broadcasters, software vendors, information service providers, and information equipment manufacturers, to share information on cyberattacks. The organization aims to facilitate collaboration and cooperation across industry boundaries to effectively tackle threats. NEC has actively participated in the organization since its predecessor organization, Telecom-ISAC.

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

Together with NTT Corp. and Hitachi, Ltd., we launched a study group focused on developing cybersecurity talent. Since 2017, we have transitioned to an organization within the Cyber Risk Information Center (CRIC) to further enhance our efforts in information sharing.

Joined the Cyber Threat Alliance (CTA) (October 2018)

NEC joined the Cyber Threat Alliance (CTA), a U.S.-based nonprofit organization that promotes information sharing among security firms. By sharing and utilizing threat intelligence, we strengthen our own security measures and enhance the development of our security-related services and products.

Established the Security Transparency Consortium (October 2023)

NEC launched this consortium jointly with NTT Corp. with the aim of resolving social issues such as supply chain security risks by enhancing security transparency of products, systems, and services. As a managing entity, NEC drives the creation and provision of visualized data on software components and promotes expansion of its use cases.

Interorganizational Collaboration

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

NEC developed security transparency assurance technology in partnership with NTT Corp. to drastically reduce supply chain security risks by ensuring transparency in the security of information and communication infrastructure systems.

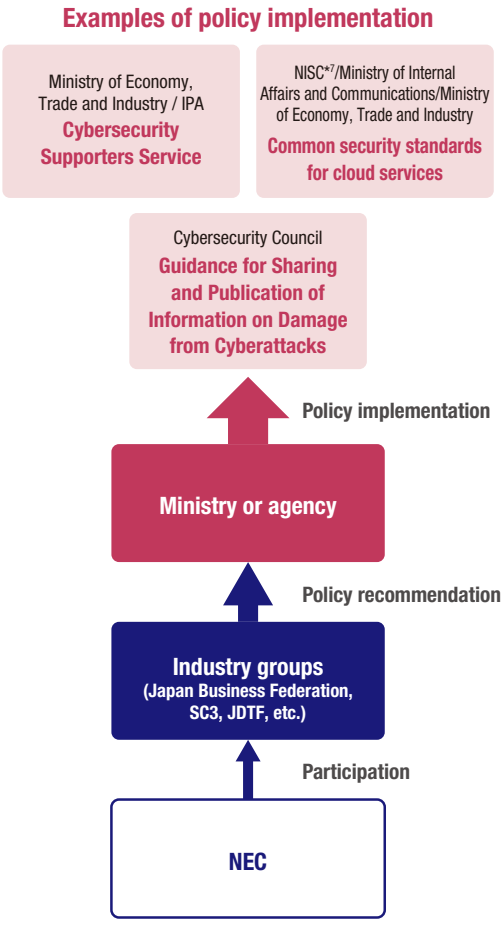
Released an ITU-T recommendation on the organizational framework for cyber risk response (November 2021)

NEC worked with NTT Corp., NTT Security Holdings, and NTT TechnoCross Corp. to develop the concept of a cyber defense centre aimed for strategically and systematically addressing cyber risks. Also, we worked towards its international standardization, particularly its build, management, and evaluation processes, resulting in 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 partnerships with 51 national technical colleges across Japan and we provide them with educational support that combines our latest security technologies and expertise. This industry-academia collaboration contributes to fostering highly skilled professionals with practical capabilities who can demonstrate greater job performance than ever before.

Policy Recommendations Made Through Industry Groups



*3 ICT-ISAC: ICT Information Sharing and Analysis Center *4 ITU-T: International Telecommunication Union Telecommunication Standardization Sector *5 Chief operating officer
*6 JDTF: Japan Digital Trust Forum *7 NISC: National center of Incident readiness and Strategy for Cybersecurity

3 | World-Leading Human Resources and Technologies

❶ Organizational Structure for Offering Advanced Services

The NEC Group includes companies that offer highly sophisticated services like NEC Security Ltd. and Cyber Defense Institute, Inc. 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.

❷ Development of In-House Human Resources

NEC and its group companies have also focused on developing security personnel (for details, see “Information Security Personnel” on page 12). Some of our experts have won prizes in international security skill competitions.

❸ Development of Security Human Resources in Japan

In July 2022, NEC signed a comprehensive partnership agreement with the National Institute of Technology (KOSEN) to strengthen capacity-building efforts in the field of cybersecurity. This agreement aims to promote industry-academia collaborative educational support by combining KOSEN's 60 years of experience in educating highly skilled professionals to meet social needs with 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.

