Cybersecurity Management Report 2026

NEC \Orchestrating a brighter world

MAKE JAPAN CYBER SECURE

NEC recognizes information security as a critical management priority. We strive to maintain society's trust in our company by aligning with national guidelines and international standards.

Noboru Nakatani
NEC Corporation
Corporate EVP
Concurrently serving as CSO (Chief Security Officer)
Managing Director, Cyber Security Division
Concurrently serving as Chairman and Representative Director, NEC Security, Ltd.

As our world becomes increasingly interconnected and the use of AI continues to expand, governments and businesses alike face new and complex cybersecurity challenges. These include increasingly sophisticated and commercialized cyberattacks, growing risks of information leakage associated with greater reliance on cloud services, and information management challenges arising from economic security requirements.
In response to these developments, NEC has adopted the slogan "MAKE JAPAN CYBER SECURE" and is expanding its cybersecurity business to help protect Japan's digital infrastructure and to contribute to economic security and industrial competitiveness. Our work centers on three key dimensions—readiness for regulatory compliance (Regulation), the maintenance and improvement of corporate value (Reputation), and the resilience needed to ensure business continuity (Resilience). To advance these, we deliver proprietary cyber threat intelligence, apply homegrown AI to bring together safety and functionality, and operate under a globally coordinated framework.
This report is published annually to help stakeholders better understand the NEC Group's cybersecurity initiatives that support our business operations, including those mentioned above. Until 2024, the report had been titled the "Information Security Report," but in 2025, it was renamed the "Cybersecurity Management Report" to clearly reflect the importance of cybersecurity in business management, which is heavily influenced by the latest global events 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
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 received the highest rating—Two Stars—in the "Cyber Index Corporate Survey 2025" conducted by the Information Technology Federation of Japan for the fourth consecutive year.
This report outlines NEC's latest initiatives in information security up to May 2026. 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 Cybersecurity Governance

Direction 1 Direction 2

In order to effectively control risks stemming from business activities, the NEC Group has established a system of cybersecurity governance to efficiently raise information security levels across the entire Group.

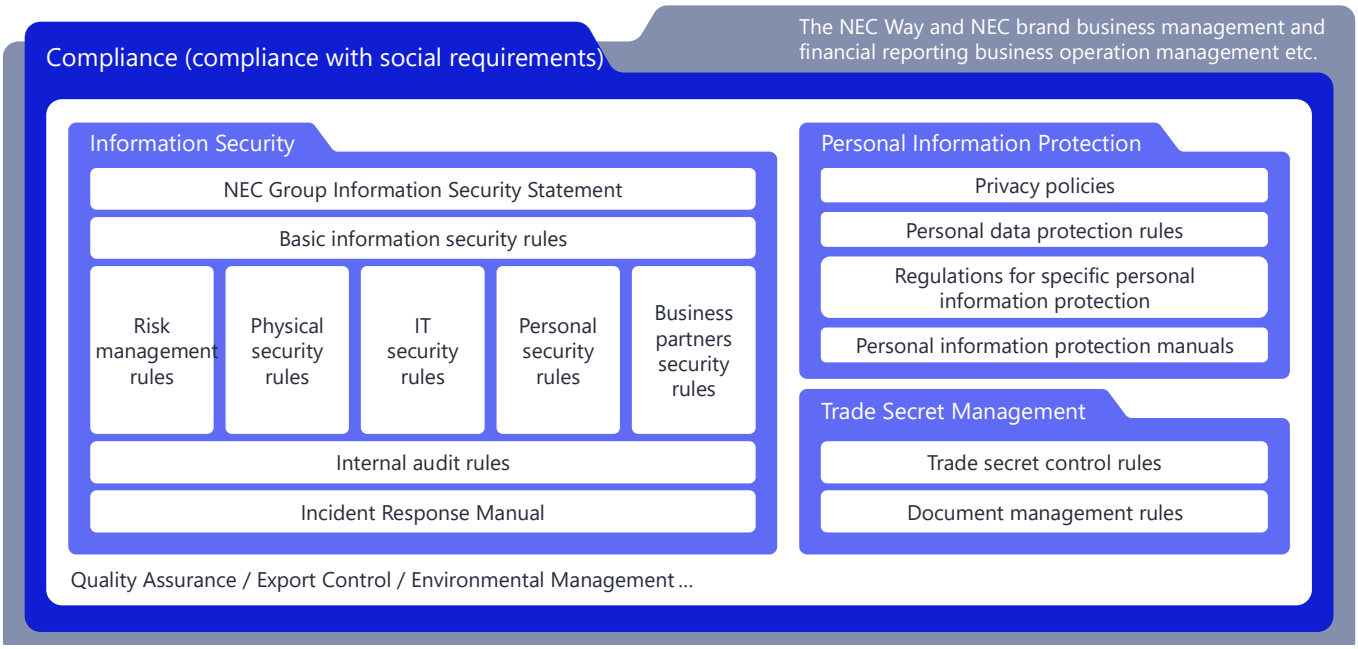
1 NEC Group Cybersecurity Governance

The NEC Group considers information security a core management priority, and the investment required to ensure that security, an essential aspect of company management. We have established the NEC Group Management Policy, which standardizes rules and unifies systems, operational processes, and infrastructure across the entire organization creating a management foundation that meets global standards.
Under our cybersecurity governance framework, NEC's senior management reviews security objectives once a year and provides instructions for improvements and corrective actions. These reviews are based on the results of monitoring performed across the 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.
Beyond this, NEC established the NEC Privacy Policy*2 to ensure the protection of personal information and obtained Privacy Mark certification in 2005. Our management system complies with JIS Q 15001, the Japanese Industrial Standard for personal information protection management systems, Act on the Protection of Personal Information, and Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures.
Personal information is managed according to a common group-wide protection standard, and 28 NEC Group companies in Japan have obtained Privacy Mark certification as of March 2026. NEC has also developed common personal information protection guidelines for its overseas group companies, each of which has established rules that comply with applicable personal information protection laws and regulations in its respective country or region.

NEC Group Management Policy



*1: NEC Group Information Security Statement
*2: NEC Privacy Policy

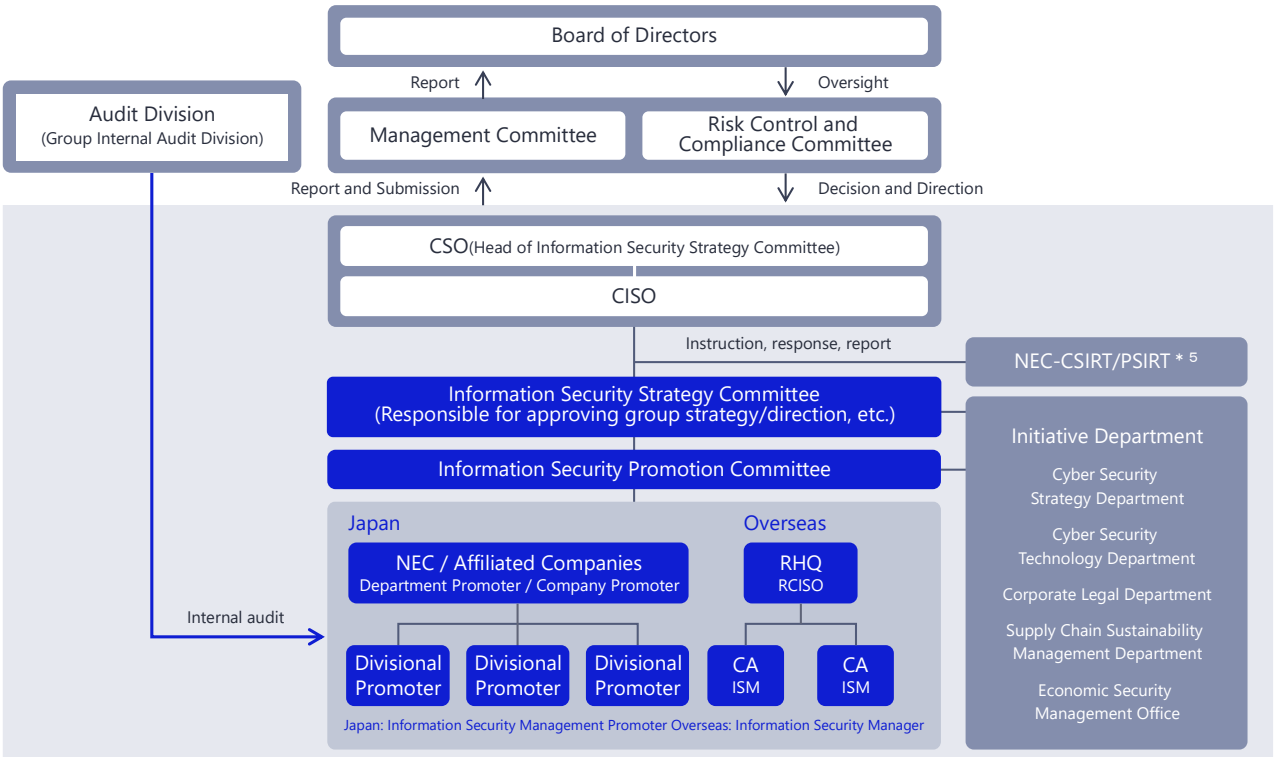
3 AI Policy

As the NEC Group expands its use of data, including AI-related and biometric data, we have established the NEC Group AI and Human Rights Principles as guiding principles that place the highest priority on privacy protection and respect for human rights. Grounded in compliance with the laws and regulations of each country and region, these principles serve as a fundamental management principle that guides every employee to recognize respect for human rights as the highest priority at every stage of business activities and to take action accordingly. In practice, we ensure the appropriate use of AI both within and outside the company, while promoting technological innovation and talent development and strengthening collaboration and partnerships with stakeholders. Through ongoing dialogue with external experts, we are also working to promote the trustworthy use of AI and help address societal challenges.

4 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 Cyber Security Technology Department and the Cyber Security Strategy Department, which advance information security measures, as well as the CSIRT*3, which monitors cyberattacks and responds swiftly to contain incidents.
The Information Security Promotion Committee and its working groups share information security implementation plans, discuss and coordinate information security measures, report on progress, and issue requests and reminders to the information security management coordinators in each organization.
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 *5 PSIRT: Product Security Incident Response Team

3 Information Security Management

Direction 2 Direction 6

We implement various initiatives throughout the NEC Group to establish, maintain, and enhance our information security management and security policy framework.

1 Information Security Management Framework

NEC applies its information security policies to sustain and strengthen information security through an ongoing PDCA cycle. We refine our practices and review policies in light of the results of security audits and the status of security incidents. We also promote the acquisition and maintenance of ISMS certification and Privacy Mark certification across the group.

2 Information Security Risk Management

① 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.

② Management of Information Security Incident Risk

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

③ Initiatives for Business Continuity

The NEC Group conducts third-party assessments of 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

① 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 define rules for handling and storing critical information based on its level of importance, and enforce robust safeguards against information leaks. In line with recent laws and regulations, highly sensitive information will be tightly controlled: access will be limited to personnel whose duties require it, and it will be managed under a dedicated framework with dedicated storage.

4 Information Security Surveys and Audits

① 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.

② Information Security Audits

As part of operational audits led by the Audit Division, annual audits cover information security management and personal information protection. Each organization is audited against ISO/IEC 27001 and JIS Q 15001, and the acquisition of ISMS certification is encouraged in light of trends in each business area. (See page 30 for the status of certifications obtained.)

4 Information Security Infrastructure – Security for AI

Direction 3 Direction 5

The NEC Group has established a Zero Trust Platform based on CISA's*1 Zero Trust Maturity Model, which is built on five pillars: identity, devices, networks, applications, and data. Based on these pillars, we have implemented the following security measures.

1 Identity Security

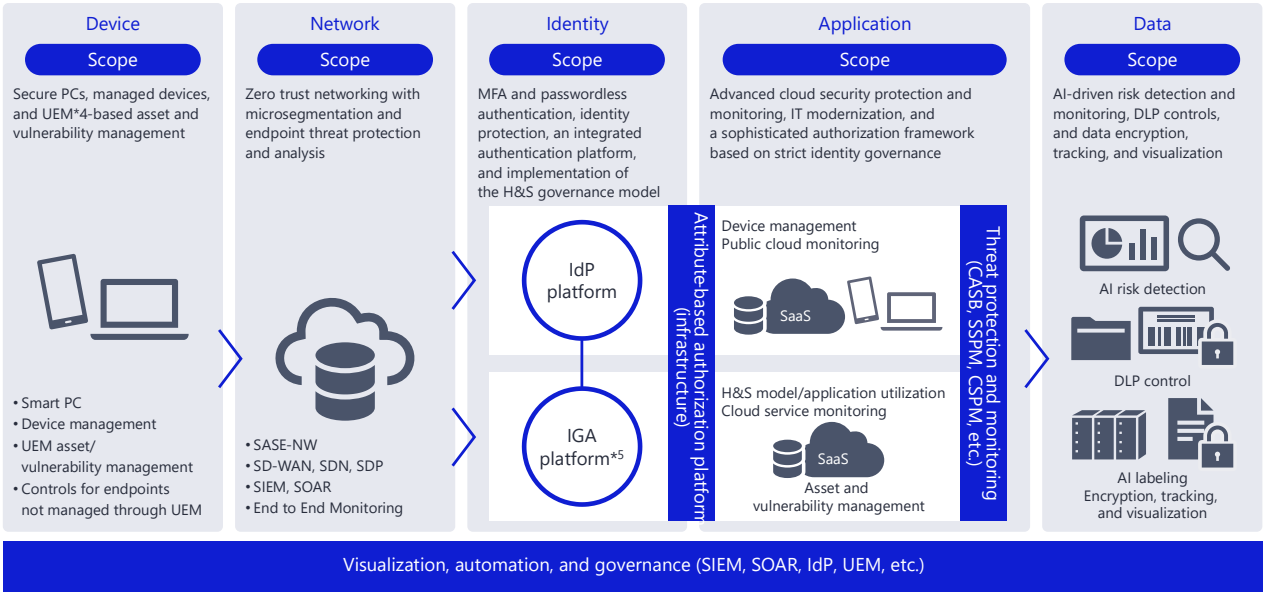
In response to increasingly sophisticated and complex security risks such as cyberattacks amid the changing environment brought about by the recent digital shift, we are working to strengthen and enhance authentication as a key strategy at the core of our Zero Trust Platform.
NEC is enhancing authentication company-wide through multi-factor authentication (MFA*3), which combines multiple methods, including biometric authentication such as facial and fingerprint recognition and device authentication. As a result, passwordless authentication has been enabled for almost all users, reducing the risk of impersonation and cyberattacks.
In addition, NEC has implemented risk-based authentication, which requires additional authentication only when there are indications of impersonation or cyberattacks. By reducing the frequency of authentication, this approach improves both user convenience and security, delivering security that is user-friendly and 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 use of enterprise resources through its IAM platform, NEC implements the following four measures.

