Empowered by Innovation NEC

Information Security Report 2014

\Orchestrating a brighter world

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.

Takashi Niino
Representative Director &
Senior Executive Vice President
NEC Corporation

The world 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 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, cyber security will be vital to every IT system. NEC is making efforts to strengthen our competitiveness by collaborating with companies that have industry-leading technologies. We also regard the 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.

Information Security Report 2014

Making full use of our core assets in these areas, NEC 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. This approach includes building an information security management system, creating an information security platform, and developing human resources skilled in information security.
- Providing customers with reliable security solutions

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.

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 August 2014.

The names of all companies, systems and products in this report are the trademarks or registered trademarks of their respective owners.

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 systems to comprehensively maintain and enhance information security on multiple levels.

Framework for thoroughly implementing information security across all organizations

Information Security Governance

Framework for creating policies and rules and implementing PDCA cycles

Information Security Management

Framework for utilizing information technologies to protect networks, business systems, PCs, and other system components from threats

Information Security Platform

Framework for developing human resources such as by raising awareness of information security and improving information security skills

Information Security Staff

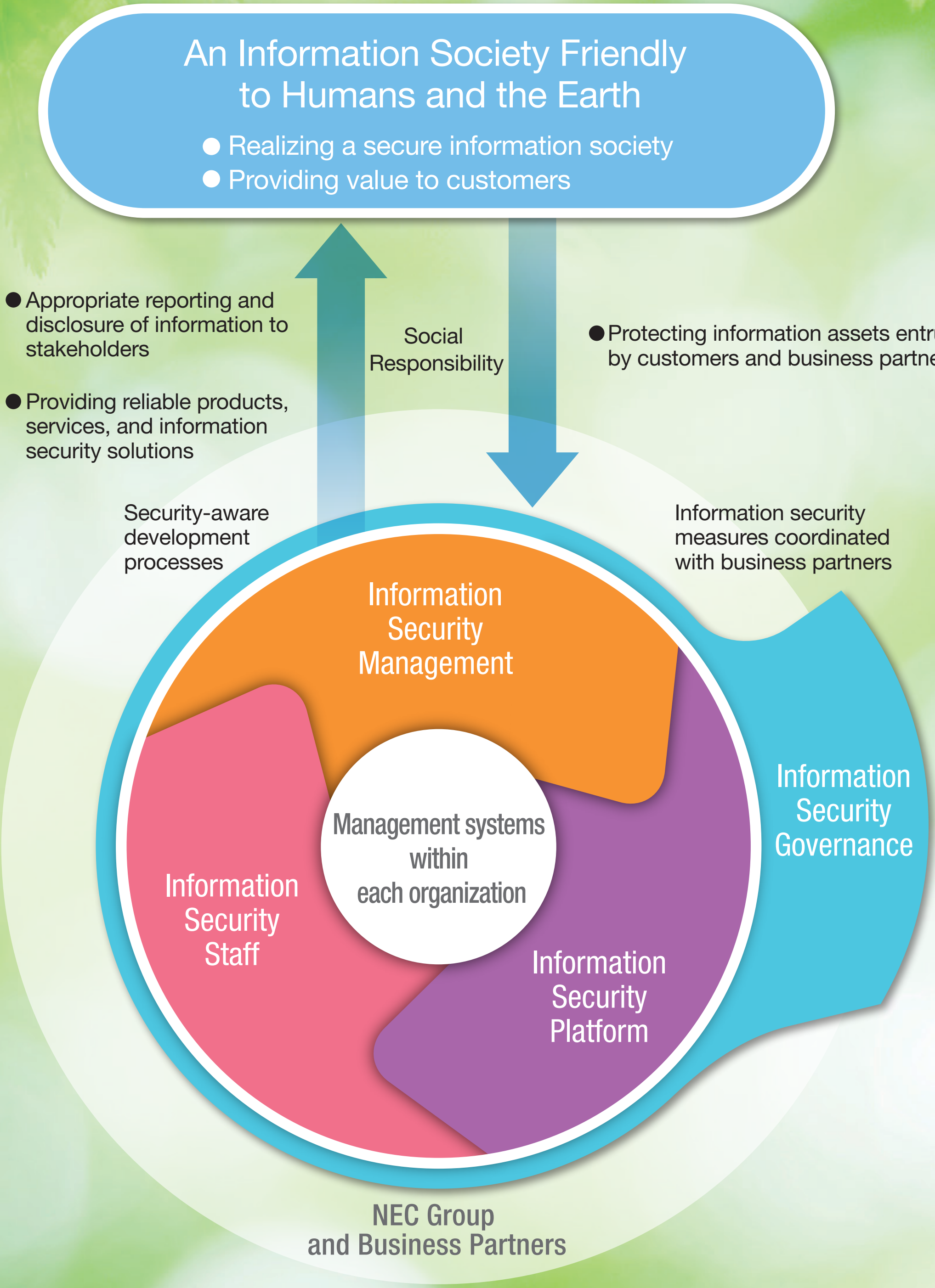
Activities based on these frameworks are divided into two categories: group-wide activities and activities conducted by each organization in the NEC Group.

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 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.

NEC Security Vision

To Become a Leading Information Security Company Trusted by Society



An Information Society Friendly to Humans and the Earth
● Realizing a secure information society
● Providing value to customers
● Appropriate reporting and disclosure of information to stakeholders
● Providing reliable products, services, and information security solutions
Social Responsibility
● Protecting information assets entrusted to us by customers and business partners
Security-aware development processes
Information security measures coordinated with business partners
Information Security Management
Management systems within each organization
Information Security Staff
Information Security Platform
Information Security Governance
NEC Group and Business Partners

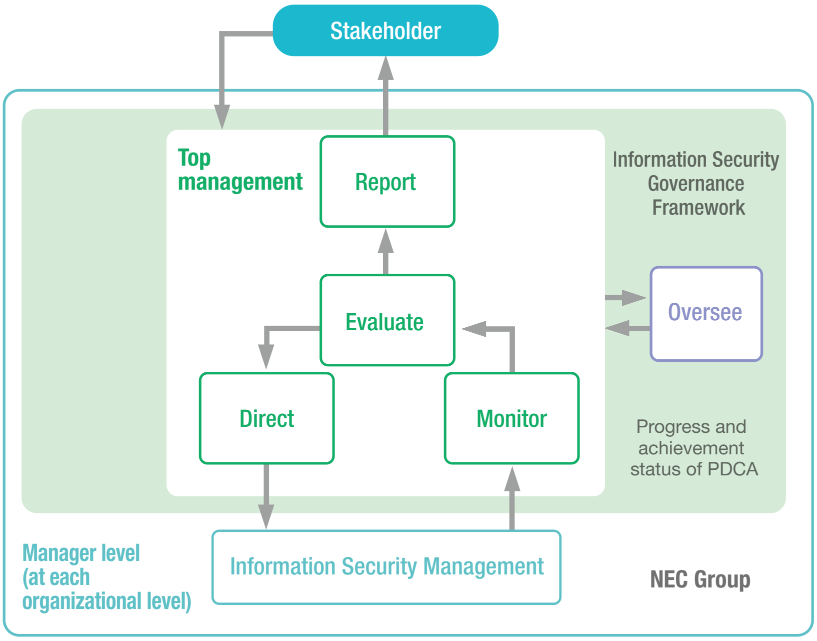
Information Security Governance

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

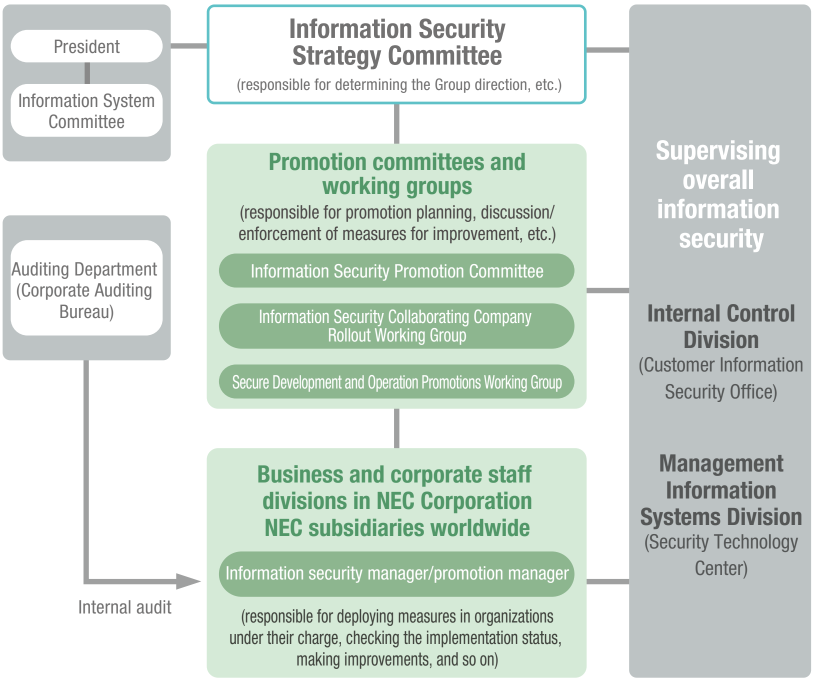

Stakeholder
Top management
Report
Evaluate
Direct
Monitor
Information Security Governance Framework
Oversee
Progress and achievement status of PDCA
Manager level (at each organizational level)
Information Security Management
NEC Group

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 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. 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


President
Information System Committee
Information Security Strategy Committee
(responsible for determining the Group direction, etc.)
Promotion committees and working groups
(responsible for promotion planning, discussion/ enforcement of measures for improvement, etc.)
Information Security Promotion Committee
Information Security Collaborating Company Rollout Working Group
Secure Development and Operation Promotions Working Group
Auditing Department (Corporate Auditing Bureau)
Internal audit
Business and corporate staff divisions in NEC Corporation NEC subsidiaries worldwide
Information security manager/promotion manager
(responsible for deploying measures in organizations under their charge, checking the implementation status, making improvements, and so on)
Supervising overall information security
Internal Control Division
(Customer Information Security Office)
Management Information Systems Division
(Security Technology Center)