In September 2023, NEC co-hosted an event with KOSEN called "K-SEC CAMP FOR GIRLS in KISARAZU," specifically designed for female students. The event featured a career workshop led by NEC's three female security engineers and a technical workshop using in-house CTF (capture the flag) challenges.

❹ Providing Training Programs for Customers

NEC offers “NEC Academy for DX,” a service offering solutions for DX human resource development. This program is aligned with the “Digital Skills Standards” proposed by the Ministry of Economy, Trade and Industry and the Information-technology Promotion Agency, Japan (IPA) in December 2022.

The program includes training for business-focused security managers who can assess risks and build an organizational structure for security, as well as specialists responsible for managing cybersecurity risks.

Technical Workshop Co-hosted by KOSEN and NEC

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. In response to the increasing number and sophistication of cyberattacks, NEC stipulated that the Cybersecurity Management Rules, complied in September 2022, has been applied to the entire company since October 2023. NEC has enhanced corporate security governance and deployment of security measures across divisions through central management of the security status and vulnerability information of business projects. (For details, see "Providing Secure Products, Systems, and Services" on page 18.)

Additionally, NEC aims to achieve security that can respond to the latest emerging threats based on the Security by Design (SBD) approach to ensure a secure environment where data and systems are intricately intertwined due to the acceleration of DX.

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 today's world, where cyber risk management is a critical concern, it is not enough to just apply cybersecurity measures; we must foster a culture that conducts data-driven cybersecurity management and takes proactive actions to properly maintain and operate these measures. This effort is essential to defend effectively against increasingly sophisticated cyberattacks.

NEC utilizes a Cybersecurity Dashboard (see page 26) to visualize the status of cyber defense of the NEC Group and risk for each group company or division. By leveraging this tool, we collect practical insights from the security operations of our global workforce of 110,000 employees. This approach enables executives to make swift decisions, raises cyber risk awareness among all employees, and promotes security improvements, such as autonomous actions, through comprehensive analysis.

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 DX accelerates, economically motivated cyberattacks are becoming more intense, targeting various systems and data, and threatening the continuity of business operations. A notable recent trend is that these attacks frequently extend beyond a single organization due to the increasing interconnectedness of systems. In response, international organizations, governments, and industries are developing laws and guidelines, such as the Economic Security Promotion Act,*1 to address security threats that jeopardize national and personal safety. Consequently, companies are now expected to implement security measures not only for themselves but also across their entire supply chain, including subcontractors.

❷ Security Risks in the Cloud Environment

Traditional network perimeter defenses are reaching their limits, given the shift of critical information from on-premises to the cloud and the rise in remote connections from outside the corporate network. As the use of cloud services becomes more prevalent within companies, there has been an increase in information leaks and unauthorized access caused by user misconfigurations and errors. Therefore, implementing security measures for cloud services has become an urgent priority.

❸ Increase in risks of intrusion from publicly accessible IT assets

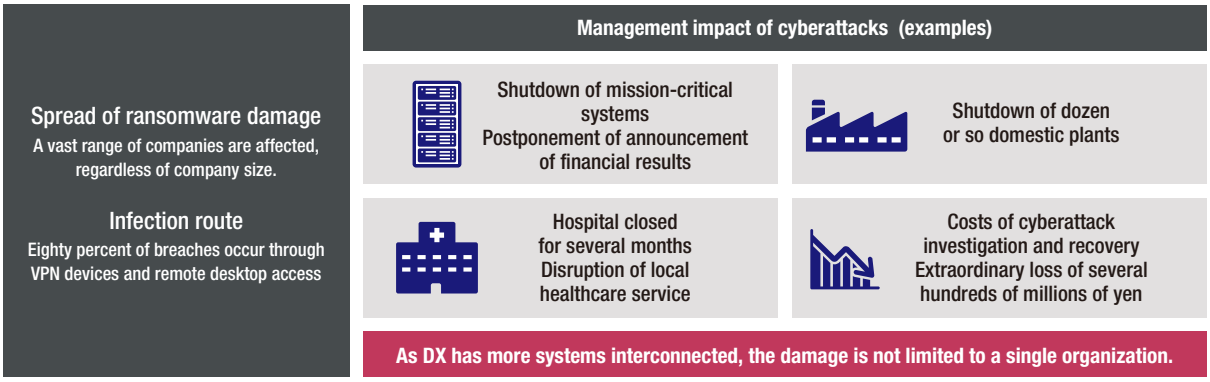
As DX progresses, the expansion of cloud services and remote work, along with the growth and dispersion of IT assets owned by companies, has led to an increase in the "attack surface"—the potential targets for cyberattacks. While traditional ransomware primarily spread through emails and websites, there has been a sharp increase in infections exploiting vulnerabilities in publicly accessible servers and network devices, causing more severe damage. From this background, there is increasing attention on attack surface management (ASM*2), which involves researching information about IT assets that can be accessed from the internet, identifying vulnerabilities, and managing them. In line with this trend, the Ministry of Economy, Trade and Industry has also released guidance on implementing ASM.*3