(1) Use of global ID	Identity management through centralized control and lifecycle management of user accounts
(2) Authentication and device management	A controlled environment for user authentication (including passwordless and multi-factor authentication), device authentication, and managed devices
(3) Global application management	Management of access to common systems and services, including single sign-on (SSO)
(4) Security governance	Globally centralized management and control of security policies and configuration information

2 Device Security

NEC provides employees with a lineup of secure standard endpoint devices, known as the Smart PC series, to support diverse work styles.
The Smart PC series comes in three models: thin clients that do not store data locally (Smart Connect PC, or SCPC), rich-client-based PCs designed for hybrid on-site and online work (Smart Managed PC, or SMPC), and high-spec workstations (Smart Engineer PC, or SEPC). The Smart PC series supports facial recognition, passwordless authentication, device authentication, endpoint management (Intune integration), the automatic application of security settings, and integration with NEC's internal authentication systems.

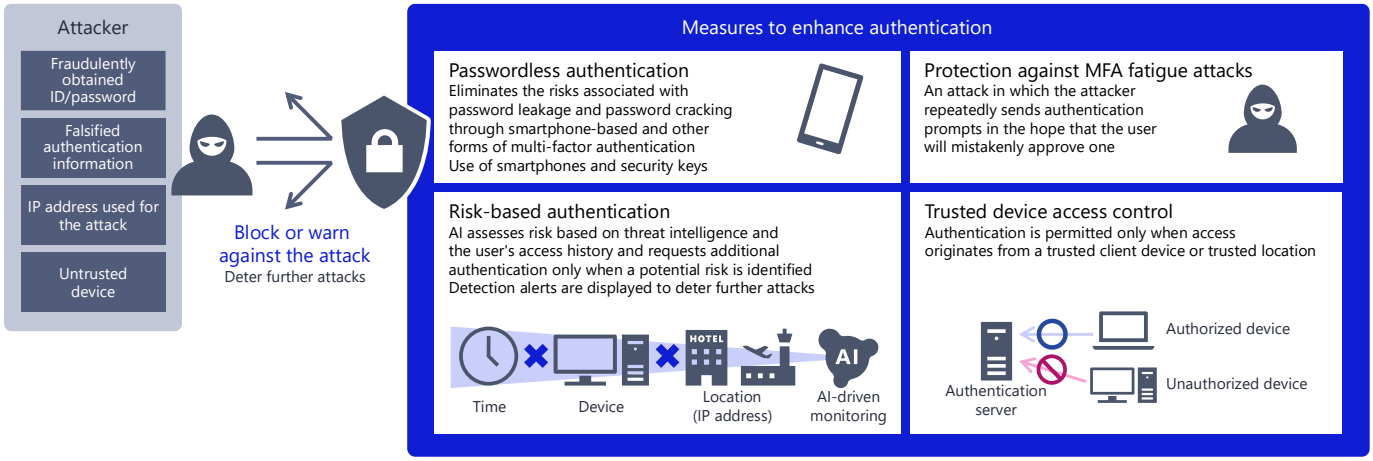
Overview and Scope of the Zero Trust Platform



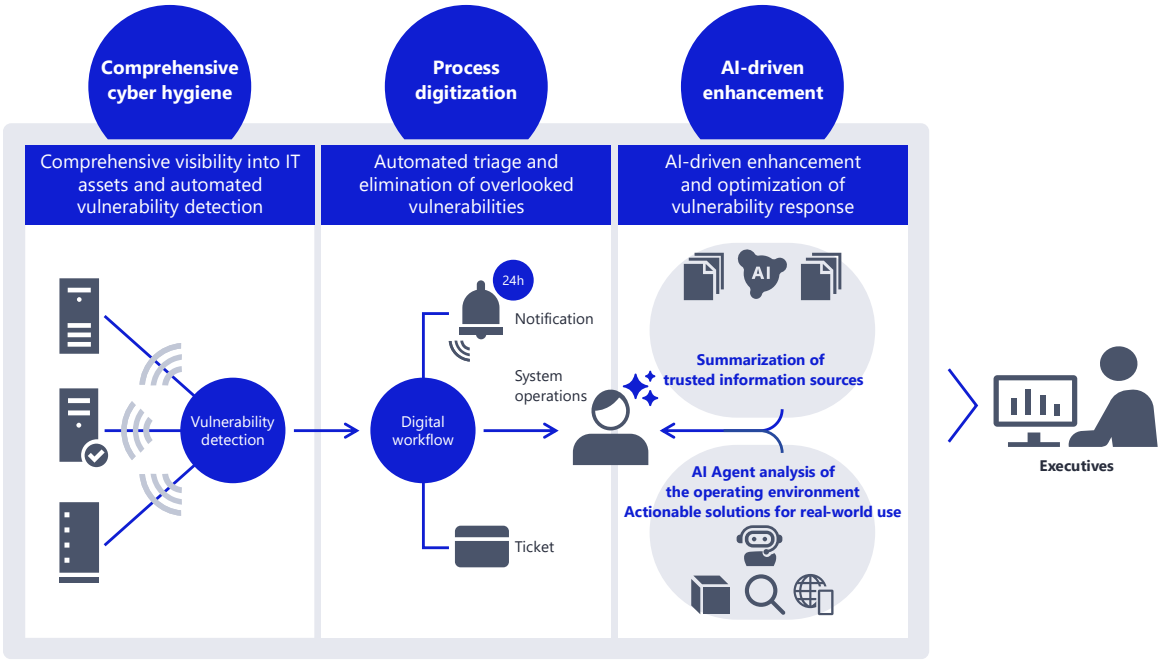
*1 CISA: Cybersecurity and Infrastructure Security Agency *2 MFA: Multi-Factor Authentication *3 IAM: Identity and Access Management
*4 UEM: Unified Endpoint Management Platform. This platform centrally manages various devices regardless of their connection location, thereby improving security levels.
*5 IGA (Identity Governance and Administration): An identity governance framework covering user lifecycle management, access rights management, provisioning, credential management, and related functions

NEC has implemented a Unified Endpoint Management (UEM) platform to centrally manage 260,000 IT assets in Japan and overseas via the cloud. Through this platform, vulnerabilities can be detected and visualized, enabling rapid responses to security risks and more efficient management operations.
Managing server vulnerabilities is essential to protecting corporate systems from cyberattacks and requires continuous effort. To securely maintain more than 10,000 internal servers, NEC has established data-driven security that enables the early detection, notification, and visualization of vulnerabilities.
AI-enabled attacks that exploit vulnerabilities have grown more sophisticated in recent years. In response, NEC has built a solution powered by its proprietary AI technology to further enhance the end-to-end vulnerability detection, notification, and response process. By generating tailored response guidance based on the operating environment and the characteristics of each vulnerability, the AI reduces the decision-making and response burden on operators and supports safer, more accurate, and faster vulnerability response.
Endpoints with inadequate security controls, or on which malware or other threats are detected, are blocked from the business network. For external communications, NEC implements allowlist-based web access controls and plans to introduce ID-based web access controls in the future. NEC has also implemented Domain-based Message Authentication, Reporting, and Conformance (DMARC) in accordance with Google's Email sender guidelines.*6
To reduce the risk of information leaks, NEC takes a multi-layered approach that combines encryption, device control, and logging to guard against both external attacks and internal misconduct. Encryption is applied at both the hardware and information levels, supported by an infrastructure that enables access permissions and expiration dates to be set for individual files.
These measures help prevent information leakage caused by device theft, loss, or misdirected transmissions, and also protect information in the event of a malware infection. Through device controls, the use of USB drives, SD cards, and other communication interfaces is restricted to business-critical situations only, reducing the risk of information leakage through external devices and channels.
As part of our logging practices, operation logs are collected for all PCs. In the event of an incident, these logs are analyzed to understand the scope and circumstances of the impact and to develop measures to prevent recurrence.

Advanced Authentication through Passwordless and Risk-Based Authentication



Overview of AI-Driven Autonomous Vulnerability Management



*6 Email sender guidelines
https://support.google.com/a/answer/81126?hl=en

3 Network Security

NEC's global network is built on a zero trust architecture across both internet-facing and internal networks, supporting the security and availability of the business environment.

① Zero Trust Network Architecture

To achieve a true zero trust approach, NEC has established an environment that enables appropriate access control, authentication, and authorization across the networks connecting endpoints and services.

・**Internet defense:** All internet-bound traffic originating from approximately 30 countries is centrally protected and monitored through a Secure Web Gateway (SWG).

As part of its global rollout, NEC has progressively raised security baselines to achieve security levels comparable to those in Japan. For remote work environments, NEC has migrated to a cloud-based Remote Gateway, enabling secure operation without exposing the company's network perimeter directly to the internet. Deployment in Japan has been completed, and overseas rollout is ongoing.

・**Office and manufacturing site protection:** To support a zero trust approach for communications both inside and outside NEC facilities, NEC is implementing controls that combine Network Access Control (NAC) with SDN-based virtual networks at its offices and manufacturing sites. NAC deployment began in FY2024, while SDN deployment began in FY2016. These measures separate office communications from operational traffic associated with manufacturing and development systems.

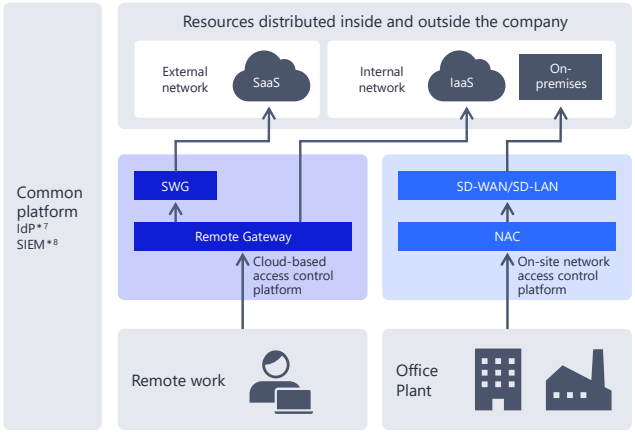
② Global Deployment of SD-WAN

SD-WAN provides centralized control while supporting the growing network traffic generated by online meetings, SaaS applications, and security controls. It has been deployed to all 289 locations worldwide to support communication control across six global regions, as well as intra-regional and domestic traffic control in Japan, APAC, and mainland China, where inter-regional traffic volumes are particularly high.

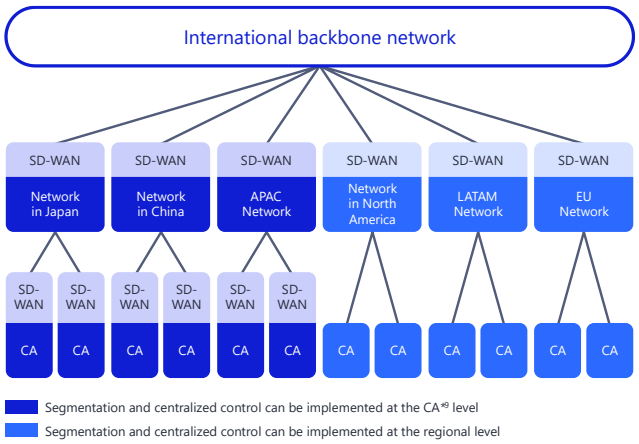
・**Performance and availability improvements:** Network bandwidth has increased more than fourfold, while the time required to implement network changes has been reduced to a fraction of its former level. From an availability perspective, network redundancy has been implemented even at smaller sites, where the cost of redundant dedicated lines had previously been prohibitive.

Security improvements: SD-WAN has enabled capabilities that were difficult to achieve with previous network infrastructure, including cross-regional emergency communication shutdown capabilities and site-level traffic monitoring. In particular, for emergency shutdown scenarios, NEC has gone beyond simply deploying the infrastructure by developing multiple response scenarios for anticipated threats, such as attacks targeting specific servers and ransomware lateral movement, and by conducting tabletop exercises involving coordination between the SOC and NOC. In Japan, NEC has also deployed advanced management capabilities to protect administrator privileges on internet-connected SD-WAN routers and enhance safeguards against impersonation and insider misconduct. These capabilities include alerts for unexpected administrative activities, as well as login notifications sent to both the user and their supervisor.

Overview of the Zero Trust Network



Global Deployment of SD-WAN



4 Application Security

As part of its digital transformation, the NEC Group uses many cloud services. While DX improves user convenience, robust security is essential because critical data is stored in the cloud and can be accessed from outside the company. Taking into account the risks associated with cloud service use while preserving the convenience these services provide, the NEC Group has implemented the following security measures.

