\Orchestrating a brighter world NEC

Information Security Report 2016

NEC's Approach to Information Security

The NEC Group positions information security as an important management activity in our efforts to create new values through Solutions for Society.

Information Security Report 2016

Yasujiro Ryuno

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

Human civilization is currently facing global challenges such as rapid population growth, increased urbanization, and growing demand for energy and food.
To help overcome these challenges, NEC Group is creating social values that can be used to solve global social problems so that people can lead happy lives filled with a sense of safety, security, efficiency, and equality.
By respecting not only our customers but also all the people, cultures and diversity in every country and region in the world, NEC can help create a promising future where people live bright and prosperous lives in societies that are efficient and refined. This is the objective of NEC's Solutions for Society business and the core concept of our business brand message to customers and partners in the world—"Orchestrating a brighter world."

The values provided from the social infrastructure realized by our Solutions for Society business will continue to increase as the range of used information widens. In this context, the importance of big data, cloud computing, software-defined networking (SDN), and cyber security will only increase.
Amongst these, it will be especially vital to implement cyber security in every IT system, including IoT (the Internet of Things). Aware of this, in 2015, the Ministry of Economy, Trade and Industry and the IPA (Information-technology Promotion Agency, Japan) issued the Cybersecurity Management Guidelines, a set of guidelines concerning cyber security measures critical to corporate management. The importance of cyber security is not only growing, but is becoming intrinsically linked with corporate survival. Since 2013, the NEC Group has been making efforts to strengthen our competitiveness by collaborating with companies that have industry-leading technologies. We also regard the global safety business as one of the main concepts of our global growth strategy and are accelerating the global rollout of local initiatives by leveraging the technologies we have accumulated over time, centered on our cyber security base in Singapore.

Making full use of our core assets in these areas, the NEC Group is committed to creating new values through comprehensive contributions as "One NEC." The NEC Group positions information security as an important management activity and continues to pursue the following activities so that everybody can use information and communications technologies with a sense of security, leading to the creation of a prosperous society.

- Ensuring that NEC Group companies work together as "One NEC" to maintain and enhance information security
- Rolling out measures not only in the NEC Group but also for our business partners
- Balancing appropriate information protection and appropriate information sharing and use
- Maintaining and enhancing information security on multiple levels with a comprehensive approach in three areas: information security management, information security platforms, and information security human resources
- Providing customers with reliable security solutions that have been proven in house

This report introduces the NEC Group's information security activities. We will continue to improve our corporate activities and communicate thoroughly with all our stakeholders to achieve our goal of being an information security company trusted by society. We invite you to read this report and find out more of what the NEC Group is doing in the field of information security.

Information Security Report 2016

On the Publication of This Report

The purpose of this report is to provide stakeholders with information on the information security activities of the NEC Group. The report covers our activities up to June 2016.

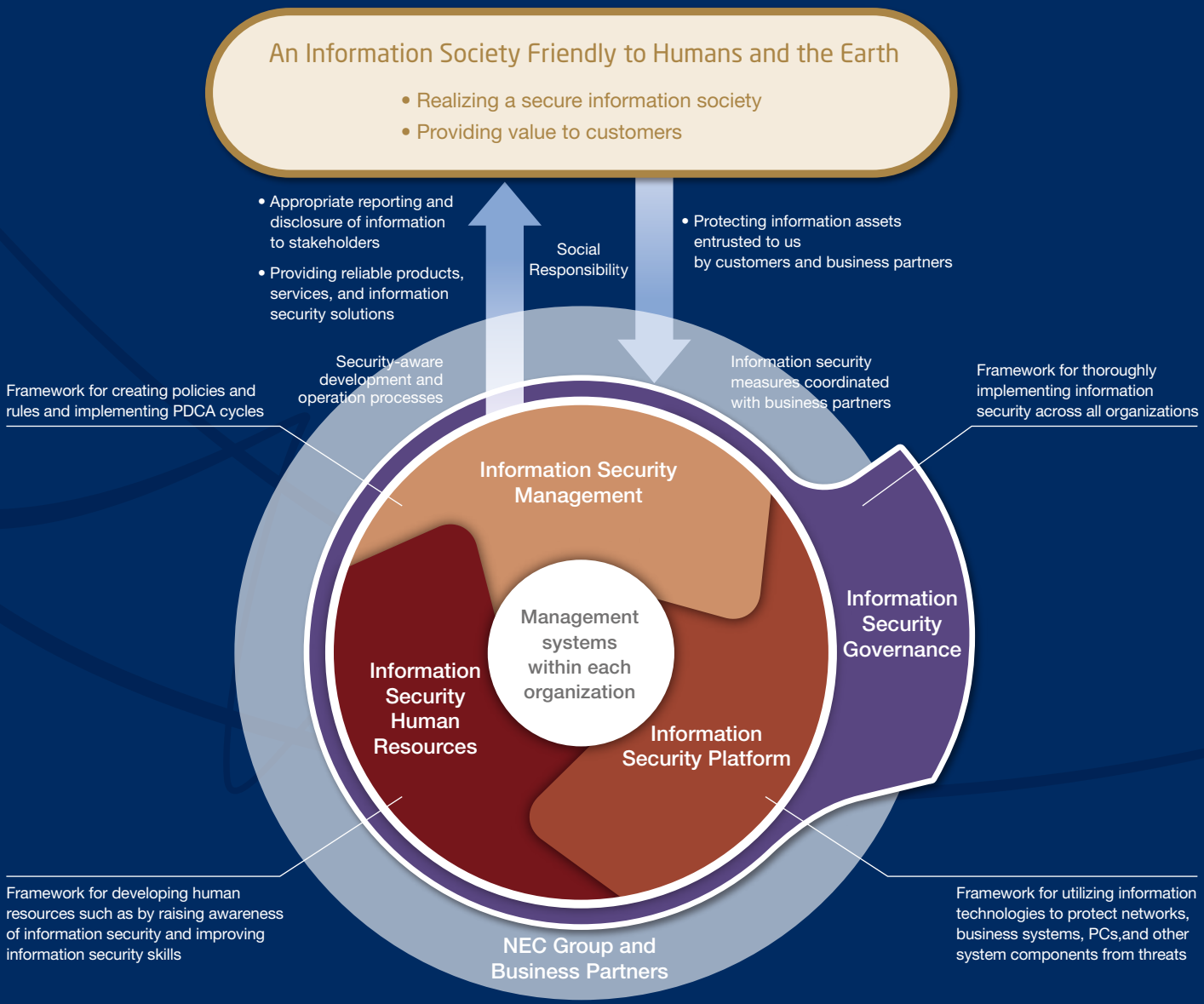
For inquiries regarding this report, please contact:

Security Technology Center
Management Information Systems Division
NEC Corporation
NEC Headquarters, 7-1 Shiba 5-chome, Minato-ku,
Tokyo 108-8001
Phone: 03-3798-6980

Information Security Promotion Framework

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

Information security threats change every day in our society, which has become highly sophisticated through IT. Information security is therefore a critical issue for all businesses. The NEC Group has established an information security promotion framework to fulfill our responsibilities to society as a trusted company. This framework enables us to realize a secure information society and provide value to our customers by protecting the information assets entrusted to us by our customers and business partners; by providing reliable products, services, and information security solutions; and by properly reporting and disclosing information to our stakeholders. To protect information assets, we combine the following four elements (information security governance, information security management, information security human resources, and information security platform) to comprehensively maintain and enhance information security on multiple levels.



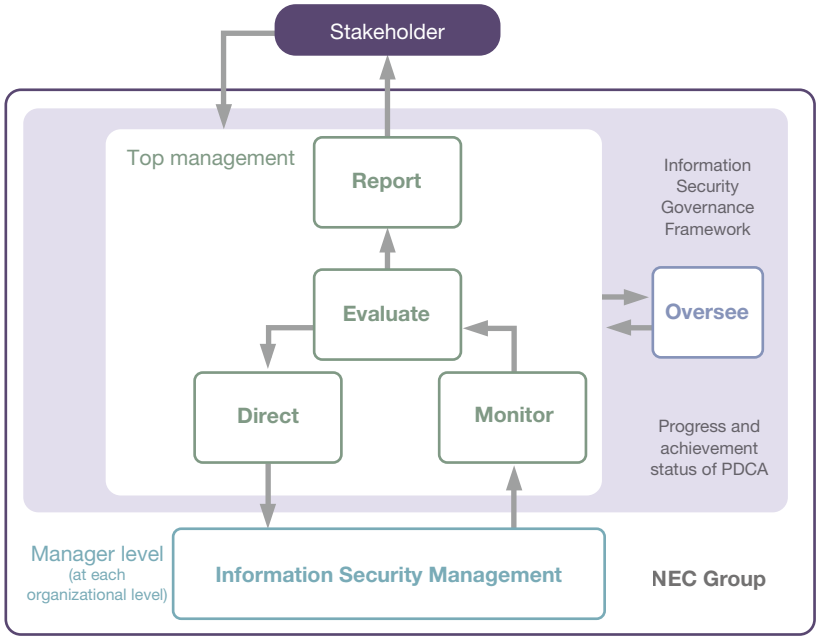
Activities based on these frameworks are divided into two categories: group-wide activities and activities conducted by each organization in the NEC Group.
Group-wide activities include the establishment of the NEC Information Security Statement and group-wide rules and the development of a common information security platform, as well as planning, implementation, revision and improvement of operational systems for providing education, awareness-raising, and human resource development. The Information Security Governance framework enables us to effectively and efficiently deploy these activities across the NEC Group. Not only do we do this internally but we also work with our business partners to deploy security measures and to advocate the establishment of development and operation processes to deliver reliable products, services, and solutions to our customers.
In addition to these group-wide activities, each individual organization performs management tailored to its own business environment and organizational structure while keeping in line with Group directions.

Information Security Governance

The NEC Group has established information security governance to align business activities with information security; to efficiently and effectively raise the information security level across the entire NEC Group; and to control risks resulting from business activities.

1 ‖ Information Security Governance in the NEC Group

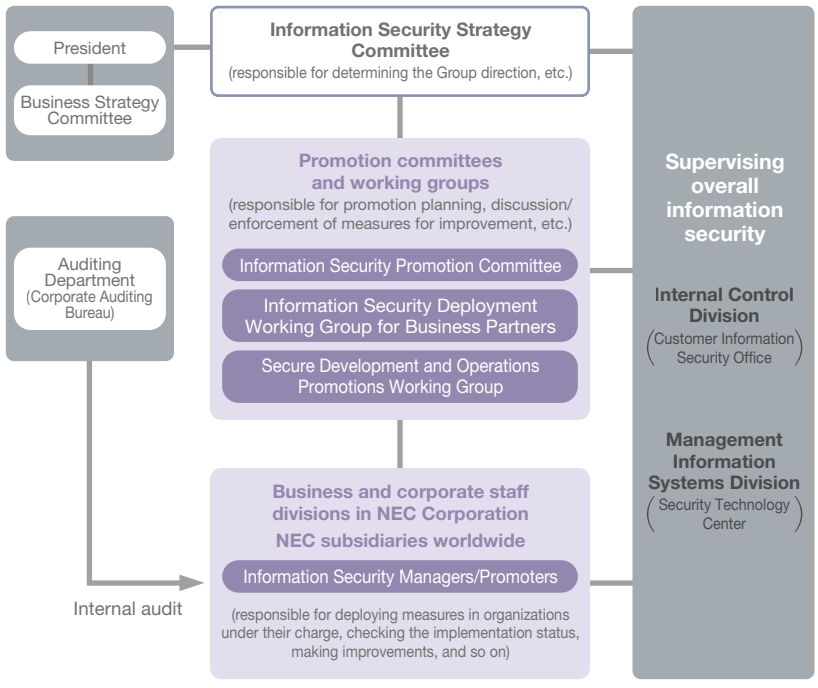
NEC has established the NEC Group Management Policy, a set of standardized rules related to the conduct of business, unified systems, business processes, and infrastructure to create a foundation from which to achieve standard global management so that the whole Group can make a comprehensive contribution. Information security governance is required to enhance the overall security level as “One NEC.” At the top management level, security goals are set and group strategies, organizational structures, allocation of business resources and other critical matters to achieve these goals are determined. At the organization level, the progress and achievement status of security measures as well as the occurrence of information security incidents are monitored, and new directions are set by evaluating requirement compliance. Each organization is then provided with the necessary instructions and the system is improved. We purse total optimization for our group by cycling these processes at the top management level and the organizational level and by implementing an oversight function. We also properly disclose information to stakeholders and continue to improve our corporate value.



Information Security Governance

2 ‖ Information Security Promotion Organizational Structure of the NEC Group

The information security promotion organizational structure of the NEC Group consists of the Information Security Strategy Committee, its subordinate organs, and the promotion structure at each organization level.
The Information Security Strategy Committee, headed by the CISO (chief information security officer) 1) evaluates and discusses how to improve information security measures, 2) discusses the causes of major incidents and the direction of recurrence prevention measures, and 3) discusses how to apply the results to NEC's information security business to address information security risks, including risks related cyber security. Under the committee, three subordinate organs (a sub-committee and two working groups) discuss and coordinate security plans and implementation measures, enforce instructions to achieve them, and manage the progress for group companies worldwide, for business partners, and for driving the Secure Development and Operations initiative, respectively.
The information security manager in each organization has primary responsibility for information security management including the group companies under their supervision. They continuously enforce information security rules within their organizations, introduce and deploy measures to assess the implementation status, and implement further improvement measures to maintain and enhance information security.



Information Security Promotion Structure

Security Aspects That the NEC Group Is Focusing On

Strengthening measures against cyber attacks

Amid the increasing ingenuity and sophistication of cyber attacks,
NEC is implementing advanced countermeasures within Japan and overseas based on cyber security risk analysis, and responds to incidents through its CSIRT*1 to achieve robust cyber security management.

*1 CSIRT: Computer Security Incident Response Team

1 ‖ Cyber Security Risk Analysis

The NEC Group performs risk analysis of cyber attack threats that occur in daily business operations, including targeted attacks, ransomware (a kind of malware that encrypts files and then demands a ransom in exchange for decryption), and indiscriminate email attacks (attacks similar to targeted attacks, but aimed at unspecified, large numbers of people), and implements measures against cyber attacks based on the analysis results. NEC sorts risk analysis into the following four types:

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

Monitoring operations analysis
We perform appropriate reviews of our current monitoring processes, research new operations that will allow us to keep abreast of the changing trends in cyber threats, and identify any operational issues.

Solution and IT analysis
We investigate countermeasure products, services, and market trends to assess ever-evolving technologies. We also evaluate PoCs*2 and, through internal IT environment surveys of the NEC Group, analyze matters including the applicability of countermeasure products and services to the Group's internal IT environment.

*2 PoCs: Proofs of Concept

Countermeasure analysis
Working on the basis of cyber threat analysis, monitoring operations analysis, and solution and IT analysis, we investigate the countermeasures required by the NEC Group, and determine the targeted scope of the countermeasures, their effects, and their costs.