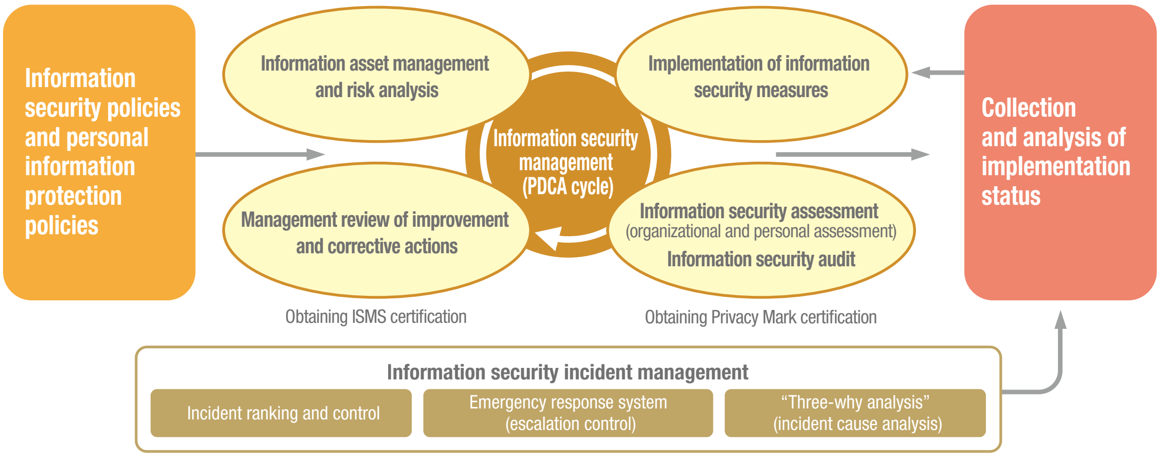
Information Security Management

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



Information security policies and personal information protection policies

Information asset management and risk analysis

Implementation of information security measures

Information security management (PDCA cycle)

Management review of improvement and corrective actions

Information security assessment (organizational and personal assessment)
Information security audit

Collection and analysis of implementation status

Obtaining ISMS certification

Obtaining Privacy Mark certification

Information security incident management

Incident ranking and control

Emergency response system (escalation control)

"Three-why analysis" (incident cause analysis)

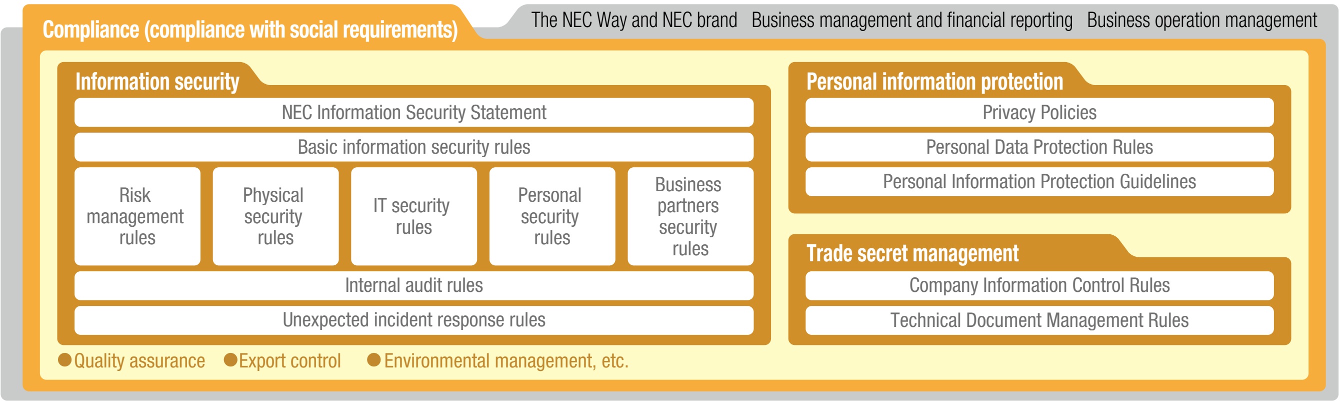
2 Information Security Policies

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 management rules, personal information protection rules, 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 the 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. The NEC Group requires employees to handle personal information at the same protection management level throughout the entire Group. As of August 2014, 28 companies have acquired the Privacy Mark certification.

NEC Group Management Policy



Compliance (compliance with social requirements)

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

Information security

NEC Information Security Statement

Basic information security rules

Risk management rules | Physical security rules | IT security rules | Personal security rules | Business partners security rules

Internal audit rules

Unexpected incident response rules

Personal information protection

Privacy Policies

Personal Data Protection Rules

Personal Information Protection Guidelines

Trade secret management

Company Information Control Rules

Technical Document Management Rules

●Quality assurance ●Export control ●Environmental management, etc.

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 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 New Rules Related to Information Security

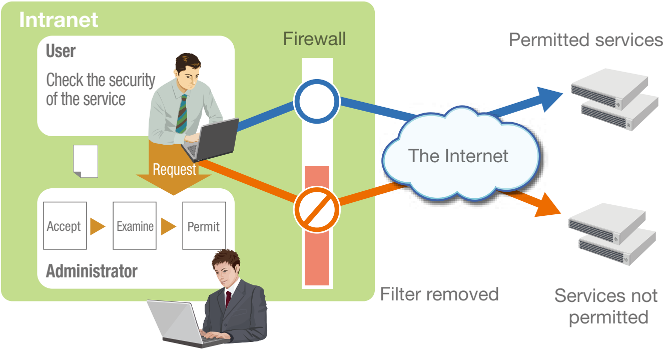
We are establishing rules and operations to keep pace with state-of-the-art information and communications technologies (ICT) such as smartphones, tablets and cloud computing.

① Establishment of External Service Standards

Rapid diffusion of cloud services not only makes it possible to rapidly and easily use sophisticated services via the Internet but also increases the risk of information leaks because trade secrets and other confidential data is processed on external systems. The NEC Group implements standards for using cloud and other external services for business purposes.

Specifically, we provide users with a check sheet that enables them to assess security measures taken by the external service provider with regard to datacenters, system technologies and administration, in order to confirm in advance if the provider provides safe services. Based on this check sheet, the user submits a request for using the service and the request is granted after examination. While some frequently used services are pre-assessed and permitted without request, use of services considered to be risky is prohibited.

Procedure for Starting Use of an External Service



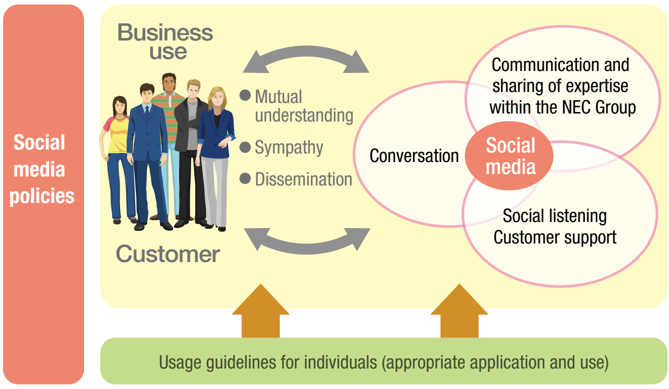
② Rules for Using Smart Devices

As mobile devices such as smartphones and tablets are increasingly used on many occasions, we have established rules for safely using them. While these devices have functionality equivalent to PCs, many of them do not implement sufficient security measures. Therefore, our employees must use only devices recommended by the company, apply patches and upgrades, take antivirus measures, install only reliable applications, and enable automatic lock settings. They are also required to store only the minimum necessary information and promptly report theft or loss.

③ Support for Social Media

The NEC Group has released social media policies and established social media guidelines for business and personal usage. Widespread use of social media allows us to promote interactive communication with customers, but it also increases the risk of information leaks, including trade secrets and private information, denouncements or criticism on the Internet, and personal use of social media in the office. Against this background, we have revised the guidelines for personal use, while keeping basic policies intact. The purpose of the revision is to promote safe usage of information by making employees understand the impact on the company of publishing information or making responses personally on social media, and the responsibility this involves. It will also increase awareness of the need, as NEC Group employees, to prevent leaks of trade secrets and other critical information, violation of third parties' legitimate rights, and posting of misleading remarks or inappropriate information.

Use of Social Media and Review of Guidelines



5 Information Security Assessment

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

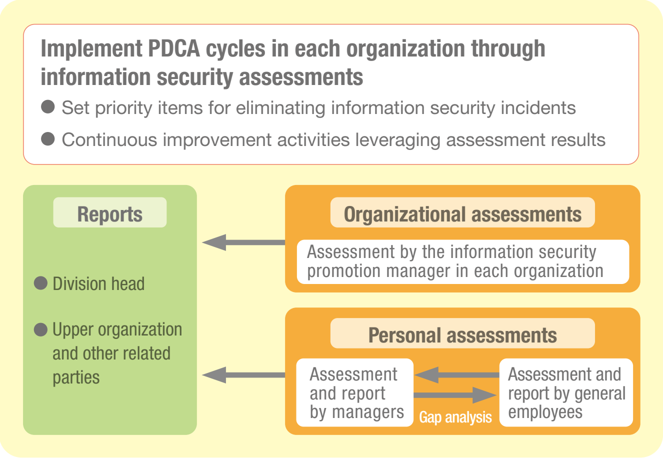
We analyze information security incidents and set priority items, mainly to eliminate information leaks. Assessments are helpful for formulating corrective measures because the assessment format allows us not only to check the implementation status but also to collect reasons why measures were not taken.

Specifically, we thoroughly implement safety measures for external storage media and work done out of the office, personal information management, confidential information management for outsourced work and prevention of email missending.

