Cybersecurity Management Report 2025

NEC \Orchestrating a brighter world

MAKE JAPAN CYBER SECURE

NEC recognizes information security as a critical management priority. By aligning with national guidelines and international standards, we aim to be a company continuously trusted by society.

Noboru Nakatani

NEC Corporation
Corporate EVP and CSO
Managing Director, Cyber Security Division
President and CEO, NEC Security, Ltd.

As the entire world is openly connected and the use AI is expanding, it is a critical issue for both nations and companies to address sophistication and commercialization of cyberattacks, increasing risk of data breaches through cloud utilization, and the challenges of information management in economic security.
In response to these developments, NEC has adopted the slogan “MAKE JAPAN CYBER SECURE" and is strengthening its cybersecurity business to contribute to the Japan’s economic security. This includes providing proprietary cyber threat intelligence, leveraging Made in Japan AI technologies to achieve both safety and functionality, and establishing a globally integrated operational framework.
This report is published annually for stakeholders to understand NEC Group’s cybersecurity initiatives that support our business operations, including those mentioned above. From 2025, the report has been renamed from “Information Security Report” to “Cybersecurity Management Report”, to clearly reflect the importance of cybersecurity to business management in recent situation and developments.
NEC will continue to advance cybersecurity management through Digital Security Transformation. As “Client Zero*1,” we deliver added value by leveraging cutting-edge technologies that we have already implemented internally, along with practical insights and operational know-how. Through these efforts, we contribute to realizing NEC’s Purpose—“Orchestrating a brighter world”—and building a safe, secure, fair, and efficient society where people can live enriched lives. Our goal is to remain a company that earns enduring trust from society.

*1 NEC’s initiative to position itself as “Client Zero”—the very first user of its own solutions—by applying advanced technologies internally and sharing the resulting insights and know-how with customers and society as added value.

10 important items in the "Cybersecurity Management Guidelines Ver. 3.0" by the Japanese Ministry of Economy, Trade and Industry

Direction 1	Recognize cybersecurity risks and develop an organization-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	Continuously improve cybersecurity measures through a PDCA cycle
Direction 7	Develop a cybersecurity incident response team and relevant procedures
Direction 8	Develop a business continuity and recovery team and relevant procedures in preparation for damage due to cyber incidents
Direction 9	Understand the status of and implement measures considering the entire supply chain including business partners and outsourcing organizations
Direction 10	Facilitate the gathering, sharing and disclosure of information on cybersecurity

For inquiries regarding this report, please contact:

NEC Corporation
Corporate CISO Office
7-1 Shiba 5-chome, Minato-ku, Tokyo 108-8001, Japan
Phone: 03-3454-1111 (Main Line)

Shinichi Fuchigami

CISSP
(Certified Information Systems Security Professional)

NEC Corporation
Corporate Executive CISO
Member of the Board, NEC Security, Ltd.

NEC has implemented robust and flexible group-wide measures based on CISA's*2 Zero Trust Maturity Model. Our cybersecurity initiatives are aligned with the Ministry of Economy, Trade and Industry's "Cybersecurity Management Guidelines Ver. 3.0" and the updated "Cybersecurity Framework 2.0" published by NIST (National Institute of Standards and Technology) in February 2024—the first version in 10 years. In response to increasingly sophisticated cyber threats, we have established a framework that strengthens both intelligence (proactive defense) and resilience (recovery capabilities). As part of our enterprise risk management efforts, we visualize cybersecurity risks through a dedicated dashboard, enabling data-driven decision-making, enhancing employee awareness, and empowering autonomous actions at the operational level—ultimately realizing effective governance.
In delivering systems and services to our customers, NEC is committed to strengthening security measures across the entire supply chain based on the principle of Security by Design (SBD), which incorporates security considerations from the design phase. To cultivate cybersecurity talent capable of driving digital transformation (DX), we actively promote the acquisition of CISSP*3—an internationally recognized information security certification—and collaborate with educational institutions to support the development of future professionals.
In recognition of these initiatives, NEC was awarded the Grand Prize and the Excellence Award in the Human Resource Development category at the "Japan Security Awards 2024" hosted by the Japan Digital Transformation Promotion Association. Additionally, NEC received the highest rating—two stars—in the "Cyber Index Corporate Survey 2024" conducted by the Japan IT Federation.
This report outlines NEC's latest initiatives in information security up to May 2025. We hope you find it informative and appreciate your interest.

*2 CISA: Cybersecurity and Infrastructure Security Agency—Cyber Defense Agency of the U.S.
*3 CISSP: Certified Information Systems Security Professional

Contents

2 | Information Security Promotion Framework

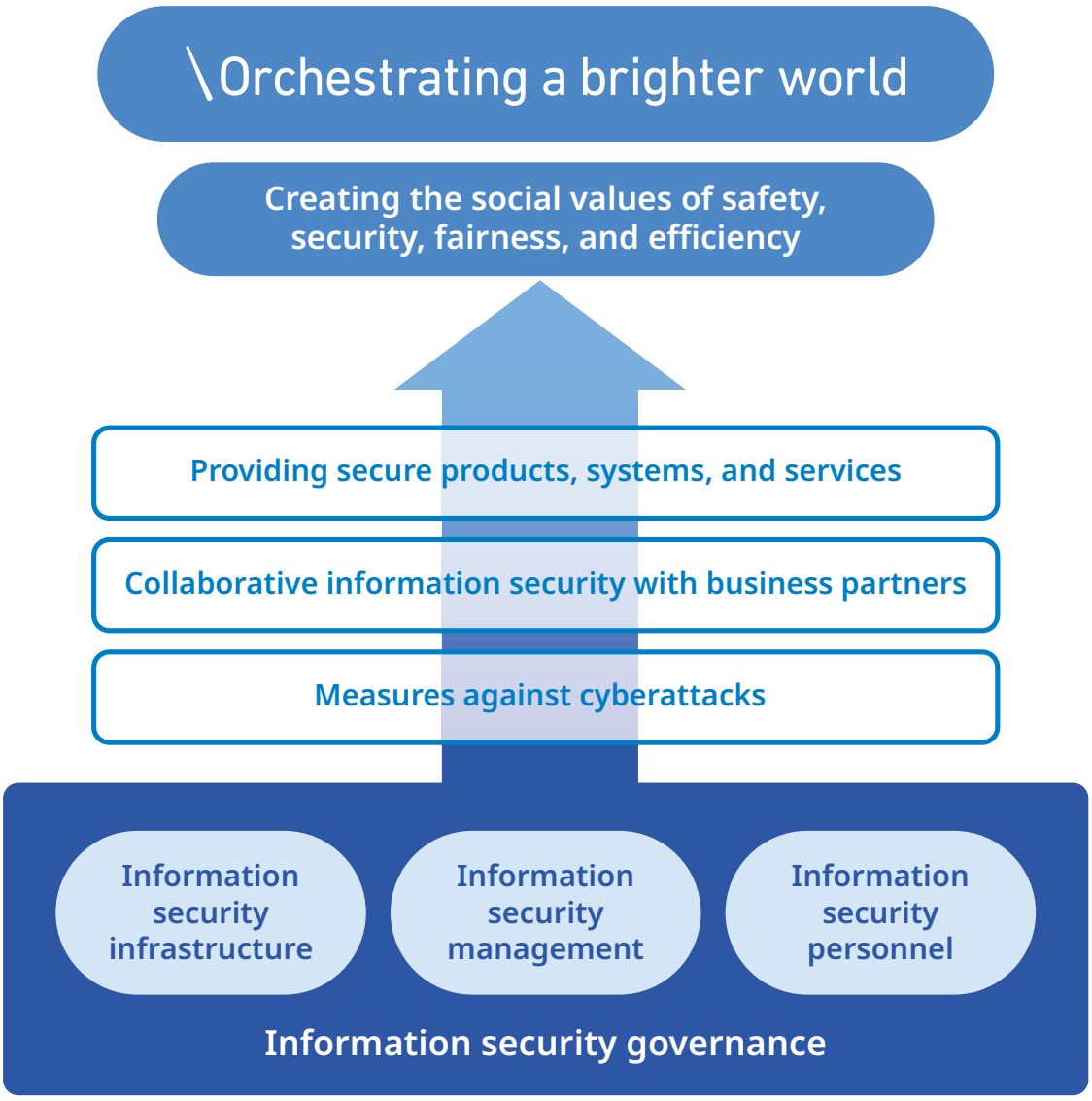
Direction 1

The NEC Group works to maintain and enhance information security throughout the entire group and aims to contribute to the realization of a people- and earth-friendly information society by providing value to customers and building a secure information society.

The NEC Group regards information security as a key management priority. We protect both the information assets entrusted to us by our customers and business partners, and our own information assets, from threats such as cyberattacks, while providing secure products, systems, and services. In response to increasing risks, we are committed to realizing a “Truly Open, Truly Trusted” society, fostering 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 maintains and enhances information security through a comprehensive, multi-layered strategy. We implement countermeasures against cyberattacks, collaborate with business partners on security initiatives, and deliver secure products, systems, and services. Our approach is built on three key pillars: information security management, infrastructure, and personnel. With thorough governance in these areas, we ensure strong and multi-layered information security throughout the NEC Group.

The NEC Group has established the NEC Group Information Security Statement and company-wide regulations, and developed a unified information security infrastructure. Top management sets security objectives, defines group-wide initiatives and structures, allocates management resources, and oversees ongoing monitoring and continuous improvements.



3 | 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.

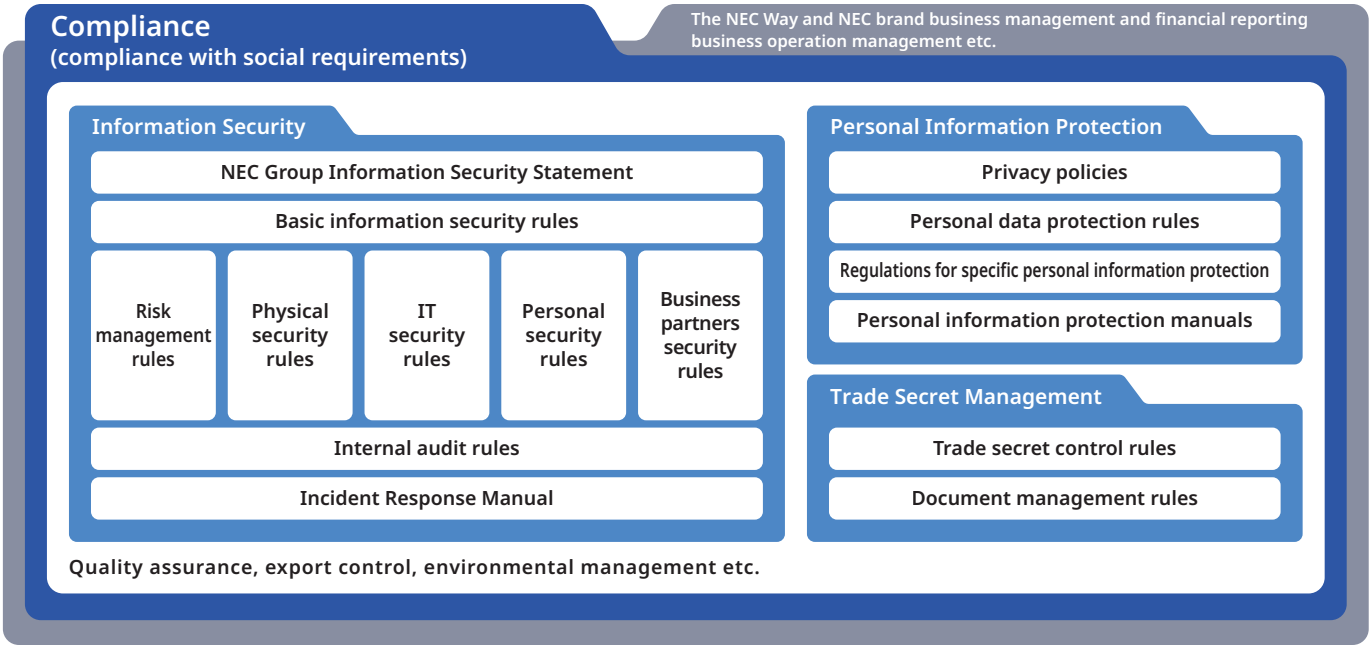
1 Information Security Governance in the NEC Group

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.
Furthermore, in line with the Three Lines Model, the NEC Group has established a framework where: the first-line risk owner divisions strictly manage information; the second-line risk management divisions monitor and support the first line's risk management; and the third-line audit division verifies the overall management status.

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 March 2025, 28 NEC Group companies have acquired Privacy Mark certification. Overseas group companies have common personal information protection guidelines in place as well as personal information protection rules in compliance with the relevant personal information protection laws and regulations of the country or region concerned.

NEC Group Management Policy



*1: NEC Group Information Security Statement https://jpn.nec.com/profile/governance/security.html
*2: NEC Privacy Policy https://jpn.nec.com/site/privacy/index.html

3 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.

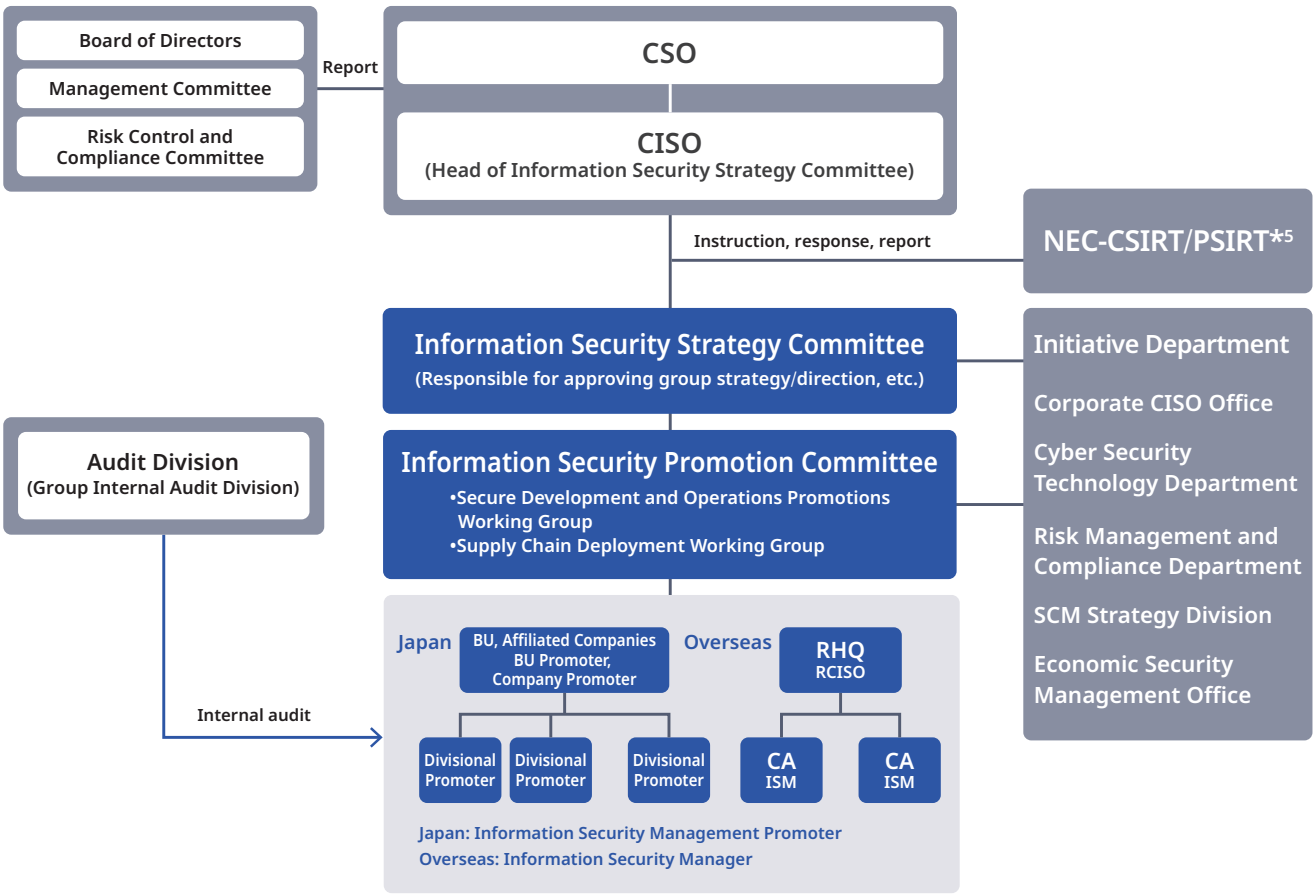
The CISO oversees the Corporate CISO Office, which promotes information security measures, and the CSIRT*3, which monitors for and swiftly responds to cyberattacks. The Information Security Promotion Committee and working groups plan and promote security implementation, discuss and coordinate implementation measures, ensure that all instructions are followed, and manage the progress of measures.