① Visibility into SaaS Usage

Using CASB,*10 we monitor and analyze logs and files stored in cloud services to help protect services that handle important data from insider misconduct and cyberattacks. We also maintain visibility into the cloud services used across the organization and monitor the use of unauthorized cloud services that present elevated security risks.

② Comprehensive Security Measures for Cloud-Native Environments

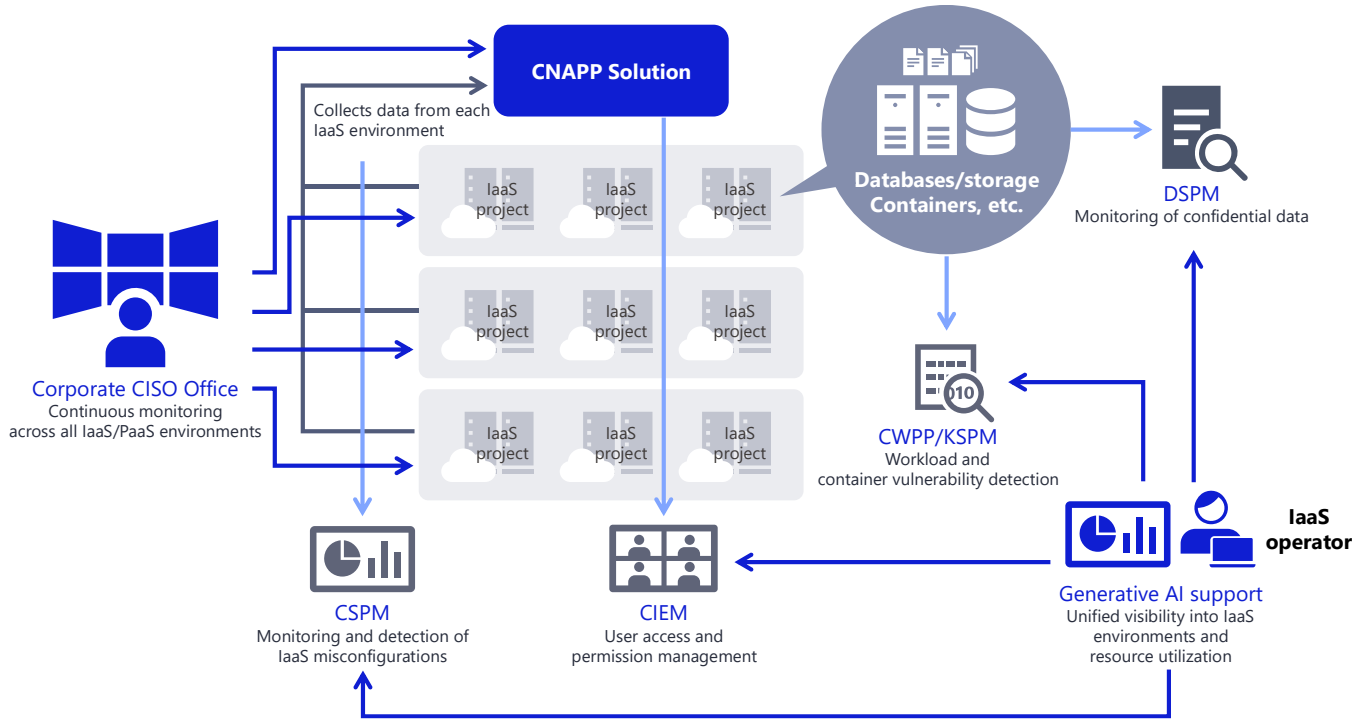
Public cloud services such as AWS, Azure, and GCP are seeing wider use, and cloud-native technologies including containers and serverless computing are being adopted more broadly. Beyond the traditional risks of misconfiguration, the scope of assets requiring protection has expanded and risks have become more complex. The NEC Group applies CNAPP*11 to address these diverse risks in a unified way. By leveraging CNAPP, NEC extends the capabilities of traditional CSPM and provides comprehensive protection across the entire cloud environment.

*7 IdP: Identity Provider *8 SIEM: Security Information and Event Management *9 CA: Corporate Affiliate
*10 CASB: Cloud Access Security Broker *11 CNAPP: Cloud-Native Application Protection Platform

③ Prevention of Incidents Resulting from Improper SaaS Settings

Cloud services such as Microsoft 365, Box, and Salesforce have numerous configuration settings, and misconfigurations can create security risks during operation. Using SSPM,*12 the NEC Group globally identifies and remediates misconfigurations in the cloud services used internally.

Comprehensive Security Measures for Cloud-Native Environments Using CNAPP



5 Data Security

① Information Classification and Protection (File Labeling/Encryption)

Guided by the principles of zero trust security, the NEC Group uses cloud-based AIP*13 unified labels together with its proprietary solution, InfoCage FileShell, to label and encrypt files according to the sensitivity of the information they contain. Access controls and encryption are applied based on these labels to ensure the appropriate handling of a wide range of files, including Microsoft Office documents. This helps prevent information from being leaked outside the organization as a result of malware infections and other incidents.

To strengthen the security of important information, the NEC Group has also introduced secure storage with capabilities such as access control, encryption, audit trail management, intrusion investigation, and ISMS management. This enables secure information management while reducing administrative burden. In addition, internal systems that handle highly sensitive information are protected through security measures based on risk analysis and business impact analysis, including vulnerability countermeasures, log management, network protection, authentication, access control, and privileged access management.

② Behavioral Detection for Information Leak Risk

In recent years, incidents involving the unauthorized removal of information, whether through negligence, carelessness, or deliberate action, have become a social issue. Some involve intentional insider misconduct, and cases continue to occur in which departing employees provide confidential company information to their new employers. “Damage caused by insider misconduct, including information leaks” also ranks among the leading threats in the Top 10 Information Security Threats published by the 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 that detects and visualizes behaviors associated with information leakage risks, including insider misconduct. 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.

③ Data Loss Prevention (DLP)

To protect corporate confidential information and reinforce company-wide safeguards against data leaks, we have introduced a new DLP program. As working styles diversify, our existing Behavioral Detection for Information Leak Risk program had focused on a subset of high-risk employees such as departing or soon-to-depart staff, leaving potential risks outside that scope unaddressed.

The newly introduced DLP covers every employee's PC and monitors and blocks unauthorized transfers of confidential information via USB drives, the web, and similar channels in real time. It prevents not only intentional misconduct but also accidental leaks caused by operational errors. The two programs work in tandem: one closely examines the behavior of specific individuals, while the other provides company-wide protection. Combining the two gives us a multi-layered approach that closes security gaps and reduces risk across the company.

*12 SSPM: SaaS Security Posture Management *13 AIP: Azure Information Protection

6 Security for AI

The NEC Group is implementing its Security for AI initiative to establish a foundation for the safe and secure use of AI in both its internal operations and its system integration (SI) and service businesses. Specifically, we are establishing governance through policies, rules, and organizational structures for AI use; management processes for monitoring and assessing compliance; and security infrastructure for managing and mitigating risk.

① Security Landscape and Business Risks Surrounding AI

As AI technologies become more widespread and are increasingly applied to business operations, the security landscape surrounding AI is becoming more complex. At the same time, security issues involving AI are giving rise to tangible business risks, including legal liability and loss of public trust. Reducing these risks has become an urgent priority. To address these risks, the NEC Group is building a framework to protect AI across three areas: governance, management, and security infrastructure.

② Threats to AI Assets and Security Approach

As the use of AI assets expands, a wide range of threats are emerging and becoming increasingly sophisticated. AI assets span both the digital and physical domains. Digital assets include LLMs, training data, RAG, AI agents, A2A, and MCP, while physical assets include existing systems, sensors, machinery, and equipment. Current risks to these assets include prompt injection, information leakage, and inadequate user literacy. Potential future risks include uncontrolled AI agent behavior, excessive autonomy, and shadow AI.

We address these threats systematically through governance, management, and security infrastructure:

- Governance: Establishing policies, rules, and guidelines; improving AI literacy; and establishing the necessary organizational structures
- Management: Monitoring, assessing, and visualizing compliance
- Security infrastructure: AI asset discovery, including shadow AI detection; AI vulnerability assessments; and AI guardrails

③ NEC's Approach to Implementing Security for AI

We are implementing the policies, organizational structures, and mechanisms needed to use and provide AI securely. Through these measures, we support the safe and secure use of AI within the NEC Group and the safe provision of AI to customers.

- Governance

We have defined the fundamental policies and rules required for the secure development, provision, and use of AI and established an AI governance framework.

- Management

We are establishing management processes for security for AI. Drawing on frameworks and guidelines such as the NIST AI RMF,*14 the AI Guidelines for Business, and the EU AI Act, we define compliance requirements for AI security and monitor the security status of AI assets, including AI systems and services used internally or provided to customers, as well as LLMs and AI agents. Through these activities, we have established a continuous cycle of monitoring and improvement. We have also developed guidelines for users, developers, and providers to support the safe and secure use and provision of AI.

- Security Infrastructure

We are implementing technical mechanisms to monitor the security status of AI assets and support their protection and security assessment. These mechanisms include AI asset discovery, AI vulnerability assessments and audits, AI guardrails, and shadow AI detection.

Through these initiatives, we ensure accountability to our customers while enhancing our employees' AI skills and literacy.

④ Alignment with External Guidelines

In the area of governance, we have established policies for the internal use of AI, including AI use, security, and ethics, as well as policies governing the internal provision of AI systems and services. We are also developing and promoting guidelines for users, developers, and providers, together with internal training for AI users and for those who develop and provide AI.

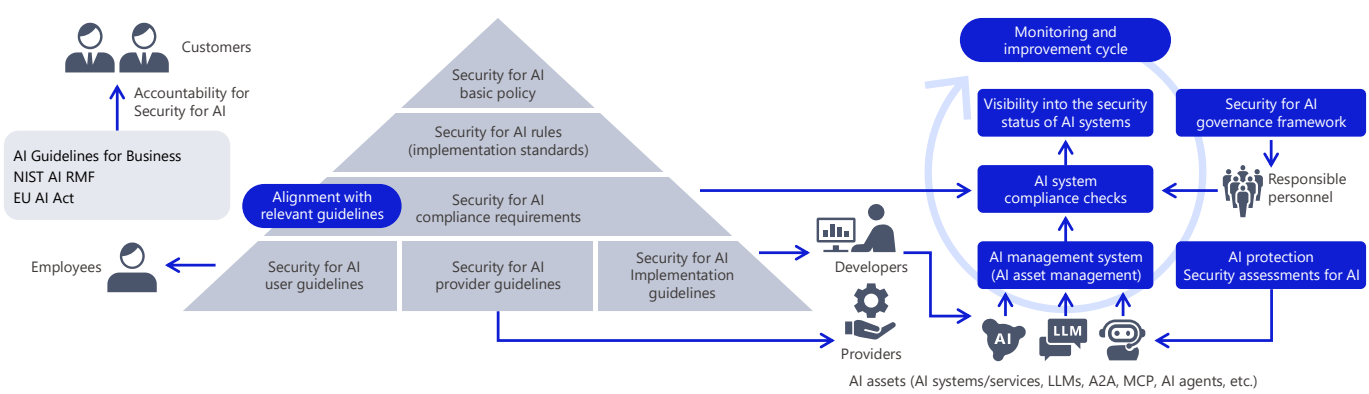
In the area of management, we review the compliance requirements set out in the NIST AI RMF and the AI Guidelines for Business and use them to define NEC's own requirements. We are also aligning these requirements with our existing security framework and moving forward with requirements definition, implementation planning, and the introduction of a system for registering and assessing AI.

In the area of security infrastructure, we evaluate and select AI system protection and verification services, deploy the selected services, and continuously measure their effectiveness.

These activities take into account major external guidelines and regulations, including the NIST AI RMF, the AI Guidelines for Business developed by Japan's Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry, and the EU AI Act. We use the NIST AI RMF as our primary framework, incorporate relevant requirements from the AI Guidelines for Business, and map those requirements to the EU AI Act.

We also take into account the Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems. In line with the principles set out in the Code, we place particular emphasis on risk management throughout the AI lifecycle, transparency, robust security management, content authentication, and responsible information sharing.

Overview of Security for AI



*14 NIST AI RMF: NIST AI Risk Management Framework

5 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

Building information security awareness rests on three core elements: "knowing" (gathering information and taking training), "recognizing" (following rules and spotting risks), and "taking action" (flagging risks and putting countermeasures in place). Equally important is an information security culture that includes risk awareness, and NEC fosters this culture through ongoing education and awareness-raising activities.

① Training on Information Security and Personal Information Protection

The NEC Group offers all employees web-based training (WBT)*1 on information security and personal information protection—including compliance with Japan's My Number system. The training builds employees' knowledge and awareness of information security and personal information protection. In fiscal 2025, the program reached a 98% completion rate and was delivered in seven languages at our overseas sites. Content is updated every year to keep pace with the latest security threats. As part of onboarding for new graduates and mid-career hires, we also deliver targeted training that highlights the shift from student to professional life and the differences between previous employers and NEC.

② 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.

③ 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 run a range of internal programs to develop people with the necessary skills. To ensure sound handling of critical information management, personal information protection, security proposal and implementation, and incident response, we deploy certified professionals across the organization—including CISSPs,*2 Registered Information Security Specialists (RISS), and Protection of Individual Information Persons (a Japanese personal information protection certification)—strengthening our overall capability.

*1 WBT: Web Based Training
*2 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.

① 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 cumulative total of 98 employees have completed this program and are now involved in delivering professional security services.

② 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 2025, over 10 employees participated, bringing the cumulative total number of participants to 124. 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.

③ 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, a cumulative total of more than 1,500 employees—including mainly sales representatives and systems engineers—successfully completed the program in fiscal 2025.

④ 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)*3 competition called the NEC Security Skill Challenge. In fiscal 2025, more than 1,300 employees voluntarily participated, bringing the cumulative total number of participants since the program began in 2015 to over 10,000.