2 Information Security Assessment Methods

NEC implements the following two information security assessments: organizational assessments and personal assessments. In organizational assessments, the information security manager 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 have expanded the implementation targets of personal assessments 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.

Information Security Assessments (Organizational and Personal Assessments)


Implement PDCA cycles in each organization through information security assessments
● Set priority items for eliminating information security incidents
● Continuous improvement activities leveraging assessment results
Reports
● Division head
● Upper organization and other related parties
Organizational assessments
Assessment by the information security promotion manager in each organization
Personal assessments
Assessment and report by managers
Gap analysis
Assessment and report by general employees

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.

6 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.

7 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. We also provide this system, which has been used by many organizations in the NEC Group and our business partners, as a solution (the “NetSociety for ISMS” service) that leverages our experience and expertise.

Information Security Platform

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

1 Features and Configuration of Information Security Platform

Three information security platforms 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.

The IT platform for user management and control is used to implement security measures including those to prevent malicious system use through spoofing and to prevent unnecessary privileges being assigned to users. The IT platform for PC and network protection protects PCs and networks from viruses and worms, protects the intranet from unauthorized access, prohibits installation of inappropriate software, and prevents business suspension resulting from the spread of viruses and other causes. The IT platform for information protection is used to prevent information leaks and ensure safe information usage by encrypting information equipment and information itself, thereby preventing malicious use of information obtained illegally by an unauthorized person through, for example, a targeted attack. This platform also prevents email sending errors and allows people to work safely while out of the office and safely exchange information with external locations.

2 IT Platform for User Management and Control

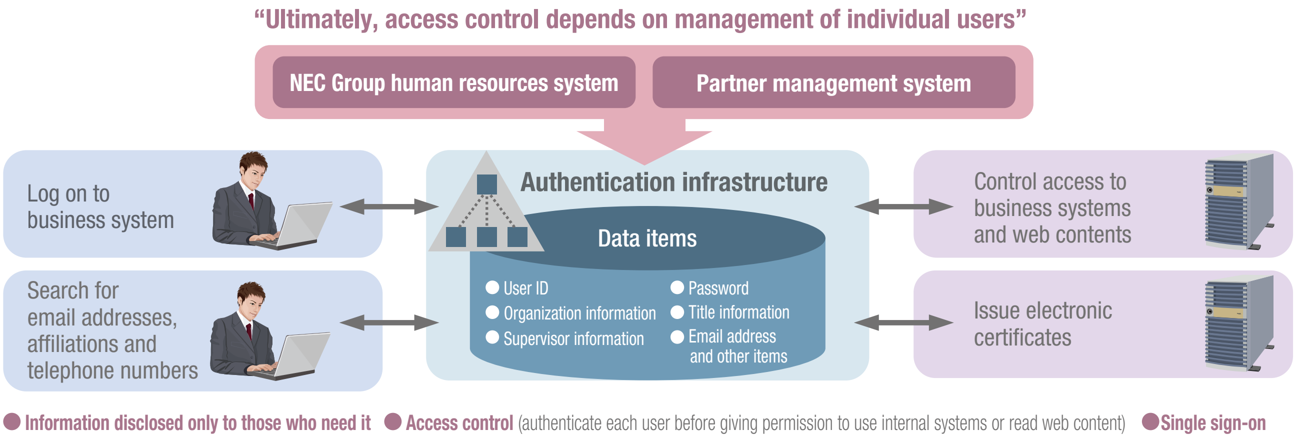
The basis of information security management is the user authentication infrastructure. Using a system to identify individuals enables proper control of access to information assets and prevents spoofing using electronic certificates.

1 Appropriate Access Control Realized by the Authentication Infrastructure

It is important to identify users and give them correct privileges so that they can access information assets appropriately. The NEC Group has built an authentication infrastructure to centrally manage information that covers not only our employees but also some business partners and other related parties if needed for business.

We control access from each user by using organization, title and other information as well as user IDs and passwords as authentication information. We also centrally manage the authentication information of each NEC Group company (e.g., where the information is used and for what purpose). We also implement IC card authentication for printer (paper) output.

NEC Group Authentication infrastructure


"Ultimately, access control depends on management of individual users"
NEC Group human resources system
Partner management system
Authentication infrastructure
Data items
● User ID
● Organization information
● Supervisor information
● Password
● Title information
● Email address and other items
Log on to business system
Search for email addresses, affiliations and telephone numbers
Control access to business systems and web contents
Issue electronic certificates
● Information disclosed only to those who need it
● Access control (authenticate each user before giving permission to use internal systems or read web content)
● Single sign-on

2 Encryption and Electronic Signatures Using Email Certificates

The NEC Group issues email certificates to employees to identify their company and themselves by linking the NEC Group authentication infrastructure with third-party certification authorities. When sending important information such as customer information via email, employees use these email certificates to securely exchange emails by preventing spoofing and encrypting data with S/MIME. We also electronically sign email sent as evidence for internal control or compliance to the Japanese Financial Instruments and Exchange Law (J-SOX) using this email certificate to reliably assure the identity of the sender.

3 IT Platform for PC and Network Protection

The IT platform for PC and network protection maintains the security of information devices connected to the NEC Intranet and protects our PCs and networks from viruses, worms, and other attacks. 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 anti-virus software.

1 PC Protection from Viruses and Worms

Support for user environments

The NEC Group requires employees to install software to check the statuses of PCs and networks when connecting to the NEC Intranet. By visualizing the statuses of PCs and networks in this way, we can install all the necessary security software in all PCs. In addition, the system automatically distributes security patches and updates of definition files for anti-virus software. We also define prohibited software and monitor whether users are using software properly.

Network management

In addition to visualizing PC statuses, we have an intrusion detection system on our intranet. When a PC for which security measures are not sufficiently implemented is connected to the intranet or a worm is detected on the intranet, that PC or LAN is disconnected from the intranet. We also control external communications (by using web access filtering based on prohibited categories, prohibiting the use of free email accounts, and by using SPF authentication).

Centralized management of operating statuses

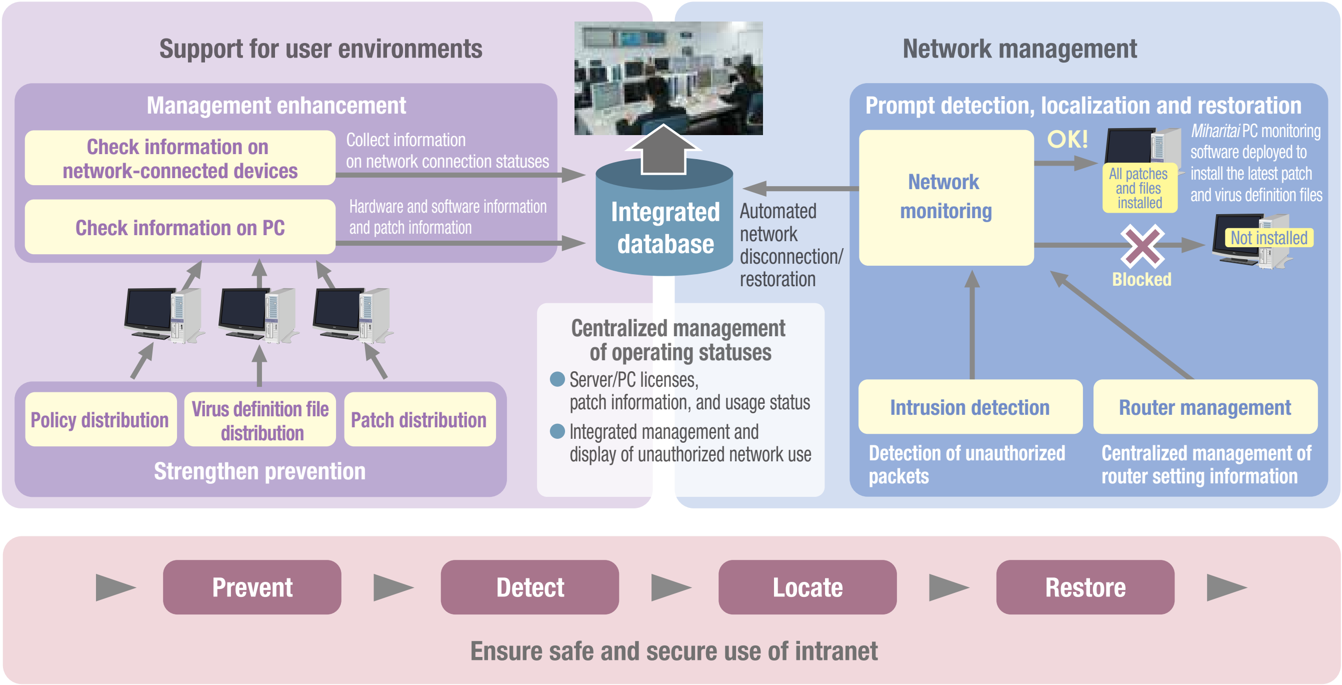
Data on the implementation status of security measures, including installation of patch programs and anti-virus software, is collected in a management system so that information security managers and security promotion managers can see the implementation status in their department in a timely fashion. 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 following 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



Support for user environments
Management enhancement
Check information on network-connected devices
Collect information on network connection statuses
Check information on PC
Hardware and software information and patch information
Integrated database
Automated network disconnection/ restoration
Policy distribution
Virus definition file distribution
Patch distribution
Strengthen prevention
Centralized management of operating statuses
Server/PC licenses, patch information, and usage status
Integrated management and display of unauthorized network use
Network management
Prompt detection, localization and restoration
Network monitoring
OK!
All patches and files installed
Miharitai PC monitoring software deployed to install the latest patch and virus definition files
Not installed
Blocked
Intrusion detection
Detection of unauthorized packets
Router management
Centralized management of router setting information
Prevent
Detect
Locate
Restore
Ensure safe and secure use of intranet

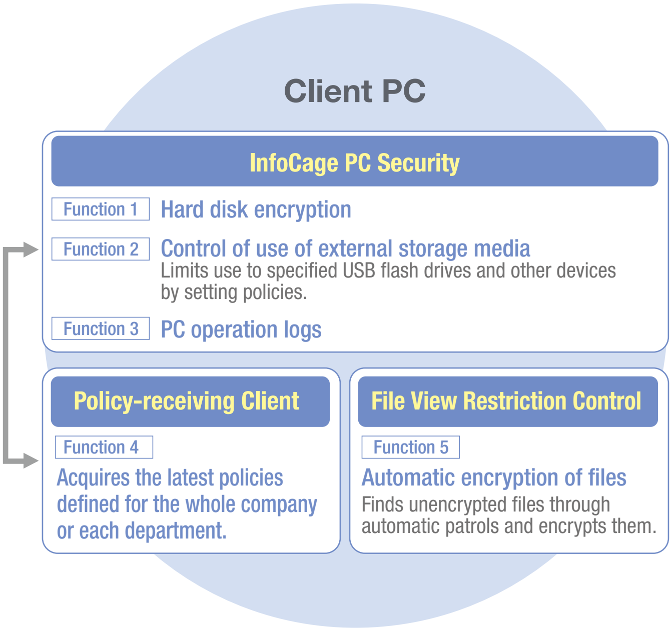
4 IT Platform for Information Protection

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 taking the characteristics and risks of networks, PCs, electronic media, and other IT components into consideration.