At NEC, 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. At affiliate companies in Japan, the president or executive level officers serve as the Information Security Manager. They continually raise awareness of security rules, introduce and execute measures, monitor implementation, and drive improvements.

In addition to this structure, the board members engage in and supervise cybersecurity efforts.

Additionally, NEC appoints an ISM*4 at each site located overseas, and these ISMs are responsible for the security management of their respective site and the outcomes thereof. Furthermore, by having Regional CISOs oversee entire regions, global governance is being strengthened.

Information Security Promotion Structure



*3 CSIRT: Computer Security Incident Response Team *4 ISM: Information Security Manager
*4 ISM: Information Security Manager
*5 PSIRT: Product Security Incident Response Team

4 | 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 policies, NEC strives to maintain and improve information security by continuously applying the PDCA cycle, and promotes improvements and policy reviews based on the results of security audits and incident statuses. We also encourage the acquisition and maintenance of ISMS and Privacy Mark certifications within the group.

2 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.

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.

3 Critical Information Management

❶ 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.

4 Information Security Surveys and Audits

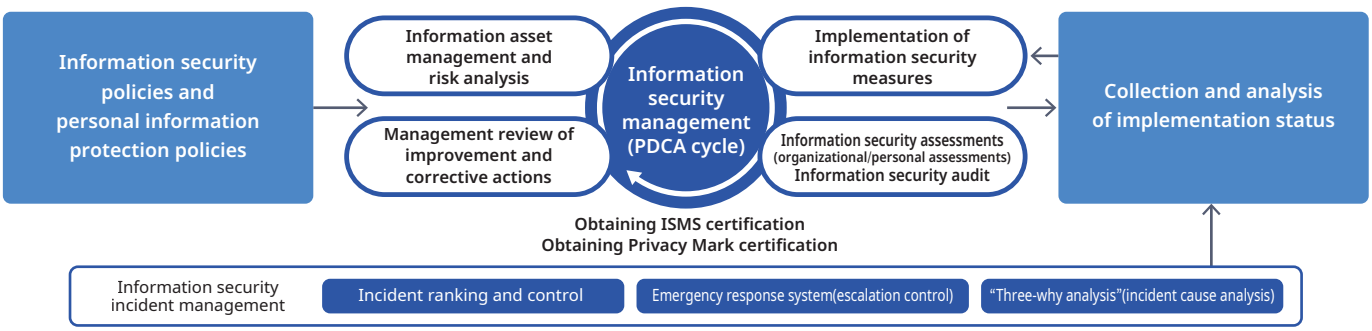
❶ Information Security Surveys

Information security surveys are initiatives aimed to foster an advanced security culture by evaluating and quantifying the security awareness levels of employees on a continuous basis and making improvements. Security awareness refers to the mindset necessary for employees to recognize potential security risks in daily work, make appropriate decisions, and respond accordingly.
This initiative enables each employee to become more conscious of security and to develop the habit of acting with risk in mind, thereby contributing to the improvement of the organization's overall security culture.

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's Information Security Management



5 | Information Security Infrastructure

Direction 3 Direction 5

The NEC Group has realized a "Zero Trust Platform" based on the Zero Trust Maturity Model from CISA*1. This model consists of five pillars—identity, devices, networks, applications, and data—and the NEC Group has implemented the following security measures for each.

1 Identity Security

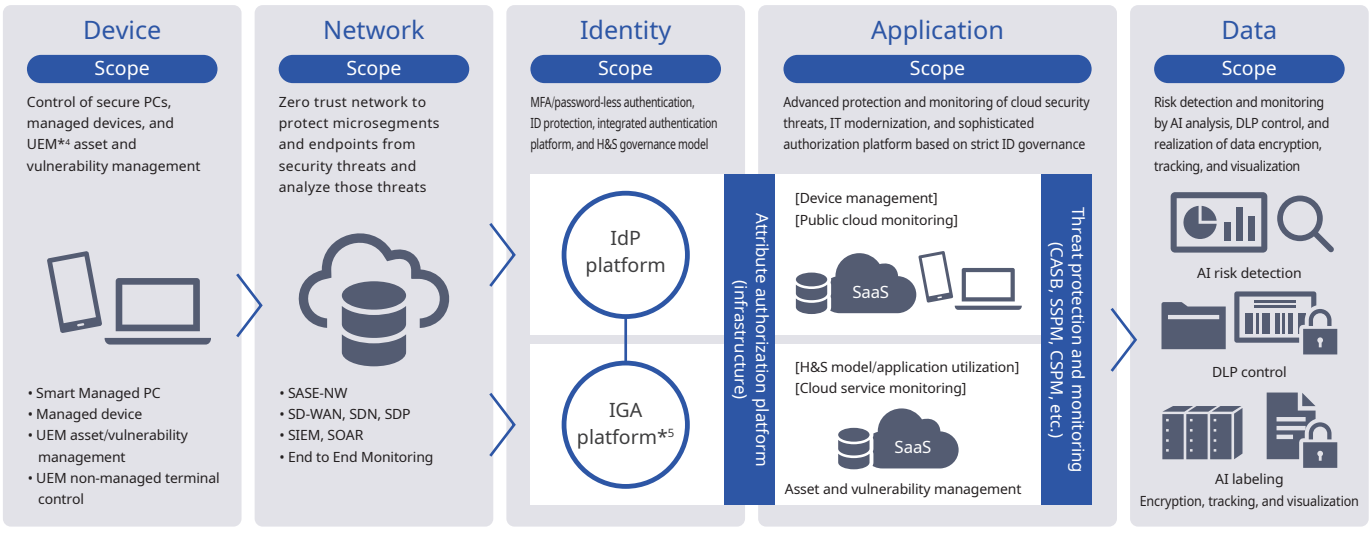
In response to increasingly sophisticated and complex security risks such as cyberattacks amid the changing environment brought about by the recent digital shift, we are working to strengthen and enhance authentication as a key strategy at the core of our zero trust infrastructure.
NEC is strengthening and advancing authentication company-wide through multi-factor authentication (MFA*2), which combines methods like biometric (face, fingerprint, etc.) and device authentication. This has enabled us to achieve passwordless access for almost all users, reducing the risks of spoofing and cyberattacks.
In addition, 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 with 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 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.

Overview and Scope of the Zero Trust Platform



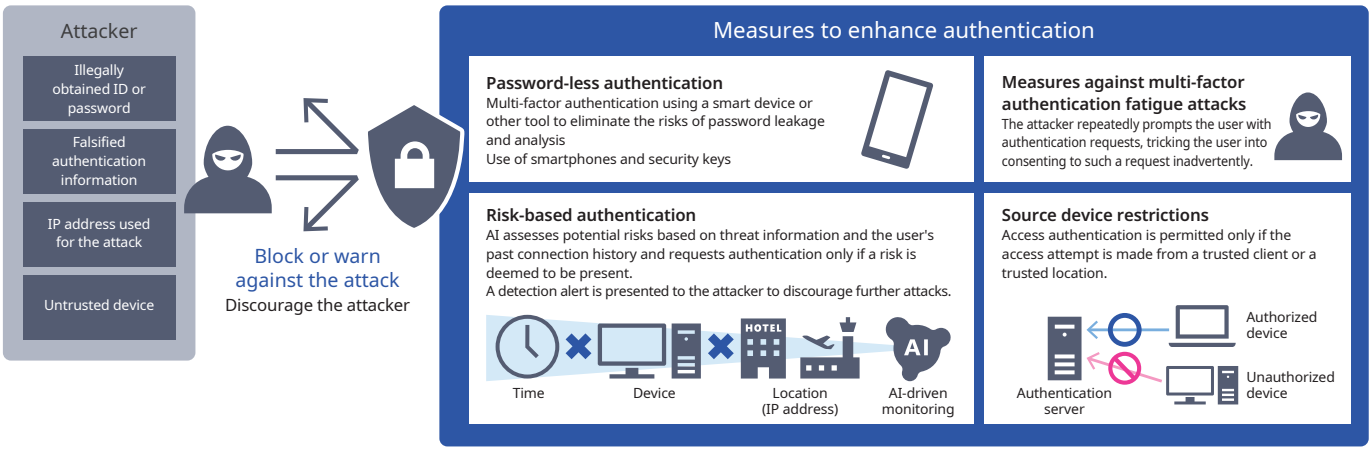
★1 CISA: Cybersecurity and Infrastructure Security Agency ★2 MFA: Multi-Factor Authentication ★3 IAM: Identity and Access Management
★4 UEM: Unified Endpoint Management Platform. This platform enables centralized management of various devices and enhances security levels, regardless of the connection location.
★5 IGA(Identity Governance and Administration): Framework for identity governance including lifecycle management, access privilege management, provisioning, and qualification information management for users and others

NEC has implemented a Unified Endpoint Management (UEM) platform as a measure against endpoint vulnerabilities. By mandating the installation of UEM agent software, we manage the information on our 260,000 IT assets, both in Japan and overseas, in a centralized manner using the cloud. This enables us to better address security risks and improve the efficiency of our management operations.

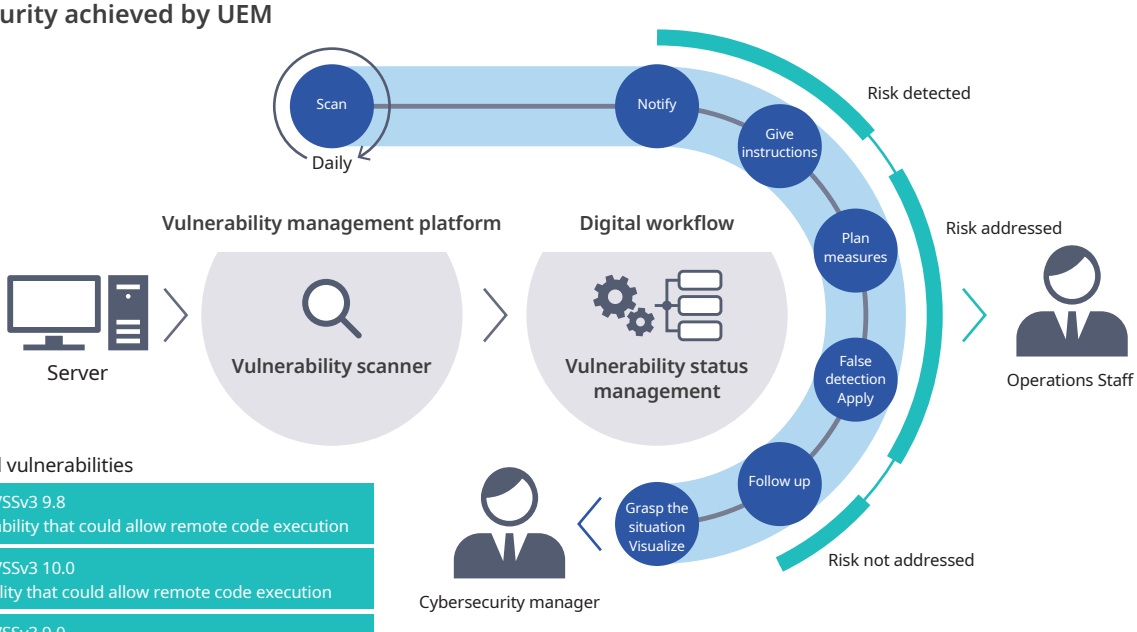
Managing server OS vulnerabilities is essential for enterprise system protection against cyberattacks, and continuous efforts are vital. To keep our more than 10,000 internal servers secure, in fiscal year 2024 we implemented data-driven security that enables early detection and notification of vulnerabilities, continuous monitoring, and visualization of the vulnerability status. Used in combination with cybersecurity dashboards, this data-driven security approach enables visualization of the status and trends of vulnerability responses, helping executives make better management decisions and raising IT system security awareness. Any devices with insufficient security or found to be infected with malware or other malicious software are 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.

For information leakage risk countermeasures, we use a multi-faceted approach that includes encryption, device control, and log recording to prevent external attacks and internal fraud. Encryption is carried out at both the hardware and data levels, and we have developed an infrastructure that assigns access rights and usage periods to each individual file. This prevents information leakage due to theft, loss, or erroneous transmission, and protects information even in the event of malware infection. For device control, the use of devices such as USB memory sticks, SD cards, and various communications is restricted to only those cases necessary for business purposes in order to prevent the risk of information leakage from external sources. Log recording involves recording the operation logs of all PCs, and in the event of an incident, log analysis is used to understand the scope and circumstances of the impact, and to formulate measures to prevent recurrence.

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



Data-driven security achieved by UEM



Examples of detected vulnerabilities

- CVE-2023-50164 and CVSSv3 9.8
  Apache Struts 2 vulnerability that could allow remote code execution
- CVE-2021-44228 and CVSSv3 10.0
  Apache Log4j vulnerability that could allow remote code execution
- CVE-2021-45046 and CVSSv3 9.0
  Apache Log4j vulnerability that could allow remote code execution

*6 Email Sender Guidelines
https://support.google.com/mail/answer/81126

3 Network Security

NEC's global network deploys zero trust-oriented infrastructure regardless of whether it is the internet or internal networks, supporting both the security and availability of the business environment.