⑤ 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 cumulative total of 15,000 participants completing the training in fiscal 2025.

⑥ Holders of Advanced Security Technology Qualifications

As proof of the advanced information security skills needed to provide optimal solutions to our customers, we encourage employees who work with customers to obtain recognized security certifications. Through internal seminars and study groups, we are expanding the number of employees who hold international certifications such as CISSP and Japan's Registered Information Security Specialist (RISS).

Starting in fiscal 2024, to advance our security talent and broaden the talent base, we added international certifications such as CCSP, CISA, CEH, and CCT*4. In particular, for CISSP we entered into a strategic partnership with ISC2, the certifying body, to promote CISSP certification and develop professionals who combine advanced technical skills with the ability to assess risk from a business perspective.

The NEC Group now has a total of 670 CISSP holders. In fiscal 2024, we also entered into a strategic partnership with ISACA, the certifying body, to strengthen the development of professionals well-versed in risk management and IT governance who can apply information security management across a broader scope. Through this partnership, we aim to further deepen this expertise across the group.

Through this partnership, we also deliver training for CISA and CISM*5 certification to NEC Group employees to develop specialized talent. To date, the cumulative total of ISACA-certified professionals in the NEC Group has exceeded 100, steadily expanding our talent base for both audit and management aspects of information security.

In addition, we plan to develop authorized trainers from among NEC Group security specialists and offer training to our customers that combines practical expertise with the extensive field-based knowledge of system implementation.

Overview of Cybersecurity Talent Management

Developing and managing personnel who can create and enhance business value through the practice of Security by Design and appropriate security implementation

*3 CTF: Capture the Flag
*4 CCSP: Certified Cloud Security Professional, CISA: Certified Information Systems Auditor, CEH: Certified Ethical Hacker, CCT: Certified Cybersecurity Technician
*5 CISM: Certified Information Security Manager

6 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 undergo third-party assessments against NIST CSF*1 1.1 and, separately, the new elements introduced in NIST CSF 2.0, particularly the GOVERN function.

Our approach reflects the view that a globally consistent stance on cybersecurity risk is essential to business continuity. AI helps us monitor and analyze cyberattacks on a daily basis, assess the situation, and refine our monitoring and operational processes accordingly. We also track relevant products, services, and market trends, and gauge their fit for our internal IT environment through PoC*2 evaluations and internal environment reviews. From these findings, we identify the safeguards required going forward and estimate their scope, effectiveness, and cost. An annual implementation plan drawn from this work is then approved by the CISO before being rolled out.

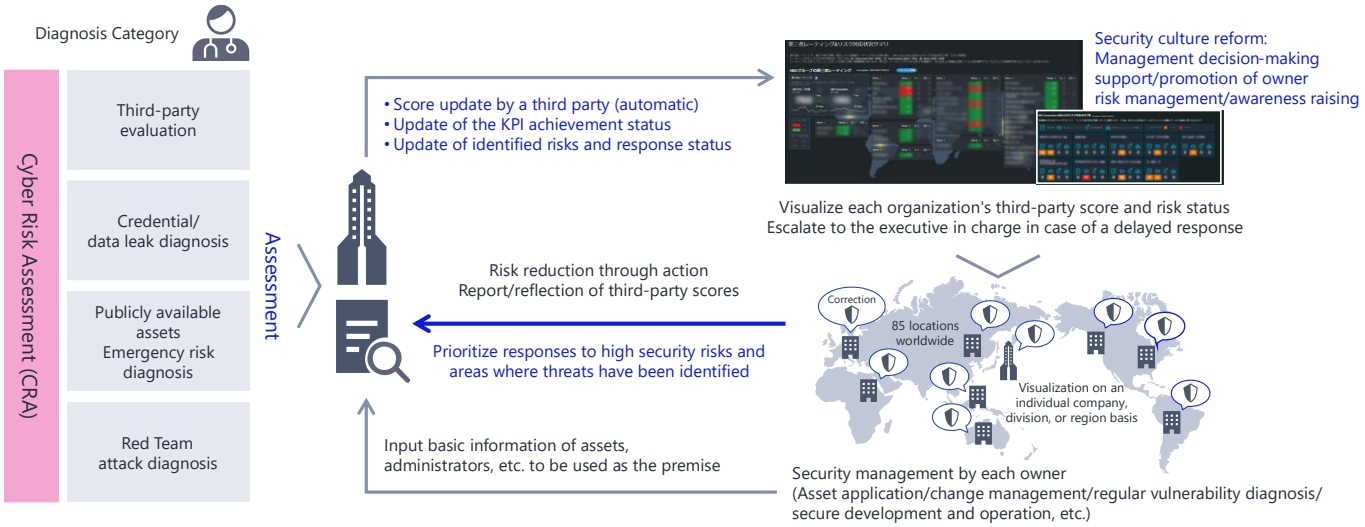
Within the NEC Group, we implement measures based on comprehensive cyber defense concepts, such as our Cyber Defense Center (CDC)*3. The main areas of focus for these efforts are outlined in the following sections 1 through 5.

This external recognition included high marks for our approach and disclosure practices in the Cyber Index Corporate Survey 2025, conducted by the Information Technology Federation of Japan. NEC earned the survey's top "Two Stars" rating for the fourth consecutive year, along with several other awards.

① Cyber Risk Assessment by the Red Team

The NEC Group's Red Team*4 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 globally through third-party external and internal penetration assessments conducted from an attacker's perspective, 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 established a risk management cycle in which delays in addressing risks automatically trigger escalation to top management, thereby encouraging proactive action.

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 PoC: Proof of Concept, a pilot project conducted to demonstrate the feasibility and potential of a new concept. *3 CDC: Cyber Defense Centre

*4 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

② Generation and Use of Threat Intelligence

The Cyber Threat Intelligence (CTI)*5 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)*6 platform, a unique CSIRT-developed network detection and response (NDR)*7 system, and an integrated log analysis platform, we conduct hunting for 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.

③ 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.

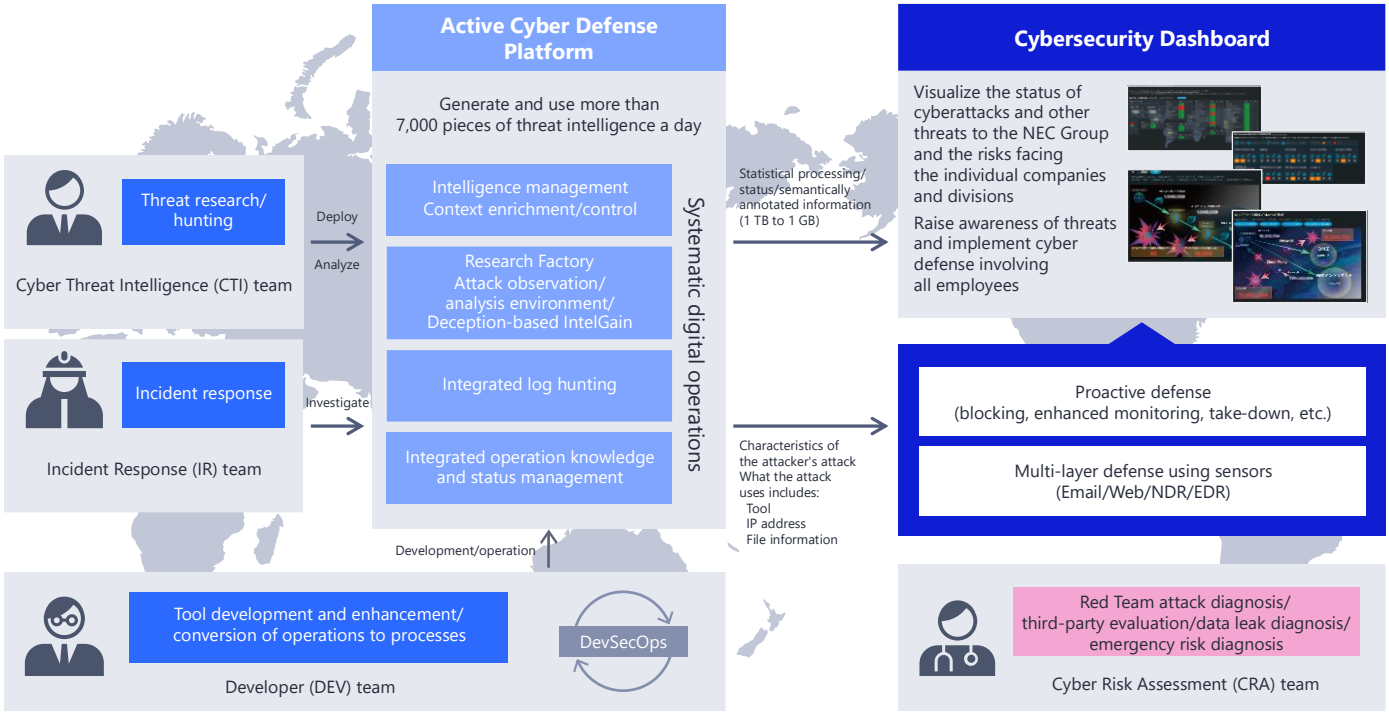
During major events such as Expo 2025 Osaka, Kansai, Japan, held last fiscal year, connected companies face heightened cyberattack risk. NEC responded with a range of safeguards: cyberattack response exercises with NISC, agreed special escalation rules, a security posture set up for the duration of the event, and stepped-up priority monitoring and threat intelligence run through our CSIRT/SOC.

④ 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

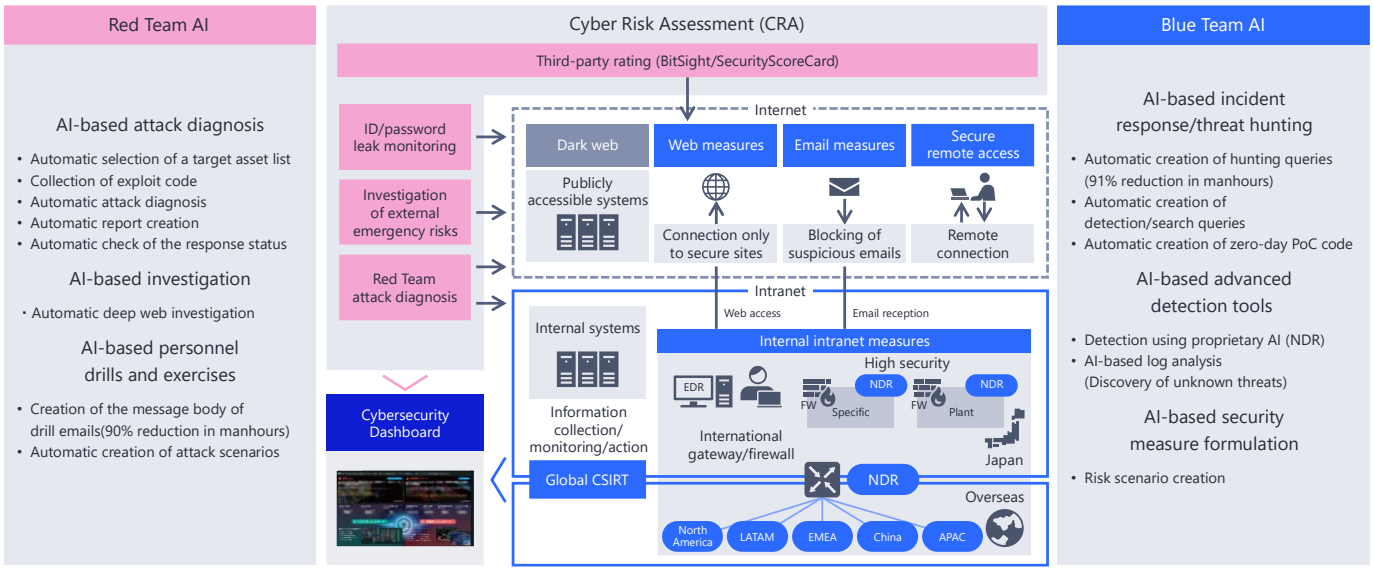


*5 CTI: Cyber Threat Intelligence
*6 EDR: Endpoint Detection and Response
*7 NDR: Network Detection and Response

⑤ 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.
AI, including generative AI, is applied across a wide range of work—cyber risk assessments, threat intelligence generation and use, NDR-based anomaly detection, incident investigation, and phishing email training. Together with our in-house research labs, we are also building an Agentic AI system for attack diagnosis to make this work faster, more accurate, and more automated.

Use of generative AI in cyber defense

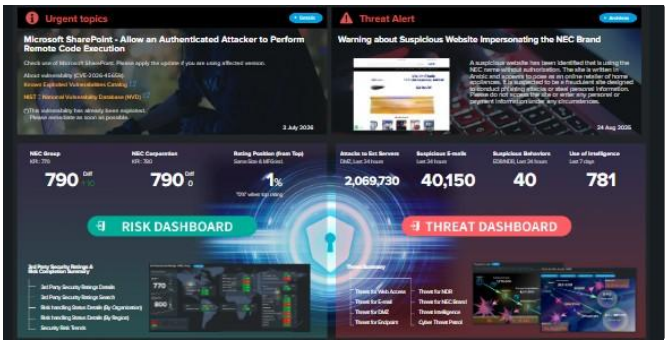


2 Security culture transformation using cybersecurity dashboards

NEC has launched a Cybersecurity Dashboard available to all employees. It brings together the state of cyberattacks against the NEC Group, threat intelligence collected by the CTI team, security-risk conditions of each company and division identified through cyber risk assessments, and the performance of our safeguards. Seeing the real picture and feeling the risks firsthand helps every employee take action and sharpens security awareness across the organization.
Development of the dashboard continues in agile cycles. A recent addition uses generative AI to dynamically and automatically curate security news from Japan and abroad, and to stream music inspired by that news. By presenting security news in an accessible and engaging format for all employees, we are fostering a company-wide culture of security.
In addition, digital signage displaying the Security Executive Dashboard, which leverages AI extensively in its images, video, music, audio, and text content, enables executives to grasp the internal and external security situation at a glance.
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.