1 System to Prevent Information Leaks in the NEC Group

The NEC Group has an information leakage prevention system based on our own InfoCage Series. This system encrypts hard disks and files, controls the use of USB flash drives and other external storage media, and records and monitors PC operations to prevent important information leaks and minimize damage in case of theft or loss. This system contributes significantly to preventing information leak incidents, incident analysis and implementation of recurrence prevention measures, for example by allowing us to analyze PC operation records to identify the range of effect of information leak incidents and precisely understand the situation. We also take measures such as managing the PC operation logs of employees engaged in important work and controlling the writing of data to removable media not permitted by the company.

Overview of Information Leakage Prevention System



Client PC

InfoCage PC Security

Function 1 Hard disk encryption

Function 2 Control of use of external storage media
Limits use to specified USB flash drives and other devices by setting policies.

Function 3 PC operation logs

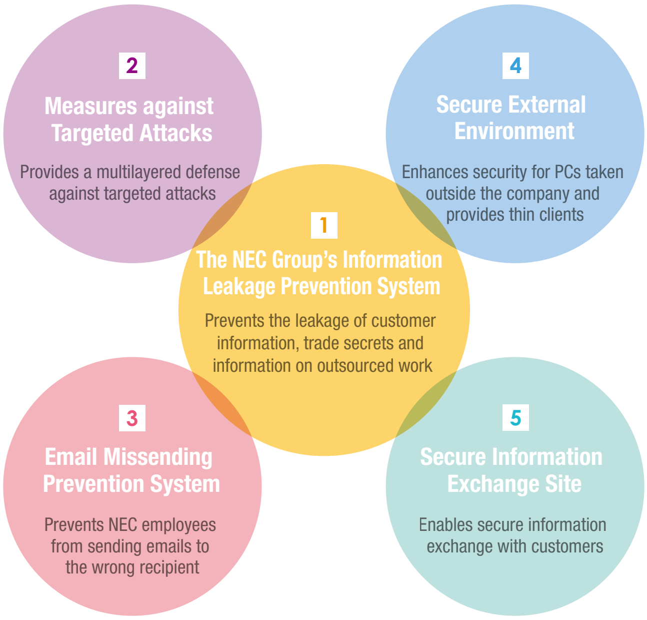
Policy-receiving Client

Function 4 Acquires the latest policies defined for the whole company or each department.

File View Restriction Control

Function 5 Automatic encryption of files
Finds unencrypted files through automatic patrols and encrypts them.

Overview of IT Platform for Information Protection



1 The NEC Group's Information Leakage Prevention System
Prevents the leakage of customer information, trade secrets and information on outsourced work

2 Measures against Targeted Attacks
Provides a multilayered defense against targeted attacks

3 Email Missending Prevention System
Prevents NEC employees from sending emails to the wrong recipient

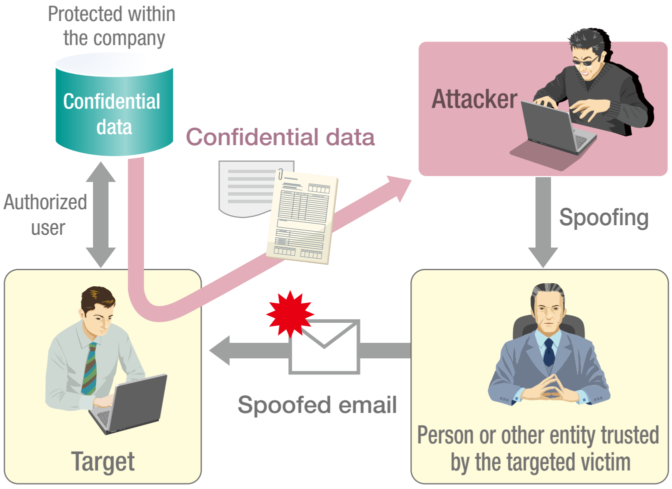
4 Secure External Environment
Enhances security for PCs taken outside the company and provides thin clients

5 Secure Information Exchange Site
Enables secure information exchange with customers

2 Measures against Targeted Attacks

The number of targeted attacks is increasing recently, posing a serious threat to organizations and companies. A targeted attack is a kind of cyber attack in which unknown malware (virus) is sent mainly by email. The attacker tries to trick the targeted victims and infect their environment so that they can steal critical information assets.

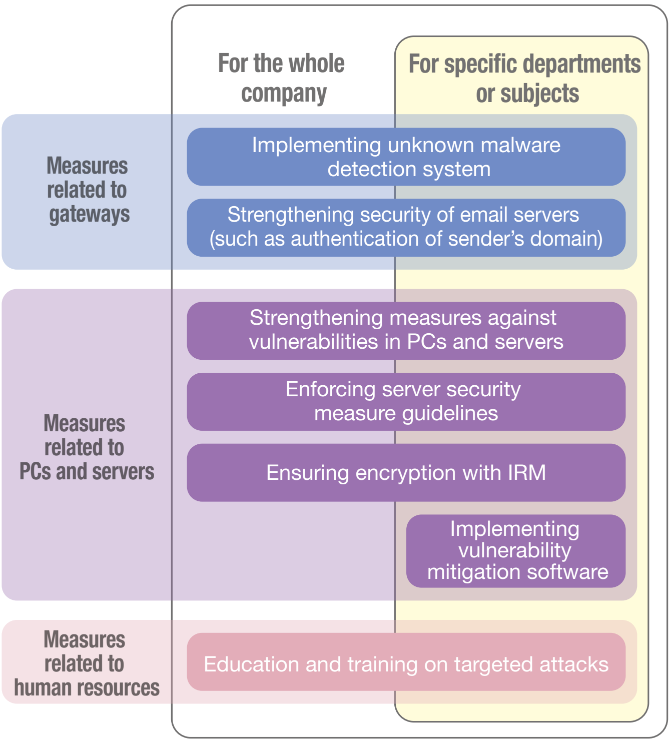
Targeted Attacks



In the NEC Group's policies to strengthen measures against targeted attacks we are focusing on detection (visualization) of unknown malware, while adopting the concept of multilayered defense. We take measures to enhance protection for the whole company as well as for departments and subjects that require special care.

Specifically, we strengthen security measures related to gateways, PCs, servers and human resources in the whole company and for certain departments.

Concept of Multilayered Defense as Measure against Targeted Attacks

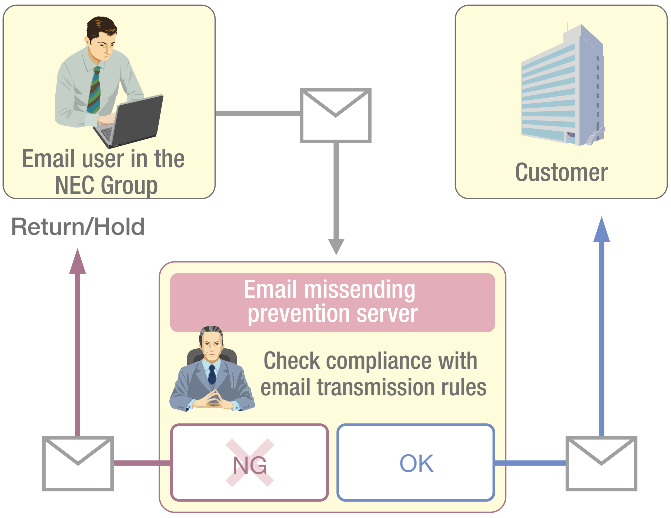

For the whole company
For specific departments or subjects
Measures related to gateways
Implementing unknown malware detection system
Strengthening security of email servers (such as authentication of sender's domain)
Measures related to PCs and servers
Strengthening measures against vulnerabilities in PCs and servers
Enforcing server security measure guidelines
Ensuring encryption with IRM
Implementing vulnerability mitigation software
Measures related to human resources
Education and training on targeted attacks

❸ Email Missending Prevention System

Information leak incidents can be caused by small mistakes such as an incorrectly entered email address or a file that should not be attached.

The NEC Group has implemented an email missending prevention system to always check the destination and the content of attached files before sending emails out from NEC Group companies. It is also possible to set restrictions so that, for example, emails cannot be sent until a supervisor or other third party checks details such as the destination and contents. This further reduces errors and prevents information leaks due to intentional forwarding or other action.

Email Missending Prevention System


Email user in the NEC Group
Customer
Return/Hold
Email missending prevention server
Check compliance with email transmission rules
NG
OK

❹ Secure External Environment

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.

Strengthening security for PCs taken outside the company

PCs used outside the office are subject to more threats than when used in-house.