❶ Zero trust-oriented network

To achieve a true zero trust approach, we have established an environment for appropriate access control, authentication, and authorization of connections within the network that links endpoints and services.

- Internet Defense: All communications destined for the internet from approximately 30 countries worldwide are centrally protected and monitored by a Secure Web Gateway. For remote environments, primarily within Japan, a cloud-based Remote Gateway is used to operate communications securely without exposing the company's network boundary to the internet.
- Office and plant defense: To realize a zero trust approach for communications both inside and outside our facilities, we are implementing controls within sites that combine Network Access Control (NAC) and SDN-based virtual networks (with NAC introduced from fiscal 2024 and SDN introduced from fiscal 2016). This enables the separation of office operations communications from specialized operations communications (such as production and development).

❷ Global Deployment of SD-WAN

The SD-WAN addresses the increase in traffic caused by online meetings and other SaaS applications and the need for security control, while achieving centralized control. By fiscal year 2024, we have successfully deployed the SD-WAN in all of our 289 locations to support communications control across six global regions, as well as regional and domestic control within high-traffic areas such as Japan, APAC, and mainland China.

- Performance and availability innovation: The total network bandwidth has been more than quadrupled, thus reducing the network change lead time to a fraction of what it previously was. In terms of availability, line redundancy has been achieved even for smaller sites where dedicated lines would be costly.
- Security innovation: We have made it possible to simultaneously shut down emergency communication across regions and monitor communications on a site-by-site basis, which was difficult to achieve with conventional platforms. For shutdowns of emergency communications, we have not only introduced the necessary platform but also prepared multiple scenarios for responding to expected threats (such as attacks against specific servers or lateral movement of ransomware), including tabletop exercises for SOC/NOC collaboration. Also, as a way of defending administrator privileges of SD-WAN routers with internet access (enhanced measures to prevent spoofing and internal fraud),we have deployed advanced management features in Japan, including alerts for unscheduled tasks and login notifications sent to the user and their supervisor.

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.

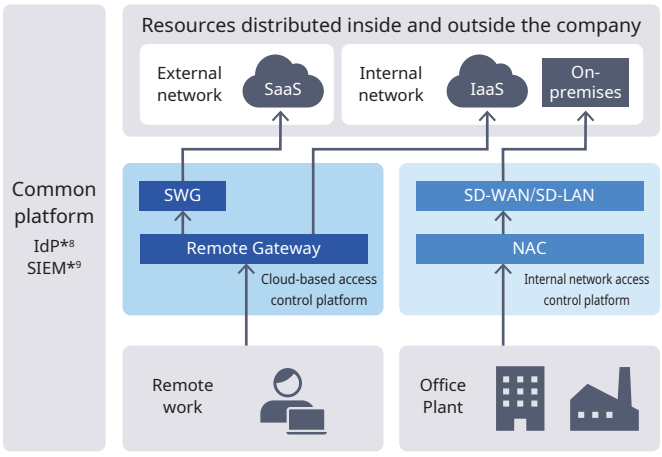
❷ Prevention of Incidents Resulting from Improper Public Cloud Settings

The use of public cloud services like AWS, Azure, and GCP is on the rise. While easy to use, they carry the risk of information leaks due to configuration errors. The NEC Group employs CSPM*10 to constantly monitor the configurations of public cloud services used within the group, verifying their adherence to security standards and continuously identifying potential risks.

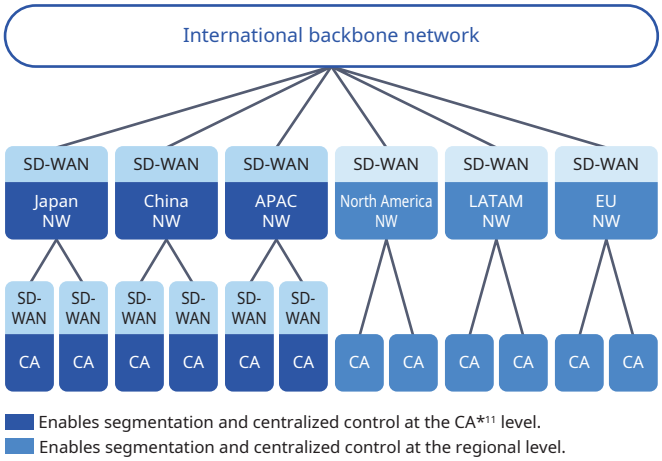
❸ Prevention of Incidents Resulting from Improper SaaS Settings

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. To address this, the NEC Group uses SSPM*12 to globally identify and correct configuration errors in the cloud services we use internally.

Overview of the zero trust network



Global Deployment of SD-WAN



*7 CASB: Cloud Access Security Broker *8 IdP: Identity Provider *9 SIEM: Security Information and Event Management *10 CSPM: Cloud Security Posture Management *11 CA: Corporate Affiliate
*12 SSPM: SaaS Security Posture Management

5 Data Security

❶ File label/encryption

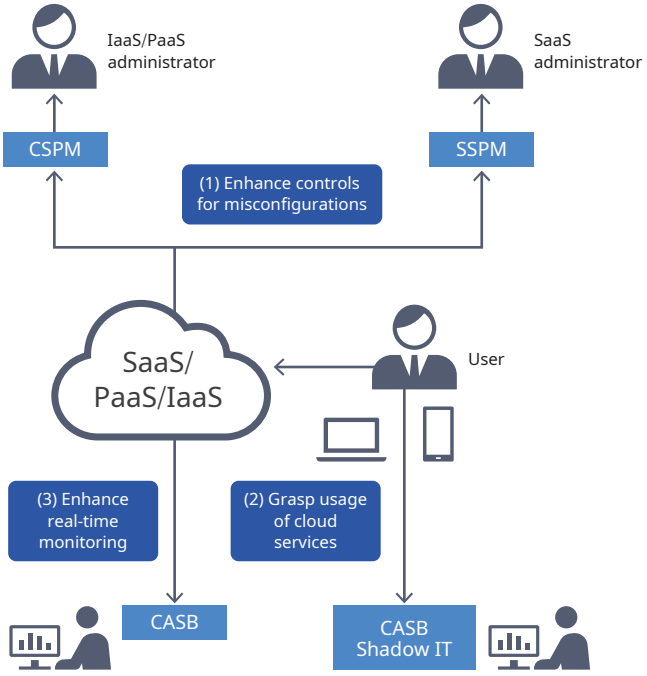
The NEC Group takes a zero-trust security approach by using cloud-compatible AIP*13 unified labels and our proprietary solution, InfoCage FileShell. This enables us to automatically classify, encrypt, track, and manage access permissions for various files, not just Office documents. These measures help 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.

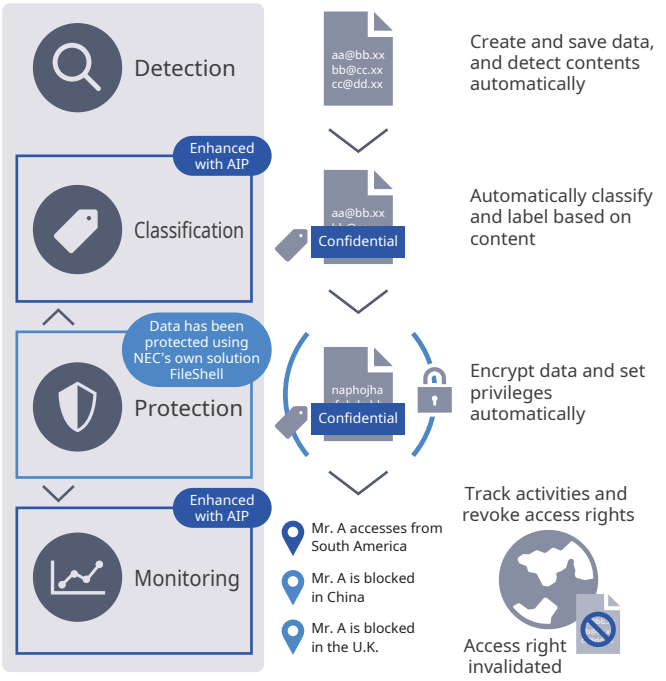
❷ Detection of risky behaviors leading to information leaks

Recently, information leaks caused by data or devices being taken off company premises, whether inadvertently or intentionally, have become a social issue. Some cases involve deliberate misconduct, such as insider fraud, and there are a growing number of cases where people switching jobs leak confidential information to their new employers. In addition, “damage caused by insider fraud, such as information leaks,” is ranked among the top threats in the “Top 10 Information Security Threats” published by Information-technology Promotion Agency, Japan (IPA). Background factors include increased job mobility, the spread of telework creating an environment where psychological barriers to misconduct are lower, and the diversification of information leakage routes due to the advancement of digital transformation (DX). In response to these circumstances, the NEC Group has introduced a system to detect and visualize behaviors that carry the risk of information leakage, including insider fraud. This system enables warnings and alerts to be issued to relevant individuals, thereby helping to deter, suppress, and prevent risky behaviors that could lead to information leaks.

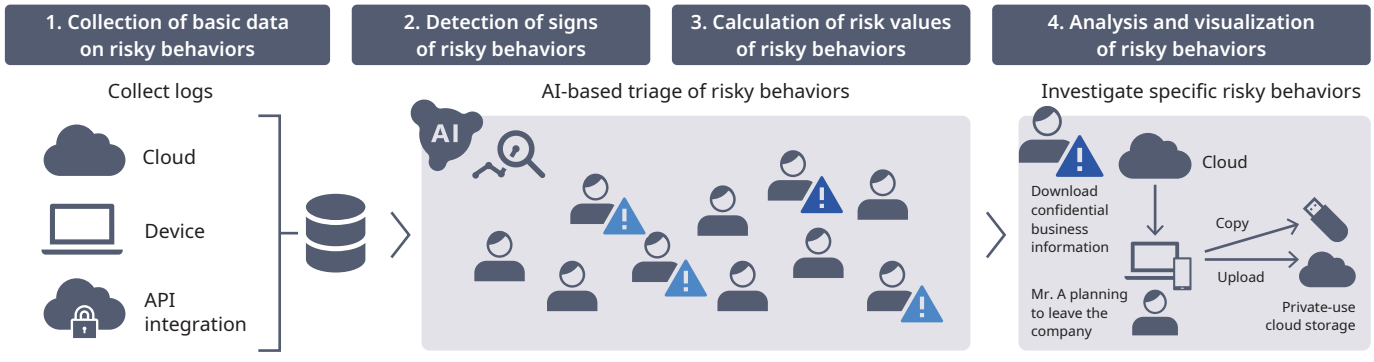
Security Measures for Using Cloud Services



Data Security through File Encryption



Detection of risky behaviors leading to information leaks



*13 AIP: Azure Information Protection

6 | Information Security Personnel

Direction 3

NEC develops human resources from three perspectives: raising information security awareness among all employees; cultivating personnel who can promote and implement security measures; and developing professionals capable of delivering value to our customers.

1 Developing Information Security Personnel

NEC develops human resources from three perspectives: raising information security awareness among all employees; cultivating personnel who can promote and implement security measures; and developing professionals capable of delivering value to our customers.

2 Raising Awareness of Information Security

To enhance information security awareness, it is essential to cultivate a keen sense of information security risks, provide knowledge for proper information handling, and foster a strong risk-aware culture. The NEC Group supports these goals through ongoing education and awareness-raising activities.

❶ Training on Information Security and Personal Information Protection

The NEC Group provides all employees with web-based training (WBT) on information security and protection of personal information (including compliance with the My Number system in Japan). This training is designed to increase employees' knowledge and awareness of information security and privacy protection. In fiscal 2024, the program achieved a completion rate of 98% and was offered in seven languages for overseas locations. The training content is updated annually to reflect the latest trends in security threats. Additionally, when welcoming new graduates and mid-career hires, we provide targeted training that highlights differences between student and professional responsibilities, as well as differences between previous employers and NEC.

❷ Commitment to Information Security Compliance

The NEC Group has established the Basic Rules for Customer Related Work and Trade Secrets, which set out requirements that must be observed when handling customer information, personal information (including My Number in Japan), and trade secrets. All NEC Group employees are required to formally pledge their compliance with these rules.

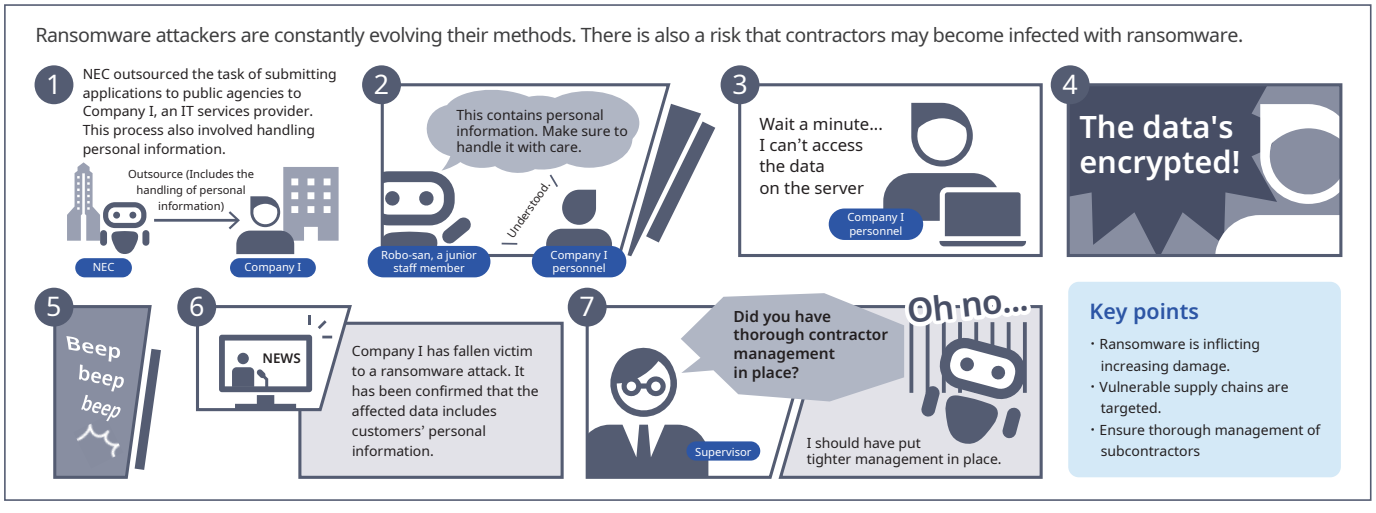
❸ Initiatives to Enhance Information Security Awareness

To increase employees' sensitivity to information security risks and enable them to think, judge, and act independently, NEC implements a range of information security awareness initiatives. For example, quarterly workplace discussions called Micro-Theme Talks use security-focused videos as a basis for group conversations. These sessions aim to develop each employee's risk analysis and decision-making skills, while also fostering a strong organizational culture of information security. The security videos are created annually to reflect the latest trends in security threats, real-world internal and external incidents, and near-miss cases. According to survey results, these efforts have led to steady improvements in both information security awareness and employees' overall sense of security risk.