2 | The Concepts of Security Changing with the Architecture

The progressing adoption of telework and cloud services due to DX makes it challenging to ensure security using the traditional approach of protecting information assets within internal network perimeters. To safely advance DX, it is essential to adopt a zero-trust model, where no one is trusted by default and every access is continuously authenticated and authorized. Additionally, maintaining strict cyber hygiene practices to consistently eliminate vulnerabilities is critical. It is also crucial to safeguard against internal information being removed and leaked externally, even by authenticated and authorized users, whether due to intentional actions, negligence, or external factors. Beyond technological solutions, ongoing education to boost security awareness and literacy is necessary to enhance defenses against human-targeted cyberattacks.

In the context of DX, where vulnerabilities are dispersed and

Changes in Security Risks



*1 Economic Security Promotion Act (Cabinet Office): https://www.cao.go.jp/keizai_anzen_hosho/index.html *2 ASM: Attack Surface Management
*3 Guidance on the Introduction of ASM (Ministry of Economy, Trade and Industry): https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

data/systems are intricately interconnected, comprehensively understanding and managing overall security risks becomes challenging. Consequently, risks that need addressing tend to remain hidden. At NEC, we prioritize visualizing security risks across the entire organization and addressing them through a consistent process—encompassing strategy formulation, design, operation, and monitoring. Shifting from partial to holistic optimization is a crucial focus in today's security environment.

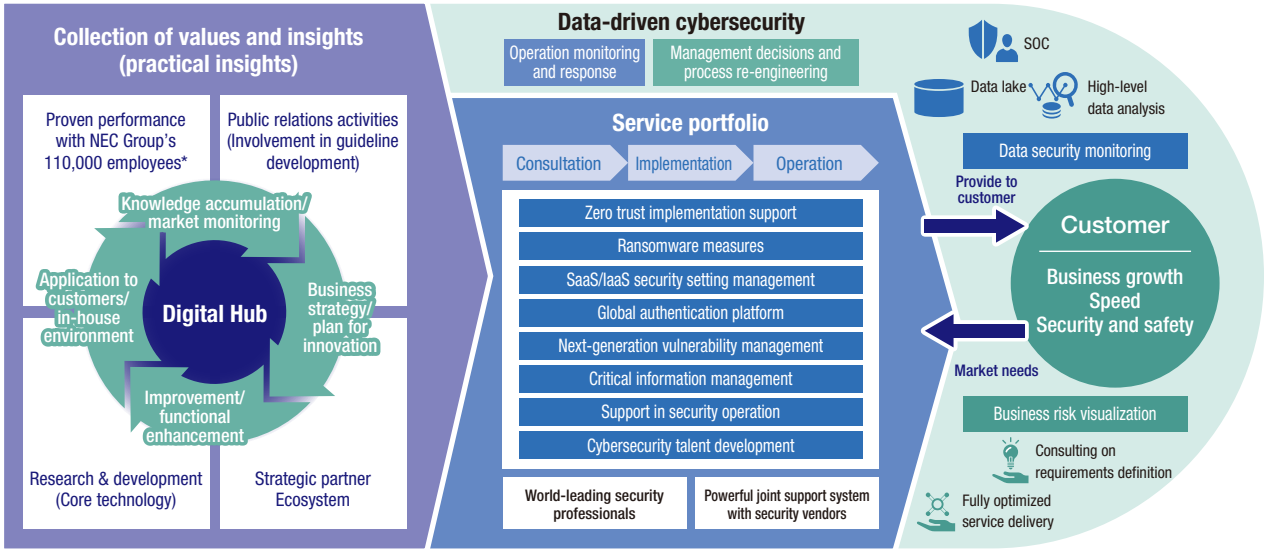
3 | What NEC Can Do to Help Customers Promote DX Safely

NEC is promoting the "client zero" initiative, where we are the first to implement cutting-edge technologies in our operations, leveraging our extensive research, development, and strategic partnerships. Additionally, we have gathered and accumulated a wealth of valuable insights and expertise—what we call "practical insights"—from our own security measures and extensive track record of supporting numerous customers. We have packaged this expertise into a comprehensive service portfolio that provides end-to-end support, from consulting to implementation and operation, tailored to meet the unique needs and challenges of our customers.