Therefore, the NEC Group has introduced secure PCs ("trusted PCs") equipped with fully encrypted HDDs and features to further protect information in the case of theft or loss, such as pre-boot authentication before OS startup, and remote data deletion/PC locking. Trusted PCs are also equipped with a function to mitigate attacks that exploit unknown vulnerabilities as well as an automated anti-virus function to keep pace with recent increases in cyber attacks.

Thin clients

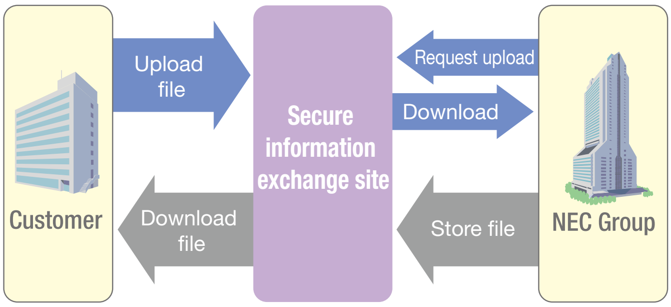
The thin client system adopts a virtual PC method for more efficient administration and to enhance environmental protection. As the system administrator applies security patches to virtual PCs at once, it is possible to quickly complete application of countermeasures. This is especially useful when new vulnerabilities are exploited in a targeted or other form of attack. In a thin client environment, users can be free from implementing cumbersome security measures and concentrate on their work to create value.

Regarding thin client terminals, we use devices that support advanced security including unknown vulnerability countermeasures while maintaining the convenience of Windows. We have also developed a model that can be started from a CD or USB flash drive. This makes it possible to convert personally-owned PCs into secure thin client terminals that can be connected to the company's networks. This system plays an important role in maintaining social infrastructure operations in the event of disaster such as earthquake or pandemic.

❺ 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. The system uses a one-time URL, which can be accessed only once, and a password to securely exchange files. With this system, employees no longer have to carry USB flash drives or other external storage devices, reducing the risk of information leak incidents due to theft or loss of such devices.

Secure Information Exchange Site



Information Security Staff

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 for all employees in the NEC Group to increase knowledge and skills in the information security field. The content of this training course, reviewed every year, is practical and not only provides knowledge about information handling and raises awareness but also helps employees develop the capability to address risks and identifies points to be noted through case studies of information security incidents.

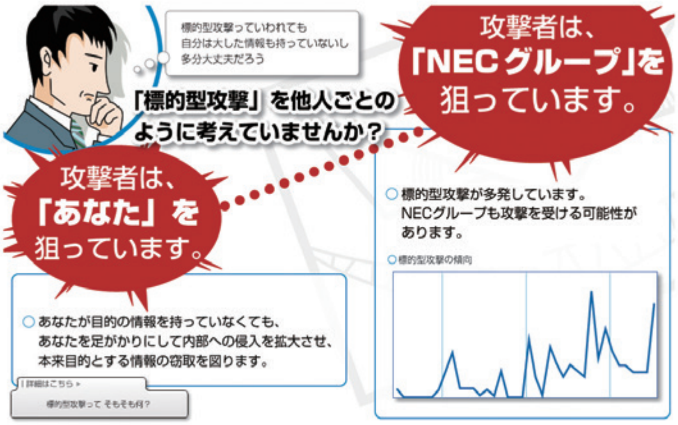
2 Simulated Training on Targeted Email Attacks

As the risks of unauthorized invasion, information theft and other incidents caused by targeted email attacks increases, having employees know about and recognize these attacks is becoming more critical. The NEC Group has organized a simulated training course to learn how to identify targeted email attacks and properly handle the situation when receiving such email. Attendees are required to operate the email screen based on a real-world scenario and to identify which e-mails are sent for targeted attacks. Through this training, they can develop a real sense of crisis and how it should be responded to.

3 Commitment to Following Information Security Rules

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

Screenshot from Targeted Email Attack Training Course



標的型攻撃っていわれても
自分は大した情報も持っていないし
多分大丈夫だろう

「標的型攻撃」を他人ごとのように考えていませんか？

攻撃者は、「NECグループ」を狙っています。

攻撃者は、「あなた」を狙っています。

○標的型攻撃が多発しています。
NECグループも攻撃を受ける可能性があります。

○あなたが目的の情報を持っていなくても、
あなたを足がかりにして内部への侵入を拡大させ、
本来目的とする情報の窃取を図ります。

4 Activities to Raise Awareness of Information Security

The NEC Group performs awareness-raising activities using video dramas about information loss incidents, email missending 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. The NEC Group encourages employees to raise their awareness by discussing security issues with colleagues and to improve their analysis and judgment skills by using workplace discussions, three-why analysis, video presentations, and other methods appropriate to each organization.

3 Developing Personnel to Promote Security Measures

The NEC Group has an information security promotion structure and deploys a variety of measures to promote information security. Since the promotion manager 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 Promotion Managers

The NEC Group carries out NEC Group information security promotion training for new managers so that the promotion manager 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 information security risk control skill improvement training exercises that use 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.

❷ Training Staff Members on Secure Development and Operations

To raise the security quality of products and services provided to customers, the NEC Group provides secure development training on secure design, server fortification, secure coding and other themes for secure development and operation promotion managers, product and service developers and those in charge of quality assurance to further develop human resources engaged in secure development and operation through acquisition and firm establishment of expertise.

❸ Auditor Training

The NEC Group visits business partners to conduct information security audits (onsite inspections) so as to maintain and improve information security at our business partners. We have standardized the method and established a system to develop auditors for onsite inspections and are developing lead auditors and regular auditors.

4 Developing Experts

The NEC Group is developing information security experts to provide value to customers by offering reliable products, services and information security solutions.

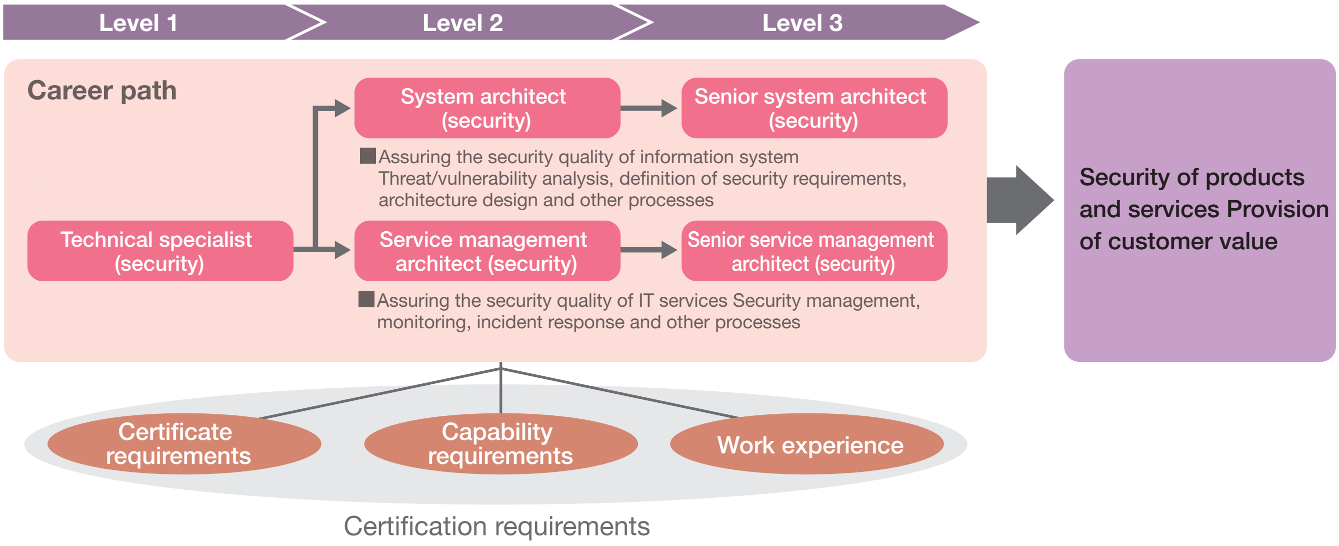
❶ Increasing and Developing Security Staff

The NEC Group operates an expert certification system to develop human resources with highly specialized skills. We have added advanced security staff certification to the expert certification system in line with changes in IT environments, including measures against increasingly complex security threats, advanced technologies such as cloud computing and smart devices, and governmental and industrial movements for reinforcing security staff development.

To systematically develop and strengthen human resources, in addition to our conventional technical specialist (security), we have defined a system architect (security), who focuses on upstream security design to assure the security quality of the information system, and a service management architect (security), who assures the security quality of IT services including cyber security measures.

Employees who have advanced skills, work experience and/or certification in the information security field take the lead in securing products and services and help provide customers with optimal solutions.

■ Career Roadmap for Information Security Expert


Level 1
Level 2
Level 3
Career path
System architect (security)
Senior system architect (security)
■Assuring the security quality of information system Threat/vulnerability analysis, definition of security requirements, architecture design and other processes
Technical specialist (security)
Service management architect (security)
Senior service management architect (security)
■Assuring the security quality of IT services Security management, monitoring, incident response and other processes
Security of products and services Provision of customer value
Certificate requirements
Capability requirements
Work experience
Certification requirements

❷ Practical Cyber Drills

The NEC Group has introduced a practical cyber drill called CTF (Capture The Flag) as training to improve security response capability. CTF is a game to capture the other team's flag. Attendees receive training challenges such as "Find traces of hacking in server logs and clarify how the system was hacked" or "Analyze the application server to find evidences of malpractice" and compete to reach the answer as soon as possible by making the most of their abilities. This training method is highly effective as attendees truly understand the topic and acquire techniques by finding and realizing the well hidden answer by themselves.