3 Developing Personnel to Promote Information Security Measures

Under our information security promotion framework, we implement a range of internal initiatives to develop personnel with the necessary skills. We assign certified professionals—including CISSPs,*1 Registered Information Security Specialists, and Personal Information Protection Managers—to ensure appropriate management of sensitive information, protection of personal data, secure development and operations, and effective incident response. By doing so, we are continuously strengthening our organization's information security capabilities.

Sample of the Information Security Training Material



*1 CISSP: Certified Information Systems Security Professional, a globally recognized, vendor-neutral certification for information security professionals

4 Initiatives for Fostering Security by Design Practitioners and the Activities for Expanding our Talent Base

The NEC Group is dedicated to developing security personnel to ensure the proper implementation of security measures in the products, systems, and services we provide. Through these efforts, we aim to help our customers reduce their business risks.

❶ NCSA (NEC Cyber Security Analyst) Training

With the aim of strengthening top-level security talent, we offer a six-month intensive program for employees with knowledge of security technologies. Through this program, participants acquire practical technical skills required for advanced security services, such as CSIRT operations and risk hunting. To date, a total of 84 employees have completed this program and are now involved in delivering professional security services.

❷ SBD Specialist Training

Since fiscal 2019, each business division has been developing specialist personnel to practice Security by Design (SBD) as an organization. We offer two courses: an "Assistant Development Course" that trains personnel to support CyberSecurity Managers, and a "Sales Course" that trains sales representatives to take the lead in making security proposals. Through these courses, participants acquire the skills necessary for appropriate security proposals and implementations. In fiscal 2024, over 20 employees participated, bringing the total number of participants to 107. Centered around these specialists, we oversee all processes involved in system development to ensure thorough and appropriate implementation of security measures, enabling us to deliver safe and secure systems to our customers.

❸ NEC Cybersecurity Training Site

We provide training for all employees involved in customer systems, offering opportunities to learn the knowledge and skills necessary for effective security communication, including risk assessment. In addition, as a venue for hands-on security training, we offer a dedicated virtual environment that simulates an e-commerce (EC) site, enabling participants to acquire system hardening techniques during the system development phase. Utilizing this remote-access training environment, more than 1,700 employees—including mainly sales representatives and systems engineers—successfully completed the program in fiscal 2024.

❹ Group-wide CTF

To broaden the base of security talent, improve security skills, and enhance security awareness, we host an in-house Capture The Flag (CTF) competition called the NEC Security Skill Challenge. In fiscal 2024, more than 1,000 employees voluntarily participated, bringing the total number of participants since the program began in 2015 to over 9,000.

❺ Basic Training for Security Proposal and Implementation Personnel

All employees involved in customer proposal and implementation processes were surveyed to assess their understanding of the tasks they are required to carry out, based on the Cybersecurity Management Rules enacted in October 2023 and according to their respective roles. After the survey, we provided training tailored to each individual's level of understanding as indicated by their survey results, with a total of 13,500 participants completing the training in fiscal 2024.

❻ Holders of Advanced Security Technology Qualifications

To deliver optimal solutions to our customers, NEC encourages employees who work with customers to obtain officially recognized security certifications as proof of their advanced information security skills. We are increasing the number of employees holding international certifications such as CISSP and Registered Information Security Specialist (RISS) through internal seminars and study sessions.

From fiscal year 2024, as part of our efforts to further advance and broaden the base of our security talent, we have added new international qualifications including CCSP, CISA, CEH, and CCT.*2 In particular, with regard to CISSP certification, we have entered into a strategic partnership with ISC2, the certifying organization, to promote acquisition of this credential. Our aim is not only to cultivate personnel with advanced technical expertise, but also those who can evaluate risk from a business perspective. As a result, the number of CISSP holders in the NEC Group has reached 560.

Additionally, in fiscal 2024, to further strengthen the development of personnel with expertise in risk management and IT governance—enabling broader information security management capabilities—we formed a strategic partnership with ISACA, an international certifying organization. Through this partnership, we are implementing CISA and CISM*3 certified training for NEC Group employees, thereby nurturing more specialized personnel.

Furthermore, we plan to certify official trainers from among the NEC Group's security specialists, who will be able to provide customers with training programs that are enhanced by the practical skills and extensive, field-based knowledge in system implementation that these specialists have gained.

Overview of Cybersecurity Talent Management

Developing and managing personnel who can create and enhance business value by practicing SBD and implementing effective security measures

*2 CCSP: Certified Cloud Security Professional, CISA: Certified Information Systems Auditor, CEH: Certified Ethical Hacker, CCT: Certified Cybersecurity Technician
*3 CISM: Certified Information Security Manager

7 | Measures Against Cyberattacks

Direction 4 | Direction 5 | Direction 7 | Direction 8 | Direction 10

As cyberattacks become more sophisticated, NEC is globally deploying advanced security measures and driving cybersecurity management under proactive executive leadership.

1 Global Measures Against Cyberattacks

NEC ensures cyber resilience by implementing advanced and standardized measures based on cybersecurity risk analysis across its operations in both Japan and overseas, while responding to incidents through its CSIRT. To further strengthen our security posture, we also engage third-party evaluations focused on new items, particularly in the GOVERN domain of NIST CSF*1 versions 1.1 and 2.0.
Specifically, based on our belief that taking a globally unified approach to cybersecurity risk is essential for business continuity, we utilize AI to continuously monitor, understand, and analyze daily cyberattacks. At the same time, we review and improve our monitoring and operational processes as needed. In addition, we keep up with the latest trends in security products, services, and the market, and assess the compatibility of these products and services with our internal IT environment through proof of concept (PoC) evaluations and internal IT assessments. Drawing on the results of these activities, we identify future measures that will be required and calculate their scope, effectiveness, and cost. Each year, we formulate a promotion plan based on these activities and implement the required measures with the approval of our CISO.
Within the NEC Group, we implement measures based on comprehensive cyber defense concepts, such as our Cyber Defense Center (CDC). The main areas of focus for these efforts are outlined in the following sections 1 through 5.
These initiatives have earned external recognition, including the receipt of the Grand Prize in the Security Measures and Operations category at the 2024 Japan Security Awards presented by the Japan Digital Transformation Promotion Association, as well as several other awards.

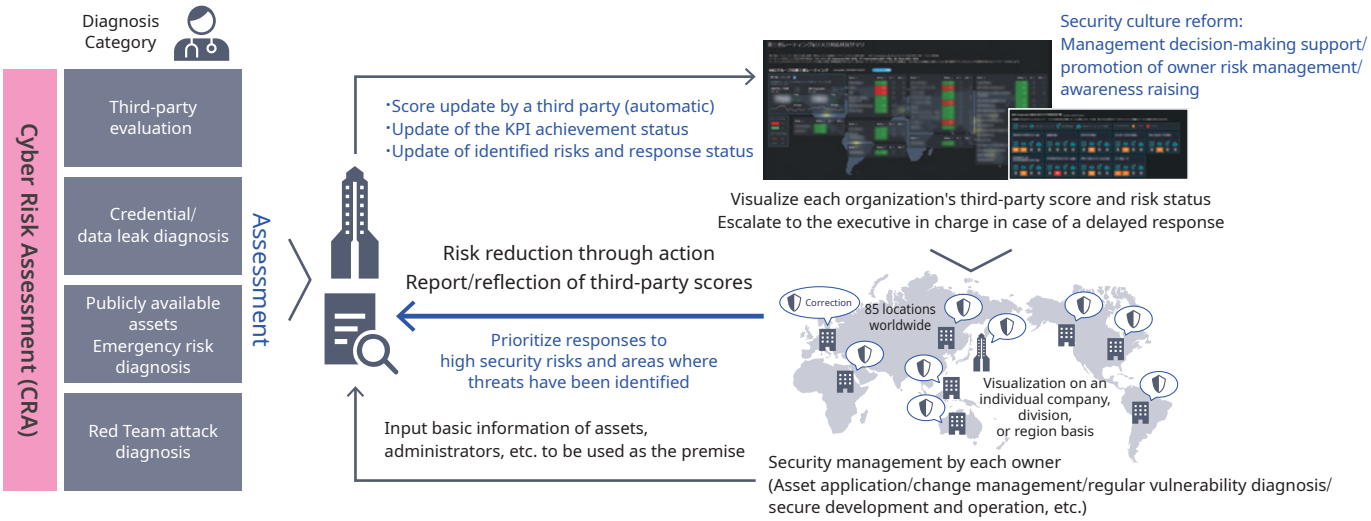
Award Presentation Ceremony

❶ Cyber Risk Assessment by the Red Team

The NEC Group's Red Team*2 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

Cyber Risk Assessment



*1 NIST CSF: Cybersecurity Framework is a set of guidelines developed by the US National Institute of Standards and Technology (NIST) to help organizations improve critical infrastructure cybersecurity
*2 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

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. The Dashboard shows the status of response to identified risks. We have a risk management cycle where any delayed response triggers escalation to top management, thus prompting spontaneous action.

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 through systematic digital operations. Using a group-wide endpoint detection and response (EDR) platform, a unique CSIRT-developed network detection and response (NDR) platform, and an integrated log analysis platform, the team hunts unknown threats.
We also have a research factory and a deception environment in place for enhancing our ability to generate unique CTI proactively and analyze threats in detail. Using the generated unique CTI for proactive defense and threat hunting enables active cyber defense.

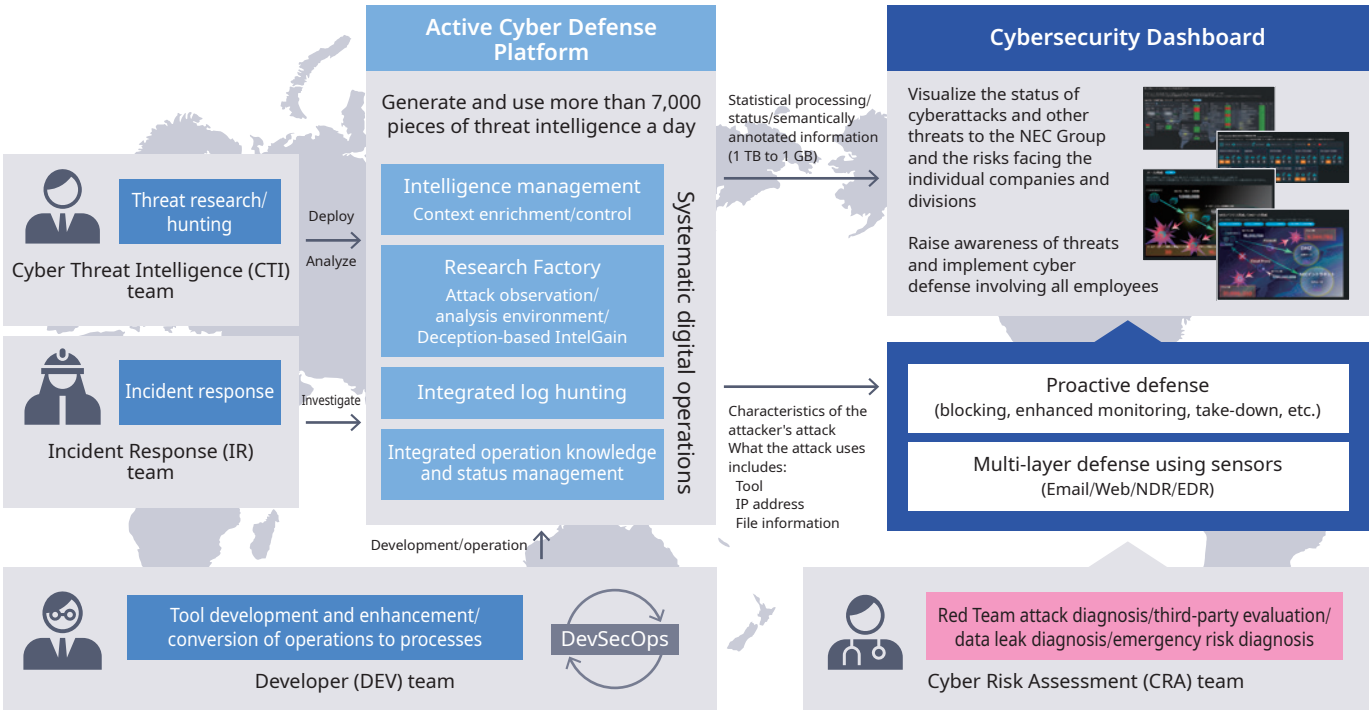
❸ Enhancement of the CSIRT Structure

A CSIRT has been established under the authority of the CISO to monitor for cyberattacks, analyze the characteristics of attack methods and malware, and share information with relevant organizations. In the event of an incident, the team conducts preservation and analysis of the attack, works to identify the cause, and brings the situation to resolution.
The CSIRT is composed of four teams: the CTI team, which leverages threat intelligence; the IR team, which responds to incidents; the SOC team, which monitors security device alerts 24/7; and the Developer team, which works to enhance tools, platforms, and operational processes. For overseas subsidiaries, we have established a system in Singapore to monitor for cyberattacks around the clock, sharing information such as detection results and indicators of compromise globally in cooperation with the CSIRT in Japan.
When an incident occurs, the CSIRT collaborates with related departments and, while taking risk considerations into account, handles the response through to recovery with the approval of the CISO.
Furthermore, during large-scale events such as Expo 2025 Osaka, Kansai, there is an increased risk that related companies may become targets of cyberattacks. To address this, NEC implements exercises for cyberattack response in cooperation with NISC, establishes special escalation rules, builds a dedicated security structure during the event, and strengthens focused monitoring and threat intelligence through CSIRT and SOC.

❹ Enhancement of Systematic Security Resilience

Recognizing global threats such as ransomware as significant management risks, we are working to increase our organizational resilience to attacks. We conduct training for employees on handling malicious emails, and have developed a security incident response manual. To ensure a prompt response in the event of an incident, the manual clearly specifies responsibilities and roles based on the Three Lines Model, as well as procedures for external communications and legal responses.
In addition, based on the Cybersecurity Management Guidelines Ver. 3.0 established by the Ministry of Economy, Trade and Industry, we conduct incident response drills at least once a year with participation from management, related departments, and experts, ensuring management's active involvement in incident response.