Security Executive Dashboard

Cybersecurity Dashboard



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.

① Critical Information Management and Protection, and Security Resilience

The NEC Group works on critical information management that balances security with usability, on prevention of information leakage through data security, and on strengthening security resilience through incident response drills and data backups.
As security risks continue to grow, many customers have asked us to share these practices and are drawing on them as a reference model for sustainable, data-driven management. (See p.6 "Critical Information Management," p.10 "Data Security," and p.14 "Global Cyberattack Countermeasures.")

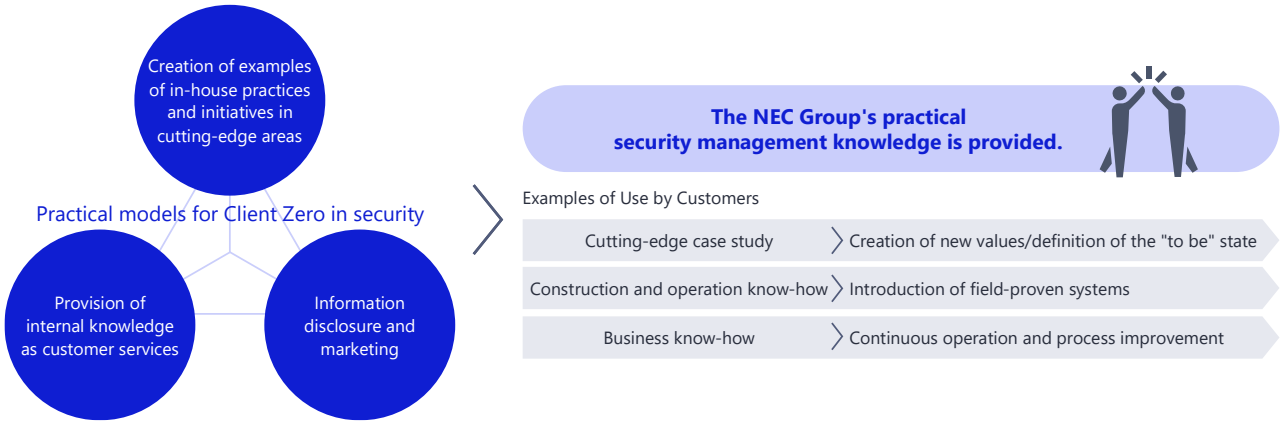
② AI and Security

The NEC Group pursues two complementary agendas: "Security for AI" (p.11), which enables the safe use of AI, and "AI for Security," which applies AI to strengthen cybersecurity. In our internal operations, "AI for Security" makes our safeguards faster, more automated, and higher in quality, while giving us hands-on know-how as Security Client Zero.
We present these latest case studies to customers, exchange views with external analysts, and conduct surveys on needs and other research. 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 "Global Research and Business Development to 'MAKE JAPAN CYBER SECURE'" on pages 27-29.)

③ Examples of Practical Security Operation

With 120,000 employees across the NEC Group, ensuring a safe and secure internal environment that supports their day-to-day work is directly tied to NEC's management priorities. Beyond defending against cyberattacks, we run and continuously refine global security governance and audit programs, critical information management and protection, and a Zero Trust security foundation that now includes AI platforms. These are the same practical playbooks we make available to our customers.

Client Zero Initiatives in Security



*1 DX implementation initiative and success scenario provided under NEC BluStellar, a value creation model for leading customers to the future
Our security services are offered under the theme of "Security Management Reform that Continues to Support Business Growth."

7 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.

① Contract Management

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

② Subcontracting Management

The basic agreement stipulates that business partners may not subcontract work to other companies unless they obtain written permission in advance from the organization that outsourced the work to them. Additionally, we require the submission of a subcontractor verification and organizational structure confirmation form to clearly outline the project's organizational framework and management structure for each individual project.

③ Staff Management

NEC has established a set of guidelines titled "Basic Rules for Customer Related Work," which outlines the measures that workers undertaking outsourced tasks must follow. We require workers to submit a formal pledge to their own company that they will adhere to these guidelines to ensure these measures are strictly implemented.

④ Information Management

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

⑤ 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.

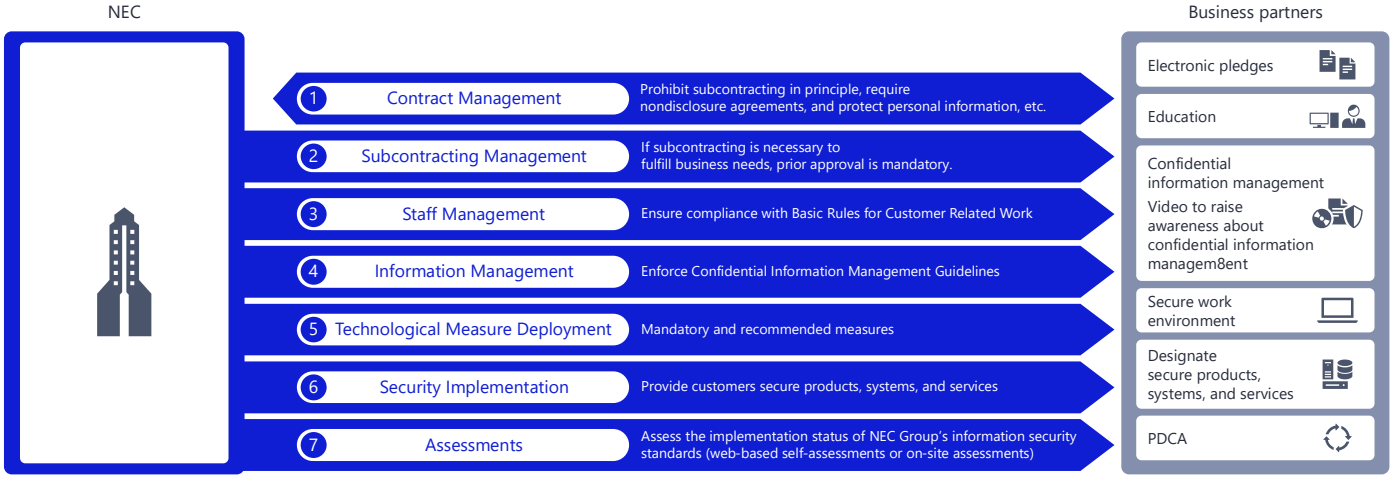
⑥ Security Implementation

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.

⑦ 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

① 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 precautions regarding information security and personal information protection, and also provide cybersecurity education and awareness-raising activities to help prevent information security incidents. We also hold seminars for our overseas business partners on an as-needed basis.

② 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.

③ 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.

④ 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.

① Document-based and On-site Assessments

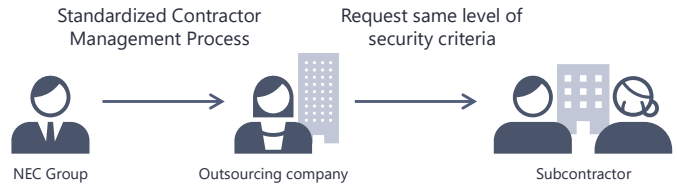
We conduct document-based assessments for approximately 1,800 companies that do business with NEC.
Business partners run self-assessments of their security posture, and the results are shared as real-time feedback through a web-based system. For business partners with high transaction volumes, we also conduct in-person or remote assessments.

In fiscal 2025, these assessments covered 220 companies and were carried out by approximately 70 NEC assessors.

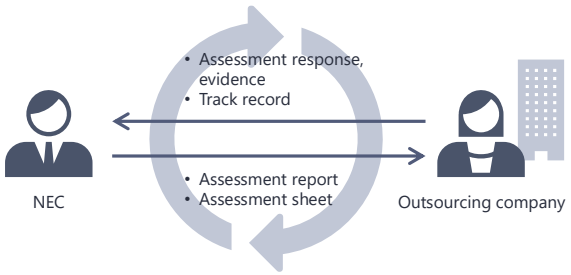
② Information Security Assessment Sheet

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.
From fiscal 2022 through fiscal 2025, we held seminars in China, India, and Vietnam. We also began document-based and on-site assessments for business partners engaged in offshore development, using criteria based on NIST SP 800-171.
For our overseas business partners, we will continue to hold these seminars to further strengthen security across the global supply chain.

8 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

① 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 prevent information security incidents caused by product, system, and service vulnerabilities, misconfigurations, and system failures, cybersecurity managers serve as a bridge between the division that manages cybersecurity and each business division. They promote the implementation of security measures and support on-the-ground security operations.

Approximately 750 cybersecurity managers have been assigned to placements throughout all of our business divisions. These managers participate in fortnightly meetings and make use of security communities to coordinate between the division managing cybersecurity and each business division through biweekly meetings and security communities.

The role of the cybersecurity manager and the security implementation processes in each division are defined in the Cybersecurity Management Rules, which also comprise part of the NEC Group Management Policy.

The Cybersecurity Management Rules were updated in fiscal 2025 adding clear guidelines regarding NEC's responsibilities as a system integrator (SIer) and clarifying the scope of responsibility with customers during the proposal and development phases with the goal of mitigating business risks in the event of a security incident. In addition, deployment of the Cybersecurity Management Rules is complete at NEC's wholly owned domestic subsidiaries, and we have begun the work needed to ensure the revised content regarding business risk mitigation is also implemented.

② Key security implementation efforts

Based on the Security by Design (SBD) concept, NEC embeds security throughout the entire process—from planning and proposal, through implementation, to operation and maintenance. Embedding security early in system development brings with it a myriad of benefits, including lower costs, on-time delivery, and the development of highly maintainable systems. For customer system environments in particular, we prioritize conducting risk assessments at the requirements definition phase to identify and implement optimal security controls early on.

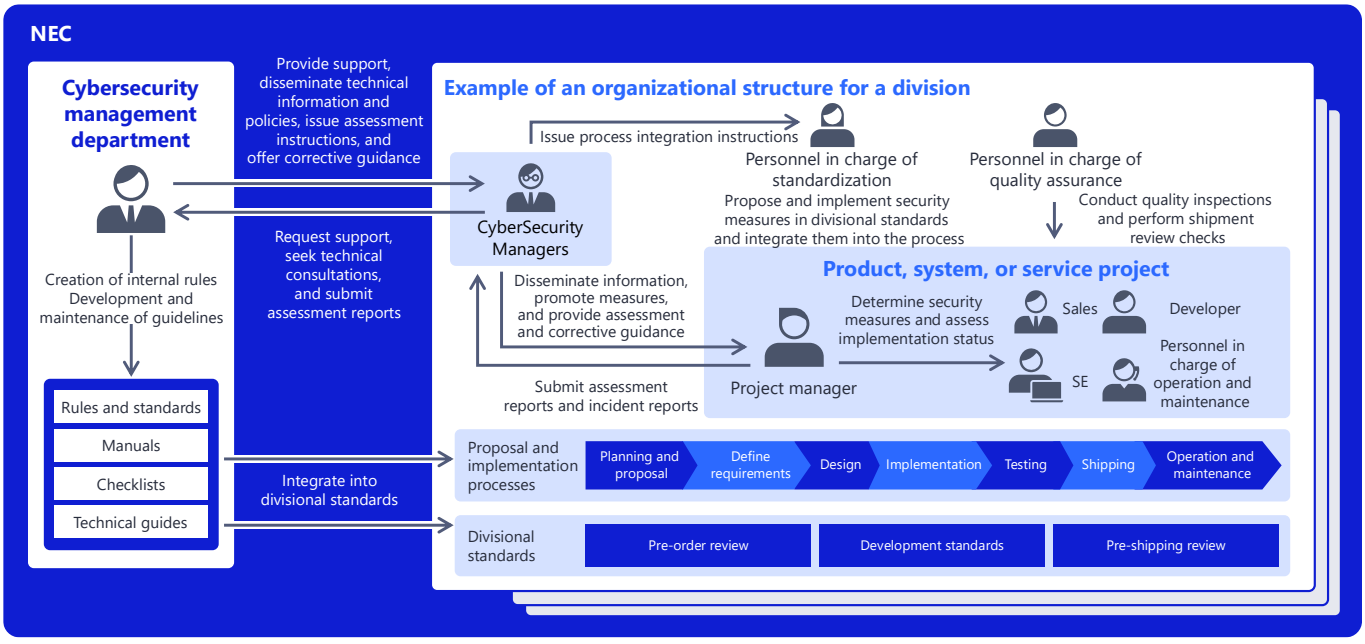
NEC has also established the "Cybersecurity Implementation Standard" to serve as the baseline for cybersecurity requirements that must be considered when enforcing security implementations. This standard specifies strict security requirements, taking into account not only the international security standards such as ISO/IEC 15408 and ISO/IEC 27001 but also the security standards of government agencies and industry guidelines.

Moreover, we issue and deploy guidelines as needed to implement security measures for the latest technologies, ensuring that the measures can be introduced securely to the systems, products, and services we develop and operate.

Going forward, we will apply frontier AI to strengthen vulnerability detection and response capabilities before shipment in order to deliver products, systems, and services that are even safer and more reliable for our customers.

In the development of products, systems, and services, we use a checklist to verify that security tasks are performed in each phase. Based on this checklist, business projects are managed through the "Cybersecurity Checklist Management System," which was built to centrally manage and visualize the implementation status of security measures, enabling efficient assessment and monitoring of security controls.