Examples of Security Solutions Needed for DX and Cloud Shift

Issue	Key measures to implement	Solution example
Integrated ID and access management	• Centralize the management of login information and access privileges for distributed systems, applications, and SaaS platforms • Employ strong authentication methods such as single sign-on (SSO) and multi-factor authentication (MFA)	• SECUREMASTER and Okta
Critical information management	• Classify data based on its confidentiality and importance • Control access to data that has been classified as confidential	• Critical information protection solution introduction service
Cyber hygiene	• Identify internal IT assets and vulnerabilities • Identify and eliminate vulnerabilities in IT assets in real-time	• UEM (Unified Endpoint Management)
Cloud configuration management	• Continuously visualize and automatically correct cloud configuration issues and other mistakes	• CSPM*4 and SSPM*5
Security risk visualization and mitigation	• Perform thorough visualization and analysis of security risks within the organization • Implement continuous and efficient security risk management processes	• Data-driven cybersecurity service
Enhancing employee security awareness and literacy	• Visualize the security levels of employees • Provide ongoing and effective security education and training	• NEC security awareness training

Provision of Offerings for Promoting DX Safely



* As of June 2024

*4 CSPM: Cloud Security Posture Managementl *5 SSPM: SaaS Security Posture Management

In 2023, we established NEC Security Ltd. by bringing together highly specialized and experienced security professionals from the former Infosec Corporation, which had extensive experience in providing and managing security services for government agencies and critical infrastructure companies. Starting in 2024, we integrated NEC's cybersecurity business into the new company, enabling us to offer advanced and comprehensive cybersecurity solutions and services.

By combining the extensive knowledge developed by the former Infosec Corporation with our experience in managing the information security infrastructure for 110,000 NEC Group employees, and the expertise of our specialized security professionals supporting the provision of NEC's advanced services, we help our customers achieve efficient and effective end-to-end security risk management. This support spans the entire security process, from strategy formulation to implementation, operation, monitoring, and response.

4 | What NEC Can Do to Help Customers Achieve Total Optimization

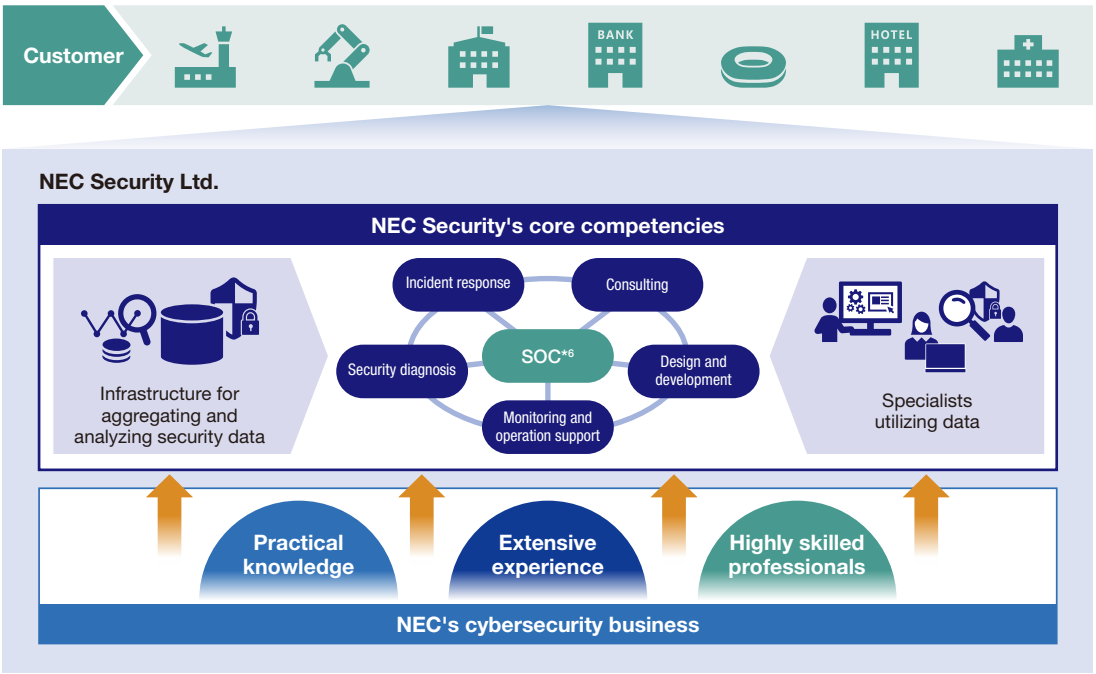
To effectively address latent security risks, it is important to continuously understand the current situation and the extent to which countermeasures have been implemented across the entire system. To achieve this, NEC has developed an original cybersecurity dashboard that visualizes the necessary data from the perspectives of system administrators, employees, and executives. This enables data-driven security risk management and the implementation of cybersecurity management.