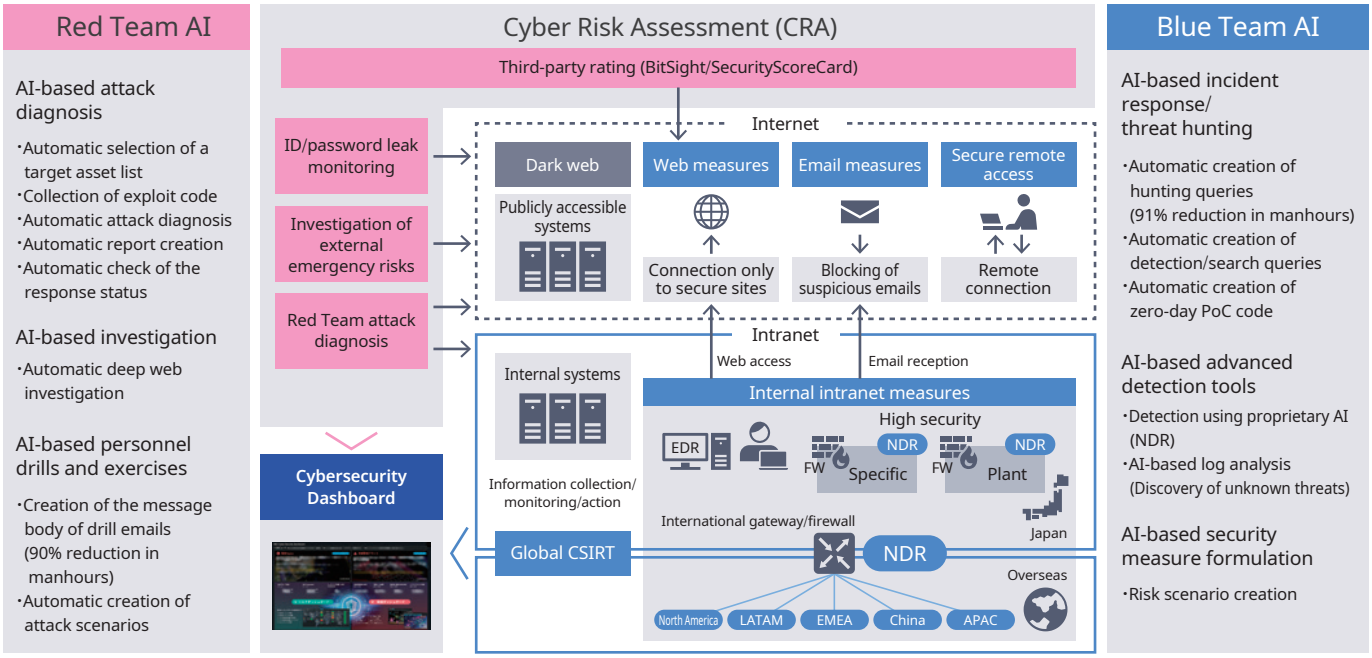
Overview of Our Cybersecurity Measures



❺ AI-based Advanced Cybersecurity Measures

To counter the increasingly active AI-based attacks, our defense team implements next-generation measures against cyberattacks using Red Team AI and Blue Team AI.
We are leveraging a variety of AI technologies, including generative AI, in a wide range of fields, including cyber risk assessments, threat intelligence generation and utilization, NDR-based anomaly detection, incident research, and phishing email training. We are working with our internal laboratories to develop agentic AI for attack diagnosis in order to enhance, automate, and streamline cybersecurity tasks.

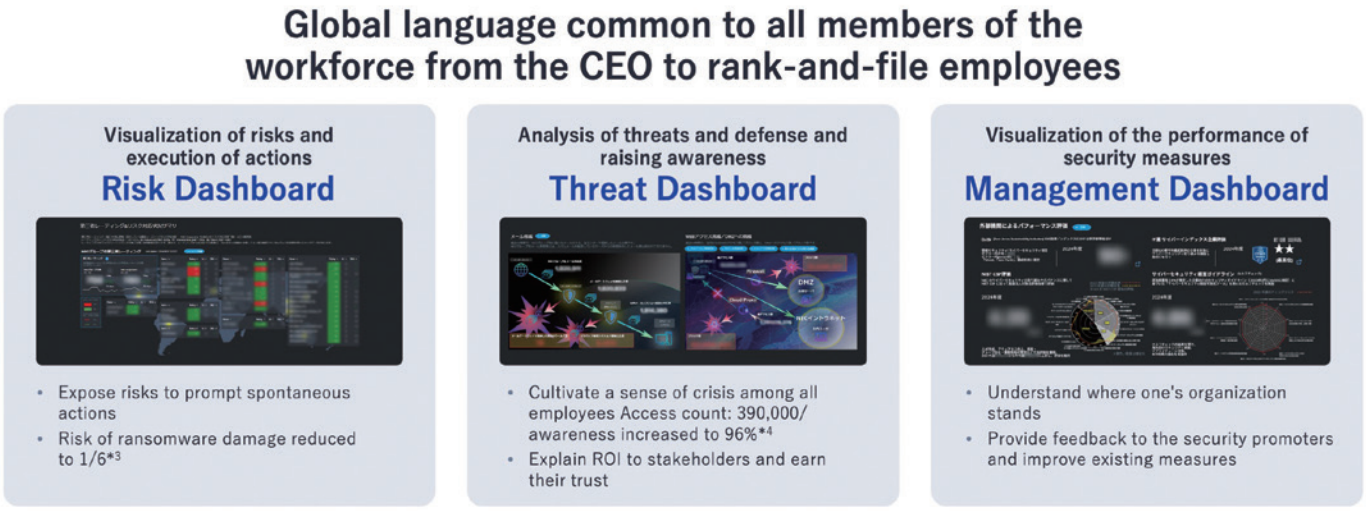
Use of generative AI in cyber defense



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, the security risks of the individual companies and divisions found by the cyber risk assessment, and the performance of security measures among others. These dashboards are available to all employees.
Having each employee understand the actual situation and risks prompts them to take actions for improvement and helps raise their security awareness.
The agile development of the dashboards is still in progress. We have added features that automatically and dynamically distribute domestic

Cybersecurity Dashboards



*3 An organization whose rating is 600 points or less is 6.4 times more likely to incur ransomware damage than one whose rating is 750 points or more.
https://www.bitsight.com/blog/ransomware-prevention
*4 Calculated from NEC survey results.

and overseas security news and pieces of music inspired by those news stories using generative AI tools for language, audio, video, and music. Familiarizing employees with security news ensures the engagement of all members of our workforce in security.

With accountability expected to become more crucial in the coming digital world, NEC intends to play an even bigger role as a value creator in realizing a safe, secure, and sustainable society.

Promotion of Client Zero in Security

Client Zero advocated by NEC and relevant initiatives in the area of cybersecurity

Client Zero Initiatives in the Area of Cybersecurity

Seeing itself as the zeroth client (Client Zero), NEC provides customers and society with the knowledge and know-how that it has gained through first-hand in-house experiences.
Since 2014, we have issued this report on a continuous basis to highlight the NEC Group's efforts in the area of cybersecurity.
Our Client Zero initiatives include working with NEC BluStellar Scenario*1 from the planning phase, sorting out challenges and designing policies based on in-house experiences, deploying and operating solutions with members who have internal operational know-how, and collaborating with laboratories to develop leading-edge technologies. We offer various knowledge and know-how for diverse customers to use.
As Client Zero, we continue to address new security risks, put cutting-edge technologies into practical use, and expand our knowledge and know-how in order to help customers conduct business and social activities in a safe and secure manner.

Examples of Client Zero in Security

As part of the Client Zero initiatives in security, we provide customers and society with the NEC Group's knowledge about practical security management on a continuous basis, as outlined below.

❶ Cybersecurity Dashboard

This initiative leads NEC's data-driven management. With security risks increasing on a global scale in both cyber and physical spaces recently, many customers have asked us about it. The cybersecurity dashboard is used to visualize and integrate siloed security measures and implement sustainable measures against security risks. (See "Security culture transformation using cybersecurity dashboards" on page 16 and "What NEC can do to help" on page 24.)

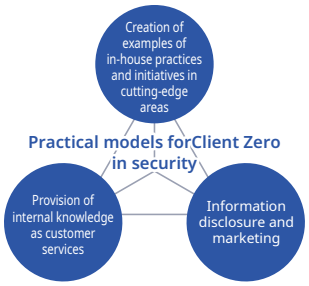
❷ AI and Security

The NEC Group is pushing forward two initiatives: "Security for AI" to ensure the safe use of AI and "AI for Security" to use AI for security measures. We implement "AI for Security" in our internal security measures to streamline and automate the measures and improve their quality. At the same time, we are accumulating know-how of Client Zero in security.
We present these latest case studies to customers, exchange views with external analysts, and conduct surveys on needs and other researches. We have a framework in place whereby we provide feedback to the cybersecurity business so that we can quickly deliver results to customers and society. Under this promotional framework, the high-level security knowledge of NEC Security Ltd. is integrated into the technologies developed by laboratories and offered to customers. The knowledge is used to explore ways to create new values and achieve the "to be" state. (See "Technology, research, and business development to make Japan cyber secure" on pages 27-29.)

❸ Examples of Practical Security Operation

The NEC Group has 120,000 employees, and ensuring the internal security and safety, which is essential for these employees, is a challenge that is directly linked to NEC's management. That is why we have not only measures against cyberattacks but also global security governance and auditing systems, critical information management and protection, zero trust security infrastructure, among others. We ensure their stable operation and improve them continuously. These operation examples are used as more practical know-how.

Client Zero Initiatives in Security



The NEC Group's practical security management knowledge is provided.

Examples of Use by Customers

Cutting-edge case study	Creation of new values/definition of the "to be" state
Construction and operation know-how	Introduction of field-proven systems
Business know-how	Continuous operation and process improvement

*1 DX implementation initiative and success scenario provided under NEC BluStellar, a value creation model for leading customers to the future

8 | Information Security in Cooperation with Business Partners

Direction 9

In order to protect our customers valuable information, NEC works with our business partners as one to promote the dissemination of information security measures and corrective actions to improve security levels across the entire supply chain.

1 Framework

When collaborating with business partners, NEC believes that in addition to their technical capabilities, it is important that their level of information security standards also meets the standards set by NEC. We classify business partners into different security levels according to the status of their information security measures and employ a mechanism whereby we can outsource work to business partners that meet the appropriate security level standards. This reduces the risk of information security incidents occurring at our business partners.
The seven categories of information security measures that NEC requires business partners to implement are: (1) contract management, (2) subcontracting management, (3) staff management, (4) information management, (5) technology measure deployment, (6) security implementation, and (7) assessments.

❶ 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.

❷ Subcontracting Management

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

❸ 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. We require workers to submit a formal pledge to NEC that they will adhere to these guidelines to ensure these measures are strictly implemented,

❹ Information Management

NEC has guidelines in place concerning the management of confidential information handled when carrying out work. This ensures that the disclosure of confidential information, taking of confidential information outside the company, and disposal or return of confidential information are all properly managed.

❺ Technological Measure 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 ask our business partners to implement these measures accordingly.

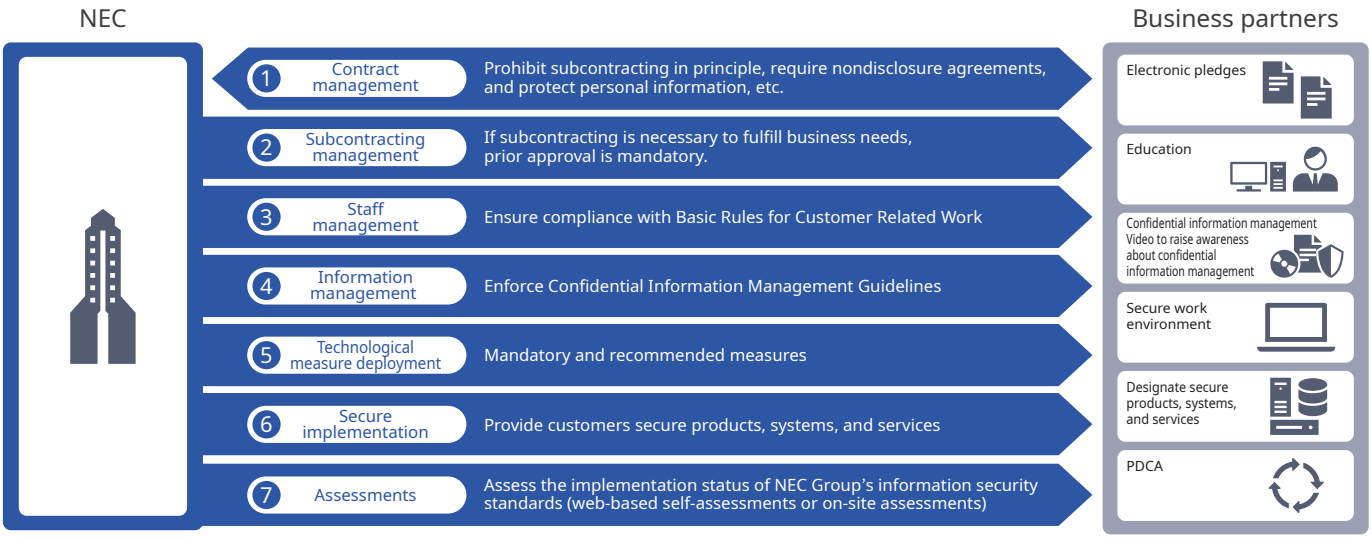
❻ Security Implementation

NEC has guidelines in place concerning the development and operation of customer-facing products, systems, and services and asks business partners to conduct development and operation with security in mind.

❼ Assessments

NEC assesses the implementation status of information security measures at each business partner and provides guidance 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 Activities Promoting the Dissemination of Security Measures to 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. In these seminars, we share the latest trends and important points regarding information security and personal data protection, provide education on cybersecurity, and conduct awareness activities to prevent information security incidents. 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 firms associated with software development) to encourage them to thoroughly implement security measures and improve their skills. Additionally, our CISO gives lectures on cybersecurity to raise awareness about information security.

❸ Distribution of Measure Implementation Guidebooks

NEC provides an implementation guidebook to facilitate the smoother implementation of security measures at business partners' companies. We have issued a variety of guidebooks for achieving required standards, such as a guidebook to information security standards, a guidebook for antivirus measures, and a guidebook for development environment security measures.

❹ Standardization of the 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 and on-site assessments. We review the assessment items every year, taking into account factors such as the status of security incidents. We then provide feedback to our business partners in the form of a report summarizing the assessment results. We also offer follow-up support on issues that need improvement to help improve the security levels of our business partners.

❶ Document-based and On-site Assessments

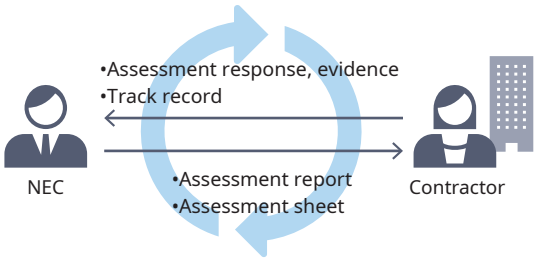
There are about 1,800 companies that do business with NEC that are subject to document-based assessments. These business partners perform an assessment of the implementation status of security measures and enter the assessment results in our web system in real time. For those business partners with whom we conduct a high volume of business, we carry out on-site assessments by visiting them directly or remotely. The number of these visits is increasing each year, reaching around 350 companies in fiscal year 2025, facilitated by about 100 NEC inspectors.

❷ Information Security Assessment Sheet

Along with the assessment results, the implementation status of various information security measures 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 Corrective Actions for Business Partners



4 Enhancement of Cybersecurity Measures

To enhance our cybersecurity measures, we revised our information security standards 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 to raise awareness about information security. Between fiscal years 2022 and 2024, we held seminars in China, India, and Vietnam, and we plan on continuing to hold these seminars going forward to improve the security level of our entire global supply chain.