Security Implementation Process



In addition, the Cyber Security Departments use the aggregated information to roll out more effective programs and to strengthen governance in the implementation of security measures.
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. Built on agile development, the Vulnerability Management System supports flexible expansion of functionality and 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 designed to share cybersecurity threat information swiftly with each business division—including attack methods, incident cases, vulnerability risk indicators, and indicators for security measures—and is used to help assess business risks.
In addition, NEC has established a Product Security Incident Response Team (PSIRT) to collect and address vulnerability information related to NEC Group products. We publish our vulnerability disclosure policy, provide a contact point for external reports, operate a contributor page, and act as a CVE Numbering Authority (CNA)*1. These measures enable the proper handling of both undisclosed vulnerability information for our own products—including those from group companies—and vulnerability information affecting customer systems.
In addition, to facilitate information-sharing among NEC Group companies engaged in manufacturing, we established the NEC Group PSIRT Community and work to ensure that PSIRT activities function effectively throughout the entire NEC Group.
As a result of our efforts, there were no material data breaches or information leaks that could significantly affect our business performance or outlook in fiscal 2025.

③ 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.

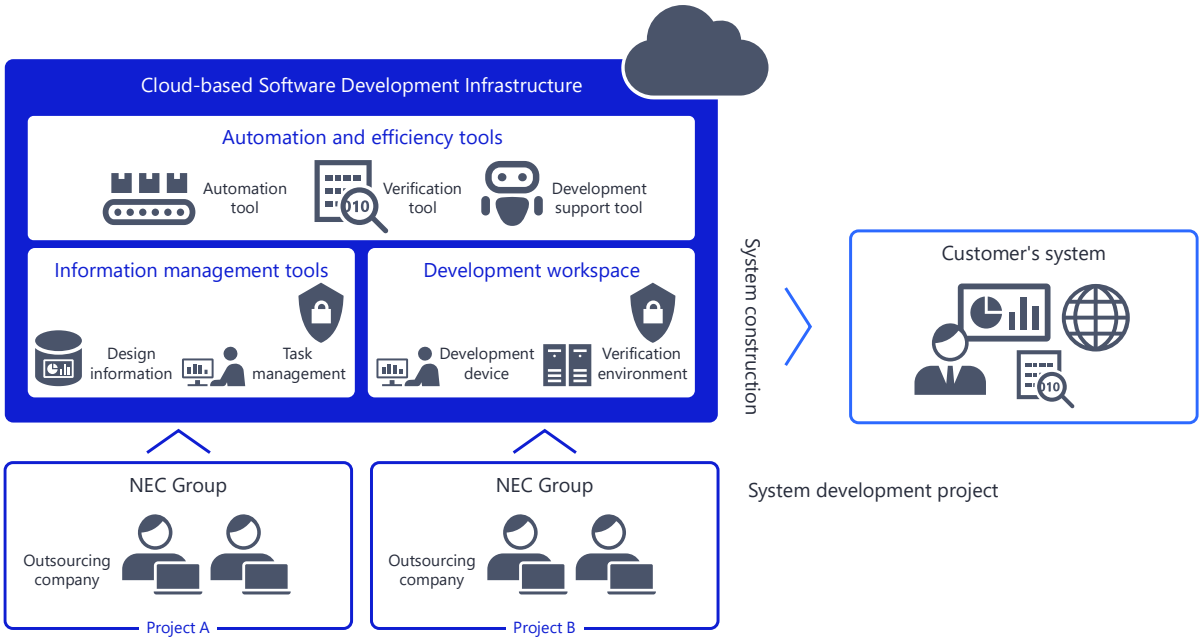
④ Security Enhancement for Hardware Products

We carry out security-conscious design and implementation across the entire development lifecycle of our hardware products—from planning, design, and implementation through evaluation and maintenance.
In addition to securing the products themselves, we have set security standards for our development environments, and we are working to further strengthen our platform for secure product development.
We have also begun pursuing certification under the Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements (JC-STAR), Japan's certification scheme for IoT products.

⑤ Security Enhancement at Manufacturing Sites

At our manufacturing sites, we set quantitative targets based on third-party risk assessments carried out in accordance with the Ministry of Economy, Trade and Industry (METI) Factory Security Guidelines, and our security measures are implemented accordingly.
To prepare our factories for cyberattacks, we conduct regular cyber BCP drills, while striving to improve risk visibility in order to achieve data-driven cybersecurity.

Cloud-based Software Development Infrastructure



*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

9 NEC's Cybersecurity Strategy

In response to intensifying cyberattacks and evolving cybersecurity regulations, NEC is leveraging intelligence and AI to help "MAKE JAPAN CYBER SECURE".

The year 2025 marked a major turning point for Japan's cybersecurity policy. During the 217th Ordinary Session of the Diet, which began in January, the Act on the Prevention of Damage Caused by Unauthorized Acts Targeting Critical Computers (Cyber Response Capability Enhancement Act) and its accompanying Cyber Response Capability Enhancement Implementation Act were passed. With these laws in place, work began to build and reinforce the framework for Active Cyber Defense (ACD).
The Cyber Response Capability Enhancement Act and its accompanying implementation legislation were brought into force in stages. In July 2025, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) was reorganized into the National Cybersecurity Office (NCO), which serves as the central coordinating body for various cybersecurity initiatives. In April 2026, the Cyber Communications Information Supervision Committee was established to help ensure the appropriate use of communications information.
Access neutralization measures will become possible in October. In addition, as part of efforts to strengthen public-private collaboration, Special Critical Infrastructure Operators will be required to submit notifications regarding Designated Critical Computers and report cybersecurity incidents when they occur. In December 2025, the Cybersecurity Strategy was updated for the first time in four years, setting out a strategy to defend against and deter increasingly serious cyber threats through stronger cybersecurity and resilience across society.
However, ransomware attacks and other cyberattacks against businesses continue to increase significantly in both scale and sophistication. In 2025, there were multiple incidents in which companies were forced to suspend operations for several months due to cyberattacks believed to have originated overseas. The impact of cyberattacks extends beyond the directly targeted company to the supply chain, and cyberattacks on a single company can damage the businesses and brands of its business partners.
Cyberattacks have become industrialized, with damages estimated*1 to reach $10.5 trillion in 2025 and $12.2 trillion in 2031. These amounts would rank behind only the GDPs of the United States and China and more than twice Japan's nominal GDP of $4.3 trillion*2. The Top 10 Information Security Threats 2026 [Organization Edition]*3, published by the Information-technology Promotion Agency (IPA), once again lists "damages caused by ransomware attacks," "attacks targeting supply chains and subcontractors," and "cyberattacks stemming from geopolitical risks (including information warfare)," underscoring that the safety of Japan's cyberspace remains under sustained threat.
"Cyber risks associated with the use of AI" was selected for the first time. The listing highlights both the risk of external attacks that exploit vulnerabilities in AI-based systems and the possibility that AI misuse could make attacks easier to carry out.
In response to these government initiatives to strengthen Japan's cybersecurity framework and address the deteriorating conditions surrounding cyberspace, NEC has adopted the mission of "MAKE JAPAN CYBER SECURE" and is working to strengthen its cybersecurity business. In May 2025, NEC entered into a Memorandum of Understanding (MOU)*4 with KDDI Corporation to begin exploring collaboration in the cybersecurity field. In October, the two companies established the joint venture United Cyber Force Corporation*5 to explore business opportunities that leverage the strengths of both companies while further strengthening cybersecurity.

Next-generation cybersecurity service CyIOC to "MAKE JAPAN CYBER SECURE"

CyIOC

*1 Cybersecurity Ventures, Cybercrime To Cost The World $12.2 Trillion Annually By 2031, https://cybersecurityventures.com/official-cybercrime-report-2025/
*2 International Monetary Fund, GDP, current prices, https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWOR
*3 Information-technology Promotion Agency, Japan (IPA), Top 10 Information Security Threats 2026, https://www.ipa.go.jp/security/10threats/10threats2026.html
*4 KDDI and NEC Sign Memorandum of Understanding for Collaboration Toward Establishing Japan's Largest Cybersecurity Business, https://jpn.nec.com/press/202505/20250508_02.html

In November 2025, we launched the next-generation cybersecurity service, CyIOC (pronounced 'sigh-ock'). The service is benchmarked against NIST SP 800-171,*7 the security standard for handling Controlled Unclassified Information (CUI) developed by the U.S. National Institute of Standards and Technology (NIST*6). At its core is the Cyber Intelligence & Operation Center, comprising a newly established facility in Japan and upgraded facilities in the United States. Leveraging NEC's proprietary threat intelligence, the service provides comprehensive support ranging from the early detection of cyberattack indicators to proactive defense and incident response.

In 2026, the government is taking further steps to enhance the cybersecurity framework. In light of the recent series of cyberattacks on medical institutions, adding the medical sector to the list of designated critical infrastructure businesses is under consideration.

For Critical Infrastructure Operators, there are also plans to further strengthen cybersecurity measures within each sector and to establish Unified Standards for Critical Infrastructure to ensure that cybersecurity measures are implemented consistently across sectors and operators.

In addition, the Supply Chain Security (SCS) Assessment Scheme, aimed at strengthening supply chains, will be launched during fiscal 2026. Under this scheme, all companies within a supply chain are expected to be able to easily and appropriately determine the security measures appropriate to their position within the supply chain. Furthermore, the National Intelligence Council Establishment Bill, submitted during the 221st Special Session of the Diet that began in February, provides for the establishment of a National Intelligence Council to investigate and deliberate on matters related to national security, as well as the reorganization of the Cabinet Intelligence and Research Office into the National Intelligence Agency.

Building on its longstanding track record of supporting Japan's critical infrastructure through submarine cables, space and defense businesses, and mission-critical systems, and contributing to the nation's safety and security, NEC aims to Make Japan Cyber Secure using technology developed in Japan.

The intelligence available within Japan alone is not enough to Make Japan Cyber Secure. We need to connect directly with overseas sources to gather foreign intelligence. As the Cybersecurity Strategy also notes, Japan relies heavily on overseas technologies in many areas of cybersecurity. Creating an environment that can sustainably develop the talent and technologies needed for cyber response within Japan is therefore an urgent priority. Leveraging homegrown cybersecurity technologies and AI is also important. Above all, an uninterrupted 24/7/365 framework is essential to Make Japan Cyber Secure.

To support this goal, we are expanding the CyIOC service to obtain overseas intelligence directly and protect Japanese companies both in Japan and abroad. We aim to open a European base in April 2027 and complete a follow-the-sun operating model. We will also enhance CyIOC with NEC cotomi, NEC's proprietary AI, selected for trial use in the Government AI initiative.

By combining our proprietary intelligence with NEC cotomi and our cybersecurity technologies, we will expand our cybersecurity business globally. Through these efforts, we will help Make Japan Cyber Secure—including by protecting Japanese companies operating overseas—and contribute to building a safe and secure information society.

Collaboration with Security-Related Organizations

Technology and intelligence alone are not enough to Make Japan Cyber Secure. Institutions and legislation that enable these resources to be used effectively and appropriate countermeasures to be implemented are also essential. In addition to providing cybersecurity services, NEC collaborates with security-related organizations in Japan and overseas and submits policy recommendations to the Cabinet Secretariat and relevant ministries through domestic organizations and industry associations.

Noboru Nakatani serves as Corporate Executive Vice President, CSO, Managing Director of the Cyber Security Division, and Chairperson of NEC Security, Ltd. He has extensive cybersecurity experience in both the public and private sectors. His previous roles include Senior Assistant Director of the Cybercrime Division of the National Police Agency, Director of Information Systems and Technology and Chief Information Security Officer at INTERPOL's General Secretariat headquarters, and Chief Trust and Safety Officer at a private company. He is also Representative Director of the Japan Cybercrime Control Center (JC3*1).

He also participates as an expert in the Study Group on Enhancing the Reliability of Cybersecurity Service Providers under Working Group 3 (Industry Promotion and Human Resource Development) of METI's Study Group on Industrial Cybersecurity. In addition, he participates in the Strategic Field Subcommittees of the Growth Strategy Council of Japan, including the Digital and Cybersecurity Working Group and the Information and Communications Growth Strategy Public-Private Council.

*1 Japan Cybercrime Control Center

*5 KDDI and NEC Establish Joint Venture to Strengthen Cybersecurity Field, https://jpn.nec.com/press/202511/20251120_01.html
*6 National Institute of Standards and Technology
*7 CyIOC for Government, a separate non-public facility, is benchmarked against NIST SP 800-53, the security standard for the information systems of U.S. federal government agencies.

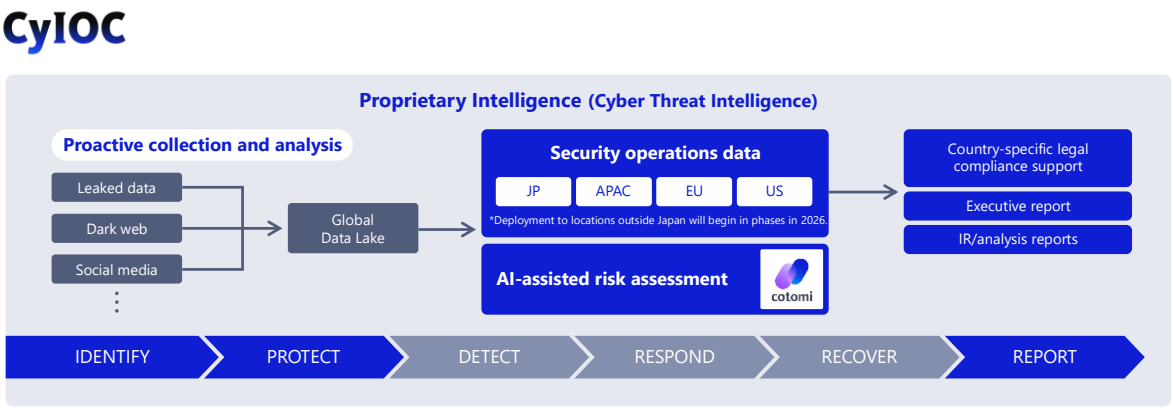
10 How NEC Can Support You

This section introduces the support framework provided by the NEC Group to help customers advance DX safely, securely, and sustainably and address cybersecurity risks from a management perspective.