Drawing from the extensive knowledge gained through the development and operation of our internal cybersecurity dashboard, NEC provides data-driven security services to our customers, supporting the DX of their security operations.

Cybersecurity 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. For the latter, it is designed to easily visualize management risks, such as the number and percentage of unpatched vulnerabilities and suspected cyberattacks. Through these cybersecurity dashboards, customers can gain a comprehensive understanding of their overall security status and current risks, as well as address any suboptimal aspects of their existing solutions.

Services Provided by NEC Security Ltd.



*6 SOC: Security Operation Center

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.

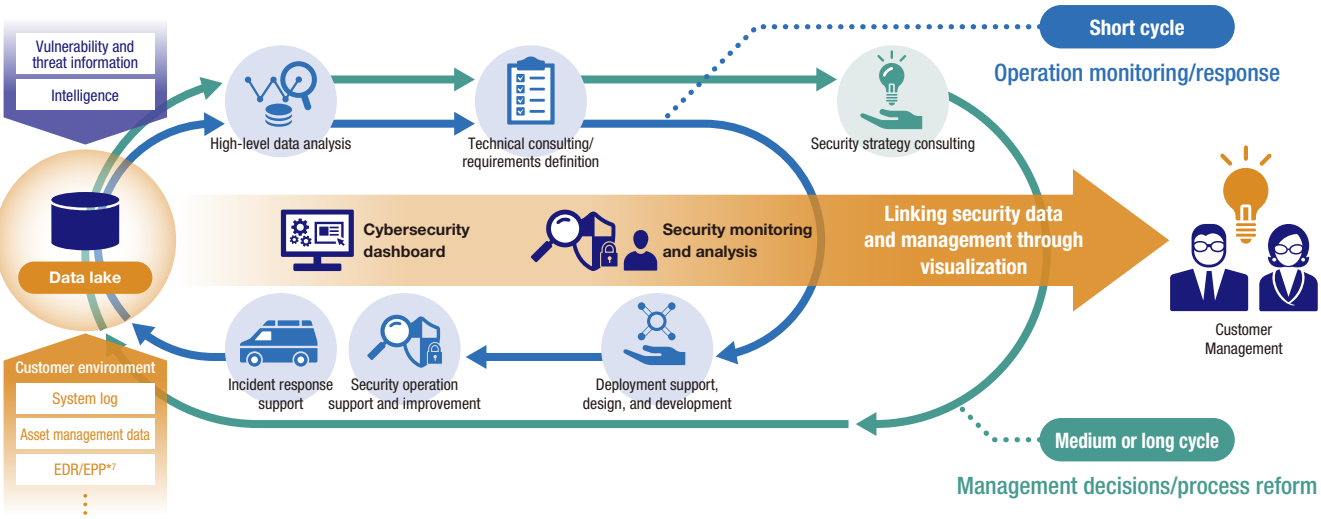
External IT Asset Risk Visualization Service:

We analyze and visualize risks with a focus on the vulnerabilities of externally exposed IT assets and leaked authentication information, which are frequently exploited in recent cyberattacks such as ransomware. These areas are critical focal points for implementing effective security measures.