Every day
General frequency
Quarterly

	Items analyzed	Activities	Related investigation/reporting committees
Cyber threat analysis	•Status of attacks (frequency, scope) •Attack method and characteristics •Malware characteristics/behavior •Attack source and destination of communication •Risk level •Methods for handling	•Attack monitoring, handling •Cyber incident response •Malware analysis •Use of intelligence services •Collection of threat/vulnerability information •Information sharing with related organizations	•Cyber Attack Countermeasure Investigation Committee •CSIRT Technological Countermeasure Investigation Committee •Information sharing among SOCs
Monitoring operations analysis	•Details of internal operations •Operational level targets •Operational rules and processes •Issues and problems in current operations	•Cyber security operations by Security Control Center (SOC) and CSIRT	•Cyber Attack Countermeasure Investigation Committee •Information sharing among SOCs
Solution and IT analysis	•Details of countermeasure products/services •Comparison with competitors •Market trends •Applicability to internal environment	•Participation in domestic and overseas conferences, surveys •PoC evaluation •Information sharing with external organizations •Meetings with vendors	•Cyber Attack Countermeasure Investigation Committee •Information sharing among SOCs •Information Security Strategy Committee
Countermeasure analysis	•Details of countermeasures •Expected effect of countermeasures •Residual risk after countermeasures •Cost •Targeted scope (assets, department, etc.)	•Consideration of countermeasures •Plan deliberation/approval/ performance evaluation by the Information Security Strategy Committee	•Information Security Strategy Committee

Formulate plans based on the results of analysis, while also providing feedback into measures

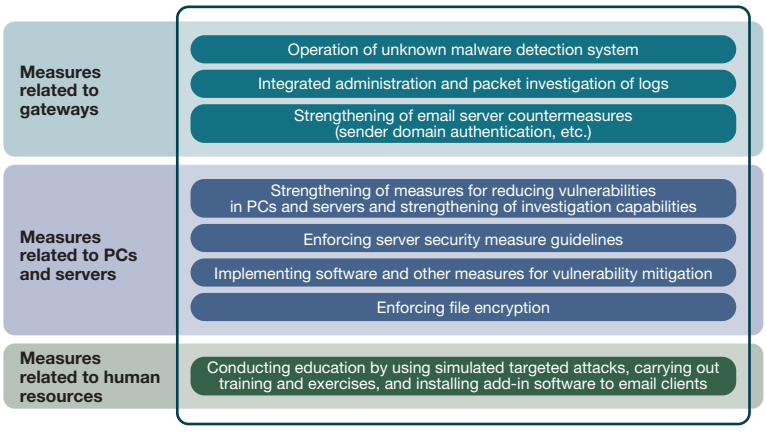
Cyber security risk analysis

2 ‖ Measures Against Cyber Attacks

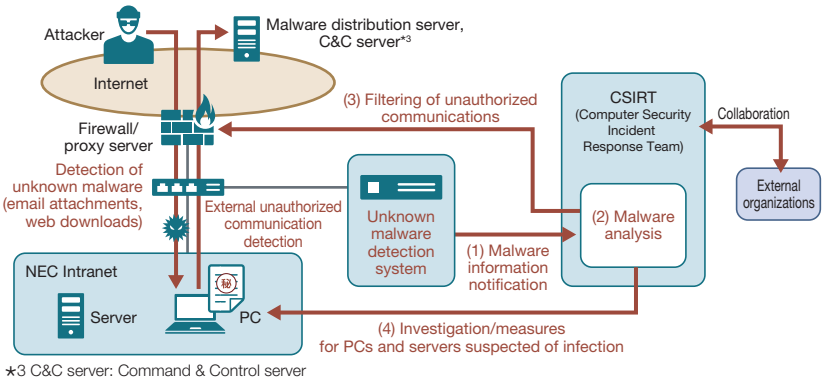
The NEC Group formulates plans for countermeasures based on cyber security risk analysis, and implements the countermeasures with the approval of the CISO (Chief Information Security Officer). In particular, we position detection of attacks by unknown malware as a priority measure against targeted attacks, and implement measures related to gateways, to PCs and servers, and to human resources, in a multilayered approach.

(1) Measures Related to Gateways

As entrance and exit countermeasures, we implement unknown malware detection systems, monitor web communications, email transmissions and other communications, and, based on information about detected unknown malware, filter out improper communications and take measures to handle PCs and servers suspected of infection. NEC also performs integrated administration, analysis, and packet investigation of communication and operation log data for the Group's entire 100,000-person workforce, and analyzes and investigates traces left by attackers.

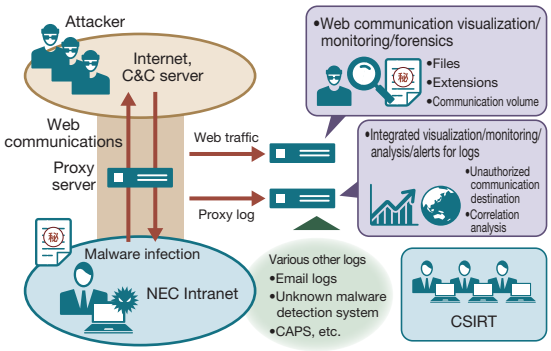


Measures against targeted attacks in the NEC Group



*3 C&C server: Command & Control server

Detection of unknown malware and unauthorized communications



Integrated analysis of logs and investigation of packets

(2) Measures Related to PCs and Servers

From fiscal 2016, NEC is rolling out the GCAPS*4 (sold externally as a solution under the name NCSP*5) to the entire Group, for the purposes of strengthening measures related to PC and server vulnerabilities and increasing the efficiency of incident response.

Under GCAPS, we are working to strengthen measures related to PCs and servers from two standpoints: "Proactive Defense" performed on the basis of risk recognition, and "Incident Response" when an incident has been detected.

*4 GCAPS: Global Cyber Attack Protection System

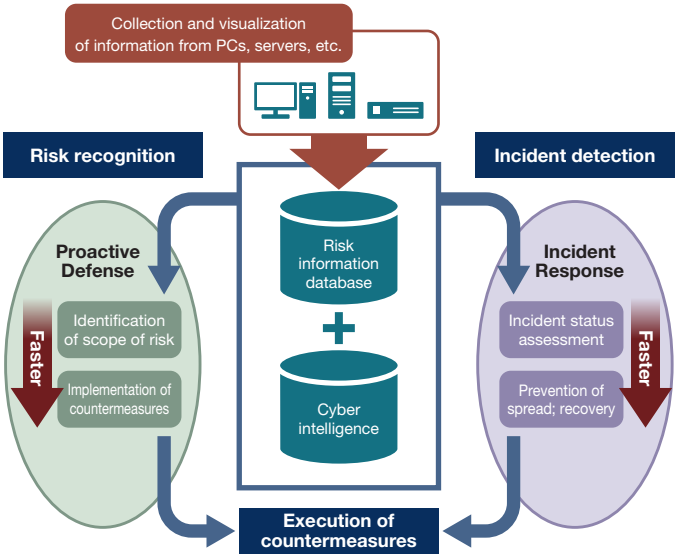
*5 NCSP: NEC Cyber Security Platform

(3) Measures Related to Human Resources

The NEC Group conducts targeted attack simulation training for all employees to strengthen our response capabilities with respect to sophisticated attacks. Further, we have implemented OMCA*6 in all PCs across the Group and carry out measures that create awareness of suspicious email.

In addition to these measures, we implement training for designated divisions and conduct comprehensive exercises with top management and their related divisions.

*6 OMCA: Outlook Mail Check AddIn

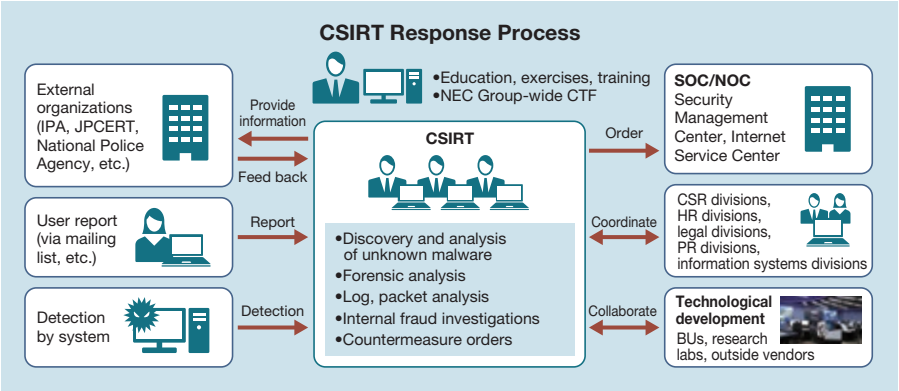


Concept of GCAPS

3 CSIRT Activities

The NEC Group has established a CSIRT (Computer Security Incident Response Team), headed by the CISO (chief information security officer). The CSIRT monitors for cyber attacks, analyzes the features of discovered attacks and malware, and shares the information with related departments. If an incident occurs, the CSIRT takes immediate steps to protect the company's systems and find out what type of attack they are facing. The team then analyzes the cause of the incident and implements measures to bring the attack to an end. Members of the CSIRT also undergo training and exercises to improve their technical skills, as well as participate in the Group-wide CTF*7 security contest.

*7 CTF: Capture the flag



Overview of CSIRT

4 Global Cyber Attack Countermeasures

The NEC Group implements cyber attack countermeasures in its overseas subsidiaries along the same lines as those implemented in Group companies in Japan. We have built a framework in which cyber intelligence concerning detected cyber attacks and unauthorized communications is shared with all Group companies throughout the world and incidents are handled properly by all overseas subsidiaries.

Security Aspects That the NEC Group Is Focusing On

Information Security at Overseas Subsidiaries

The NEC Group implements information security measures (policies and rules, management, and infrastructure) in its overseas subsidiaries with the goal of achieving the same high level of information security as that of domestic group companies.

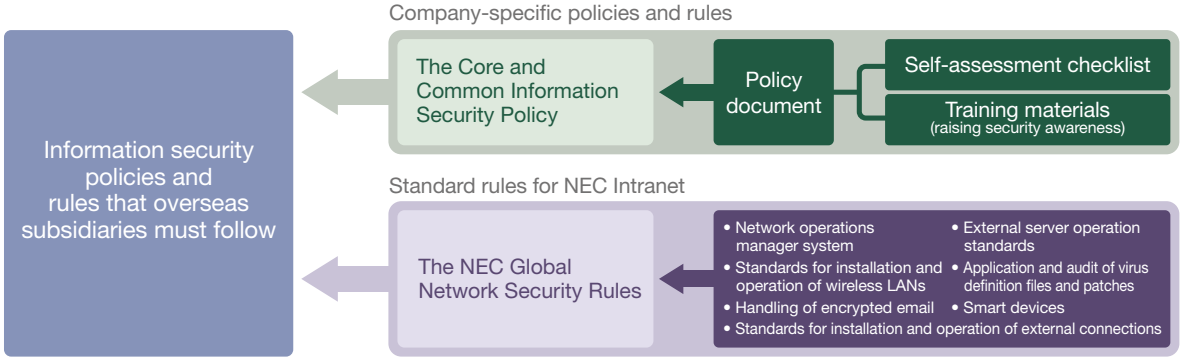
1 ‖ Global NEC Intranet

The NEC Group connects more than 150 overseas offices by using regional intranets, establishing a global intranet. The company responsible for general administration in each region manages each regional intranet, while NEC headquarters centrally administers global operations such as interconnections between regional networks.

Global NEC Intranet

2 ‖ Information Security Policy and Rules

All overseas subsidiaries in the NEC Group define their information security policies and rules based on the Group's standards.
To help overseas subsidiaries create their information security policies and rules and at the same time allow the NEC Group to implement security measures that are consistent across the entire Group, NEC provides "The Core and Common Information Security Policy" template that each company can adjust to maintain compliance with laws and regulations applicable to their country or region and onto which they can map the roles in their organization. This template is based on the ISO 27001 standard and its documentation system can easily be applied across the globe. Additions and modifications made by each company must be verified and approved by NEC. For example, an NEC Group company engaging in software development can strengthen their information security policies by adding items to the template.
The NEC Group has also established the NEC Global Network Security Rules. Overseas subsidiaries that use the NEC Intranet must follow these rules as standard. The rules cover management systems, connection to the Internet, and in-house networks, and are revised as needed to ensure the thorough implementation of countermeasures to new information security threats such as cyber attacks.



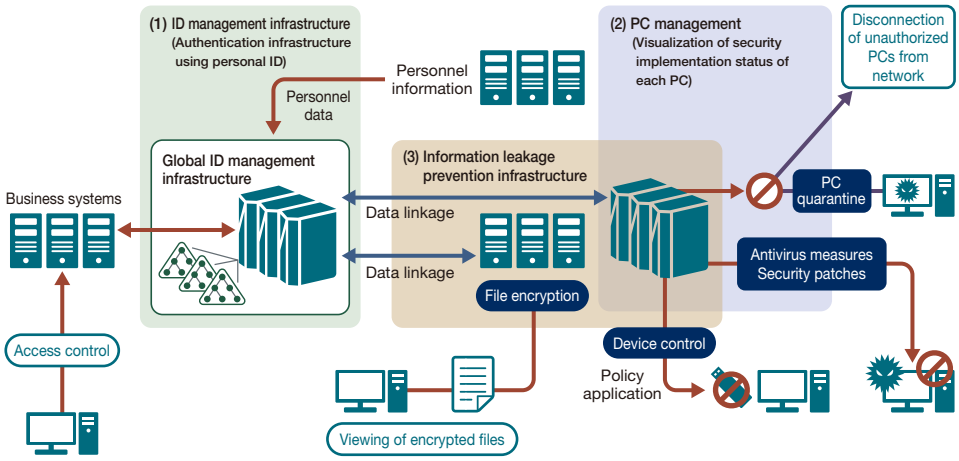
Global Information Security Policies and Rules

3 ‖ Information Security Management

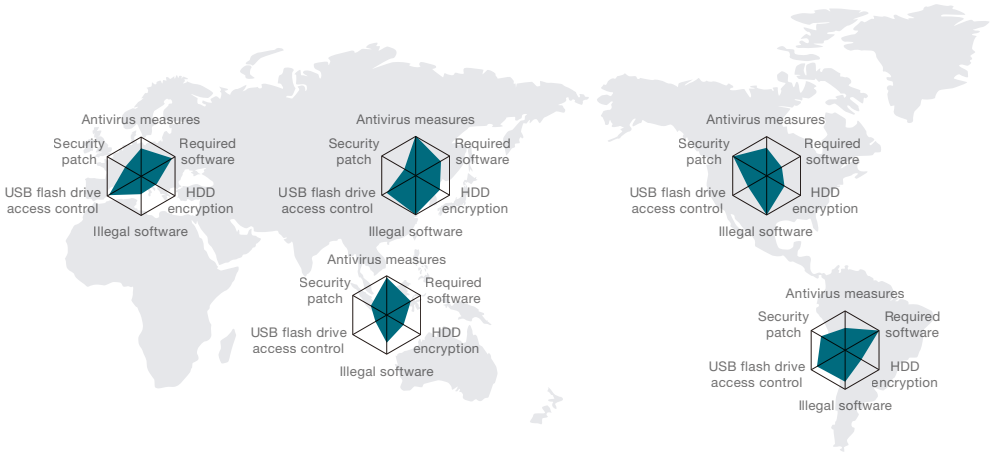
NEC has created information security training contents for employees of overseas subsidiaries and provides web-based training every year. NEC aims to raise information security awareness among employees in overseas subsidiaries by creating training contents in seven languages so that every user can receive the training in their own language.
In addition to the above-mentioned web-based training, the NEC Group assesses information security every year to check the implementation status of information security measures in each company. Based on the results of these assessments, NEC instructs companies to implement improvement measures and regularly follows up with each company to make sure that the required measures are being taken.
To check the implementation status of network security in each company, NEC also conducts network security audits every year in each region based on the standard global NEC Intranet rules and checks back regularly to confirm that network security is being implemented properly.

4 ‖ Information Security Infrastructure

As information leakage prevention infrastructure, NEC has implemented file view limitation management though which files handled within the Group are encrypted and can only be viewed by authorized users. In our overseas subsidiaries, as in Japan, we distribute a unique user ID to every employee and use our global ID management infrastructure for centralized ID management. We encrypt office documents using these user IDs, preventing the leak of information to third parties.
We also perform visualization of the security implementation status of all PCs in overseas subsidiaries, and implement mechanisms to ensure the application of antivirus measures and security patches, and disk encryption. We are also rolling out access control (device control) for USB flash drives and other external storage media, and network quarantines for unauthorized PCs.



Global Information Security Infrastructure



Visualization of Implementation Status of PC Security Measures (Sample)

5 ‖ Global Trends in Personal Information Protection

Laws and regulations related to personal information protection are becoming stricter in many countries, as evidenced by the recently revised EU directive on the protection of personal data. The directive was revised due to the rapid evolution of ICT and globalization, and the consequent expansion of risks, and the overly complex procedures used in the existing data protection systems. It is necessary to keep pace with trends in rule enhancement as they are likely to impact our global business activities in terms of restrictions on data transfer and the development of innovative services such as cloud computing.
Because the authentication information upon which the information security platform is based is also regarded as personal information, the NEC Group works together with related departments and specialists to track international trends in personal information protection from the viewpoint of legal compliance, and takes steps to enforce compliance if so required.

Security Aspects That the NEC Group Is Focusing On

Information Security Coordinated with Business Partners

The NEC Group raises the level of information security at business partners by promoting thorough rollout of information security measures, security assessments, and corrective actions in close coordination with business partners in order to protect customer information.

1 Framework

The NEC Group carries out business with business partners. We believe that, in addition to technical capabilities, it is extremely important for business partners to meet the high standard of information security that the NEC Group has set. The NEC Group classifies the information security implementation status of business partners into security levels, and has introduced a mechanism by which we can select business partners that meet the information security level required by the outsourced work. Through this, we promote the maintenance of business partners' information security levels, and reduce the risk of information security incidents occurring at our business partners.

Level (risk level)	Contractor acceptability
A (low risk)	Acceptable contractor.
B (middle risk)	Acceptable contractor. However, only if the contractor completes the required security improvements.
Z (high risk)	Unacceptable contractor. Outsourcing is possible only under certain special circumstances, and only if the contractor completes the required security improvements.

Information Security Levels

NEC Group requires business partners to implement information security measures classified into seven categories: 1) contract management, 2) subcontracting management, 3) staff management, 4) information management, 5) introduction of technical measures, 6) Secure Development and Operations and 7) assessments.

(1) Contract Management

The NEC Group and business partners to which we entrust work must sign comprehensive agreements that include nondisclosure obligations (basic agreement).

(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.