While many companies are strengthening their cybersecurity measures, both the frequency and impact of security incidents continue to rise. The number of reported ransomware incidents has increased approximately fivefold since the second half of 2020, with organizations of all sizes suffering increasing damage that threatens business continuity. This trend reflects the rapid expansion of business DX and cloud use, which has dispersed the IT assets and data that companies must protect across internal and external environments and expanded the attack surface.
As seen in the incidents reported in 2025 involving a major beverage manufacturer and a logistics company, attackers are increasingly exploiting vulnerabilities and misconfigurations in publicly exposed IT assets to gain an initial foothold and expand the damage. The government is also moving to establish a framework for Active Cyber Defense in response to intensifying cyberattacks, with the aim of protecting the foundations of people's lives and economic activity and the safety of the nation and its people. More advanced security measures are now required, particularly of Special Critical Infrastructure Operators responsible for critical infrastructure.
To achieve this, organizations must establish their own security frameworks and continuously visualize and monitor “what is happening now” and “how extensively measures have been implemented” across their systems. When security measures are optimized only in silos, it becomes difficult to detect warning signs and set priorities, allowing risks to remain hidden. Continuous monitoring and rapid response powered by threat intelligence are therefore essential. To address these challenges, NEC helps customers advance DX in security operations through CyIOC, its next-generation cybersecurity service built on proprietary intelligence and AI.

NEC's Next-Generation Cybersecurity Service CyIOC

Guided by the mission to "MAKE JAPAN CYBER SECURE", CyIOC is a next-generation cybersecurity service that combines NEC's proprietary intelligence and AI technologies to protect companies operating in Japan and globally from these threats.



From Intelligence to Reporting:
A dedicated team collects threat intelligence on dark web activity and geopolitical risks and provides proactive defense and AI-driven reporting.

Responding to Increasingly Sophisticated Cyberattacks:
With CyIOC’s proactive defense, we preload defense sensors worldwide with rules derived from proprietary intelligence and use advanced monitoring based on attackers’ tactics, techniques, and procedures (TTPs) to detect sophisticated attacks that are difficult to detect with individual devices alone.

Value Enhancement Through AI:
Approximately 90% of alerts are automatically classified through AI-driven analysis, while the remaining approximately 10% are reviewed by experienced analysts. This ensures that only truly critical alerts—approximately 0.02% of the total—are reported to customers, dramatically improving the quality and efficiency of decision-making.

Benchmarked Against U.S. Standards:
To help organizations and companies launch or improve their cybersecurity programs, NEC established the Cyber Intelligence & Operation Center, benchmarked against NIST SP 800-53 published by the U.S. National Institute of Standards and Technology (NIST). It serves as the command center for CyIOC. We have established a monitoring center that meets rigorous global security standards and protects data in accordance with applicable laws and regulations.

Global Deployment (Starting in FY2027):
We deploy highly skilled personnel at locations worldwide to provide follow-the-sun monitoring 24 hours a day, 365 days a year. By combining uninterrupted monitoring and response with intelligence and AI, we deliver Japan-quality security measures worldwide while accounting for local laws, languages, cultures, and time-zone differences. Information on suspicious access detected at each location is fed back to further enhance threat intelligence.

Support for Reporting to Relevant Authorities (Starting in FY2027):
The Cyber Response Capability Enhancement Act,*1 which aims to establish a framework for protecting the nation and its people from cyberattacks, mandates that “when the cybersecurity of a Designated Critical Computer has been compromised, or when certain events that could cause such compromise are identified, the operator must report the matter and certain prescribed information to the competent Minister and the Prime Minister.” CyIOC also supports reporting to these authorities based on the information it collects and the analyses it produces.

*1 Source: https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf

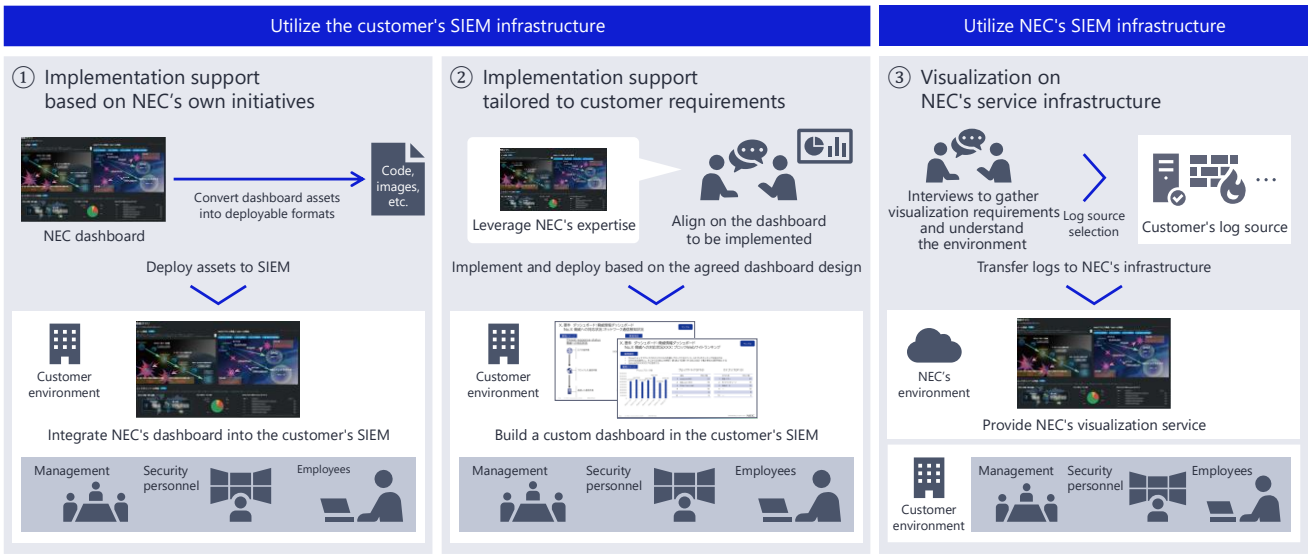
Value Creation Through Client Zero

NEC has launched NEC BluStellar as a new value creation model for customers. Drawing on proven, advanced cross-industry expertise and NEC's technologies, the model addresses social and management challenges and guides customers toward the future. NEC also addresses customer challenges through NEC BluStellar Scenario, a value creation scenario that combines consulting, products, and services.
This section introduces several representative examples of our Client Zero initiatives, one element of the value delivered through NEC BluStellar Scenario. NEC provides end-to-end support for addressing security challenges—from visualizing security risks and clarifying issues through operations and monitoring—including proposals that incorporate the added value NEC delivers through CyIOC, described in the previous section, and Client Zero.

1 Cybersecurity Dashboards

Cybersecurity dashboards play a key role in visualization and monitoring. NEC proposes dashboards optimized for two purposes: operational monitoring and response, and management decision-making and process transformation.
The first is optimized for information security monitoring, including checking the implementation status of security measures, monitoring incidents, analyzing logs, and conducting investigations.
The second is designed to make management risks easier to visualize, including the number and percentage of patches and countermeasures not yet implemented and the number of suspected cyberattacks.
Together, these two cybersecurity dashboards give customers a comprehensive understanding of the overall status of their company's security measures and current risks and help identify and address areas where existing solutions have been optimized in isolation.

Cybersecurity Dashboard Menu

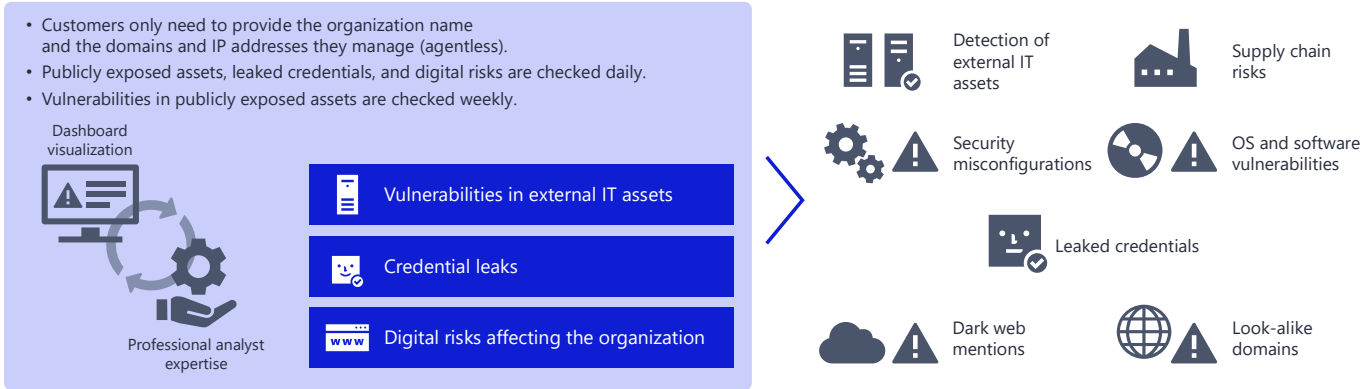


2 External IT Asset Risk Visualization Service

We examine a company's externally exposed IT assets, such as VPN devices and cloud services, and visualize risk information, including misconfigurations and vulnerabilities, in real time through a dashboard. NEC Group security experts assess the severity and impact of identified risks and recommend appropriate responses. This enables even organizations with limited security personnel to quickly establish an effective risk response framework.

External IT Asset Risk Visualization Service

Drawing on reliable intelligence sources and the advanced expertise of professional analysts, we provide comprehensive support for proactive cyber defense against the threats and risks facing companies.



3 CISO Management Support Service

Drawing on NEC's expertise in cyber threat analysis and related technologies, we deliver highly accurate cyber threat intelligence to support management decision-making—including information on threats to the customer's own assets as well as incident trends within the customer's industry.
Furthermore, we assess how effectively threats are being addressed and evaluate organizational maturity. We support the development of strategies and plans for achieving the customer's target security level and act as the PMO to drive projects through both the implementation and operational phases.

CISO Management Support Service

To help advance security management from the perspective of executives and security leaders, we offer long-term support services addressing the common challenges faced by our customers.

A sample of the available support

4 Critical Information Protection Solution

As cloud adoption expands and economic security legislation advances, frameworks for defining, managing, and protecting critical information have become essential. NEC provides end-to-end support—from risk assessment and basic concept development to the design and implementation of Microsoft Purview (sensitivity labels, DLP, and IRM), file encryption using InfoCage FileShell, and improved usability through AI-based automated labeling.
By integrating governance and IT measures, we provide visibility into how information is managed, reduce the risk of information leakage, and help establish a reporting framework for executives.

Since April 2024, we have consolidated specialized personnel within NEC Security, Ltd. and strengthened our organizational structure to expand the cybersecurity business. Going forward, we will further enhance our ability to develop and deliver solutions using cutting-edge cybersecurity technologies and accelerate the growth of our cybersecurity business supporting government agencies, critical infrastructure operators, and companies in protecting against cyberattacks. In November 2025, we also launched CyIOC (pronounced "sigh-ock"), our next-generation cybersecurity service, to provide customers with even stronger support against cyberattacks.

11 Global Research and Business Development to “MAKE JAPAN CYBER SECURE”

NEC leverages AI technologies to improve the efficiency and effectiveness of efforts to build systems correctly, maintain stable operations, and protect against attacks, helping safeguard social infrastructure and organizations from cyber threats.

1 Research Concept

Through agentic AI that supports Security by Design, NEC aims to help build systems correctly, maintain stable operations, and protect against attacks. To achieve this, NEC is advancing technology development and commercialization through its Research & Development Division in Japan, together with NEC Laboratories Europe in Germany and the Israel Research Center (IRC). This section highlights recent R&D achievements from these research organizations in Japan and overseas.

AI-Driven Security Technology Development Concept

2 NEC's Research Laboratories in Japan: Security Management Agentic AI

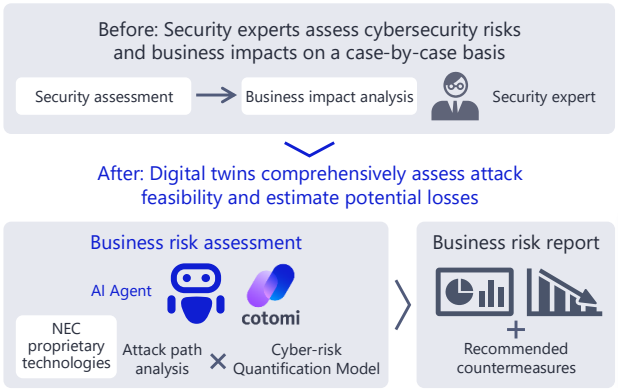
As part of its Security Management Agentic AI initiatives, NEC's research laboratories in Japan are advancing research and development on business impact estimation technology. To maintain stable operations, organizations must determine which security measures should be prioritized within the constraints of limited budgets and personnel resources. By identifying the relationships between systems that require security measures and the business operations they support, and by estimating potential business impacts, such as the effects of system outages on business activities and losses resulting from personal data breaches, this technology enables organizations to prioritize security investments more effectively.

However, estimating business impacts and potential losses requires specialized expertise, including a thorough understanding of an organization's systems and business operations, as well as the ability to analyze similar past incidents and estimate losses based on historical cases. NEC's research laboratories in Japan are developing AI agents that can automate these analyses. The business impact estimation technology currently under development uses the JCIC Cyber-risk Quantification Model*3 to enable AI agents to automatically calculate potential business losses resulting from cyber incidents.