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

Connected to more than 150 offices

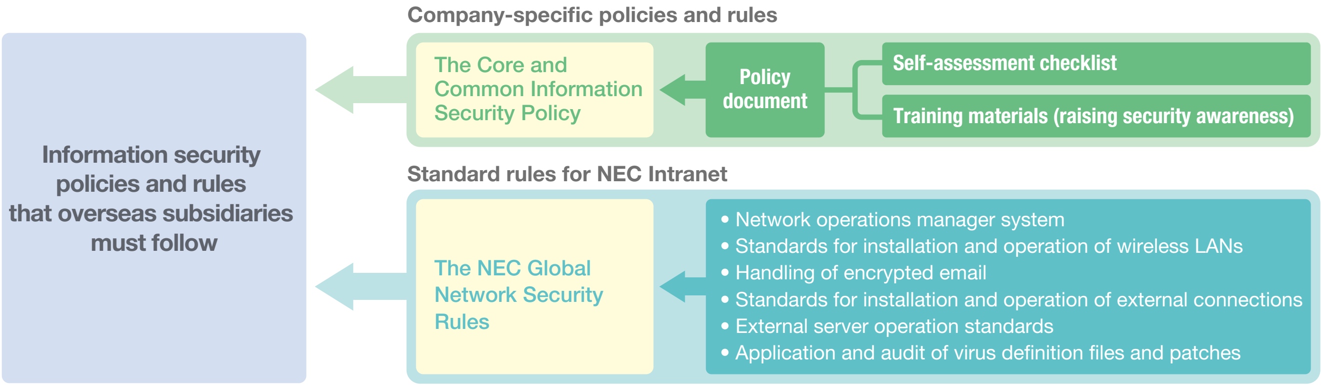
2 Information Security Policy and Rules

NEC defines standard information security policies and rules that must be followed at overseas subsidiaries.

For the information security policies and rules in each company, NEC encourages overseas subsidiaries to use the Core and Common Information Security Policy template to implement security measures at the same level as domestic subsidiaries. This template is based on the ISO 27001 standard and its documentation system can easily be applied across the globe. Each company can simply map the roles in their organization onto the template, while maintaining compliance with laws and regulations applicable to their country or region, and create information security policies and rules using the same details and format as the template. Additions and modifications made by each company must be verified and approved by NEC. For example, local companies to which NEC entrusts software development 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 intranet must follow these rules as standard. The rules cover management systems, connection to the Internet, and in-house networks.

Global Information Security Policies and Rules


Company-specific policies and rules
Information security policies and rules that overseas subsidiaries must follow
The Core and Common Information Security Policy
Policy document
Self-assessment checklist
Training materials (raising security awareness)
Standard rules for NEC Intranet
The NEC Global Network Security Rules
• Network operations manager system
• Standards for installation and operation of wireless LANs
• Handling of encrypted email
• Standards for installation and operation of external connections
• External server operation standards
• Application and audit of virus definition files and patches

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. NEC checks assessment results and follows up with each company as needed, for example, by helping them take necessary measures.

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 follows up by helping companies implement the required steps.

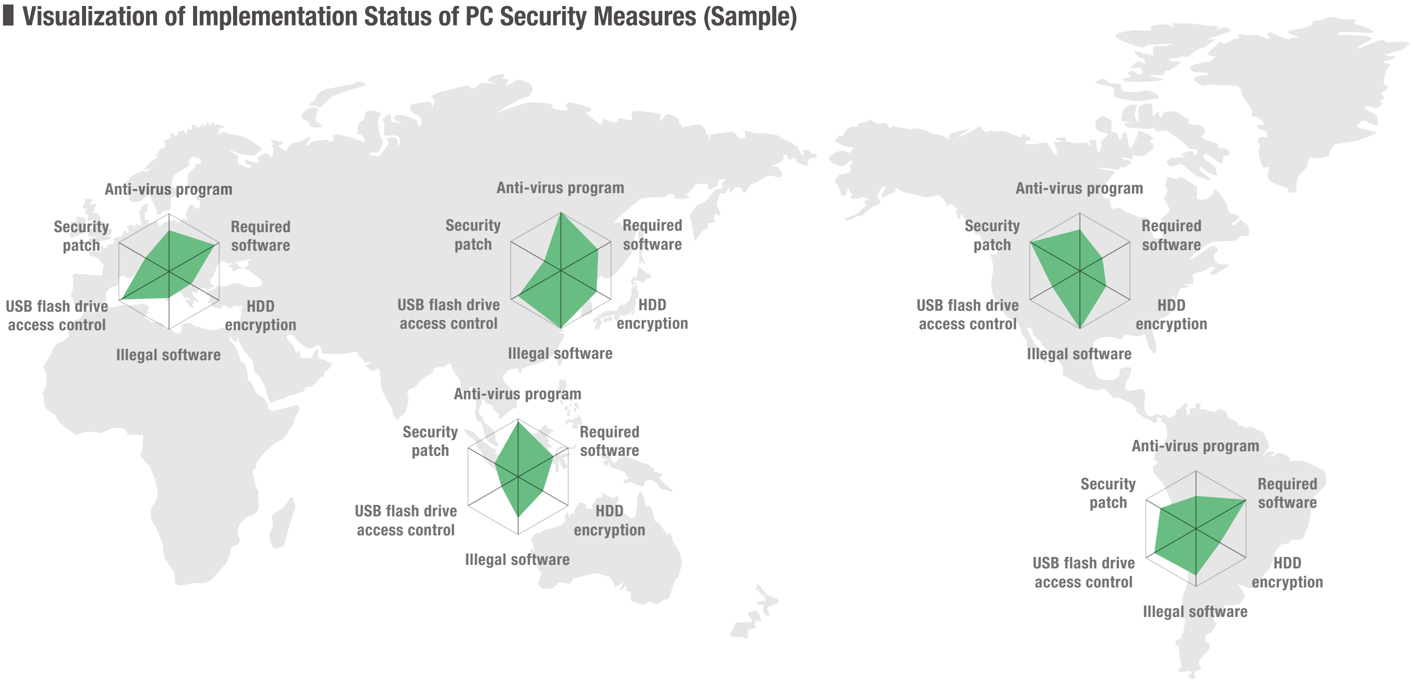
4 Information Security Platform

The NEC Group distributes a unique ID to every employee in its overseas subsidiaries and centrally manages them on the global ID management platform. These IDs can be used to encrypt business documents in the same way as in Japan.

For PC management, the NEC Group is gradually implementing a system to visualize the security status of all PCs at overseas subsidiaries and apply antivirus measures and security patches. This system allows NEC to check the security statuses of PC in each company. In addition, NEC can use this information to roll out a variety of security measures to limit access to removable media such as USB flash drives (device control) or to quarantine unauthorized PCs before they connect to the network.

* NEC has also implemented file view limitation management as an information leakage prevention platform to encrypt files transferred within the Group and allows only authorized users to open files in the same way as in Japan, preventing the leakage of information to third parties.

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, globalization and the consequent expansion of risks, and the overly complex procedures used in the existing data protection system. 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 tracks international trends in personal information protection as needed in terms of legal compliance as well as to ensure an up-to-date information system in close collaboration with related departments and specialists.

As evidence of our commitment to this goal, NEC has joined the committee of the Japan Electronics and Information Technology Industries Association (JEITA). We play an active role there and have been involved in activities such as creating a JEITA report on the EU directive on the protection of personal data, which includes opinions and requests from industry in Japan.

6 Information Security Measures around M&A

When merging and acquiring overseas companies, there may be a huge gap between the acquired company and the NEC Group in terms of information security policies and strategies due to differences in culture and values. The NEC Group has a process to ensure that the new company complies with the above-mentioned NEC Group standard information security policies and rules by assigning an information security manager to the new company so that the new company can implement information security measures as soon as possible as an NEC Group company.

We actually used this process when merging and acquiring NetCracker and NEC Energy Solutions.

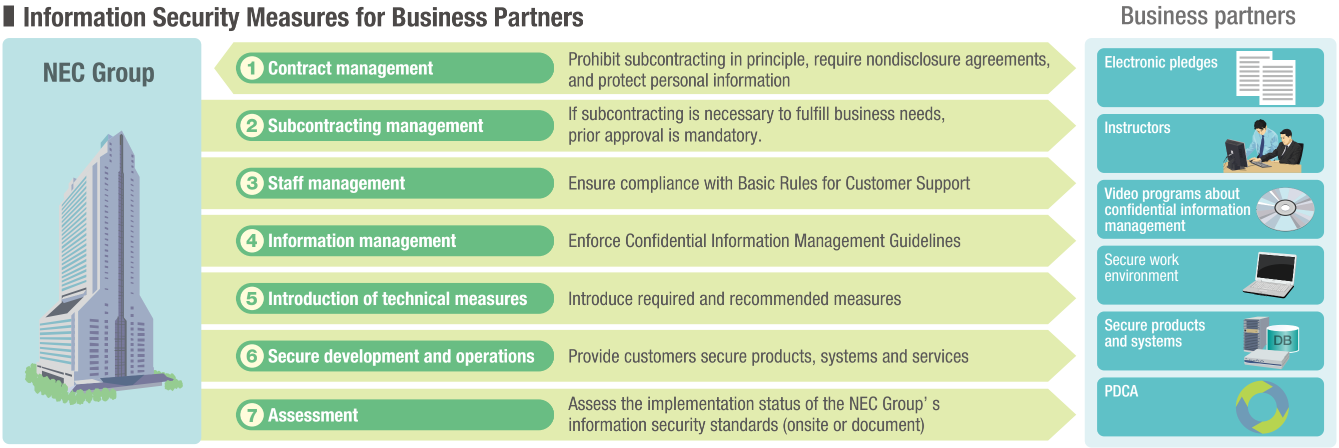
Information Security Coordinated with Business Partners

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 recognize that it is extremely important for business partners not only to have technical capabilities, but also to reach a certain information security standard. The 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 operation and 7) assessments.