(3) Staff Management

The NEC Group has compiled security measures to be implemented by people engaging in work outsourced from the NEC Group in the “Basic Rules for Customer Related Work.” We promote thorough implementation of these measures by asking workers to promise the company for which they work that they will take these measures.

(4) Information Management

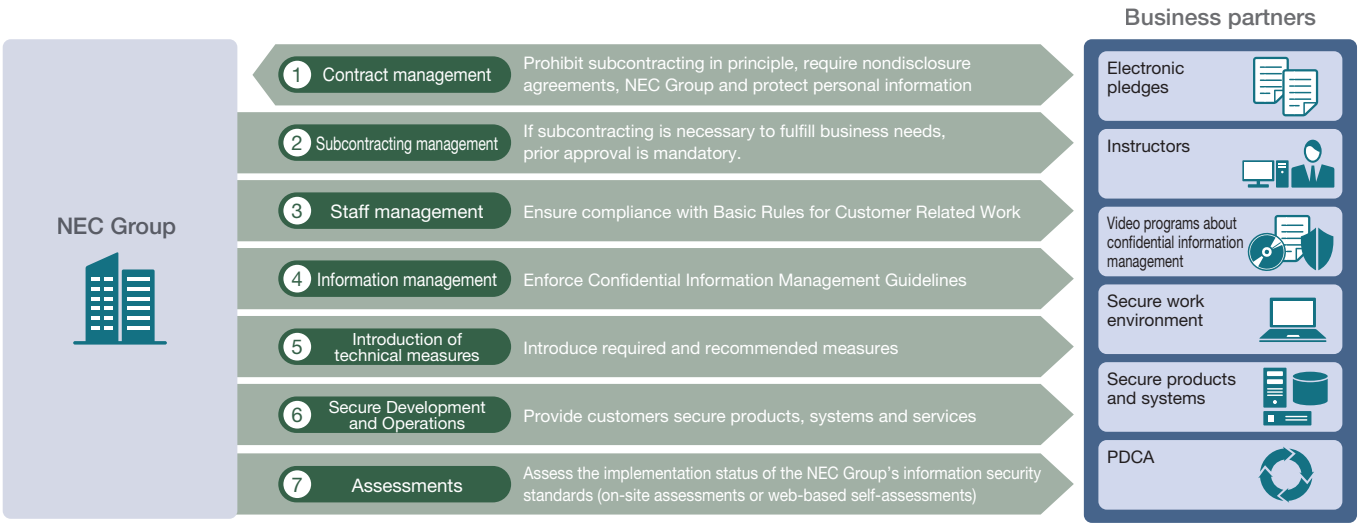
Management of confidential information handled when carrying out work outsourced from the NEC Group is prescribed by the Confidential Information Management Guidelines, in which NEC requires confidential information to be labeled, the taking of information outside the company to be controlled, and confidential information to be disposed of or returned after the work is complete. Following these guidelines is a procurement requirement.

(5) Introduction of Technical Measures

We categorize technical measures, implemented together with management measures, into required measures (e.g. encryption of all mobile electronic media) and recommended measures (establishment of an information leakage prevention system and secure information sharing platform) and ask business partners to implement them.

(6) Secure Development and Operations

The NEC Group created the Secure Development and Operation Guidelines for Business Partners concerning the development and operation of products,



Information Security Measures for Business Partners

systems and services for customers and asks business partners to consider security during development and operation.

(7) Assessments

The NEC Group checks the implementation status of information security measures at each business partner every year (or when opening an account for a new business partner) and gives instructions for improvement as needed using a group-wide standard system (framework and procedures) based on Information Security Standards for Business Partners, which defines the information security standards required for NEC Group business partners.

2 ‖ Promotion of Security Measures for Business Partners

(1) Information Security Seminars

The supply chain management and information security divisions work together to organize information security seminars at 13 places across Japan from Hokkaido to Okinawa once a year for nationwide business partners (approximately 1,600 companies, including approximately 700 ISMS certified companies) to ensure that business partners understand and implement the NEC Group's information security measures.

(2) Skill Improvement Activities for Core Businesses

The NEC Group works closely with about 100 core software business partners that frequently deal with the NEC Group to encourage them to thoroughly implement measures and improve their skills.

(3) Distribution of Videos to Maintain Awareness

The NEC Group broadcasts educational videos based on the results of analyzing security incidents at the information security seminars, distributes them to business partners and encourages their use for in-house education. The themes of past videos include compliance, confidential information management, virus infections, loss of data after going out drinking, secure email distribution, personal information protection, and incident response.

(4) Operation of Examination System

The NEC Group periodically creates and distributes examination sheets to business partners to ensure thorough implementation of the "Basic Rules for Customer Related Work," and requires business partners to implement in-house education. In addition, we have built and are operating a system by which business partners can register their examination results with the NEC Group and see their ranking among all our business partners.

(5) Distribution of Measure Implementation Guidebooks

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

(6) Standardization of Contractor Management Process

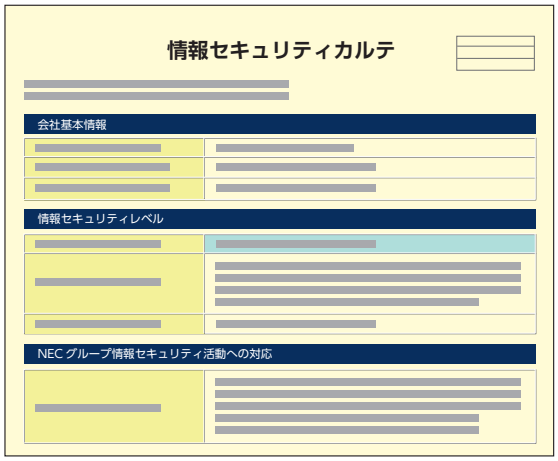
In addition to encouraging business partners to implement information security measures, the NEC Group—the outsourcing organization—has also standardized the contractor management process to ensure that a standard set of information security measures are applied across the entire supply chain.

Standardized Contractor Management Process

3 ‖ Assessments and Improvement Actions for Business Partners

Assessments of our business partners mainly consist of web-based self-assessments and on-site assessments.
Web-based self-assessments are performed at approximately 1,600 companies that deal with the NEC Group every year. New business partners receive a document assessment when opening their account. Business partners carry out self-assessments of their implementation status of security measures based on assessment items created every year that take into account the status of information security incidents and other factors, and enter the assessment results in our web system. The NEC Group creates a report of these assessment results and provides it as individual feedback to each company. The business partners can see their security level among all the business partners of NEC Group, realize the challenges they face, and make efficient improvements.
On-site assessments are carried out at about 100 companies that frequently deal with the NEC Group every year. Assessors authorized by the NEC Group (approximately 300 assessors) visit the business partners and carry out assessments onsite and uncover issues that were not found in the business partner's own assessment (i.e., web-based self-assessment).
For both assessments, business partners that need to make improvements enter their improvement plan and progress of improvement in the web system. The NEC Group follows up with them based on the entered information to help them raise their standards.

The assessment results as well as the status of implementing the required information security measures are compiled on an assessment sheet so that business partners can comprehensively understand their implementation status.



Information Security Assessment Sheet

Security Aspects That the NEC Group Is Focusing On

Providing Secure Products and Services

To offer “better products, better services” to customers from the viewpoint of safety and security, the NEC Group carries out a variety of activities to ensure high-quality security in the products and services it offers.

1 ‖ Promotion of Secure Development and Operations

(1) Group-wide Promotion Structure

In order to enable Secure Development and Operations for the products and services we offer our customers, the NEC Group has created a “Secure Development and Operations” promotion structure. This promotion structure consists of the Secure Development and Operations Promotion Workgroup, made up of representatives from the various NEC organizations and Group companies, and Secure Development and Operations promoters appointed throughout the NEC Group (approximately 400 people). The Workgroup discusses proposed measures for Secure Development and Operations directed at the eradication of information security incidents caused by product and service vulnerabilities, configuration mistakes, and system failures, and shares information on the implementation progress of adopted measures. The Secure Development and Operations measures adopted by this Workgroup are communicated to the promoters at the various divisions through the Operation Promotion Liaison Group, who ensure that the measures are fully disseminated within their respective division, carry out implementation status inspections, and continuously work on improvements.

(2) Establishment of an NEC Group Standard Framework

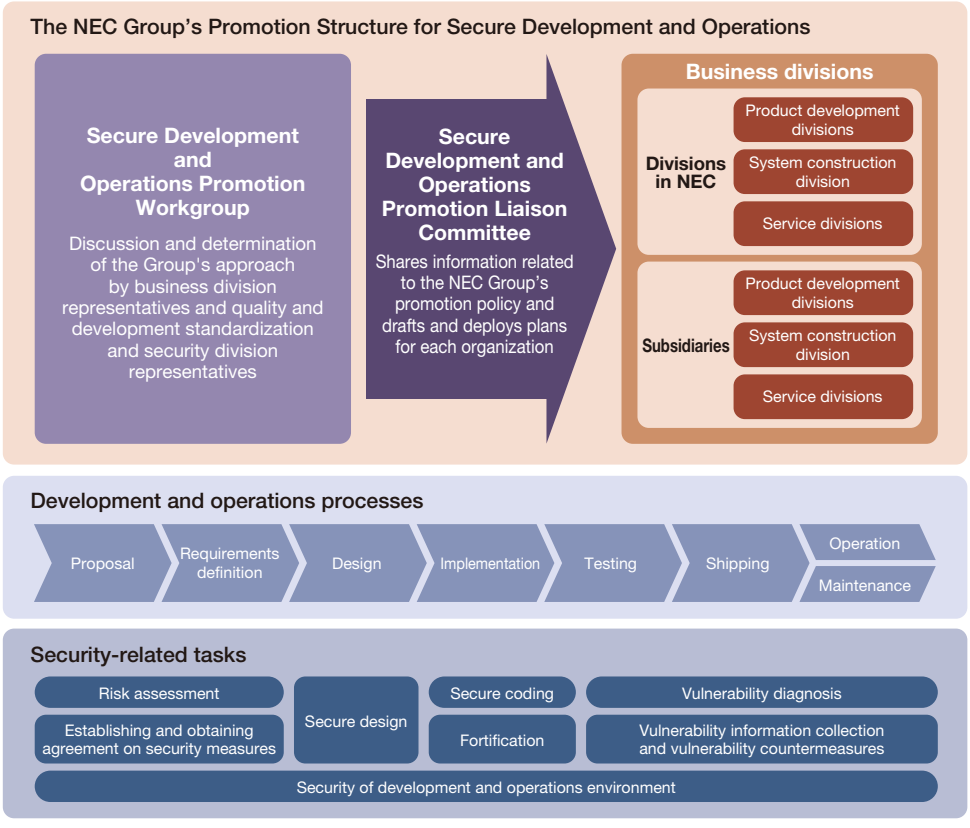
In 2014, the Secure Development and Operations Management Rules were established as part of the NEC Corporation Industrial Standards (NIS), which is a set of standards for the NEC Group. These rules define the content related to Secure Development and Operations to be implemented by the various divisions of the NEC Group (the creation of promotion structures within each division, the incorporation of division processes, Secure Development and Operations related standards, etc.).

In 2015, in response to an increase in security incidents caused by ever-more ingenious and sophisticated cyber attacks as well as cases of internal fraud, and also to reflect the increasing risk of attacks on control devices and systems, the NEC Group enhanced the security measures to be implemented and revised the Secure Development and Operations Management Rules.

(3) Ensuring Security Quality

To ensure the security quality of our products and services, we have established a Secure Development and Operations check list that defines security check items in each phase of development and operation. The check list has been designed with consideration given to various requirements such as ISO/IEC 15408 and other international security standards, the security standards of government agencies, and industry guidelines. The check list also reflects security measures to counter new threats in a timely manner. The specific items covered by the check list include risk assessment, security architecture design, secure coding, fortification, vulnerability assessment, security testing, collecting and responding to vulnerability information, and security monitoring. The check list is incorporated into the development and operations standards of the various organizations in the NEC Group, and is used at the development and operations sites of each business division.

We have also introduced the Secure Development and Operations Inspection System designed to allow the visualization of the security situation of each business project and assist in the thorough implementation of security measures for business projects with insufficient security protection. Approximately 5,000 projects are managed under this system, with Secure Development and Operations promoters conducting inspections and audits to assess the security situation reported for each business project, and improve any problematic situations.



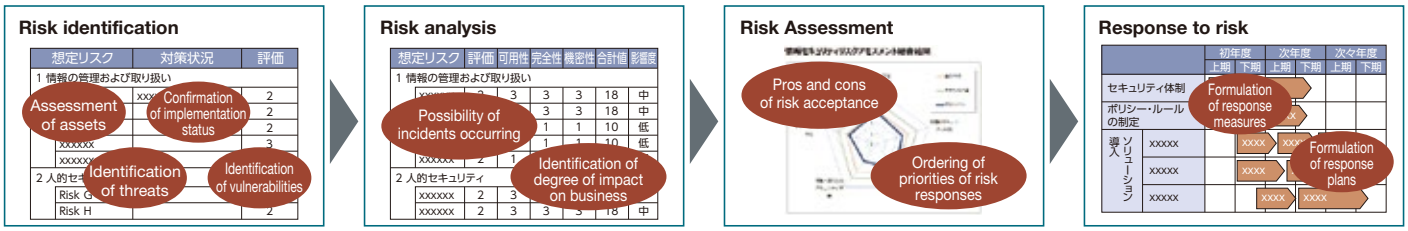
Secure Development and Operations Promotion System and Processes

(4) Strengthening Security through Risk Assessments

ICT has become indispensable to increasing the efficiency of an organization's activities and improving profitability. At the same time, the occurrence of an incident because of insufficient ICT security measures can have a serious impact on business. The Cybersecurity Management Guidelines released by the Ministry of Economy, Trade and Industry and the IPA*1 note that cyber security is an issue for business management. In addition, ensuring business continuity and corporate value created by measures against cyber attacks requires top-management decisions concerning necessary security investment. Organizations can prevent the occurrence of major incidents by appropriately assessing system risks and steadily enacting optimal security measures. Accordingly, the NEC Group undertakes security-related risk assessments to promptly make system risks visible and lessen them to the extent possible.

Risk assessment is the process of identifying and evaluating risks to work, assets, and so on that result from the operation of information systems, and ordering the priority of risk countermeasures. As an example, conducting risk assessment at the planning and proposal stages of systems for customers enables the selection of security measures with high cost effectiveness, preserving a balance between cost and safety. Risks caused by differences in on-premise, cloud service, virtual, and other environments, and risks created by internal crime, targeted attacks, and other new threats, are also possibilities. By identifying these and evaluating their degree of impact, NEC addresses varied risks stemming from different causes.

*1 IPA: Information-technology Promotion Agency, Japan



Overview of risk assessment

2 ‖ Promptly Addressing Vulnerabilities in Daily Operations

(1) Vulnerability Information Sharing Framework

To enable new vulnerabilities—which are discovered every day—to be fixed quickly and thoroughly, the NEC Group operates its own vulnerability information management system that employs approximately 600 staff members to facilitate the sharing of vulnerability information throughout the entire Group. Further, the implementation of anti-vulnerability measures is required by the quality protection rules of the NEC Group, which ensures that the system is used properly.

With regard to the NEC Group's products, we have constructed a management system for the rapid release of vulnerability information and patches in collaboration with IPA, JPCERT/CC*2, and other organizations. Under this system, if a vulnerability is detected in a product after it is shipped, the product development divisions is promptly notified and follows up the situation within the NEC Group until a patch is released publicly.

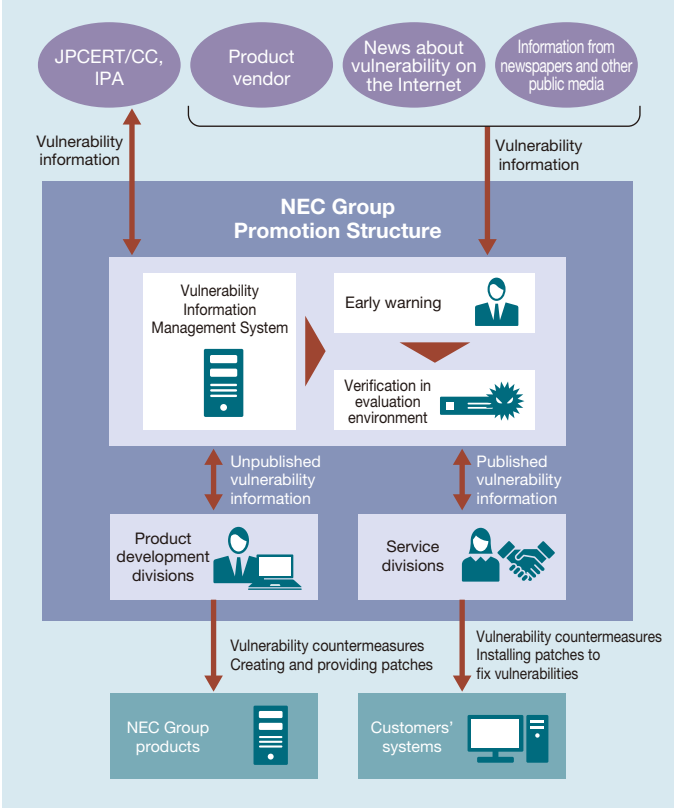
At the same time, the development and service provision divisions obtain detailed information such as the causes of the vulnerability and how to deal with it from the vulnerability information management system and implement vulnerability countermeasures for both our own products and our customers' systems. Moreover, the measure implementation status is managed on an individual project basis, and if measures are not implemented, a warning is issued, thereby ensuring systematic and thorough vulnerability handling.