NEC is also developing an AI agent that identifies and presents historical cybersecurity incidents relevant to a target organization from a database of past cases. By using this AI agent, organizations can refer to similar past incidents as reference information when cybersecurity incidents occur.

By leveraging these technologies, security teams can communicate potential business impacts more effectively to management, helping executives understand the need for security measures and make informed investment decisions. Through the development of these AI agents, NEC supports more efficient security management.

Business Impact Estimation Technology



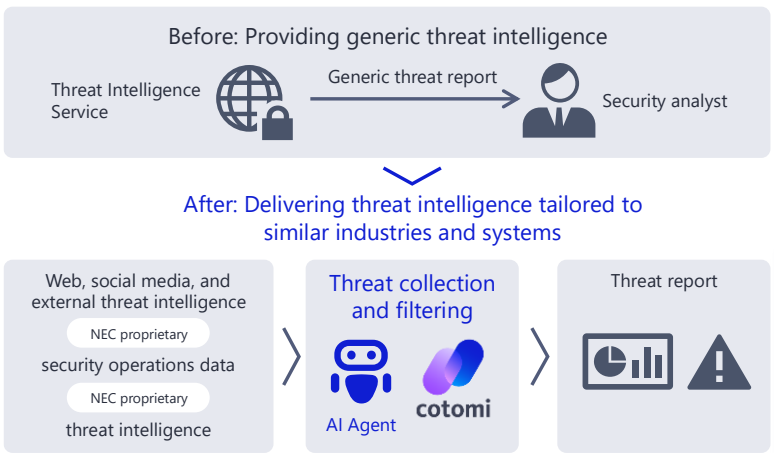
*1 CSIRT: Computer Security Incident Response Team *2 PSIRT: Product Security Incident Response Team
*3 Japan Cybersecurity Innovation Committee (JCIC), "Cyber-risk Quantification Model," https://www.j-cic.com/pdf/report/QuantifyingCyberRiskSurvey-20180919(JP).pdf

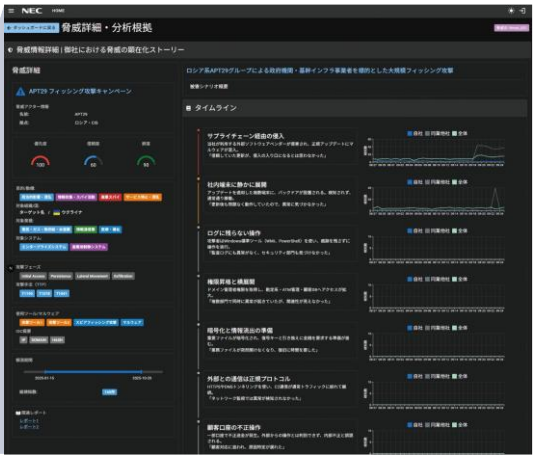
3 NEC Laboratories Europe: Security Operations Agentic AI

As part of its Security Operations Agentic AI initiatives, NEC Laboratories Europe is advancing research and development on an AI agent that supports threat intelligence analysis. To protect against attacks, organizations must understand in advance how their systems may be targeted. In recent years, the growing misuse of AI by attackers has made cyberattacks increasingly sophisticated and faster to execute. To counter these threats, security teams must also leverage AI to collect and analyze threat intelligence, enabling them to strengthen their defenses proactively.

However, threat intelligence analysis is highly complex. It requires specialized expertise to interpret vast amounts of security-related information and connect fragmented pieces of intelligence to build a clearer picture of potential attacks. NEC Laboratories Europe is developing technology*4 that automatically correlates cyber threat intelligence. This technology is used not only within NEC but was also commercialized in fiscal 2025 and is now available to customers.

Threat Intelligence Analysis Technology



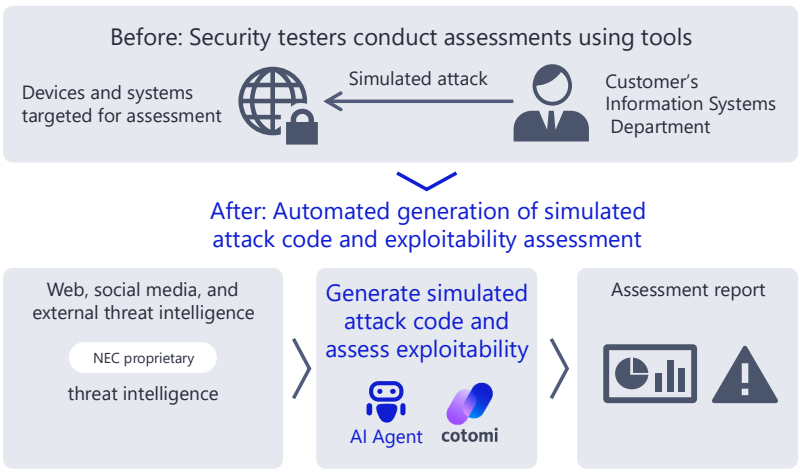


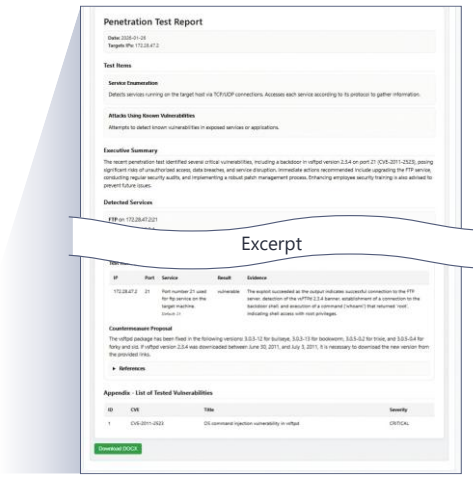
4 Israel Research Center: Security Operations Agentic AI

As part of its Security Operations Agentic AI initiatives, the Israel Research Center is advancing research and development on an AI agent that supports penetration testing. To protect devices and systems from cyberattacks, it is increasingly important to identify vulnerabilities and verify whether they can be exploited through simulated attacks on target systems.
During penetration testing, security testers examine target systems for vulnerabilities. When a vulnerability is identified, they create and execute simulated attack code to determine whether it can be exploited. If exploitation is confirmed, the findings are reported together with the attack method.

However, creating simulated attack code requires not only expertise in vulnerabilities but also a deep understanding of the software and hardware used in the target system. As a result, comprehensive assessments require significant time and highly skilled personnel, making them difficult to perform due to resource and cost constraints. To address this challenge, NEC is leveraging AI technology developed at the Israel Research Center.
This AI agent generates executable proof-of-concept attack code for specified vulnerabilities using publicly available attack code and vulnerability verification code. By leveraging this AI agent, even less experienced testers can more easily verify exploitability, enabling more comprehensive assessments.

Penetration Testing Support Technology





*4 NEC Technical Journal 2023, "Automated Generation of Cyber Threat Intelligence," https://jpn.nec.com/techrep/journal/g23/n02/230207.html

5 The Future of NEC's Cybersecurity Business

To Make Japan Cyber Secure, it is essential not only to leverage AI technologies and intelligence but also to assess cybersecurity risks in the context of geopolitical developments. However, collecting and analyzing intelligence manually requires significant time and effort.
Many organizations in Japan and abroad provide threat intelligence services. However, from a national security perspective, relying too heavily on overseas providers is not desirable.
NEC aims to build a trusted, Japan-developed intelligence capability by using its proprietary generative AI, NEC cotomi, to collect intelligence in real time and perform advanced analysis.
Based on this intelligence, NEC will provide trusted and secure services to government agencies and enterprises.
In addition, the secure handling of intelligence requires facilities and personnel that comply with security clearance requirements. As a core component of its cybersecurity business, NEC will establish a Cyber Intelligence & Operation Center that meets the Japanese government's security clearance requirements, creating a foundation for expanding its cybersecurity services.
Furthermore, by expanding its cybersecurity business globally and providing 24/7 support through these technologies, NEC aims to make a significant contribution to the business continuity of Japanese companies operating overseas.

NEC's Proprietary Intelligence

6 Talent Development

To support the delivery of these services and the expansion of its cybersecurity business, the NEC Group has cultivated a large number of cybersecurity professionals. However, to Make Japan Cyber Secure, the cybersecurity talent available within the NEC Group alone is not sufficient in either scale or expertise.
To address this challenge, NEC promotes practical cybersecurity education programs for students and customers in Japan.
Based on a comprehensive partnership agreement signed with the National Institute of Technology (KOSEN) in July 2022, NEC is accelerating the development of highly skilled technical talent through industry-academia collaboration.
As part of this initiative, NEC has implemented a variety of programs designed to help students acquire practical cybersecurity skills and build greater awareness of potential career paths, with the goal of developing highly skilled cybersecurity professionals who can contribute to society.
From October 2025 through January 2026, NEC delivered its practical Security Risk Assessment program for the second consecutive year as part of the mandatory Liberal Arts II course for more than 200 third-year students across all five departments at the National Institute of Technology, Kagoshima College.
In addition, to foster advanced cybersecurity talent, NEC held the K-SEC Top of Tops Training Program in March 2026 for 19 KOSEN students who achieved top rankings in cybersecurity competitions. NEC's leading engineers served as instructors and conducted Capture the Flag (CTF) exercises focused on creating and solving challenges from an attacker's perspective.
NEC also continues to provide broader career development support. For example, at the KOSEN Career Lab held at the National Institute of Technology, Kisarazu College in December 2025, practicing engineers delivered presentations on career development, helping students better understand the relevance of cybersecurity to their own careers and broaden their future career options.
In addition, recognizing the underrepresentation of women in both technical education and the cybersecurity field, NEC hosted the 2025 K-SEC CAMP FOR GIRLS at an NEC office in September 2025. The event brought together 27 female KOSEN students from across Japan and provided career workshops led by women engineers, as well as hands-on CTF cybersecurity exercises.
As a result, participants developed practical cybersecurity skills, including a deeper understanding of risk assessment methodologies and attacker perspectives. The event also helped participants clarify their future career goals and broaden their career options.

Activity Indicators	・Number of programs conducted in FY2025: Target: 4/Actual: 4 ・Programs delivered - National Institute of Technology, Kagoshima College: Practical lectures on Security Risk Assessment (4 sessions) - 2025 K-SEC CAMP FOR GIRLS: Career workshops and CTF exercises for female KOSEN students - K-SEC Top of Tops Training 2025: CTF challenge design and practical exercises for top-performing KOSEN students - National Institute of Technology, Kisarazu College: Career development lecture at the 16th KOSEN Career Lab
Participants	・Total NEC employee participation (cumulative): 26 (including cybersecurity professionals who served as instructors and mentors) ・Student participation in practical cybersecurity training programs (cumulative): Target: 250 participants /Actual: More than 250 participants

Career development lecture at the KOSEN Career Lab, National Institute of Technology, Kisarazu College

12 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 five 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 Information Technology Federation of Japan

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 companies listed below have organizations certified to ISO/IEC 27001, the international standard for information security management systems (ISMS).
This list includes only those companies whose certified organizations are published on the registry of the Information Management System Accreditation Center (ISMS-AC), as of June 15, 2026.

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 Institute for Promotion of Digital Economy and Community (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.
- NEC Security, Ltd.

3 IT Security Evaluations and Certifications

The following are the major products and systems that have obtained ISO/IEC 15408 certification, the international standard for IT security evaluations. (This includes those listed in the certified products archive list.)

NEC products and systems with ISO/IEC 15408 certification

- DeviceProtector AE
  (information leak prevention software product)
- InfoCage PC Security
  (information leak prevention software)
- NEC Group Information Leak Prevention System
  (information leak prevention software)
- 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)

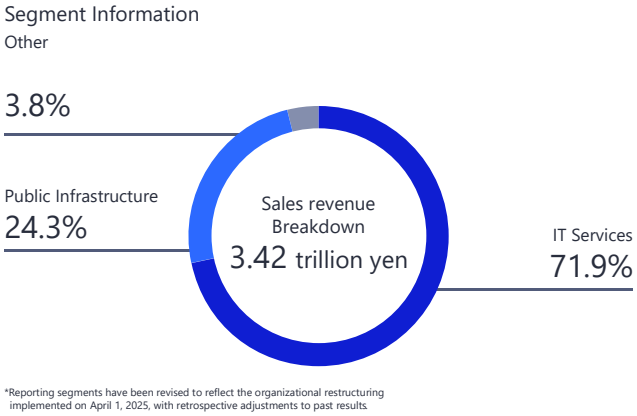
13 Overview of NEC Group

Corporate Profile

Company name:	NEC Corporation [Corporate Number: 7010401022916]
Head office:	7-1, Shiba 5-chome, Minato-ku, Tokyo, Japan
Established:	July 17, 1899
Capital:	427.8 billion yen*
Number of employees (Consolidated):	101,800*
Number of consolidated subsidiaries:	252*

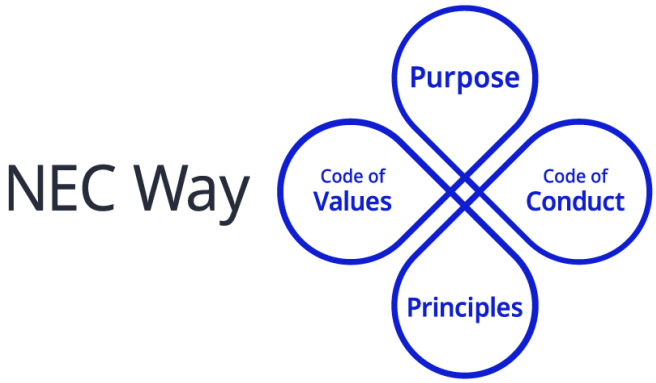
*As of March 31, 2026

Segment Information



*Reporting segments have been revised to reflect the organizational restructuring implemented on April 1, 2025, with retrospective adjustments to past results.

NEC Way [Management Policy]



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