9 | 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 departments and business divisions across the company, ensuring that security measures are fully disseminated within their respective departments and divisions and supporting employees in implementing security measures. We have about 400 cybersecurity managers assigned across all the divisions and strengthen cooperation between the cybersecurity management departments and each business division through bi-weekly meetings and community forums.

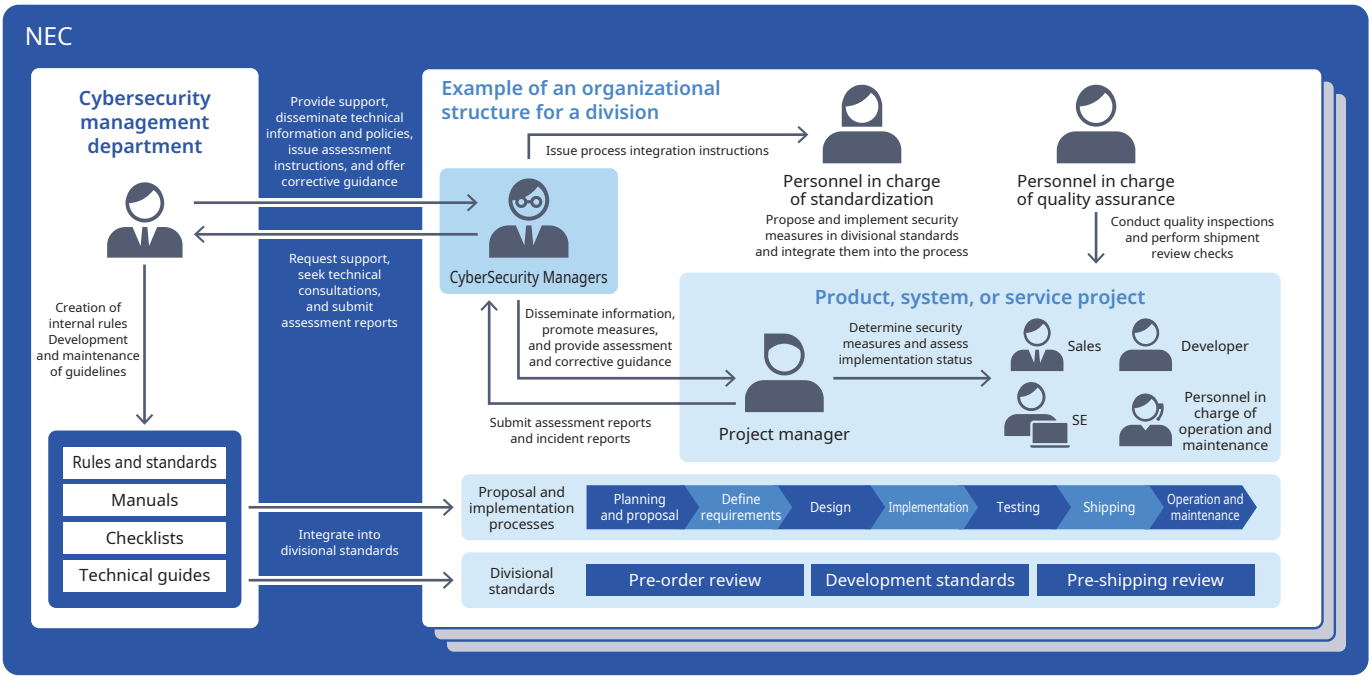
The "Cybersecurity Management Rules" define the roles of cybersecurity managers and specify the cybersecurity implementation processes in each division. These Rules are part of the NEC Group Management Policy. As a model case of the Cybersecurity Management Rules applied to overseas group companies, some of the group companies established their security implementation promotion structure and developed their own cybersecurity management rules similar to those of NEC Corporation in fiscal year 2024.

❷ Key security implementation efforts

Based on the 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,

Security Implementation Process



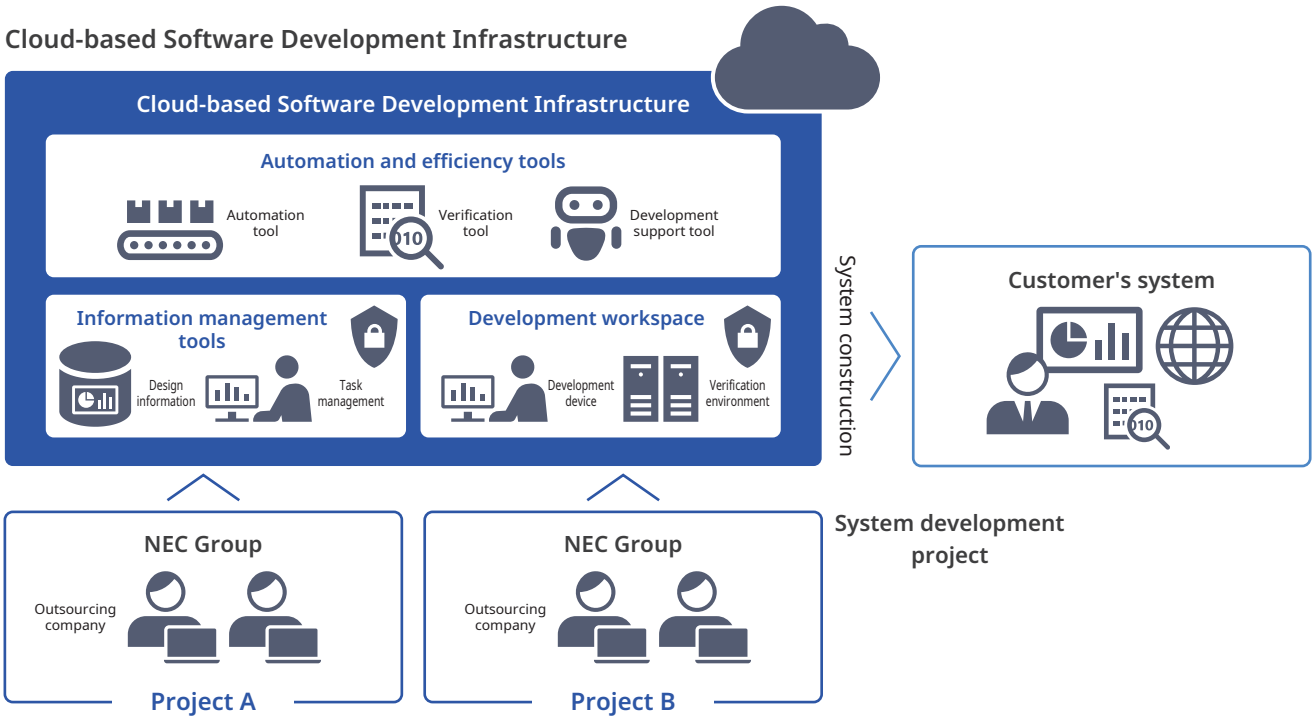
products, and services we develop and operate.
In the development of products, systems, and services, we have created a checklist to ensure that security tasks are performed in each phase. Using this checklist, business projects are managed through the “cybersecurity checklist management system”, which was developed to visualize and centrally manage the status of security implementation. This system allows us to efficiently assess and monitor the current status of security measures. 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 address vulnerability information related to NEC Group products. We have set up a contact point for receiving vulnerability reports from external sources, published our vulnerability disclosure policy, and operate as a CNA.*1 By appropriately handling undisclosed vulnerabilities in our own products and vulnerabilities in our customers’ systems, we are able to respond effectively and promptly to security issues.

❸ Software development infrastructure for security implementation

NEC has established a cloud-based software development platform as its internal standard environment for system development. This integrated development environment includes information management tools for organizing design information and tasks, automation and efficiency tools that support build and test automation as well as AI-driven development assistance, and dedicated workspaces for implementation and testing. It is also equipped with tools to streamline and automate security implementation, such as vulnerability inspection tools, thereby improving productivity, quality, and security in system development.
Furthermore, by consolidating the development environments of the entire supply chain—including business projects and external partners—into this platform, we centrally manage measures to address risks originating from development environments, such as information leaks or copyright issues related to the use of generative AI. As a result, we ensure that the security measures applied to each business project’s development environment comply with our Cybersecurity Implementation Standard, enabling the secure management of customer system design information used during development.

❹ Security enhancement in our hardware development and production facilities

At NEC’s hardware development and production facilities, regular third-party risk assessments are conducted to accurately verify that technical information is properly managed and that effective security measures are in place. In addition, at our production sites in Japan, we conduct annual business continuity plan (BCP) drills tailored to cyberattack scenarios to strengthen our risk mitigation measures and ensure preparedness in the event of a security incident.



*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

10 | NEC's Cybersecurity Strategy

NEC addresses intensifying cyberattacks and responds to legislative changes geared toward enhancing cybersecurity, leveraging intelligence and AI to contribute to efforts to "MAKE JAPAN CYBER SECURE".

1 Cyberspace Situation in Japan

In recent years, the number of reported Penal Code offenses in the physical world has continued to decline, reaching the lowest level in 2021 since World War II.*1 Meanwhile, attacks and crimes in cyberspace are becoming remarkably serious, both in terms of quantity and quality. In particular, there have been incidents where companies have had funds extorted or stolen as a result of cyberattacks, and cases where businesses have been forced to suspend operations. Cyberattacks are increasingly becoming a risk that can disrupt business continuity. The "10 Major Security Threats 2025 [For Organizations]"*2, published by the Information-technology Promotion Agency, Japan(IPA), also lists "damages caused by ransomware attacks" and "attacks targeting supply chains and subcontractors" as major threats, indicating that the safety of Japan's cyberspace is under threat.

With the expanding use of cloud services and rapid digital transformation (DX), the systems and data that companies need to protect are increasingly dispersed both inside and outside the organization. This has led to complexed IT environments. As a consequence, security risks can remain hidden throughout the company, making it easier for incidents to occur and for damage to spread. Furthermore, cyberattacks and cybercrimes are harder to see compared to crimes or attacks in the physical world, making it difficult to grasp or the current situation and the level of to what extent countermeasures that have been implemented.

In order to respond to these circumstances where the safety of cyberspace is being threatened and business continuity is increasingly at risk, and to promote DX in a safe, secure, and sustainable manner, it is necessary to visualize cybersecurity risks from a management perspective. NEC offers the Data-Driven Cybersecurity Service (DDCS), which analyzes and visualizes risks based on actual data (data-driven), and it is used by customers in their security risk management.

However, the situation surrounding cyberspace continues to worsen. The "10 Major Security Threats 2025 [For Organizations]," includes "cyberattacks stemming from geopolitical risks" for the first time. The report highlights the existence of nation-states that conduct cyberattacks with the aim of causing social disruption toward politically adversarial neighboring countries, and clearly states the necessity for organizations to continuously strengthen their countermeasures against such attacks from these nations.

In light of these changes in social circumstances, the Japanese government is accelerating its efforts to bolster the response capabilities of both the public and private sectors in the field of cybersecurity. The Act on the Promotion of Ensuring National Security Through Integrated Implementation of Economic Measures (Economic Security Promotion Act), which was passed in May 2022, requires that critical equipment used to provide essential infrastructure services,

MAKE JAPAN CYBER SECURE

*1 National Police Agency, THE POLICE WHITE PAPER 2024, p. 48, Part 2, Chapter 2, Section 1, 1. Penal Code Offenses (1) Status of Recognition and Apprehension of Penal Code Offenses (excerpt from original Japanese version)

*2 Information-technology Promotion Agency, Japan (IPA), 10 Major Security Threat 2025 [For Organizations]

such as electricity, gas, and water, be subject to screening prior to installation or use to ensure that the stable provision of these services is not disrupted by cyberattacks or other threats from outside Japan. The Act on the Protection and Utilization of Critical Economic Security Information, passed in May 2024, introduced a security clearance system. Under this system, which took effect in May 2025, screening is conducted on individuals or companies who may handle particularly sensitive information, such as cyber intelligence which includes cyber threats or countermeasures.

Also, following recommendations from the Expert Panel toward Improving Response Capabilities in the Field of Cybersecurity, which was held over approximately six months starting in June 2024, the Act Concerning the Prevention of Damage Caused by Unauthorized Acts Targeting Critical Computers (Cyber Response Capability Strengthening Act) and the Act for the Establishment of Related Acts Accompanying the Enforcement of the Act on the Prevention of Damage Caused by Unauthorized Acts Targeting Critical Computers" (Cyber Response Capability Strengthening Amendment Act) were passed at the 217th ordinary session of the Diet, which convened in January 2025. These laws aim to establish a system for Active Cyber Defense (ACD) by strengthening public-private collaboration, enabling the use of communication data, implementing measures on penetration and neutralization against cyber attacker's servers, and reorganizing the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) into a new Cabinet Secretariat organization to serve as a command center for cyber security initiatives of the Japanese government, including ACD. Under penetration and neutralization measures, the police and the Self-Defense Forces can take actions to prevent serious harm from cyberattacks. Also, the structure of NISC, which is the predecessor of the new command center, has been reinforced, including the appointment of senior officials seconded from the National Police Agency and the Ministry of Defense.

In response to these government efforts to enhance the cybersecurity framework, NEC is also developing new services and technologies to "MAKE JAPAN CYBER SECURE," protecting the cyberspace of both the Japanese government and the private sector. To respond to increasingly sophisticated cyberattakcs, including emerging new methods, it is necessary to quickly collect and analyze large amounts of intelligence and implement countermeasures. This type of intelligence is highly confidential information. As part of the public-private collaboration in the field of cybersecurity, it is expected that such intelligence will be shared with government organizations. Given the situation, such information must be handled with an adequate level of care.

NEC aims to "MAKE JAPAN CYBER SECURE" with Japanese technology building on its longstanding track records of ensuring the safety and security of Japan by supporting Japan's critical infrastructure, including submarine cables, aerospace and national security operations, and mission-critical systems. By leveraging proprietary intelligence and cotomi, NEC's generative AI, we will combine AI with cybersecurity technologies to expand its cybersecurity business globally. In order to "MAKE JAPAN CYBER SECURE" including protecting Japanese companies operating overseas, NEC will contribute to the realization of a safe and secure information society.

Collaboration with Security-Related Organizations

To "MAKE JAPAN CYBER SECURE", it requires not only developing technology and intelligence, but also establishing systems and laws that enable the effective use of these resources to implement countermeasures. While providing cyber security services, NEC engages in collaborative activities with security-related organizations both in Japan and overseas and also provides policy recommendations to the Government of Japan, including the Cabinet Offices and ministries in charge.

Nobuhiro Endo, who serves as an Executive Advisor, was appointed as a member of the Expert Panel toward Improving Response Capabilities in the Field of Cybersecurity organized by the Cabinet Secretariat of Japan. As a member of the Expert Panel, he helped compile the proposal regarding the establishment of legal frameworks and other measures necessary to realize new initiatives aimed at enhancing the capabilities of Japan in the field of cyber security to a level equal to or surpassing that of major Western nations

In addition, since May 2024, Noboru Nakatani, who has extensive experiences in cyber security in both the public and private sectors, joined NEC and serves as Corporate EVP, CSO, Managing Director of the Cybersecurity Division, and President and CEO of NEC Security, Ltd. His experiences includes Assistant Director of Cybercrime at the National Police Agency, Director of Information Systems and Technology & CISO (IPSG) at INTERPOL (International Criminal Police Organization), and Group Chief Trust & Safety Officer at a private company. He is also the Representative Director of the Japan Cybercrime Control Center (JC3*1).