*2 JPCERT/CC: Japan Computer Emergency Response Team Coordination Center

(2) Initiatives for the Collection and Verification of Vulnerability Information

Countering cyber attacks relies on the quick capture of information on vulnerabilities and preparation of countermeasures. The NEC Group performs daily collection and monitoring of vulnerability information concerning the products and technologies used in our customers' systems. We are also constructing an early warning system as a mechanism for quickly sharing information on vulnerabilities that present a particularly broad scope of impact and high risk.

The risk of attacks increases when attack tools that take advantage of vulnerabilities are released on the Internet. NEC is constructing a framework that can reliably address these vulnerabilities in every business project. Specifically, we not only share information on released patches and workarounds, but also conduct simulated attacks on evaluation environments within the NEC Group to verify the impacts of actions before and after the installation of the patches and workarounds. By sharing the results of this verification within the NEC Group, we implement vulnerability countermeasures in every business project.



Vulnerability Measures Promotion Framework

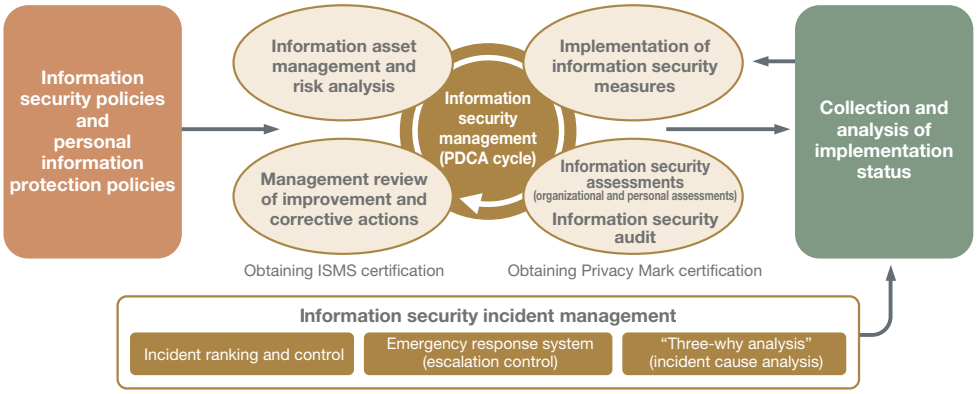
Security Elements That Are Being Maintained and Improved

Information Security Management

In order to roll out a variety of information security measures across the entire Group and have them firmly take root, the NEC Group has established an information security management framework to maintain and enhance information security through PDCA cycles.

1 ‖ Information Security Management Framework

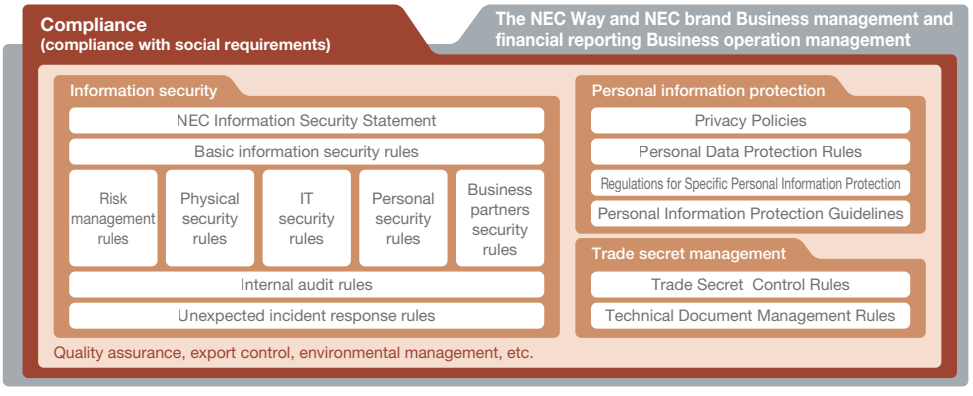
The NEC Group maintains and enhances information security by continuously implementing PDCA cycles based on information security and personal information protection policies. We track and improve the implementation status of information security measures by checking the results of information security assessments and audits as well as the situation of information security incidents among other factors, and review policies. We also promote the acquisition and maintenance of ISMS and Privacy Mark certifications considering the control level required by third-party certifications.



Information Security Management in the NEC Group

2 ‖ Information Security Policies

The NEC Group has rolled out the NEC Group Management Policy as a set of comprehensive policies for NEC Group companies all over the world. This includes information security and personal information protection policies.
The NEC Group has positioned information security and personal information protection as important matters in conducting business and been strengthening management.
For information security, NEC has released the "NEC Information Security Statement" and established and streamlined a variety of rules and standards including basic information security rules, rules for information management (Trade Secret Control Rules, Personal Data Protection Rules, Regulations for Specific Personal Information Protection, and technical document management rules), and IT security rules to enforce these basic policies.
To protect personal information, NEC established the NEC Privacy Policy and obtained Privacy Mark certification in 2005. We also established a management system that conforms to the Japan Industrial Standards Management System for the Protection of Personal Information (JIS Q 15001) and Japan's Personal Information Protection Law. Additionally, in 2015, the NEC Group added a My Number (personal identification number) management framework to its information security management system to ensure compliance with the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure ("My Number Act"). The NEC Group requires employees to handle personal information at the same protection management level throughout the entire Group. As of June 2016, 28 companies have acquired Privacy Mark certification.



NEC Group Management Policy

3 ‖ Information Security Risk Management

To manage information security effectively, we must properly assess and manage information security risks.

(1) Information Security Risk Assessment

The NEC Group assesses risk and takes measures by analyzing the difference from a baseline or by analyzing detailed risk on a case-by-case basis. We maintain security by using an information security baseline defined as the fundamental security level to be implemented across the Group. We perform analysis according to detailed risk assessment standards and take detailed measures based on the Information Security Risk Assessment Standards if advanced management is required.

(2) Management of Information Security Incident Risk

The NEC Group mandates reporting of information security incidents and analyzes and uses reported data as input when implementing PDCA cycles to manage information security risks. We centrally manage incident information according to standard rules that apply to the entire Group and analyze factors such as changes in the number of incidents, trends by organization (NEC, Group companies, business partners), and trends in types of incidents, and apply the analysis results to measures taken across the entire Group. We also use this data for effectiveness assessment and as KPIs for risk management.

In addition, we perform "three-why analysis" to pursue the true cause of information security incidents. We have established analysis methods and systems that enable the affected section to analyze the incident by itself. In the case of a serious incident, professional advisors participate in the analysis and the cost to address the incident and the effect are quantified for impact analysis. The results are reported to top management, shared across the entire Group, applied as group-wide measures and otherwise used.

4 ‖ Information Security Assessments

The NEC Group conducts information security assessments every year targeting worldwide group companies to check the implementation status of information security measures and to create and execute improvement plans for measures not completed.

(1) Details of Information Security Assessments

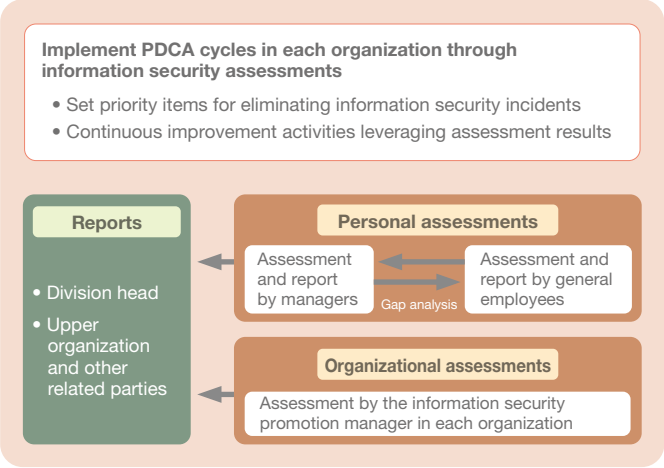
We analyze information security incidents and set priority items, mainly to eliminate information leaks. Assessments are helpful for formulating corrective measures because the assessment format allows us not only to check the implementation status but also to collect reasons why measures were not taken. Some specific examples of the information security measures that we implement thoroughly include safety measures for external storage media, measures to manage information taken outside of the company's premises, measures to ensure the safety of confidential and/or personal information, measures to manage external contractors (business partners), measures for secure email distribution, measures against targeted attack emails, and measures for Secure Development and Operations.

(2) Information Security Assessment Methods

NEC implements the following two information security assessments: organizational assessments and personal assessments. In organizational assessments, the information security promoter in each organization checks the status of the entire organization. In personal assessments, individuals indicate the status of implementing measures. Although organizational assessments have played a main role in the past, we are now implementing personal assessments throughout the Group (apart from some overseas subsidiaries) to understand the situation in the field in more detail and make more effective improvements. Personal assessments target both general employees and managers to assess execution and management. We have also improved the accuracy of assessments by analyzing the gap between employees and managers to identify any management problems.

(3) Improvements Leveraging Assessment Results

We have solved problems systematically by finding the reasons why some items were not sufficiently implemented and making improvement plans based on assessment results. In addition, we include remaining problems to be solved and items that need further enhancement in the information security promotion plan for the following fiscal year to enable continuous improvement.



Information Security Assessments (Organizational and Personal Assessments)

5 ‖ Information Security Audits

NEC's Corporate Auditing Bureau plays the main role in implementing information security management audits and obtaining the Privacy Mark. Audits are performed based on the ISO/IEC 27001 and JISQ 15001 standards to check how information security is managed in each organization.
The NEC Group implements a system whereby each organization receives a periodic internal audit by the Corporate Auditing Bureau.

6 ‖ Acquiring the ISMS Certification

The NEC Group provides services such as consultations, creation of audit systems, training, and efficient audits (e.g. auditing only changed items) for organizations that must acquire ISMS certification for their business based on standard contents designed to reliably fulfill the requirements of ISMS certification. These services are packaged and offered as a solution called NetSociety for ISMS. This solution has been successfully used by many organizations in the NEC Group as well as our business partners.

Security Elements That Are Being Maintained and Improved

Information Security Infrastructure

The NEC Group has built and operates information security infrastructure to manage and control users and to allow them to safely, securely and efficiently use PCs, networks, and business systems in order to protect customer and confidential information.

1 ‖ Features and Configuration of Information Security Infrastructure

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

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

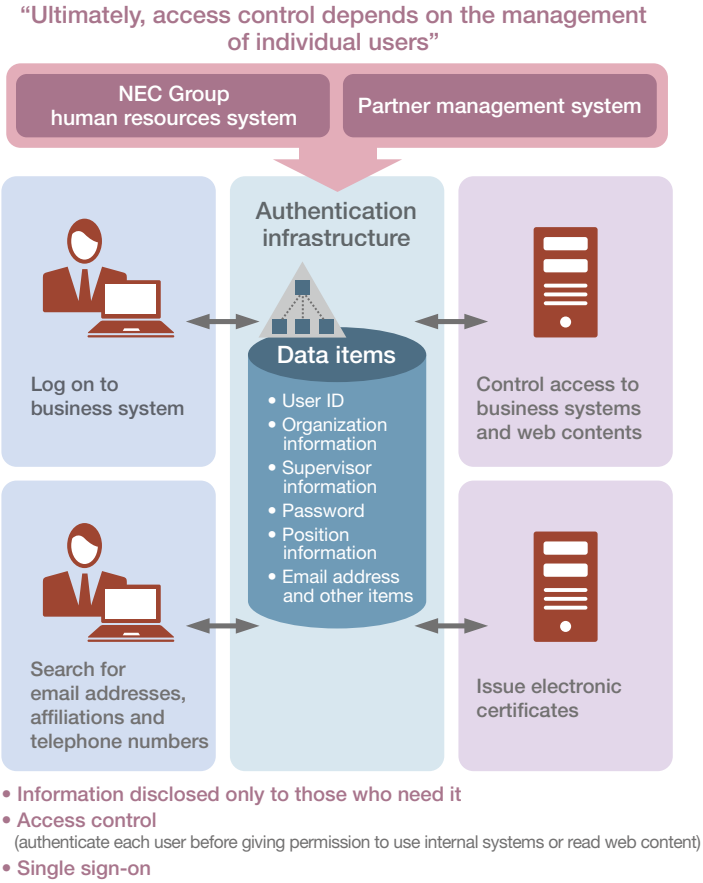
The basis of information security management is the user authentication infrastructure. Using a system to identify individuals enables proper control of access to information assets and prevents spoofing using electronic certificates. The NEC Group is currently strengthening its authentication infrastructure for user management and control.

(1) NEC Group Authentication Infrastructure

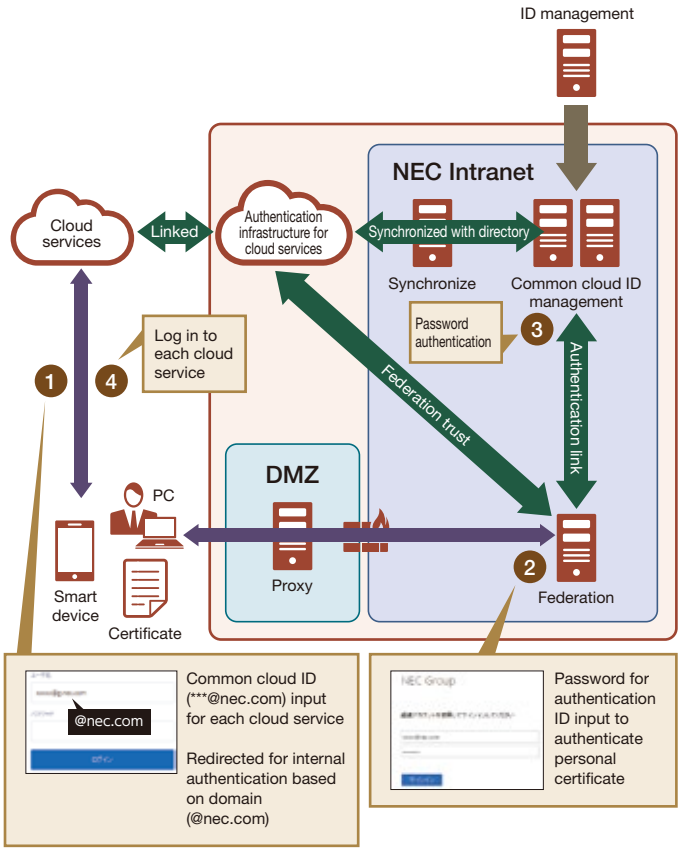
It is important to identify and authenticate users and assign them correct privileges so that they can access information assets appropriately. The NEC Group has built an authentication platform to centrally manage information used for authenticating users and assigning privileges (authorization), covering not only our employees but also some business partners and other related parties if needed for business.
The information used for authenticating and authorizing users consists of access control information such as the user's ID and password, as well as information about their organization and position. This information is used to control access to business systems and other company infrastructure on an individual basis. We also centrally manage where and for what purpose the information used for authenticating and/or authorizing users managed by each Group company is being used. We also implement IC card authentication for printer (paper) output.

(2) Linkage between Authentication Infrastructure and Cloud Services

In today's diverse business environment, there is a growing need to share information with people outside the company and utilize cloud services. The NEC Group has therefore created a system whereby cloud services are linked to the Group's internal authentication infrastructure, enabling cloud services to be used safely and securely.



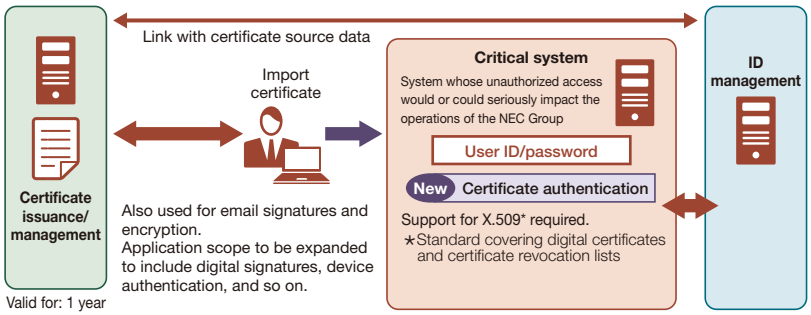
NEC Group Authentication Infrastructure



Cloud Authentication Linkage

(3) Multi-factor Authentication

To strengthen measures against internal fraud and cyber attacks (targeted attacks), we not only implement user IDs and passwords (memory-based authentication) for logging in to systems handling critical information, but also employ authentication using electronic certificates (possession-based authentication). We intend to further combine this with face authentication (biometric authentication).