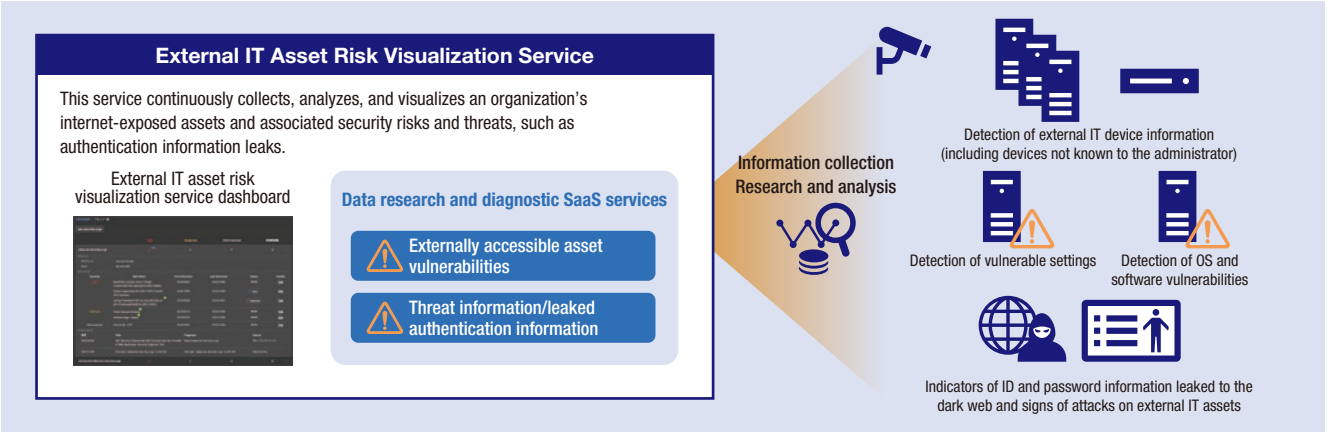
This service leverages the expertise of professionals with extensive experience in penetration testing and incident response. Drawing on their experience, these specialists design the service to visualize the key data needed for countering cyberattacks. By making visible the risks that require prompt attention, we help customers prevent and minimize the impact of cyberattacks.

Lastly, as DX accelerates, the exposure to security risks is growing, making the need for robust security measures more urgent. NEC leverages our extensive knowledge and experience to support our customers' security initiatives. Please contact NEC for more information about our wide range of solutions and support services.

Full Optimization Process for Data-driven Cybersecurity



External IT Asset Risk Visualization Service



*7 EDR/EPP: Endpoint Detection 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 create a society where everyone can use digital technology with peace of mind, the NEC Group is conducting cutting-edge research and development in both system security and data security based on the Security by Design (SBD) concept.

In this report, we present "automated secure system design," a key innovation from our system security research that automates the design of secure ICT systems. Additionally, from our data security research, we spotlight "privacy-preserving biometric authentication," a technology that performs face recognition on encrypted biometric feature, and "highly confidential hybrid federated learning," which allows organizations to build AI models without sharing their data with each other.

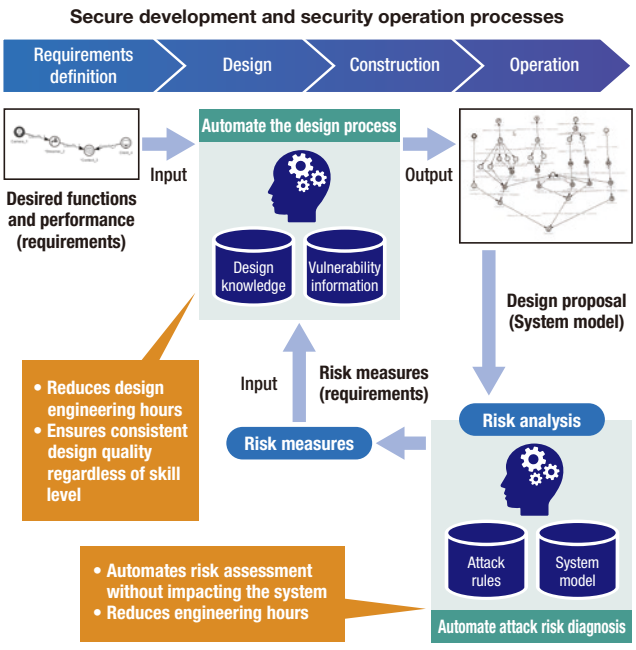
2 | Automation of Secure Development and Security Operation