*1 Japan Cybercrime Control Center

11 | Support NEC Can Provide

The NEC Group offers a support framework to advance DX in a safe, secure, and sustainable manner, addressing cybersecurity risks as a strategic management issue.

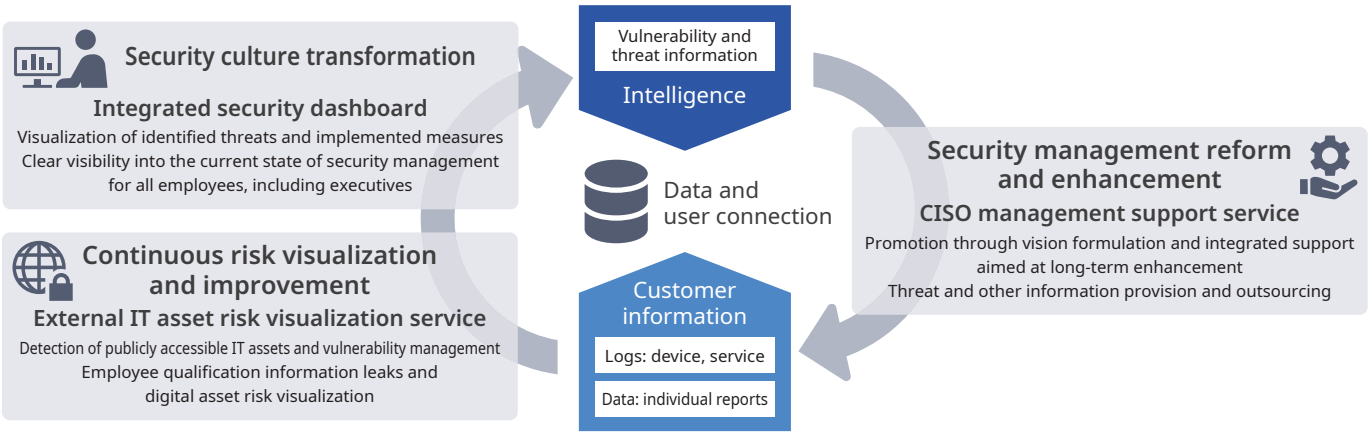
While many companies are taking steps to improve their cybersecurity, security incidents and their impact continue to rise. The number of ransomware cases has increased approximately fivefold since the second half of 2020, affecting organizations of all sizes and threatening business continuity.
This growing threat can be attributed to the rapid advancement of digital transformation (DX) and the expanding use of cloud services, which have caused critical systems and data to become increasingly dispersed across internal and external environments.
Because the assets that need protection are distributed, security measures tend to be locally optimized, making it difficult to achieve overall effectiveness. Furthermore, as systems become more complex, it becomes difficult to consider the entire process from introduction to operation when implementing measures. The repeated fragmentation of the implementation-to-operation process and the recurring local optimization of countermeasures create latent security risks at the company-wide level, making it easier for incidents to occur and for the damage to spread.
In recent years, from the perspective of economic security, there have been moves to impose obligations to ensure safety in corporate security measures and to clarify management responsibility. When security risks remain latent, it is difficult to say that appropriate measures are being implemented across the organization, which can lead directly to challenges in management, investment decisions, and corporate governance.

To eliminate latent security risks and visualize cybersecurity risks from a management perspective, it is important to continuously understand what is happening across the entire system and the extent to which countermeasures have been implemented. To achieve this, NEC has developed an original cybersecurity dashboard that visualizes the necessary data for system administrators, employees, and executives.
This enables data-driven security risk management and practical cybersecurity management.
Drawing from the knowledge we have accumulated through building and operating our in-house cybersecurity dashboard, NEC provides its Data-Driven Cybersecurity Service (DDCS) to customers, supporting the realization of digital transformation in security operations.

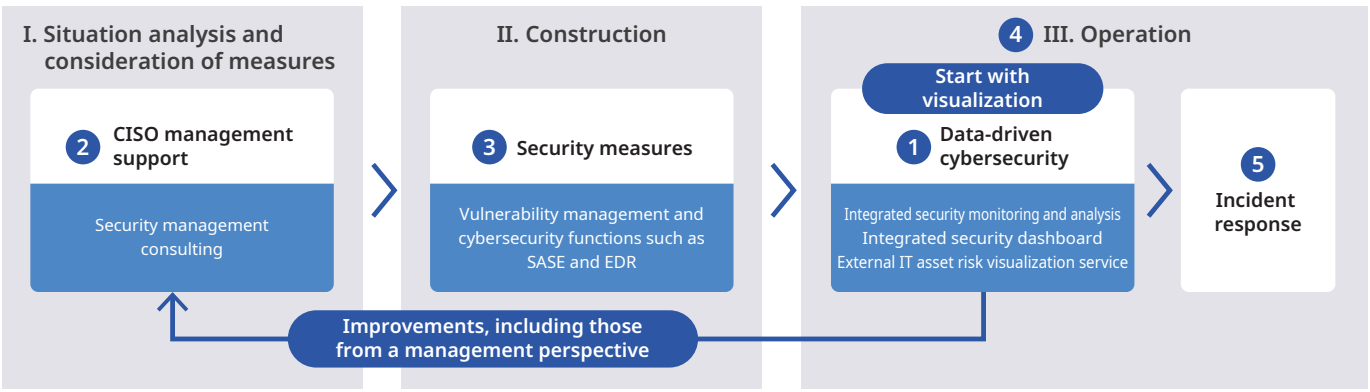
Data-Driven Cybersecurity Service overview

Data-Driven Cybersecurity Service

NEC provides the means to propel a data-driven transformation toward comprehensive and efficient security management.



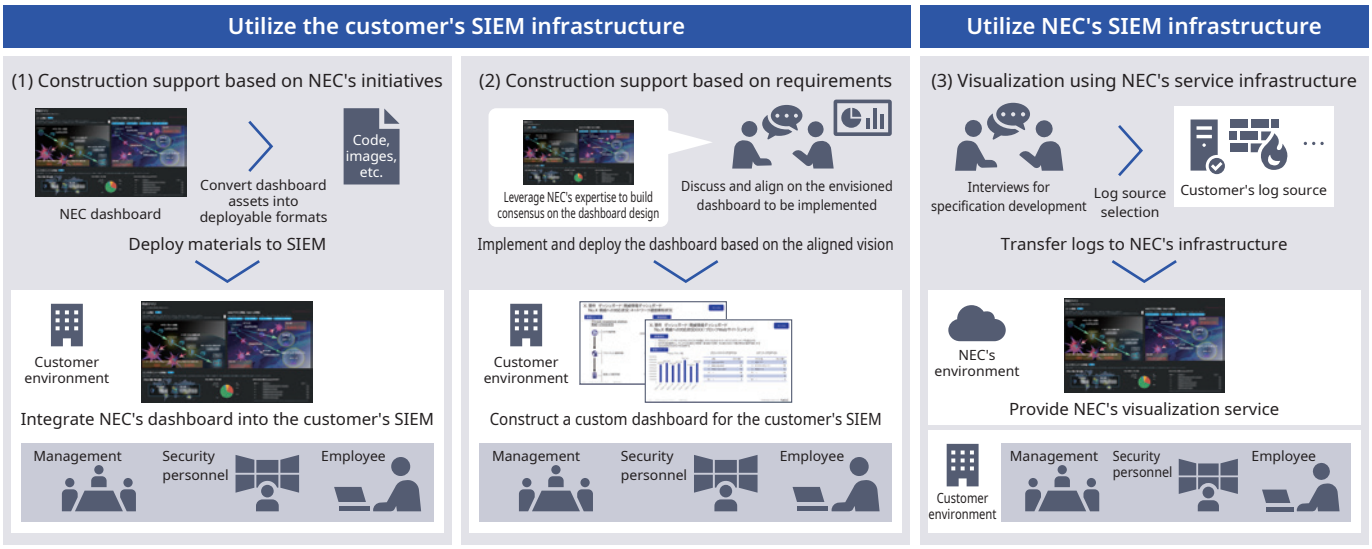
Positioning of Data-Driven Cybersecurity Service and Process



1 Cybersecurity Dashboards

The cybersecurity dashboard plays a key role in visualization and monitoring. It is tailored to serve two main purposes: operational monitoring and incident response, and supporting management decision-making and process transformation. The former is optimized for information security monitoring, such as checking the status of various security measures, understanding incident situations, log analysis, and investigations. The latter is designed to make it easier to visualize management risks, such as the number and rate of unpatched or unaddressed issues and the number of suspected cyberattacks. Through these two cybersecurity dashboards, customers can gain a comprehensive understanding of the overall status of their company's security measures and current risks, as well as address any suboptimal aspects of their existing, already-implemented solutions.

Cybersecurity dashboard menu



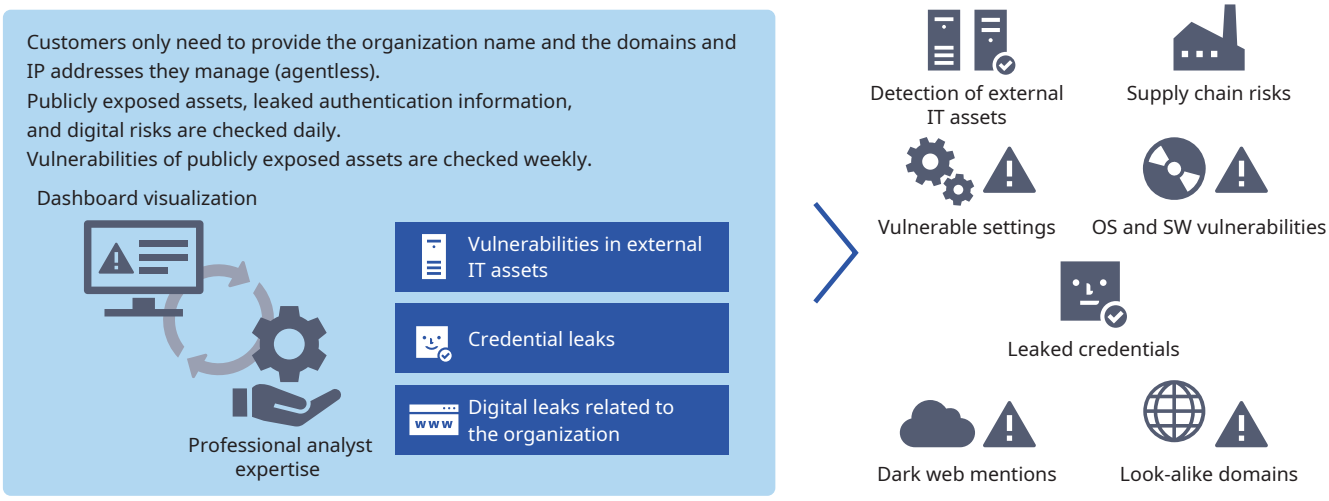
2 External IT Asset Risk Visualization Service

We inspect publicly exposed IT assets such as VPN devices and cloud services, and also visualize risk information—including misconfigurations and vulnerabilities—in real time via a dashboard. Identified risks are carefully assessed by NEC Group security experts for severity and impact, with and recommended countermeasures are provided. This enables even organizations with limited security resources to quickly implement effective risk mitigation.

In addition, the service includes features such as "supply chain risk management" (extending investigations to business partners), "credential leak detection" (identifying exposed authentication data), and "brand protection" (detecting and taking down fraudulent domains and spoofed sites). These capabilities support comprehensive and proactive defense in cyberspace.

External IT Asset Risk Visualization Service

Leveraging reliable information sources and the advanced expertise of professional analysts, we provide comprehensive support for proactive defense in cyberspace against threats and risks surrounding companies.



3 CISO Management Support Service

Security experts from the NEC Group, acting as advisors to the CISO, leverage the expertise gained through implementing security management at NEC, including on a global scale, to provide continuous support for optimizing security risk management across both short-term and long-term cycles.
Specifically, by leveraging NEC's knowledge and technologies in cyber threat analysis, we provide highly accurate cyber threat intelligence to support management decision-making. This includes information on threats to the customer's assets as well as incident trends within the customer's industry. Furthermore, we assess the status of security measures and organizational maturity, support strategic planning to achieve the target security level, and act as a PMO to drive projects through both implementation and operational phases.

CISO Management Support Service

To contribute to enhancing security management from the perspective of executives and security officers, we offer long-term support solutions to address common challenges faced by our customers.

Vision Formulation & Integrated Support	**Vision Formulation** We identify the challenges faced by both management and frontline members, formulate a vision for the ideal state of the organization, and support the development of a practical roadmap to achieve long-term enhancement and goal attainment.	**Integrated Support** We become a member of the customer's security team, working together to develop solutions for the high-priority issues identified during the vision formulation phase. By deepening our understanding of the customer's organizational structure and culture, we provide support from within, advancing initiatives that are tailored to their actual circumstances and enabling effective skill transfer.
Security Trends Ongoing Information Sharing	**Provision of Security-Related Information** ・Recent incident cases ・Trends and countermeasures based on incident cases ・Lists of damage caused by cyberattacks ・Updates on threat actors and attack campaigns, and more	**Understanding Security Trends** Executives involved in security strategy (such as CISOs and CIOs) gain an overview of security trends and incidents in Japan and overseas. They assess their organization's security management status and potential risks, aiming to reduce damage through company-wide strengthening of security measures.
Managed Services (Outsourcing)	**Managing Routine Operations** ・Monitoring and incident response (SoC/MDR) ・Outsourcing of operational tasks ・Incident response support ・Provision of vulnerability information	**Enabling Focus on Core Businesses** For organizations that face a shortage of personnel dedicated to security management and operations, yet seek to strengthen their security over the long term, we help distinguish between tasks that can be handled internally and those that can be outsourced. By leveraging outsourcing effectively, we support the creation of an environment where the organization can focus more fully on its core business activities.

A sample of the available support

At the NEC Group, we focus on developing specialists who not only possess advanced technical skills, but can also assess risks from a business perspective. We actively encourage employees to obtain the international CISSP certification, and as of June 2024, we have 450 certified professionals.
Furthermore, in April 2024, we brought together cybersecurity experts within NEC Security to strengthen our structure for expanding the cybersecurity business. Looking ahead, we will further enhance our capabilities to develop and deliver solutions utilizing the latest cybersecurity technologies. Through these efforts, we are accelerating the expansion of our cybersecurity business to support government agencies, critical infrastructure, and private enterprises in defending against cyberattacks.
In the area of digital transformation (DX), NEC provides end-to-end services—from strategy consulting to implementation—across three key pillars: business models, technology, and organization/human resources. Additionally, we are evolving from a traditional system integrator (SIer) into a "Value Driver," and have systematically organized our value creation model under the name NEC BluStellar. By leveraging advanced cross-industry insights and state-of-the-art technologies, we are transforming business models to solve both societal challenges and address our customers' management issues.