Multi-factor Authentication

3 ‖ IT Platform for PC and Network Protection

NEC has constructed an IT platform to protect the Group's PCs and networks from viruses, worms, and other attacks and maintain the security of information devices connected to the NEC Intranet. In addition, as multi-level measures are recently required to address increasing risks of targeted attacks, it is important to install all necessary security updates and antivirus software.

(1) Protecting Our PCs from Viruses and Worms

[Support for user environments]

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

[Network management]

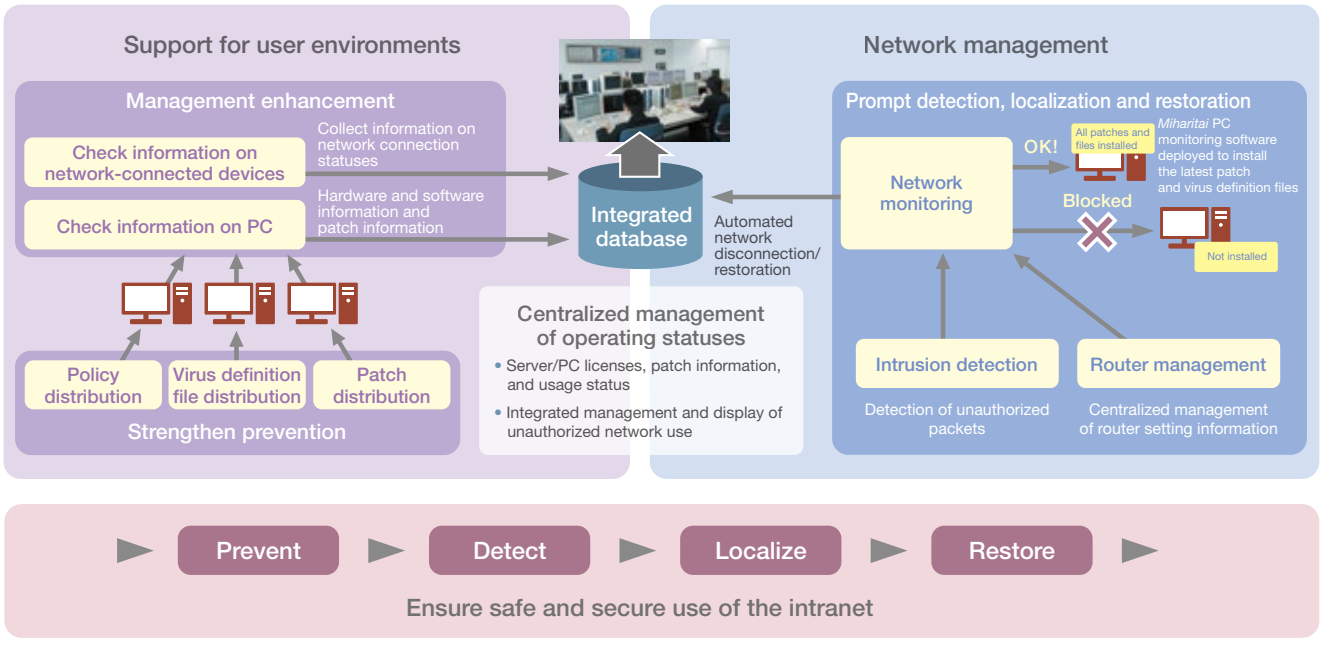
In addition to visualizing PC statuses, the NEC Intranet also includes an intrusion detection system. When a PC for which security measures are not sufficiently implemented is connected to the NEC Intranet or a worm is detected on the NEC Intranet, that PC or LAN is disconnected from the NEC Intranet. We also control communications to people or organizations outside the NEC Group by using web access filtering based on prohibited categories, prohibiting the use of free email accounts, using SPF authentication (sender domain authentication), and other methods.

[Centralized management of operating statuses]

Data on the implementation status of security measures, including installation of patch programs and antivirus software, is collected in a management system so that information security managers and security promotion managers can see the implementation status in their department in a timely fashion. This facilitates the seamless promotion and thorough implementation of a variety of measures.

(2) Checking by Using a Vulnerability Detection Tool

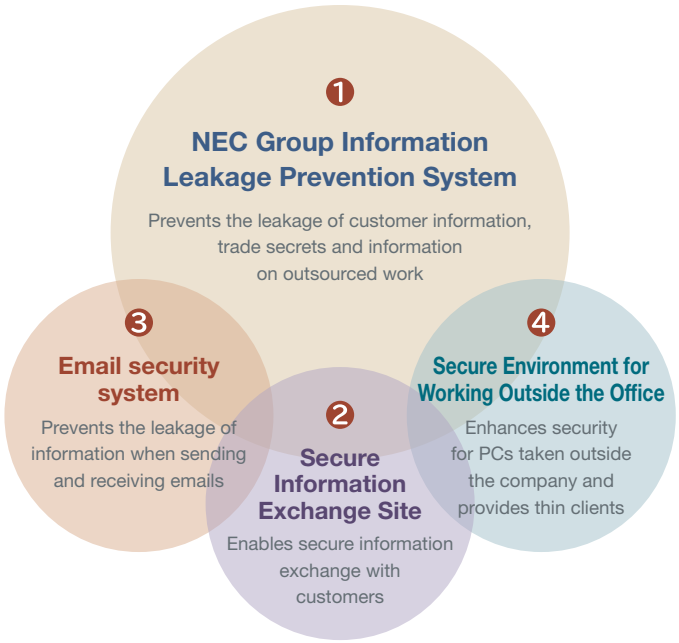
The NEC Group checks vulnerabilities in the information devices connected to the NEC Intranet by using a vulnerability detection tool.
As found vulnerabilities are centrally managed by the system, managers in each department can check the status of their department and fix the found vulnerabilities according to the specified correction procedure. The correction status is also centrally managed by the system, allowing the status of the entire NEC Group to be easily ascertained.



Protection of PCs and Networks from Viruses and Worms

4 ‖ IT Platform for Information Protection

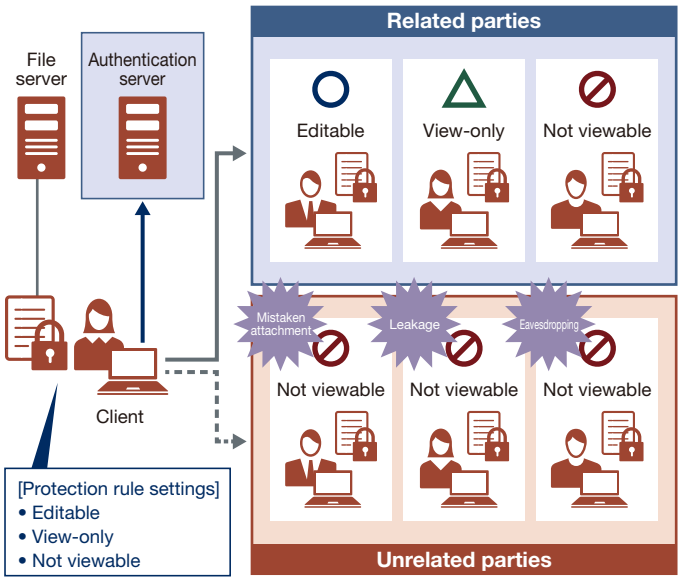
It is necessary to identify channels that can lead to information leaks, analyze risks and take appropriate measures to prevent leaks.
As the NEC Group manages not only our own information but information entrusted to us by customers and information disclosed to business partners, we implement comprehensive and multilayered measures for each channel that might lead to an information leak, taking the characteristics and risks of networks, PCs, electronic media, and other IT components into consideration.



Overview of IT Platform for Information Protection

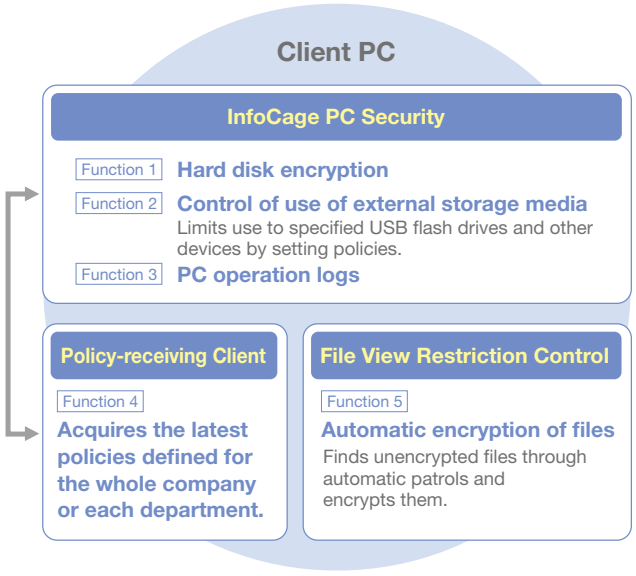
(1) NEC Group Information Leakage Prevention System

The NEC Group has constructed an information leakage prevention system that uses our InfoCage series of products. By implementing encryption, device control, and log recording/monitoring, we counter the risk of information leakage caused by external attacks or internal misconduct.
Using encryption, we encrypt PC hard disks and files to prevent the leakage of information due to theft or loss. In particular, we implement InfoCage FileShell to encrypt all files on PCs (excluding system files or other files that would create problems with operation).
We are able to set access privileges, usage period, and more with file encryption, and use the NEC Group standard setting (viewing prohibited for persons outside the NEC Group) as the minimum security level. This enables us to prevent the leakage of information even if information is sent outside the company due to malware infection or is sent accidentally by email, as has been seen in cases of personal information leaks.
Countering information leakage due to internal fraud is also required, as evidenced by the recent case of large-scale information leakage in a major distance education provider.
NEC employs device usage control in its information leakage prevention system.



File Encryption Using InfoCage FileShell and Usage Restrictions

As an example, we set usage restrictions that prohibit any recording of information on external media such as USB flash drives, SD cards, CDs, and DVDs, as well as on communications devices such as smartphones and devices using Bluetooth or infrared, and distribute and control these as a matter of NEC Group policy.
To handle cases in which specific users must use a restricted device, we have readied mechanisms that allow organization-specific customization of usage restrictions. Usable devices and usage restrictions are set for each organization or user, and are controlled by the organization to restrict usage to the minimum required.

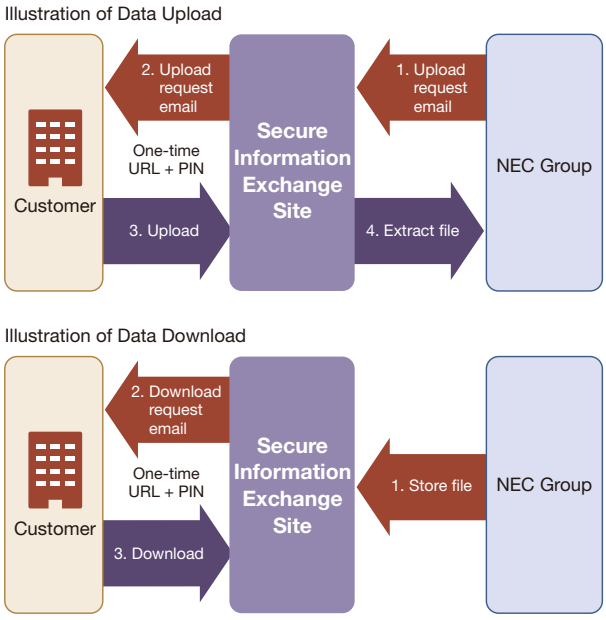


Overview of Information Leakage Prevention System

In addition to device restrictions, we also perform management through log recording and monitoring. We record all PC operation logs for employees, and, when incidents of writing onto external media not approved by the company or acquisition of large volumes of information are detected, provide corrective guidance.
In the event that an information leakage incident does occur, analysis of logs is a significant aid in analyzing the incident in terms of its scope of impact and current status, as well as in formulating measures to prevent recurrence.
The NEC Group is creating a more advanced infrastructure to quickly detect anomalous behavior and warning signs of internal fraud or external threat. This includes the implementation of a log monitoring system (data collection, aggregation, accumulation, analysis, visualization, etc.) that collects, accumulates, and analyzes logs of varied types and sources.
In addition, to prevent information leakages due to internal fraud, we specify the systems within the NEC Group that are subject to focused management, taking into account the degree of impact on the business in the event of an incident. The specific measures we implement with regard to these include 1) vulnerability information collection and handling, 2) log management, 3) network protection, 4) authentication, 5) access control, 6) privileges management, 7) secure operation and maintenance procedures, 8) operation and maintenance checking, 9) security settings, 10) physical entry controls, and 11) contractor management.

(2) Secure Information Exchange Site

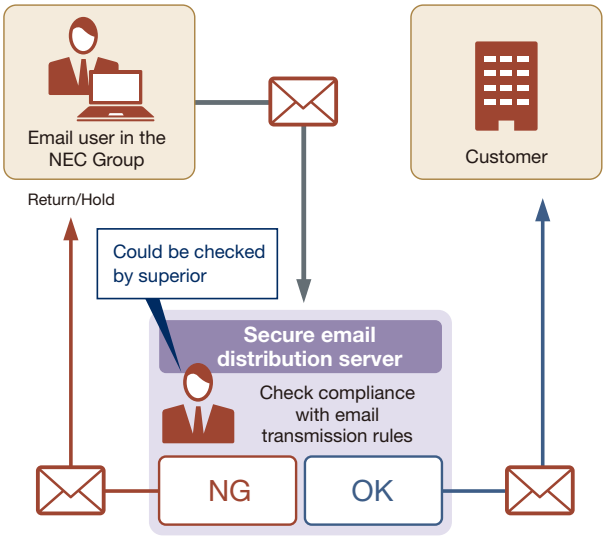
The NEC Group operates a secure information exchange site to safely and reliably exchange important information with customers and business partners.
NEC conducts the exchange of information in access-restricted areas of the secure information exchange site. Access to these areas requires the use of one-time URLs and passwords.
The one-time URLs have time limits, after which they become invalid. Use is also limited to one time only, meaning that once information is acquired it is deleted from the secure information exchange site.
Use of this site reduces the need to exchange information using USB flash drives or other external media, which in turn reduces the risk of information leakage incidents caused by theft or loss.



Secure Information Exchange Site

(3) Email Security System

The NEC Group has implemented a secure email distribution system to prevent incidents of information leakage caused by mistaken email address entry or mistaken email attachments.
The system is equipped with a function to allow superiors or other employees to check details such as email addresses, which also serves to prevent the intentional leak of information through email forwarding.
Our efforts to increase email security also include the rollout of OMCA*1 within the NEC Group. OMCA provides functionality to alert users about suspicious email that may be targeted attack email.
*1 OMCA: Outlook Mail Check AddIn



Secure Email Distribution System

(4) Secure Environment for Working Outside the Office

The NEC Group has a secure external business environment to reduce the number of information security incidents. This system is used by many employees in the Group.

PCs used outside the office are subject to more threats than when used in-house.
The NEC Group has therefore introduced thin client terminals and “Trusted PCs” with enhanced security features to protect the information on the PC in the event of theft or loss. The type of device used when outside the office can be selected according to the purpose of the work and the external environment.
To keep abreast of recent increases in cyber attacks, Trusted PCs are equipped with fully encrypted HDDs, a pre-boot authentication feature that launches before OS startup, remote data deletion/PC locking, a function to mitigate attacks that exploit unknown vulnerabilities, and a feature to block autorun viruses.

Security Elements That Are Being Maintained and Improved

Information Security Human Resources

In addition to increasing employees' awareness of information security,
the NEC Group implements a variety of measures to develop security experts and enhance security promotion skills in order to maintain the required human resources in the information security field.

1 ‖ Developing Information Security Expertise

The NEC Group implements measures to ensure that staff acquire the requisite security expertise from three points of view: 1) strengthening the knowledge and awareness of information security of all employees; 2) developing personnel who promote security measures; and 3) developing professional human resources who can provide value to customers.

2 ‖ Strengthening Knowledge and Awareness of Information Security

Knowing how to properly handle information and having a high level of awareness of information security are important to maintain and improve information security. The NEC Group provides training and awareness-raising events in these fields.

(1) Training on Information Security and Personal Information Protection

The NEC Group provides a web-based training (WBT) course on information security and personal information protection (including protection of people's personal identification numbers ["My Numbers"]) for all employees in the NEC Group to increase knowledge and skills in the information security field. The content of this training course is reviewed every year to reflect the latest trends in security threats and other security-related information. Specifically, the course aims to raise awareness about new security threats and required responses, and ensure that employees thoroughly understand NEC Group policy in important areas such as information handling, internal fraud prevention, contractor management, and Secure Development and Operations.