Information Security Measures for Business Partners



Business partners
NEC Group
1 Contract management
Prohibit subcontracting in principle, require nondisclosure agreements, and protect personal information
2 Subcontracting management
If subcontracting is necessary to fulfill business needs, prior approval is mandatory.
3 Staff management
Ensure compliance with Basic Rules for Customer Support
4 Information management
Enforce Confidential Information Management Guidelines
5 Introduction of technical measures
Introduce required and recommended measures
6 Secure development and operations
Provide customers secure products, systems and services
7 Assessment
Assess the implementation status of the NEC Group' s information security standards (onsite or document)
Electronic pledges
Instructors
Video programs about confidential information management
Secure work environment
Secure products and systems
DB
PDCA

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 prohibits subcontracting by business partners to other companies. If subcontracting is required to fulfill business needs, the business partner must 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 Support.” 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.

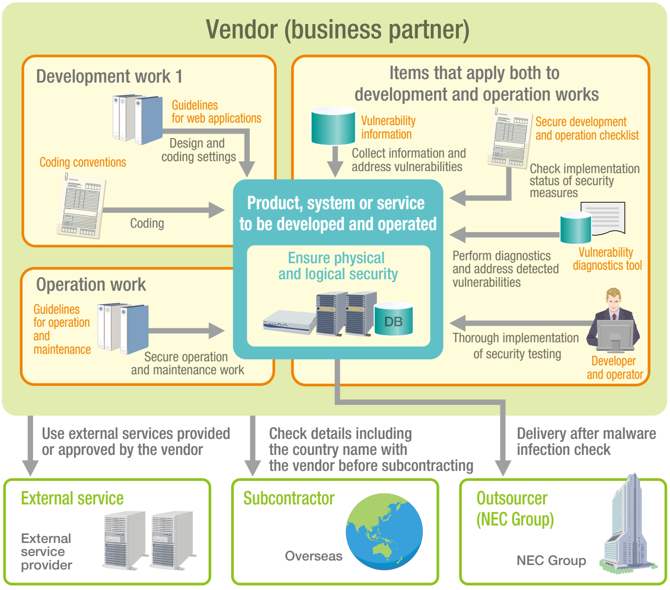
5 Introduction of Technical Measures

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

In fiscal 2013, the NEC Group created the Secure Development and Operation Guidelines for Business Partners concerning the development and operation of products, systems and services for customers and asks business partners to consider security during development and operation.

Secure Development and Operations



Vendor (business partner)
Development work 1
Guidelines for web applications
Design and coding settings
Coding conventions
Coding
Items that apply both to development and operation works
Vulnerability information
Collect information and address vulnerabilities
Secure development and operation checklist
Check implementation status of security measures
Product, system or service to be developed and operated
Ensure physical and logical security
DB
Perform diagnostics and address detected vulnerabilities
Vulnerability diagnostics tool
Operation work
Guidelines for operation and maintenance
Secure operation and maintenance work
Thorough implementation of security testing
Developer and operator
Use external services provided or approved by the vendor
Check details including the country name with the vendor before subcontracting
Delivery after malware infection check
External service
External service provider
Subcontractor
Overseas
Outsourcer (NEC Group)
NEC Group

For example, business partners must follow secure coding conventions during development and diagnose vulnerabilities before releasing products and services.

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 Suppliers (revised in fiscal 2014), which defines the information security standards required for NEC Group business partners.

2 Promotion of Security Measures for Business Partners

❶ Information Security Seminars

The procurement and information security departments work together to organize information security seminars at 12 places across Japan from Hokkaido to Kyushu once a year for nationwide business partners (approximately 2,000 companies, including approximately 700 ISMS certified companies) to ensure that business partners understand and implement the NEC Group's information security measures.

❷ Skill Improvement Activities for Core Businesses

The NEC Group organizes a skills improvement seminar once a year targeting about 100 core business partners that frequently deal with the NEC Group. We distribute an information security assessment sheet, which includes the assessment results and the implementation status of measures, to each partner to encourage them to thoroughly implement measures and improve their skills.

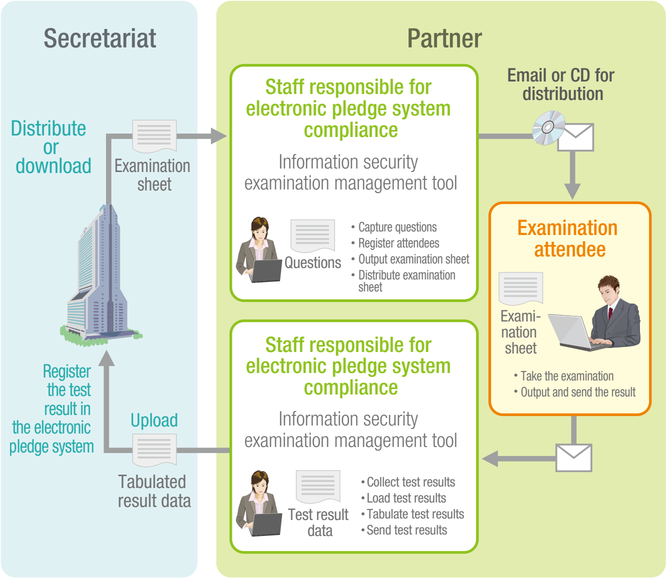
❸ Distribution of Videos to Maintain Awareness

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, information leaks through Winny, virus infections, loss of data after going out drinking, email missending and incident response.

❹ Operation of Examination System

The NEC Groups periodically distributes examination sheets to business partners that have been prepared for in-house education to ensure thorough implementation of the "Basic Rules for Customer Support." In addition, we have built and are operating a system by which a registered business partner can receive feedback that shows their ranking among all our business partners.

Overview of Examination System



Secretariat
Partner
Distribute or download
Examination sheet
Staff responsible for electronic pledge system compliance
Information security examination management tool
Questions
• Capture questions
• Register attendees
• Output examination sheet
• Distribute examination sheet
Email or CD for distribution
Examination attendee
Exami-nation sheet
• Take the examination
• Output and send the result
Register the test result in the electronic pledge system
Upload
Tabulated result data
Staff responsible for electronic pledge system compliance
Information security examination management tool
Test result data
• Collect test results
• Load test results
• Tabulate test results
• Send test results

❺ 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 secure development and operation of web systems, and rules to ensure security of smart devices.

3 Assessments and Improvement Actions for Business Partners

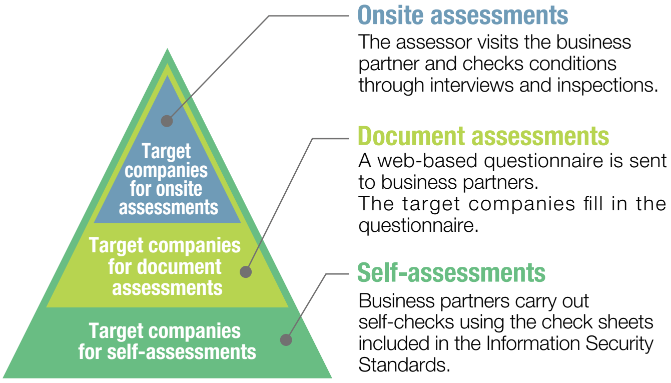
Assessments of our business partners mainly consist of document assessments and onsite assessments.

Document assessments are performed at approximately 2,000 companies that deal with the NEC Group every year. New business partners must 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 to include 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.

Onsite 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 (document 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.

Categories of Assessment Target Companies



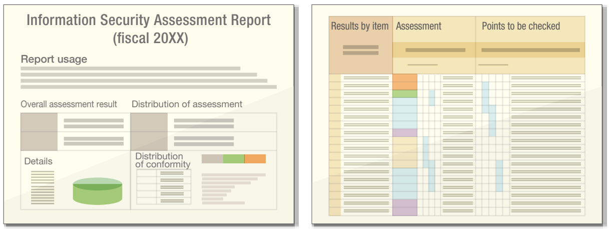
Target companies for onsite assessments
Target companies for document assessments
Target companies for self-assessments

Onsite assessments
The assessor visits the business partner and checks conditions through interviews and inspections.

Document assessments
A web-based questionnaire is sent to business partners.
The target companies fill in the questionnaire.

Self-assessments
Business partners carry out self-checks using the check sheets included in the Information Security Standards.

Onsite Assessment Report



Information Security Assessment Report (fiscal 20XX)
Report usage
Overall assessment result
Distribution of assessment
Details
Distribution of conformity
Results by item
Assessment
Points to be checked

Providing Secure Products and Services

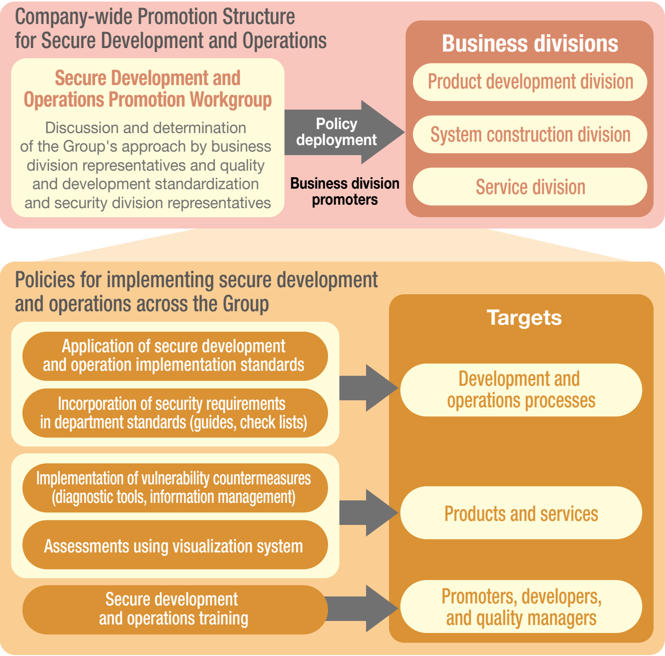
To offer "better products, better services" to customers from the viewpoint of security, the NEC Group carries out a variety of activities to ensure high-quality security in the products and services it offers.

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 business units and Group companies, and secure development and operations managers 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.