The advancement of DX for enterprise and social systems has led to increased complexity in ICT systems, thereby escalating the risk of cyberattacks. As these risks continue to rise, Security by Design becomes indispensable for fortifying the security of ICT systems. However, manually designing and developing complex ICT systems to ensure their security, as traditionally done, has become increasingly challenging and labor-intensive. In response, NEC is developing technologies to automate the design of these intricate systems. Leveraging AI, the system automatically combines and evaluates the components of an ICT system based on required functions and performance, including security needs, to derive a secure system configuration that meets all specified requirements.*1

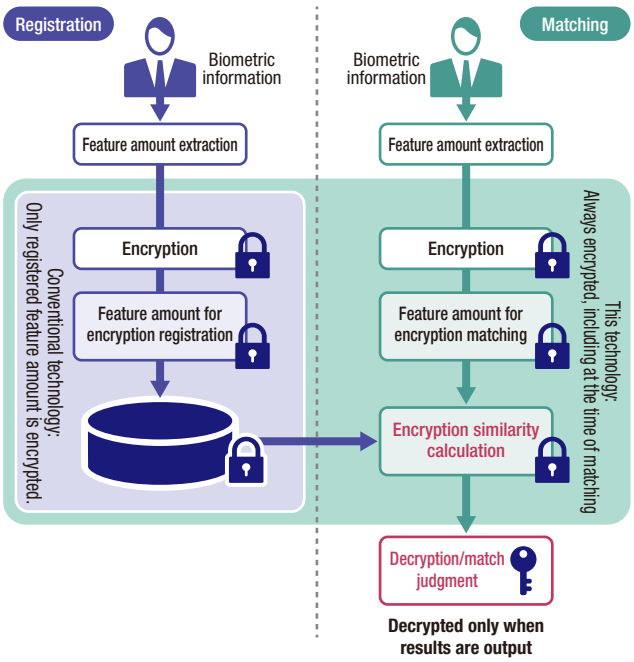
Even after a secure ICT system is constructed, the risk of cyberattacks can increase over time due to the discovery of new vulnerabilities. Therefore, it is essential to periodically assess and address security risks during system operation. Traditionally, this risk assessment involves manually investigating the actual system, a process that is both time-consuming and labor-intensive and can lead to issues such as system downtime.

NEC's cyberattack risk assessment technology offers a solution by automatically assessing potential cyberattack risks in ICT systems. This technology utilizes system information obtained through automated design and conducts comprehensive attack pattern investigations using computer simulations. As a result, security risks

Automation of Secure Development and Security Operation Processes



Privacy-Preserving Biometric Authentication Process



*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

can be automatically assessed without impacting the operational system. Furthermore, based on the assessment results, a secure system configuration can be automatically derived, ensuring ongoing system security.*2*3

By automating the secure development and security operations of systems—tasks that previously required substantial effort—NEC supports the efficient design, development, and operation of secure systems.

3 | Privacy-Preserving Biometric Authentication

As face recognition becomes increasingly adopted for personal verification, there is a risk that biometric information could be leaked. The leaked biometric information could be exploited for impersonation or other malicious activities. To address this risk of leakage, we are engaged in the research and development of "privacy-preserving biometric authentication." This approach ensures that biometric features derived from biometric information remain encrypted not only during registration but also throughout the matching process.*4*5

In privacy-preserving biometric authentication, secure computation techniques such as "multi-party computation" and "homomorphic encryption" are utilized to perform face recognition matching while keeping the features encrypted. For large-scale applications, a multi-party computation-based approach is optimal, allowing face recognition matching within one second for up to approximately one million registered users. For medium to small-scale applications, a homomorphic encryption-based approach is ideal, enabling fac recognition matching within one second for up to approximately 10,000 registered users on a single server.*6 Additionally, we have developed a technology that applies this concept to digital signatures by generating digital signatures from biometric features.*7 By verifying these digital signatures, we can confirm that the data's authenticity has been assured by the legitimate individual.

Through the use of these technologies, we aim to enhance the safe and secure utilization of biometric authentication, including face recognition.