(2) Commitment to Following Information Security Rules

The NEC Group has established the Basic Rules for Customer Related Work and Trade Secrets, a set of basic rules that must be followed when handling customer information, personal information (including My Numbers), and trade secrets. NEC Group employees are obliged to clearly understand and follow these rules, and pledge to observe all of them. We efficiently manage and thoroughly obtain pledges by using NEC's Electronic Pledge System.

(3) Activities to Raise Awareness of Information Security

The NEC Group performs awareness-raising activities using video dramas about information loss incidents, security incidents that can occur during system development and operation, and other possible mistakes mainly caused by human actions so that employees gain a sense of crisis concerning information security risks and learn how to think, decide and act by themselves. These activities are conducted at each organization in the NEC Group using methods that are most effective for that organization (such as workplace discussions, three-why analysis, video presentations, and other methods that encourage employees to raise their awareness by discussing security issues with colleagues and to improve their analysis and judgment skills).

3 ‖ Developing Human Resources to Promote Information Security Measures

The NEC Group has an information security promotion structure and deploys a variety of measures to promote information security. Since the information security promoter in each organization plays an important role in deploying these measures, NEC is committed to developing human resources with the necessary skills for this job.

(1) Training Information Security Promoters

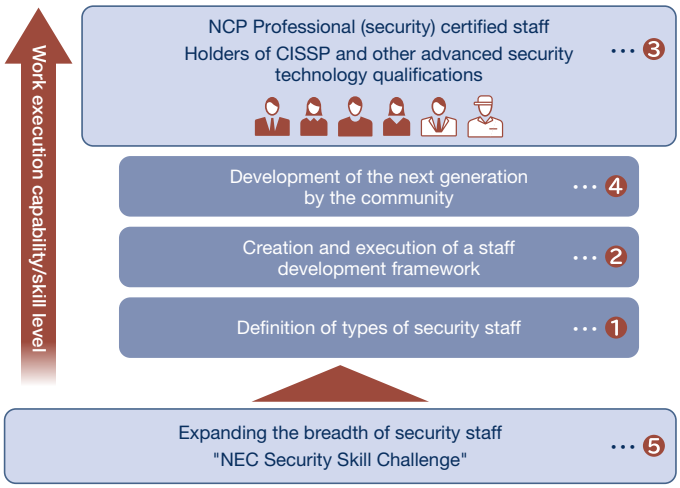
The NEC Group carries out training so that the information security promoter in each organization can gain the requisite knowledge of the management system, roles, security measures, details of promotion, and other topics required to promote information security measures. We also provide training that uses videos derived from incidents to develop practical skills and enhance risk control capabilities and voluntary thinking/acting in order to obtain the skills required to manage risks, which differ depending on each organization.

(2) Auditor Training

The NEC Group visits business partners to conduct information security audits ("on-site assessments") so as to maintain and improve information security at our business partners. We have established a training system based on standardized auditing methods and are training auditors to perform on-site assessments using these methods.

4 Developing Experts

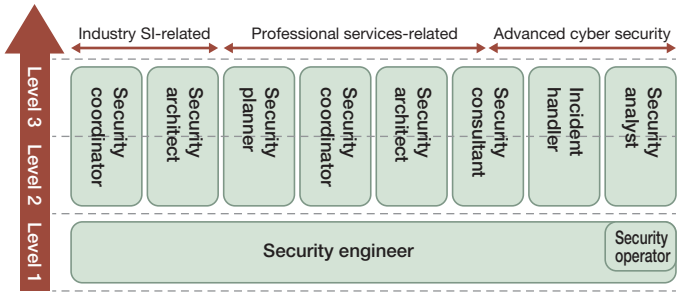
NEC is actively developing security experts to expand our cyber security business, enhance our security response capabilities in products, systems, and services, and contribute to our customers in a variety of areas.



Professional Staff Development

(1) Definition of Types of Security Staff

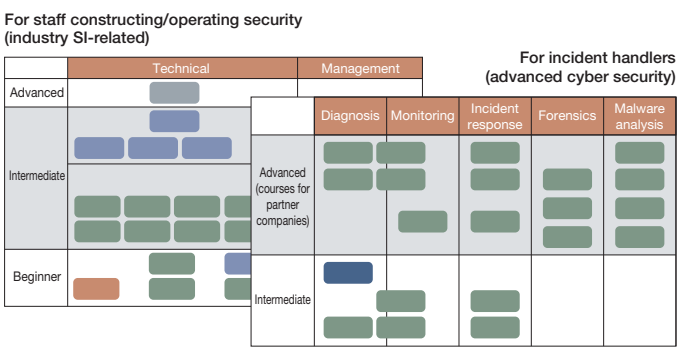
We define the security staff necessary for the NEC Group and work to develop staff in each category. We also ensure that our definitions are aligned with the types of staff required by our customers, and continue to adjust our definitions as required.



Types of Security Staff

(2) Creation and Execution of Staff Development Framework

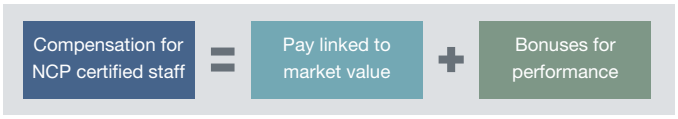
We collaborate with the Cyber Defense Institute and other NEC Group companies and partner companies to optimize training for each type of staff. We are also expanding the targets of training to enable our customers to undergo our training courses as appropriate.



Training Courses

(3) Certification System and Compensation Packages to Maintain Top Staff

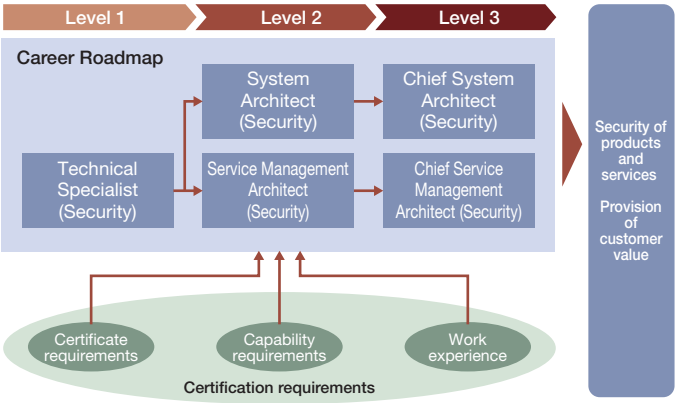
NEC has established a professional certification system (NCP certification system) to certify staff holding high-level security expertise and to provide compensation packages linked to market value.



NCP Senior Professional Compensation Framework

NEC also strongly recommends the acquisition of official qualifications for security, and is expanding the number of staff with CISSP*1, which is an international certification, Information-Technology Engineers Examination for Information Security Specialist, and the upcoming qualification for information processing safety assurance support staff.
Employees who have advanced skills, work experience and/or certification in the information security field take the lead in providing customers with optimal solutions.

*1 CISSP Certified Information Systems Security Professional



- **System Architect (Security) : Assuring the security quality of information system**
  Threat/vulnerability analysis, definition of security requirements, architecture design and other processes
- **Service Management Architect (Security) : Assuring the security quality of IT services**
  Security management, monitoring, incident response and other processes

Professional Certification System (Security)

(4) Development of the Next Generation by the Community

In order to expand the NEC Group's cyber security business while responding to the expectations of customers, we must systematically and continuously develop the next generation of professional staff. The NEC Group already has a community made up of over 300 professional staff, and follows up on professional development of the next generation through means that include holding regular workshops on topics such as sharing of intelligence and investigation of technology.

(5) Implementation of CTF across the Group

The NEC Group conducts the NEC Security Skill Challenge, an internal Capture the Flag (CTF) event aimed at all of our employees. In fiscal 2015, about 600 staff took part in the competition, undertaking about 100 questions over the course of two weeks. With over half of the participants engaged in work other than security work, the event leads to expanding the breadth of our security human resources.

NEC's Cyber Security for Customers

NEC's Cyber Security Strategy

Cyber attacks go beyond national borders, creating a problem for global society.
By leveraging the strength of our Group to provide safe, secure, and comfortable environments in cyber space, NEC will help achieve an information society that is friendly to humans and the earth.

1 ‖ Basic Policies

In a keynote speech titled "Shaping the Communications Industry to Meet the Ever-Changing Needs of Society " in October 1977, the NEC Group put forth "C&C (Computer & Communication)" as its slogan for achieving the integration of computers and communications. In line with this declaration, by connecting the world's computers, we have been able to connect people with things and things with things, contributing to societal development that meets many of society's needs.
The NEC Group has built up and leverages many technologies that have supported infrastructure vital to society, from domestic traffic control systems, firefighting and disaster prevention systems, water management systems, ATMs, and logistics systems, to systems used on the ocean floor and in outer space. In doing so, we are engaged in global development of total security that fuses the physical and the cyber.
Looking ahead, with the appearance of the IoT*1, automobiles, smart meters, and other objects will connect over cyber space to make our lives more convenient. At the same time, however, the threat of cyber attacks is becoming a global social issue, and the problem of "cyber-physical attacks"—attacks from cyber space that have an impact on the real world—is becoming more severe.

Cyber security, too, is moving ahead, driven by research and development into new security technologies such as automated prediction and defense. These technologies leverage not only the defense and detection technologies of the past but also big data, SDN*2, and cloud computing.
Amid this, we are advancing the practical realization of mechanisms to support intelligence-based decisions (i.e., decisions made based on learned data), and systems that use AI (artificial intelligence) to automate decisions to isolate systems based on detection of abnormalities, and thereby localize damage.
With regard to the physical, too, we are undertaking testbed demonstrations that analyze signal data from sensors and make use of cyber space in a variety of areas, including achievement of failure prediction, a solution to locate lost children by analyzing human behavior from surveillance camera footage, and tracking of stolen automobiles or items.
The NEC Group will advance the fusion of the physical and the cyber, create secure cyber spaces, achieve a society and lifestyles rich with bright hope, and connect these to a better future.

★1 IoT: Internet of Things
★2 SDN: Software-Defined Networking

NEC's Business Domains That Support Social Infrastructure

2 ‖ Investments in Cyber Security

(1) Human Resources and Technology

Human resources, technology, and information are the engines that drive NEC's cyber security business. NEC continues to make investments not only in Japan but around the globe. We welcomed the Cyber Defense Institute, Inc. into our Group in 2013, followed by Infosec Corporation in 2014. In that year we also concluded an agreement with the Singapore Economic Development Board to accept trainees from the Strategic Attachment and Training (STRAT) Programme, took part in the practical cyber defense training CYDER*3 and in CTF*4 security contests with outside organizations, and established an endowed lecture series at the Japan Advanced Institute of Science and Technology (JAIST) to actively develop human resources. Through these activities, we are contributing to a stronger security human resource base for Japan.

⋆3 CYDER: Cyber Defense Exercise with Recurrence
⋆4 CTF: Capture the Flag

Strengthening the human resource base

Cyber Defense Institute, Inc. becomes a Group company (March 2013)
Strengthening of top human resources with advanced skills and knowledge

Infosec Corporation becomes a Group company (February 2014)
Strengthening of security monitoring know-how and monitoring business

Joint human resources development with the government of Singapore (September 2014)
Development of cyber security experts, which are lacking internationally

Practical cyber defense training CYDER (October 2014)
Accepted commission of Ministry of Internal Affairs and Communications' "Testbed Demonstration of Model Practical Training for Cyber Attack Analysis and Defense" project from fiscal 2013. NEC created and operated training program.

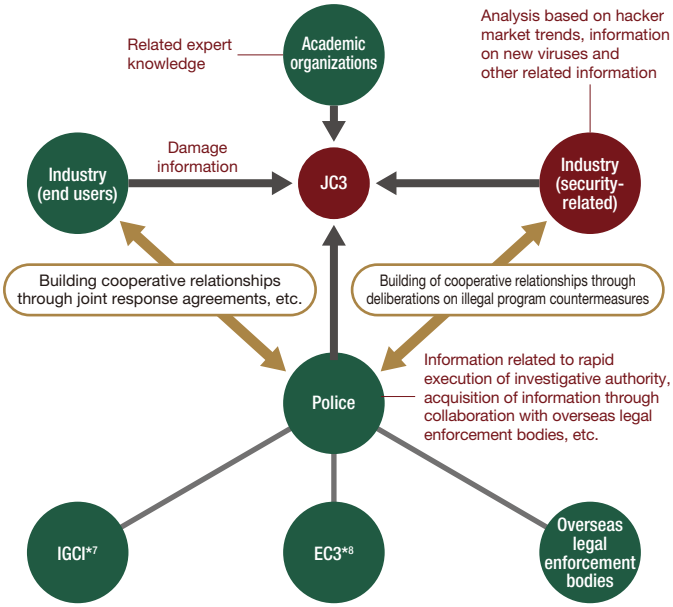
Establishment of endowed lecture series at the Japan Advanced Institute of Science and Technology (JAIST) (November 2014)
Name of lecture series: "Cyber Range Organization and Design (CROND): Cyber Security Education and Training"

In 2015, the Ministry of Economy, Trade and Industry and the IPA*5 released "Cybersecurity Management Guidelines" aimed at small-to-medium companies. Cyber security measures are now being advanced by many of our customers. However, with a lack of cyber security human resources a pressing issue, NEC is making efforts to develop human resources in cooperation with a large number of customers, business partners, and related organizations.
The education programs offered by the NEC Group contain a variety of programs such as training for targeted email attacks. Among these, in our cyber attack training program persons in charge of security in information system departments learn through actual experience with the flow of actions in incident handling, including incident discovery, reporting, identification of problem areas, isolation, analysis, and confirmation of damage status. Through this experience, we hope that the program will offer a venue for improvement of customers' technical capabilities and for confirming the sufficiency of cyber security measures for the ICT platforms that support customers.
This program is increasingly used by CSIRT*6 personnel, and is used by customers not only in Japan but widely across the globe.

⋆5 IPA: Information-technology Promotion Agency, Japan
⋆6 CSIRT: Computer Security Incident Response Team

(2) Strengthening of Information Platforms

To strengthen information platforms against increasing cyber crimes, we collaborate with related organizations in Japan and overseas. In addition to participating in the Control System Security Center, in 2015 we participated in the Japan Cybercrime Control Center (JC3), and are contributing to the creation of a safe, sound, and comfortable environment by promoting government-industry-academia collaboration with domestic academic research organizations, industry, and legal enforcement bodies, by enhancing cyber crime response, and by returning the gains from these activities to society.



⋆7 IGCI: The INTERPOL Global Complex for Innovation
⋆8 EC3: European Cybercrime Centre

Framework centered on the Japan Cybercrime Control Center

In 2012, NEC cooperated with INTERPOL (The International Criminal Police Organization) on global cyber security countermeasures. The purpose of this cooperation was to investigate and analyze increasingly more complex and high-level cyber crimes through INTERPOL's international network and NEC's cutting-edge cyber security solutions, to strengthen cyber security at the international level. Also in 2015, NEC provided core systems for the Digital Crime Centre established in the INTERPOL Global Complex for Innovation opened by INTERPOL Singapore.

Operation center (Cyber Fusion Centre)

3 ‖ Global Expansion

(1) Trends in Cyber Security Around the World

The threat of cyber attacks goes beyond national boundaries to create a global-scale social problem, and interest in this field is increasing each year. NEC engages in global-level deliberations on the latest initiatives and participates in a number of international meetings, conferences, and forums on cyber attacks and crimes that leverage cyberspace, addressing topics that range from laws, policy, and organizational theory to the latest technological trends. With this situation remaining unchanged in 2016, more active deliberation is expected, focusing on themes that include IoT security, Internet governance, information sharing frameworks, technological support for developing countries, and other key global trends.
In Japan, too, following the enactment of the Cyber Security Basic Law in 2014 and the "My Number" (individual number) system (for social security, taxes, etc.) in 2015, the importance of cyber security is growing and measures against terrorism and cyber attacks are becoming a pressing matter.

(2) Global Safety

NEC has long supported critical social infrastructure in Japan by providing safe, secure, and comfortable environments. Looking ahead, we will continue to leverage our human resources and high technological capabilities to provide total security in both the physical and cyber worlds, including the world's most accurate face and fingerprint recognition systems, national ID management systems, and payment networks. Already, NEC is rolling these out in the U.S., South Africa, Brazil, and Asian countries, while in the APAC (Asia Pacific) region, we are increasing our presence each year as a top-class security consultant and MSS*8 vendor. To meet the expectations of customers around the world, in January 2016 the NEC Group opened a cyber security center in Singapore and will continue to accelerate the global rollout of security solutions.