12 | Technology, Research, and Business Development to MAKE JAPAN CYBER SECURE

NEC leverages AI technology to enhance and streamline the processes to "build systems correctly," "maintain stable operations," and "protect against attacks," thereby safeguarding social infrastructure and organizations against the threat of cyberattacks.

1 Research Theme Concept

The NEC Group is engaged in research and development of AI technologies and agents that support Security by Design (SBD). Among these, we introduce AI Agent for System Risk Diagnosis, which assists with both maintaining stable operations and protecting against attacks. Additionally, we present AI Agent for Guideline Checking, which provides support in building systems correctly, as well as AI Agent for Information Security Internal Audits, which enhances organizational security governance and helps to maintain stable operations.

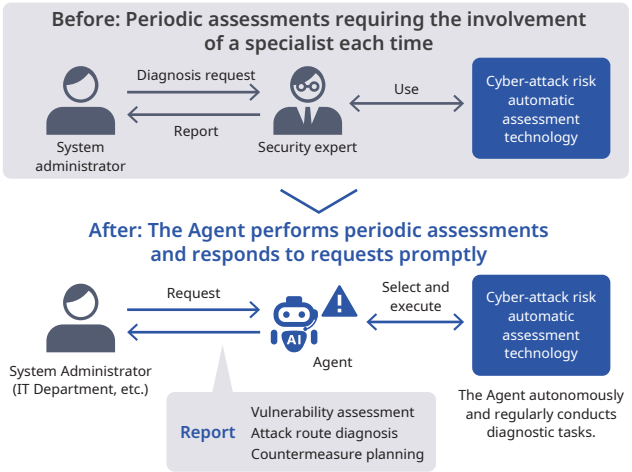
2 AI Agent for System Risk Diagnosis

As ICT systems become increasingly complex, numerous vulnerabilities and new attack techniques are continuously being reported. To address these issues, organizations must not only proactively collect intelligence on emerging threats, vulnerabilities, and attacker behaviors, but also analyze their potential impact and implement preventive measures in advance. However, these activities require significant time, effort, and specialized knowledge to make effective use of the vast amount of intelligence information available. NEC is developing AI solutions that build on its expertise in cyber-attack risk automatic assessment technology.*1 The AI Agent for System Risk Diagnosis currently under development analyzes intelligence information in place of humans and translates it into general attack knowledge information entailing what kind of attacks can be carried out under what conditions and what will result. This makes it possible to assess the impact of newly reported threats and vulnerabilities on systems, and to formulate effective countermeasures.

By using such AI-driven solutions to streamline and advance system risk analysis and diagnosis, NEC supports Security by Design practices—helping organizations maintain stable operations and protect against attacks.

AI × Security Technology Development Concept

AI Agent for System Risk Diagnosis



Background and Challenges

- The number of new attacks, threats, and vulnerabilities that threaten business continuity is increasing, and the scale of damage is expanding.
- Effective countermeasures require conducting security risk assessments to identify organizational weaknesses.
- For non-experts, performing these assessments is difficult, and it is challenging to regularly identify and diagnose threats and vulnerabilities.

Value Provided

- The AI Agent autonomously performs end-to-end processes: from checking for threats and vulnerabilities, conducting risk diagnoses, and planning countermeasures, to generating reports with diagrams and visual content.
- Delivers expert-level quality, on par with assessments performed by specialists.

Why NEC

By combining NEC's proprietary cyber-attack risk automatic diagnosis technology with AI agents, and leveraging NEC's unique knowledge database, we can carry out attack diagnostics and countermeasure planning. This allows us to propose timely and situation-specific solutions through regular assessments.

*1 "Research, Development, and Practical Application of Cyber-attack Risk Automatic Assessment Technology," by Tomohiko Yagyu, Hirofumi Ueda, Masaki Inokuchi, Shunichi Kinoshita, and Ryo Mizushima, received the Chairman's Award at the FY2022 SCAT Awards presented by the Support Center for Advanced Telecommunications Technology Research.
https://jpn.nec.com/rd/awards/2022/2022-06.html
https://www.scat.or.jp/cms/wp-content/uploads/2022/12/award-press2022.pdf

*2 CSIRT: Computer Security Incident Response Team

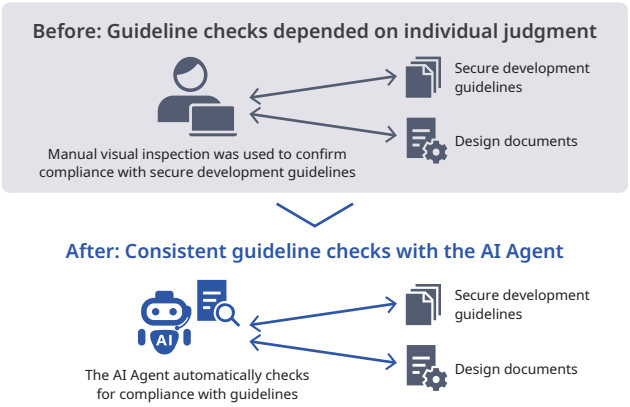
3 AI Agent for Guideline Checking

By practicing Security by Design (SBD)—incorporating security from the planning and design stages—it is possible to build secure systems. However, secure development guidelines are numerous and varied. Determining compliance often requires matching the general statements in guidelines with the specific language used in real system planning and design documents, which demands significant time, expertise, and know-how. As a result, when performed manually, omissions and interpretation errors are almost inevitable. Drawing on years of experience in secure development and knowledge gained from its proprietary secure development guidelines, NEC is conducting research and development on AI that supports guideline checks. This AI can, for example, generate contextual information (such as methods for interpretation) to bridge the gap between the general wording of guidelines and the specific descriptions found in actual system documents. The AI can then autonomously identify relevant sections in design documents that correspond to checklist items, and determine whether requirements are met.
By using this AI technology to streamline and enhance the accuracy of guideline checks within SBD, NEC supports efforts to build systems correctly.

4 AI Agent for Information Security Internal Audits

In practicing Security by Design (SBD), not only the technical aspects of the system but also the organization's security governance are crucial. By understanding the degree to which SBD is practiced and the organization's response status, overall security can be improved. NEC conducts internal information security audits across NEC Group companies, continuously striving to strengthen security. However, these audits and the preparation of audit reports are time-consuming, and the quality of audits can vary depending on the auditor. Additionally, responding to industry-specific guidelines can present significant challenges. Leveraging years of audit expertise and knowledge gained from security consulting, NEC is researching and developing AI to support information security audits. By combining AI with auditors, we aim to reduce the time required for audits, enhance report quality, and achieve greater consistency. Moreover, utilizing NEC's industry-specific expertise, it is possible to generate tailored recommendations for each industry.
Through AI that streamlines and improves the quality of internal information security audits, NEC supports organizations in enhancing their security governance and helps ensure the stable and reliable operation of customers' systems.

AI Agent for Guideline Checking



Background and Challenges

- There is a growing need to embed security into every phase—from planning and design to implementation and operations—by applying the Security by Design (SBD) approach.
- Secure development guidelines are numerous and diverse, and comparing the generic descriptions in guidelines with the specific details in actual system design requires significant effort. This increases the risk of oversights and mistakes.

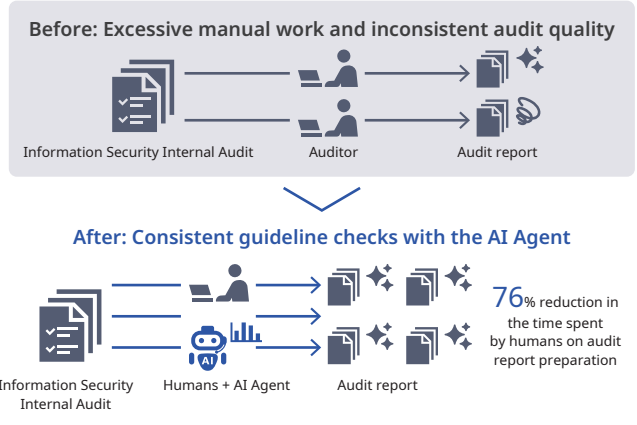
Value Provided

- Leverages machine-based inspection to prevent human-error omissions and misinterpretations.
- Automated, standardized checks ensure consistent, high-quality scrutiny, supporting the efficient development of secure IT systems.

Why NEC

The With its original features, the agent can automatically supplement design documents with contextual information, such as system background and usage scenarios, enabling high-precision checks even for industry-specific designs.

AI Agent for Information Security Internal Audits



*Based on NEC's own calculations in standard internal audits across 17 NEC Group companies

Background and Challenges

- Requests from organizations such as the U.S. Securities and Exchange Commission (SEC) and the National Institute of Standards and Technology (NIST) to strengthen security governance.

Value Provided

- Shortens audit report preparation time and improves audit quality, eliminating inconsistencies due to differences in skill levels.
- Supports checking responses to internal audit questionnaires and preparing audit reports.

Why NEC

The Agent utilizes NEC's accumulated audit expertise and security consulting knowledge as its knowledge base. In the future, the Agent will also be able to propose necessary actions, such as corrective measures tailored to industry-specific circumstances.

5 The Future of Our Cybersecurity Business

To MAKE JAPAN CYBER SECURE, it is essential to not only utilize AI technologies and intelligence but also to conduct analysis that takes geopolitical risks into account. However, collecting and analyzing intelligence manually requires enormous time and effort. There are many intelligence providers, both in Japan and overseas, but from a security standpoint, reliance on foreign sources is not desirable.
NEC aims to build a foundation of trustworthy intelligence from Japan by using its proprietary generative AI "cotomi" to collect intelligence in real time and perform advanced analysis. Based on this intelligence, NEC will provide safe and reliable services to government and corporate customers.
Additionally, in order to handle intelligence safely, facilities and personnel that comply with security clearance systems are indispensable. As a core part of its cybersecurity business, NEC will establish a Cyber Intelligence & Operation Center that meets the Japanese government's security clearance requirements and will work to expand its cybersecurity services.

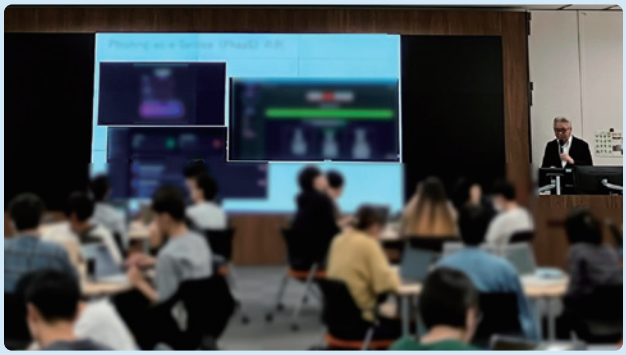
Furthermore, NEC will expand its cybersecurity business globally by utilizing these technologies and offering 24-hour support, making a strong contribution to business continuity for Japanese companies operating overseas.

NEC's Proprietary Intelligence

Human Resource Development

To provide these services and expand our business, the NEC Group has developed a large number of cybersecurity professionals. However, to "MAKE JAPAN CYBER SECURE", the quantity and quality of personnel within the NEC Group alone are not sufficient. Therefore, NEC provides security training to students and customers in Japan.
In July 2022, NEC entered a comprehensive partnership agreement with the National Institute of Technology (KOSEN) to strengthen human resource development in the field of cybersecurity. Through this agreement, we conduct industry-academia collaborative educational support by combining KOSEN's 60 years of experience in developing highly-skilled engineers through social implementation-oriented education with NEC's latest security technologies and expertise. In September 2024, NEC co-hosted the event "K-SEC CAMP FOR GIRLS in KISARAZU" with KOSEN for female KOSEN students, organizing career workshops with five female engineers from the NEC Group and a technical workshop that included a hands-on demonstration of web application vulnerability assessment. Additionally, from October 2024 to February 2025, we provided a lecture on Security Risk Assessment as one of the required classes for the general course Liberal Arts II for over 200 third-year students across all five departments, including Information Engineering and Urban Environmental Design Engineering, at Kagoshima National College of Technology.

From October to November 2024, we also provided a Secure System Design Method course at the Faculty of Information Systems, University of Nagasaki. This course was offered as a countermeasure to the growing threat of cyberattacks, with the goal of deepening students' understanding of secure development methods essential for system development. NEC engineers who lead secure development initiatives served as instructors, providing educational materials at no cost. The course featured not only classroom lectures but also practical exercises using methods employed in real-world development environments.



Secure System Design Method course at the Faculty of Information Systems, University of Nagasaki

13 | 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 2024) 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 Organization Cyber Index Corporate Survey by the Japan Federation of IT Organizations

The Information Technology Federation of Japan awarded us the highest "two star" rating, citing that NEC demonstrated a particularly outstanding commitment (to cybersecurity) and information disclosure on an ongoing basis.
(Out of the companies included in the Nikkei 500, only 13 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, 2025.

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 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
- K&N System Integrations Corporation
- NEC Shizuoka Business, Ltd.
- NEC Communication Systems, Ltd.
- Forward Integration System Service Co., Ltd.
- LanguageOne Corporation
- NEC Life Career, Ltd.

3 IT Security Evaluations and Certifications

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

NEC products and systems with ISO/IEC 15408 certification

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

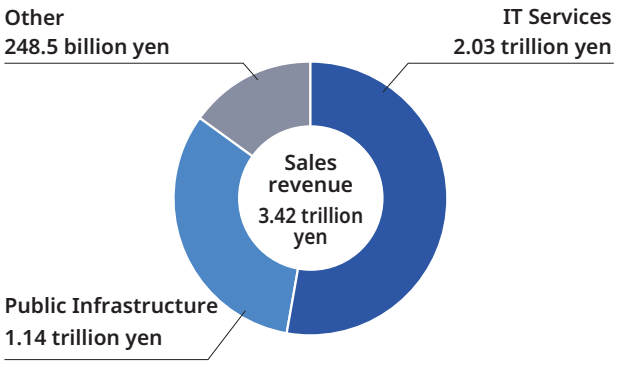
Corporate Profile

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)	104,194*
Consolidated subsidiaries	249*

*As of March 31, 2025

Segment Information

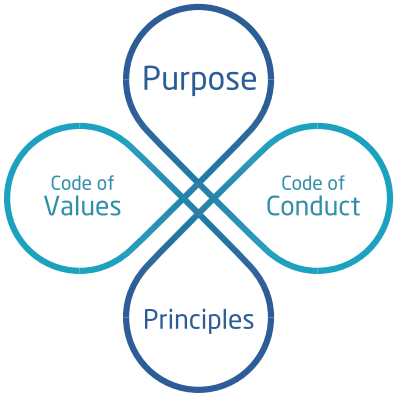
Segment Information



*As of March 31, 2025

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.

Principles

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

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.

Code of Conduct

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

Consultation and Report on Doubts and Concerns about Compliance

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

VEGETABLE OIL INK

Issued September 2025