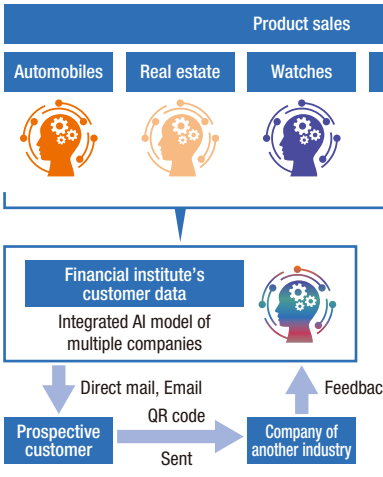
4 | Highly Confidential Hybrid Federated Learning

Companies across various industries collect data and develop AI models to enhance their sales and marketing activities. For instance, AI can be used to estimate potential customer prospects. However, extending such AI capabilities across different industry sectors—such as building an AI model that predicts real estate pricing tiers using automotive purchasing data—proves challenging. While consolidating data from both industries into a single repository would simplify developing these cross-industry AI models, this approach is not easily achievable. Confidentiality issues, including the sharing of trade secrets, and legal concerns related to personal data privacy regulations, pose significant barriers to integrating proprietary data held by different companies.

Highly confidential hybrid federated learning addresses these challenges by enabling cross-industry attribute estimation without directly aggregating data. By leveraging this technology, we aim to integrate AI capabilities from various industries, providing a unified AI platform that enables mutual attribute estimation across different sectors.*8*9

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.



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%

People who buy expensive houses tend to prefer minivans.

People who buy self-winding watches tend to prefer expensive houses.

*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 Haruna Higo, Toshiyuki Isshiki, Saki Otsuki, Kenji Yasunaga. 2023. "Fuzzy Signature with Biometric-Independent Verification." BIOSIG 2023.
*8 "Highly Confidential Federated Learning: Balancing Privacy, Confidential Information Protection, and AI Utilization." https://jpn.nec.com/rd/special/202103/index.html.
*9 Junki Mori, Ryo Furukawa, Isamu Teranishi, Jun Sakuma. 2023. "Heterogeneous Domain Adaptation with Positive and Unlabeled Data." IEEE Big Data.

Third-party Evaluations and Certifications

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

Global ESG investment Index: Dow Jones Sustainability Asia Pacific Index

NEC has been consistently recognized in the top tier within the IT sector for four consecutive years (2020 to 2023) in the categories of Information Security, Cybersecurity, and System Availability. In 2022 and 2023, 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.
(Out of the companies included in the Nikkei 500, only 14 were selected for this recognition.)

IT連 日本IT団体連盟

1 | ISMS Certification

The following companies have organizations that have achieved ISO/IEC 27001 certification for their information security management system (ISMS). This list includes only those companies that have been officially certified by the ISMS Accreditation Center and are publicly listed in their registry as of June 14, 2024.

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 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 Communication Systems, Ltd.
- Forward Integration System Service Co., Ltd.
- LanguageOne Corporation

2 | Privacy Mark Certification

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

NEC Group Companies Certified to Use the 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 Business Intelligence, Ltd.
- NEC Livex, Ltd.
- KIS Co., Ltd.
- Sunnet Corporation
- Nichiwa
- 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

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

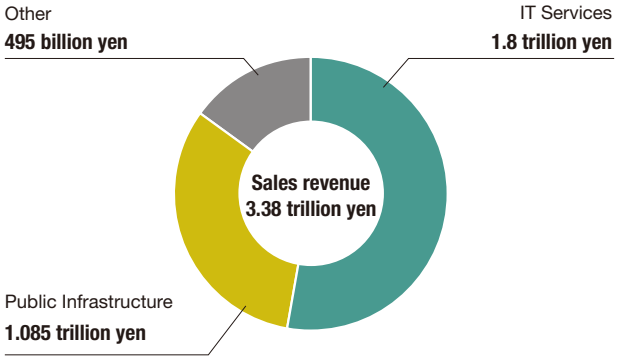
Corporate Profile

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)	105,246*
Consolidated subsidiaries	254*

*As of March 31, 2024

Segment Information

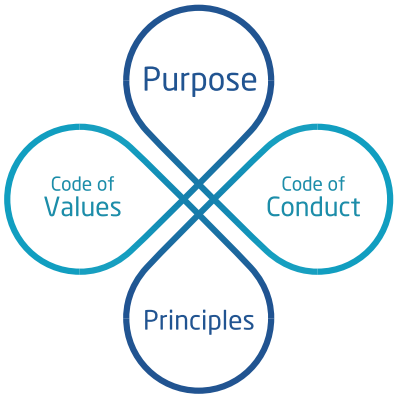
Segment Information



*As of March 31, 2024

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 2024

NEC Corporation

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

Issued July 2024