*8 MSS: Managed Security Service

Establishing the Global Safety Division (GSD) in Singapore for Global Business Execution

- Execution of business through regional competence centers in Singapore, Argentina, etc., and safety teams in multiple countries totaling 500 staff
- Establishment of fifth global research laboratory in Singapore, and focus on research and development in the safety field
- Deployment of SOCs in Japan, Singapore, Australia, and Brazil, and further expansion of global coverage

Rollout of Global Safety Around the World

4 ‖ Globalization of Security Operations Centers

To protect critical infrastructure and our many customers' ICT infrastructures in Japan from the threat of cyber attacks, the NEC Group is exerting its collective power to roll out Security Operations Centers.
Among our multiple Security Operations Centers in Japan, we established the Cyber Security Factory in Japan in 2014 as a core base for responding to the threat of cyber attacks. The new Cyber Security Factory established in Singapore in January 2016 collaborates with the core base in Japan in sharing information on cyber attack threats to offer customers safety and security 24 hours a day.
The security services provided by the NEC Group's Security Operations Centers include 24/7 security operations monitoring services, advanced security intelligence, incident response support, and other services that address diverse cyber security risks. Through One NEC, we also offer equipment and systems that can support stable and continuous operation of customers' ICT infrastructure, including network surveillance and help desks.

NEC's Cyber Security for Customers

NEC Cyber Security Solutions

Drawing on our knowledge of the latest cyber security trends and information leak incidents, we provide total support for strengthening security measures while leveraging the existing security measures in which customers have invested.

1 ‖ Provision of Solutions Based on In-house Operational Know-How

(1) Counting Management

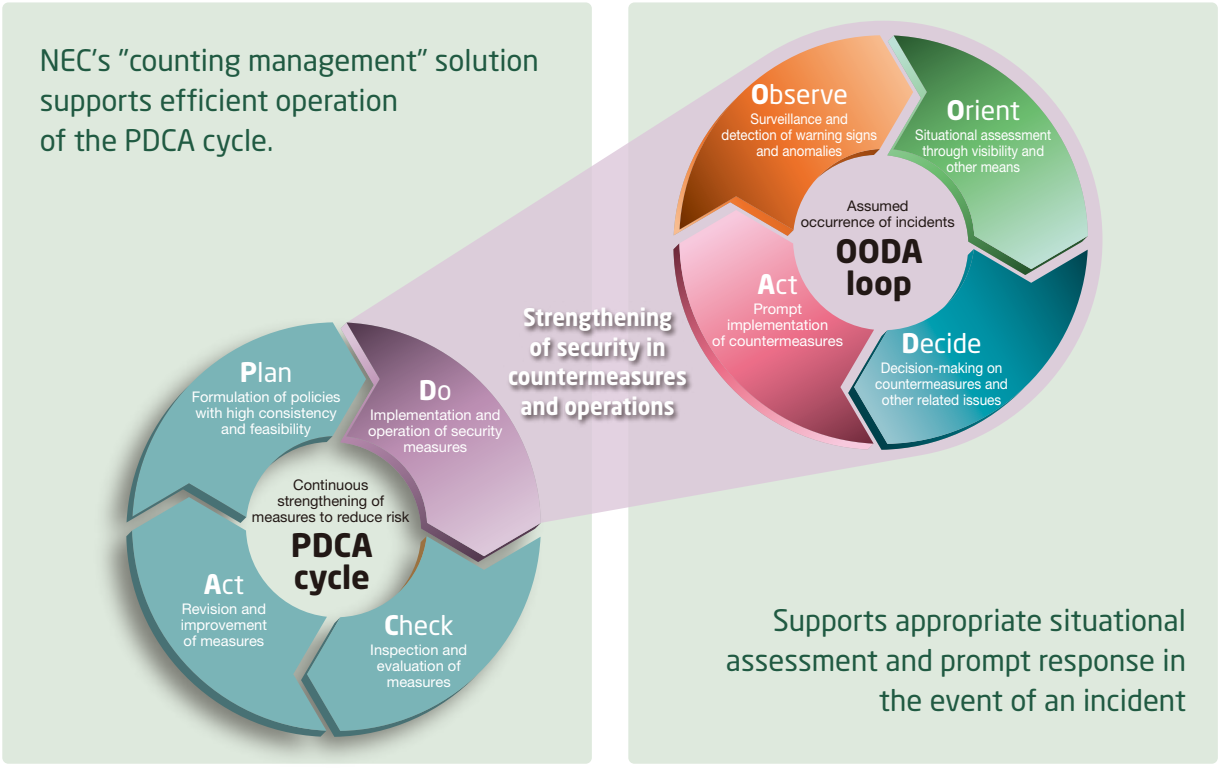
The first step in the NEC Group's security measures has been working to make people, IDs, PCs, servers, and logs more visible as numerical values in order to assess what sort of problems lie where, and deciphering these values to indicate the priority of measures in a form that anyone can understand. By making these items visible, the NEC Group's "counting management" solution can be used to resolve customer's concerns over security operations issues vulnerable to human error, such as forgetting to apply patches or install anti-virus software on PCs.

(2) Solutions Tested by the NEC Group

The NEC Group internally uses its own cyber security solutions and provides customers with only those that have demonstrated effectiveness in convenience and safety. In addition, by feeding back know-how gained from our in-house operations to our customers, we contribute to the improvement of availability and quality in maintenance and operations.

2 ‖ PDCA and OODA

Security measures do not end with the adoption of security products. It is necessary to prevent the degradation of security quality by carrying out appropriate operation and monitoring and by implementing the information security management cycle of Plan, Do, Check, and Act (PDCA).
The increasingly advanced and numerous cyber attacks of recent years occur faster than implementation of the PDCA cycle. For that reason, we have adopted the concept known as OODA, which implements fast operation of the cycle of Observe, Orient, Decide, and Act within the PDCA cycle's step of Do. This enables faster initial response through rapid detection of warning signs and incidents followed by accurate situational assessment, supporting the localization of damage.
By providing necessary security functions matched to customers' business environments, the NEC Group's cyber security solutions contribute to the creation of a safe, secure, and comfortable society together with our customers.



PDCA cycle and OODA loop

3 ‖ Support for CSIRT Construction Modeled on NEC-CSIRT

In July 2000, the NEC Group launched a team focused on in-house incident response operations, and since then has engaged in cyber security countermeasures. The team has expanded its work to investigate increases in incidents and recent trends in attacks, analyze methods of attack, and so on, and in 2005 began incident analysis and response support for incidents occurring within the NEC Group and customers alike. At present, taking the "C" in CSIRT (Computer Security Incident Response Team) to stand for "Corporate" as well as "Computer" as a key theme in management strategy, the team adopts the role of responding to incidents that threaten business continuity in both the physical and cyber worlds.

Typical CSIRT functions include incident response, forensics, recovery work, and collaboration with external organizations. However, these functions require preparation matched to customers' business scale, industry, form of business, and organization, and even when all functions are readied despite this challenge, the result can be insufficient personnel or skills and excessive investment in equipment. The NEC Group's assessment and consulting services meet a wide range of needs, from launch of required CSIRTs matched to customers' business scale and industry to support for defining their operating processes. After construction of a CSIRT for a customer, we also assist in the smooth operation of the CSIRT.

4 ‖ Intelligent Response Support System

(1) NCSP (NEC Cyber Security Platform)

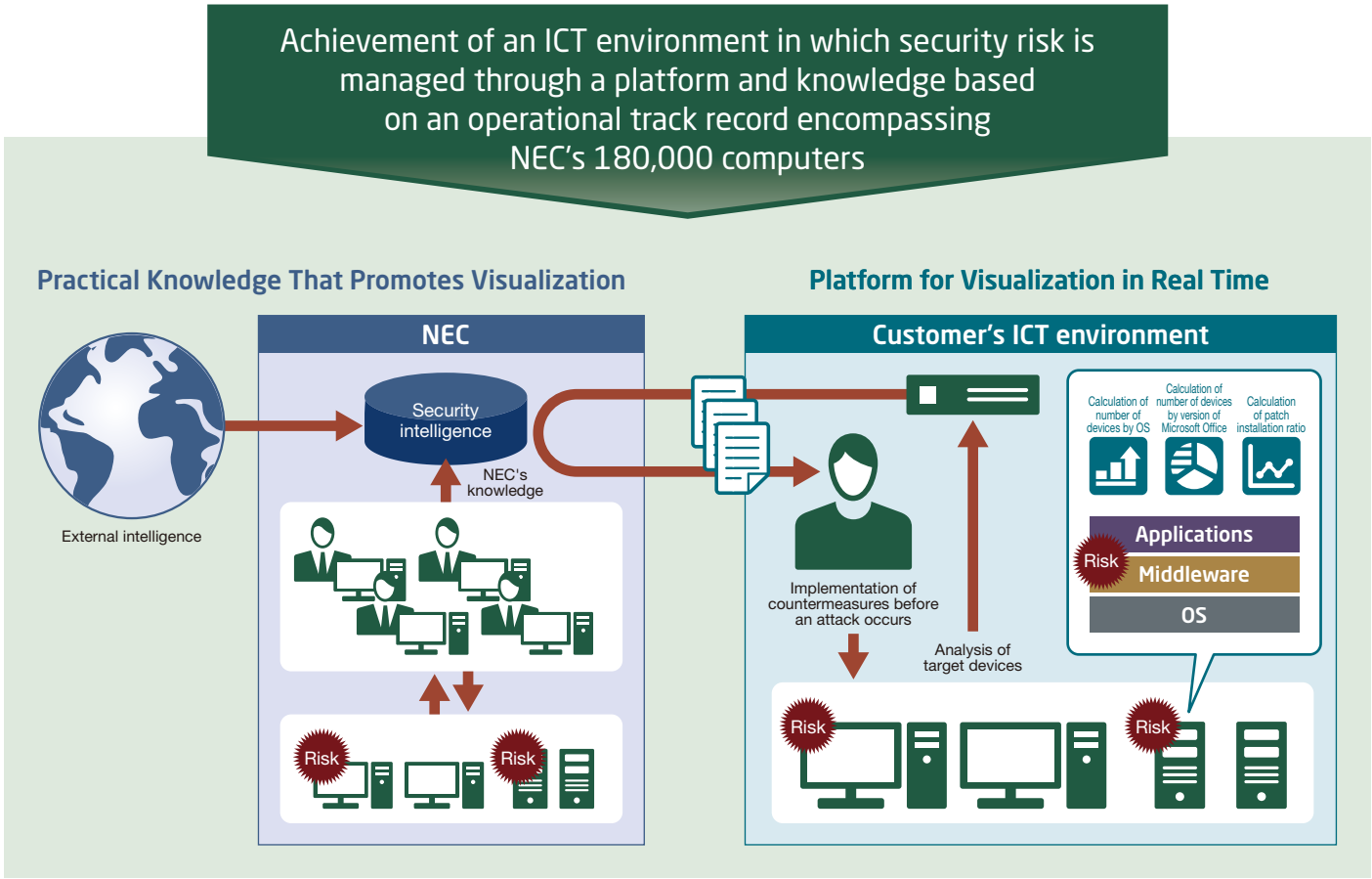
NCSP is the NEC Group's original security integration, management, and response solution to support the drafting and execution of vulnerability countermeasures and incident response. Taking advantage of the cyber intelligence provided by the NEC Group, it enables real-time visualization of the latest security risks (vulnerabilities) affecting in-house systems and supports the presentation and execution of measures against these security risks, to achieve proactive security measures before a cyber attack strikes.
The NEC Group's CSIRT uses NCSP to increase the efficiency of response to incidents occurring in the operation of 180,000 PCs and servers globally.

(2) Functions to Support Drafting and Execution of Vulnerability Countermeasures

To efficiently achieve management of vulnerabilities, the Incident Response Support System centrally manages the distribution of vulnerability information in English and Japanese, the drafting of multiple countermeasure methods, and the application and confirmation of measures. This enables rapid assessment of circumstances after information on a vulnerability has been received.

(3) Incident Response Support

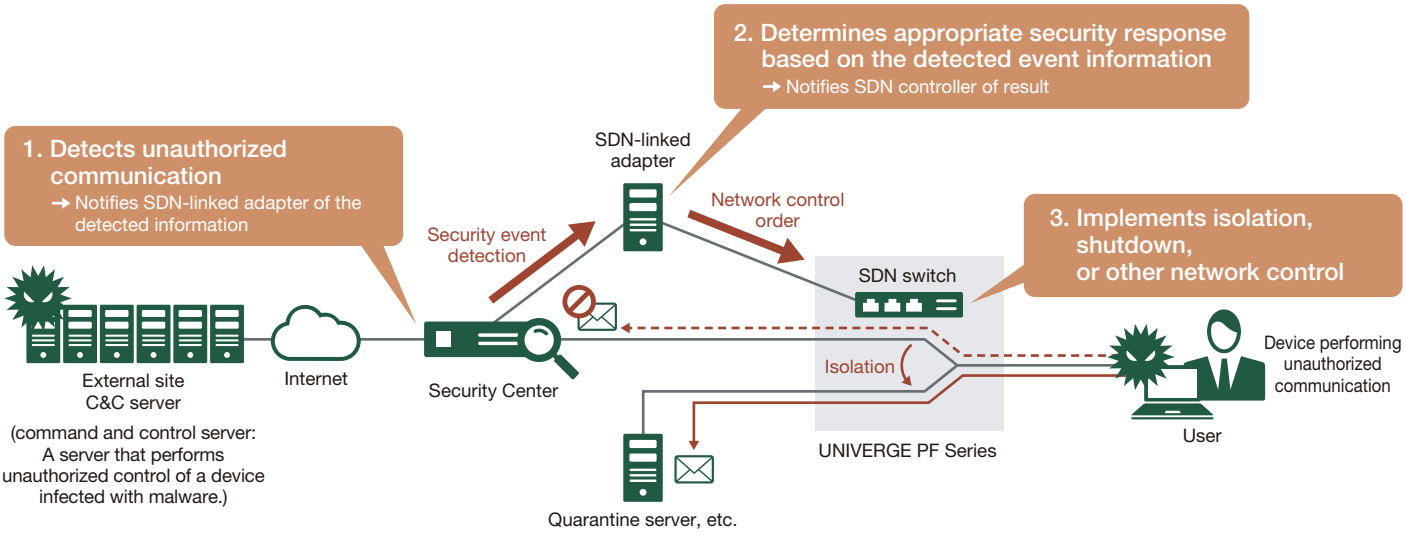
The Incident Response Support System achieves more efficient incident response work by enabling remote initial response to isolate devices when an anomaly is detected rather than cut off the network, and by supporting remote investigation and analysis of the isolated environment.



Overview of the NEC Cyber Security Platform

5 Cyber Attack Automated Defense Solution That Achieves Prompt Initial Response Even When a Professional Is Not Present

Leveraging SDN (software-defined networking), one of the core businesses of the NEC Group, we have developed and offer a cyber attack automated defense solution that achieves automatic and prompt initial response even when professional staff is not present.
This solution notifies an SDN-linked adapter of anomaly information when a security sensor connected in an SDN environment detects an anomaly. Based on the information in the notification, the SDN-linked adapter automatically directs the SDN controller to isolate the anomalous device from the corporate network, achieving prompt localization of damage.

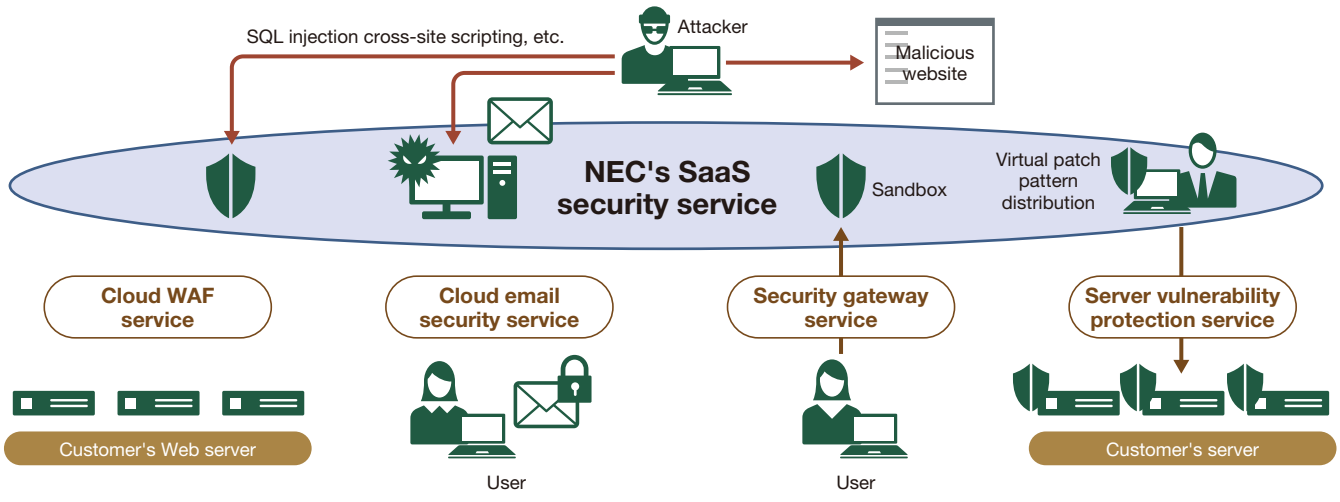


SDN-Linked Cyber Attack Automated Defense Solution

6 Cyber Security Services Provided from the Cloud

The NEC Group's cyber security services are provided through cloud services that feature NEC's high technical prowess, the high cost performance, functionality and reliability of the NEC Cloud IaaS, and strict access control that conforms with standards of CSA*1 and FISC*2 (an incorporated foundation that has developed various guidelines such as "Security Guidelines on Computer Systems for Banking and Related Financial Institutions").
The cyber security services that we offer through the cloud include WAF (Web Application Firewall), email security, security gateway, and server vulnerability protection. Customers are able to quickly begin using these safe and secure security measures over their Internet connection without deploying new security equipment.

*1 CSA: The Cloud Security Alliance
*2 FISC: The Center for Financial Industry Information Systems



Cloud-based Security Services

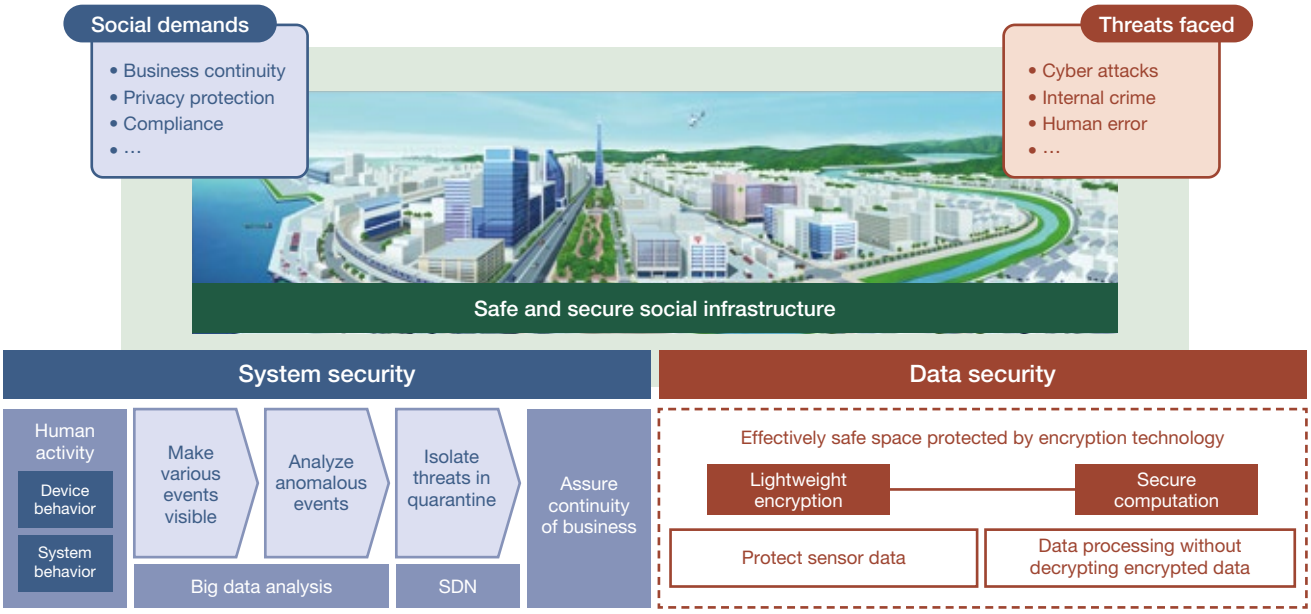
NEC's Cyber Security for Customers

Research and Development – Cutting-edge Cyber Security Technology

NEC conducts research and development into new cyber security technologies that feeds into the development of new solutions and services, strengthening our ability to respond to ever more sophisticated and advanced cyber attacks.

1 ‖ Concepts for Research Themes

Under the slogan "Futureproof security. Beyond the frontlines of cyber security," the NEC Group conducts research and development into both system security and data security for increasingly advanced social infrastructure, and, by helping to build social infrastructure that does not stop, break, or malfunction, provides customers with safe, secure, and comfortable environments.
In the field of system security, we create collaborations among multiple technological elements to combat ever more sophisticated and advanced cyber attacks and enhance defensive capability. This includes the achievement of quarantine networks that leverage SDN, and analysis of big data to defend against unknown attacks.
In the area of data security, we are developing database encryption, "lightweight encryption" to equip resource-constrained IoT devices with encryption functions, and secure computation technology that achieves the world's first processing of data that remains encrypted.



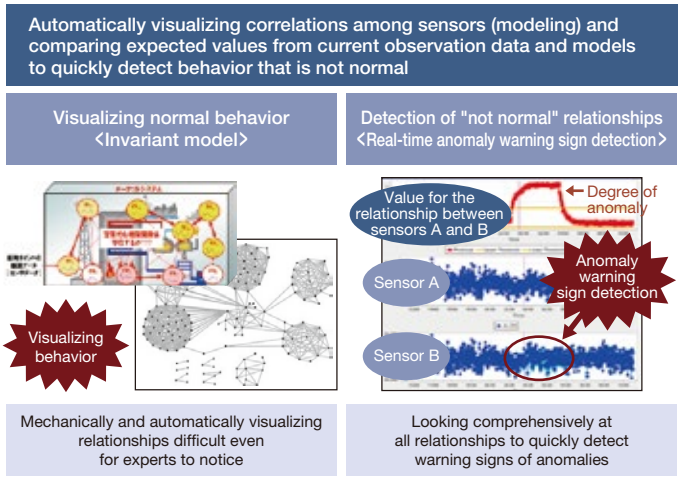
Concepts for Research Themes

2 ‖ Big Data Analysis

The NEC Group has been conducting artificial intelligence (AI) research for many years, with a particular focus on discovering new principles through advanced technologies, and research and development into detection and prediction of warning signs.

(1) Invariant Analysis

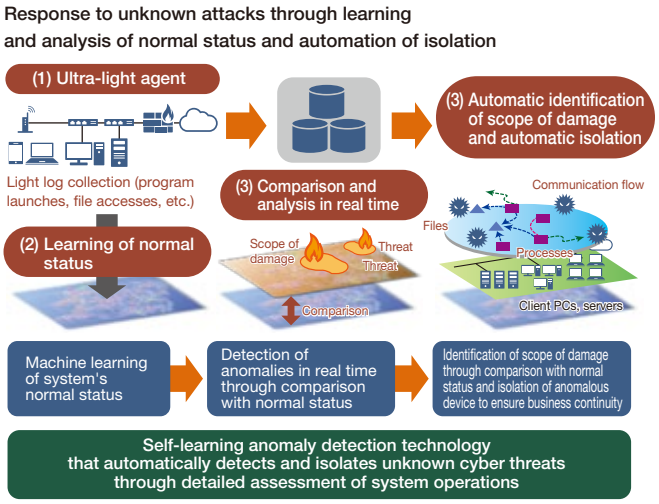
This technology analyzes large volumes of time series data from sensors to automatically create models that use the invariant relationships among sensors under normal conditions as relational expressions. These models and sensor data are used to quickly discern behaviors that are "not normal" and thereby detect warning signs of anomalies occurring in a system.
Correlations among the sensors are automatically identified through machine learning, enabling the discovery of relationships that would be difficult even for experts to notice. In addition, in the same manner as the process by which humans make "big-picture" evaluations, system statuses can be evaluated by comprehensively seeing the relationships among all the sensors.



Invariant Analysis

(2) Self-learning System Anomaly Detection Technology

This technology automatically detects unknown cyber attacks using artificial intelligence (AI). It performs machine learning of normal statuses based on the complex operational status of the entire system, including program launch and file access on devices or servers as well as communications, and conducts real-time comparison and analysis of normal statuses and current system activity to enable detection of "not normal" behaviors and response to unknown attacks. Furthermore, by linking with system management tools and SDN, the technology can perform automated isolation of anomalous devices from networks. The technology can identify the scope of damage in under one-tenth the time required for conventional response, minimizing the spread of damage without needing to stop the whole system.



Self-learning System Anomaly Detection Technology

(3) Secure Networks

The IoT and the Internet for industry are expected to proliferate in the near future. However, the cyberspace in which people and objects connect is not necessarily safe, and the reliability of the people and objects that connect in cyberspace, and the authenticity of the data they send, are not guaranteed.
The NEC Group is engaged in research and development of tomorrow's secure networks that will resolve these issues and enable all people to equally enjoy the benefits of the IoT era.

(4) Cyber Intelligence

The NEC Group is engaged in research and development that will enable fast detection of the warning signs of cyber attacks, as well as automatic implementation of effective countermeasures at the appropriate timing.
We also share information on threats to strengthen responses to cyber attacks, and are undertaking active research and development on specifications to describe cyber attack information and methods for sharing information among organizations, including the STIX*1 and TAXII*2 concepts being studied by standardization body OASIS*3.

★1 STIX: Structured threat information expression
★2 TAXII: Trusted automated exchange of indicator information
★3 OASIS:Organization for the Advancement of Structured Information Standards

3 ‖ Encryption and Secure Computation Technology

(1) Lightweight Encryption

In the coming IoT era when objects start to be connected to networks, device authentication for these objects and protection of communication data against eavesdropping will be vital. However, many sensor devices cannot be fully equipped with standard encryption technologies for performance reasons or due to insufficient resources or available power. In 2012, the NEC Group announced TWINE, lightweight encryption that achieves a high processing performance and world-class lightness even in resource-constrained devices. In 2015, we announced OTR*4, an authentication encryption method that cuts conventional data processing volume in half (a theoretical limit) through increased efficiency. In addition, the authentication encryption method AES-OTR, developed by the NEC Group, passed primary selection in a technical review held with the support of the U.S. National Institute of Standards and Technology (NIST). We plan to strengthen our authentication encryption design and implementation technology with the aim of having it adopted as the next-generation authentication encryption methodology.

★4 OTR: Offset Two-Round

(2) Secure Computation

The NEC Group has developed the world's first secure computation technology that allows data in databases to be processed while remaining encrypted.
Through this technology, information in an encrypted database can be used as it is without the need for decryption for processing by applications. This reduces the risks of leakage and theft of data.

4 ‖ Cloud Technologies

(1) Secure Storage Archives

With the proliferation of cloud storage services, important data is increasingly stored in the cloud. NEC is undertaking research and development into a technology to safely store and utilize this data so that it can be put to greater use.
With this technology, we encrypt data using a technology for secret sharing, apply distributed storage and redundancy, and perform periodic high-speed inspections, automatically restoring data even in the case of loss.
This technology assures confidentiality, integrity and availability, and creates new value that allows customers to use cloud services safely, securely, and efficiently.

Third-party Evaluations and Certifications

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

1 ISMS Certification

The following companies have units that have obtained ISMS (ISO/IEC 27001) certification, an international standard for information security management systems.

NEC Group Companies with ISMS Certified Units

- NEC Corporation
- ABeam Consulting Ltd.
- ABeam Systems Ltd.
- NEC Engineering, Ltd.
- NEC Space Technologies, Ltd.
- NEC Solution Innovators, Ltd.
- NEC Nexsolutions, Ltd.
- NEC Networks & System Integration Corporation
- NEC Network and Sensor Systems, Ltd.
- NEC Network Products, Ltd.
- NEC Business Processing, Ltd.
- NEC Fielding System Technology. Ltd.
- NEC Platforms, Ltd.
- Infosec Corporation
- NEC Informatec Systems, Ltd.
- KIS Co., Ltd.
- Cyber Defense Institute, Inc.
- Sunnet Corporation
- YEC Solutions Inc.
- Q&A Corporation
- NEC Shizuokabusiness, Ltd.
- Showa Optronics Co., Ltd.
- NEC Aerospace Systems, Ltd.
- Forward Integration System Service Co., Ltd.

2 Privacy Mark Certification

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

NEC Group Companies with Privacy Mark

- NEC Corporation
- ABeam Consulting Ltd.
- VALWAY121Net, Ltd.
- NEC Engineering, Ltd.
- NEC Solution Innovators, Ltd.
- NEC Nexsolutions, Ltd.
- NEC Networks & System Integration Corporation
- NEC Net Innovation, Ltd.
- NEC Business Processing, Ltd.
- NEC Facilities, Ltd.
- NEC Fielding, Ltd.
- NEC Fielding System Technology, Ltd.
- NEC Platforms, Ltd.
- NEC Magnus Communications, Ltd.
- NEC Management Partner, Ltd.
- NEC Informatec Systems, Ltd.
- NEC Livex, Ltd.
- KIS Co., Ltd.
- Sunnet Corporation
- Nichiwa
- YEC Solutions Inc.
- Q&A Corporation
- Q&A WORKS Co., Ltd.
- NEC Shizuokabusiness, Ltd.
- D-Cubic Corporation
- Forward Integration System Service Co., Ltd.
- LanguageOne Corporation
- LIVANCE-NET, Ltd.

3 IT Security Evaluations and Certifications

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

NEC products and systems with ISO/IEC 15408 certification

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

Corporate Data

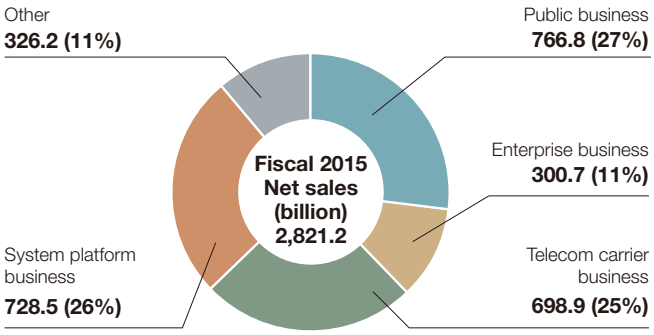
Corporate Profile

Company name	:	NEC Corporation
Address	:	7-1, Shiba 5-chome, Minato-ku, Tokyo, Japan
Established	:	July 17, 1899
Capital	:	¥397.2 billion*
Number of employees (Consolidated)	:	98,726
Consolidated subsidiaries	:	217

*As of March 31, 2016

Segment Information

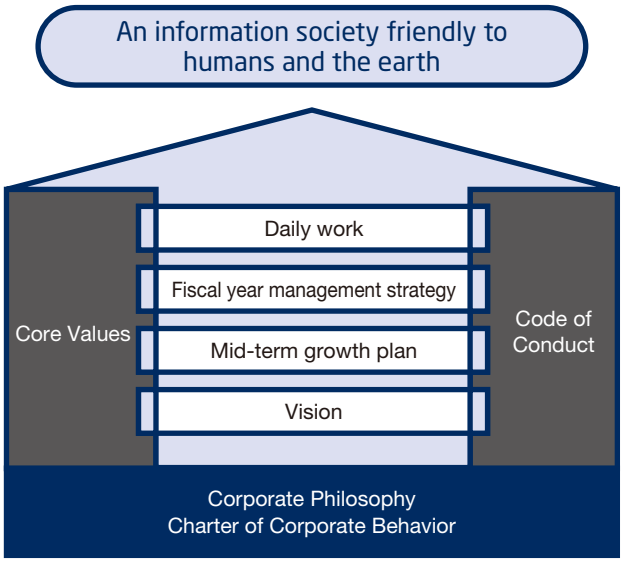
Net Sales by Segment (Percentage)



*As of March 31, 2016

NEC Way

"The NEC Way" is the collective activities of NEC Group management.
This consists of our Corporate Philosophy, Vision, Core Values, Charter of Corporate Behavior, and Code of Conduct.
We put the NEC Way into practice to contribute to our customers and society so as to create an information society that is friendly to humans and the earth.



NEC Group Corporate Philosophy

NEC strives through “C&C”
to help advance societies worldwide
toward deepened mutual understanding
and the fulfillment of human potential.

Established in 1990

NEC Group Vision 2017

The NEC Group Vision 2017 states what we envision as a company, and the society which we will strive to realize in 10 years, in pursuing our Corporate Philosophy. We set our Group Vision “2017”, since that year will mark exactly 40 years since “C&C”, the integration of Computers and Communications, was presented.

To be a leading global company leveraging
the power of innovation to realize an information society
friendly to humans and the earth

NEC Group Core Values

To pursue our Corporate Philosophy and realize NEC Group Vision 2017, we have defined the values important to the NEC Group which is built on over 100 years’ history of our company.
This is what we base our behaviors and individual activities on, as a guidance to better serve our customers and contribute to society.

Core Values	Actions driven by Core Values
[Our motivation] **Passion for Innovation**	• Explore and grasp the real essence of issues • Question the existing ways and develop new ways • Unite the intelligence and expertise around the world
[As an individual] **Self-help**	• Act with speed • Work with integrity until completion • Challenge beyond own boundary
[As a team member] **Collaboration**	• Respect each individual • Listen and learn with open mind • Collaborate beyond organizational boundaries
[For our customers] **Better Products, Better Services**	• Think from a user’s point of view • Impress and inspire our customers • Continue the pursuit of “Global Best”

NEC Corporation

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

Issued September 2016