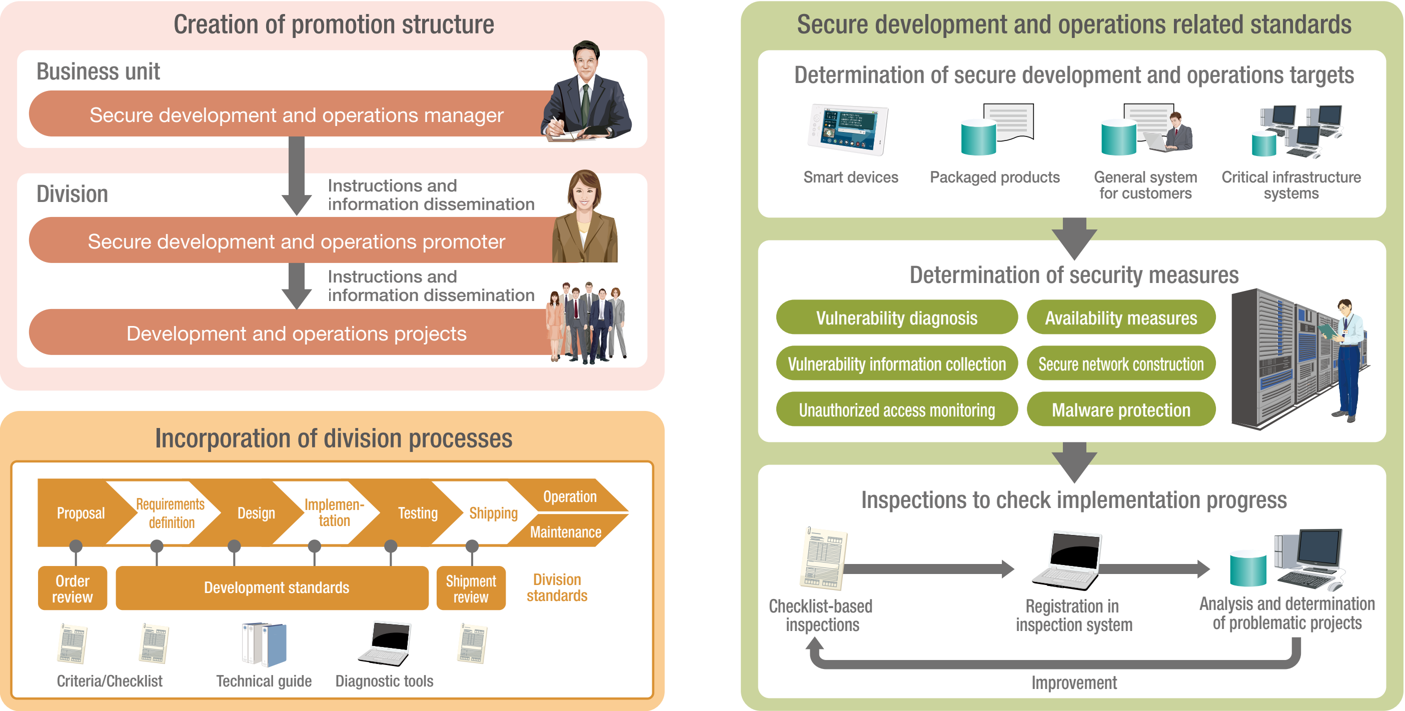
Secure Development and Operations Promotion Structure/Policy


Company-wide Promotion Structure for Secure Development and Operations
Secure Development and Operations Promotion Workgroup
Discussion and determination of the Group's approach by business division representatives and quality and development standardization and security division representatives
Policy deployment
Business division promoters
Business divisions
Product development division
System construction division
Service division
Policies for implementing secure development and operations across the Group
Application of secure development and operation implementation standards
Incorporation of security requirements in department standards (guides, check lists)
Implementation of vulnerability countermeasures (diagnostic tools, information management)
Assessments using visualization system
Secure development and operations training
Targets
Development and operations processes
Products and services
Promoters, developers, and quality managers

2 Establishment of Group-wide Standards

The Secure Development and Operations Management Rules were established as part of the NEC Corporation Industrial Standards (NIS), which is a set of company-wide standards for the NEC Group. These rules define the secure development- and operations- related content 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.).

Secure Development and Operations Management Rules


Creation of promotion structure
Business unit
Secure development and operations manager
Division
Instructions and information dissemination
Secure development and operations promoter
Instructions and information dissemination
Development and operations projects
Incorporation of division processes
Proposal
Requirements definition
Design
Implementation
Testing
Shipping
Operation
Maintenance
Order review
Development standards
Shipment review
Division standards
Criteria/Checklist
Technical guide
Diagnostic tools
Secure development and operations related standards
Determination of secure development and operations targets
Smart devices
Packaged products
General system for customers
Critical infrastructure systems
Determination of security measures
Vulnerability diagnosis
Availability measures
Vulnerability information collection
Secure network construction
Unauthorized access monitoring
Malware protection
Inspections to check implementation progress
Checklist-based inspections
Registration in inspection system
Analysis and determination of problematic projects
Improvement

In terms of secure development and operations related standards, NEC has established the "Standards for Implementing Secure Development and Operations." The main purpose of these standards is to prevent information leaks and tampering through cyber attacks against customer services. In these standards, we mandate security measures including vulnerability diagnosis (of source code, web applications and platforms), vulnerability information collection and vulnerability countermeasures. We have also established “Standards for Critical Infrastructure” aimed at preventing service interruptions of critical infrastructure caused by ever more frequent cyber attacks. In these standards, we mandate various security measures such as implementing technologies to ensure availability, constructing closed secure networks, and preventing malware attacks. Business divisions adopt these standards for applicable products and services and implement the security measures specified therein to provide secure products and services especially in the area of solutions for society, which include critical infrastructure.

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/IEC15408 and other international security standards, the security standards of government agencies, and industry guidelines. Further, security measures tailored to cyber attacks, which are now launched on a daily basis, are also reflected in a timely manner.

The check list defines security measures including threat analysis in the requirements definition phase, security architecture design in the design phase, secure coding and fortification in the production phase, vulnerability diagnosis and security testing in the test phase, and vulnerability information collection and security monitoring in the operation and maintenance phase. The check list is incorporated into the development and operations standards of the various business units and Group companies, 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 project and assist in the thorough implementation of security measures for projects with insufficient security protection. Approximately 2,000 projects are managed under this system, with promoters conducting inspections and audits to assess the security situation reported for each project, and improve any problematic situations.

④ Centralized Management and Vulnerability Diagnosis by the Software Factory

The NEC Group has established the Software Factory, a cloud-based development environment that supports safe and efficient development for software development projects within the NEC Group. Source code is centrally managed by the Software Factory, and vulnerabilities are promptly and suitably dealt with by specialist teams who diagnose vulnerabilities by using vulnerability scanners.

2 Promptly Addressing Vulnerabilities in Daily Operations

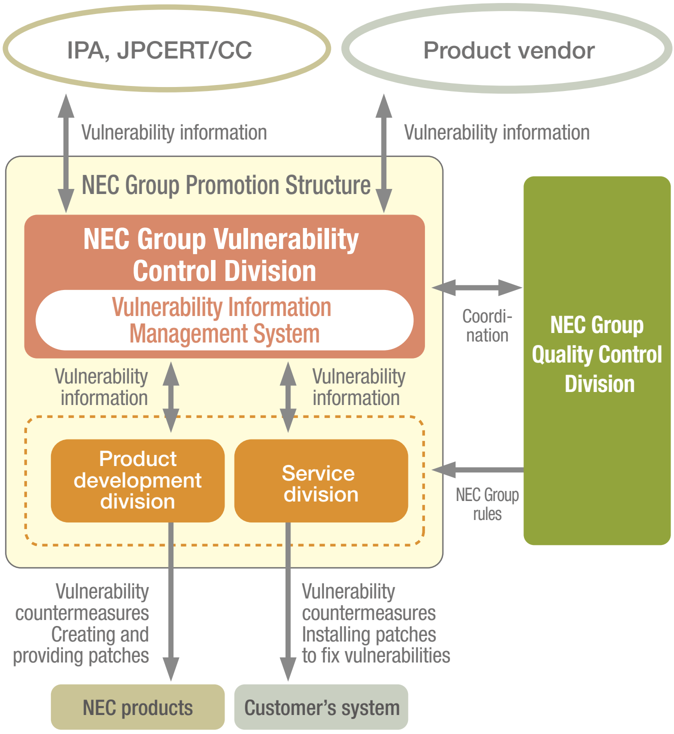
By taking security into consideration while carrying out development, we can eliminate many vulnerabilities that create security risks. However, new vulnerabilities are discovered every day in currently used operating systems and software products, and these vulnerabilities must be fixed quickly and thoroughly.

To this end, 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, and other organizations. Under this system, if a vulnerability is detected in a product after it is shipped, the product development division is promptly notified about the details of the vulnerability before information on the vulnerability is released publicly.

Additionally, for our customers’ systems as well as our own products, we have built a framework for the rapid and systematic implementation of vulnerability countermeasures. In this framework, detailed information such as the causes of vulnerabilities and how to deal with them is quickly sent to the development divisions and service divisions through the vulnerability information management system. 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.

Vulnerability Measures Promotion Framework


IPA, JPCERT/CC
Product vendor
Vulnerability information
Vulnerability information
NEC Group Promotion Structure
NEC Group Vulnerability Control Division
Vulnerability Information Management System
Vulnerability information
Vulnerability information
Product development division
Service division
Coordi-nation
NEC Group rules
NEC Group Quality Control Division
Vulnerability countermeasures Creating and providing patches
Vulnerability countermeasures Installing patches to fix vulnerabilities
NEC products
Customer’s system

Examples of Information Security Activities 1

NEC's Cyber Security Strategy

The risk of cyber attacks is growing ever more serious and the targets of such attacks continue to expand.
As part of our focus on Solutions for Society, NEC provides a safe, secure, and convenient environment in cyberspace to help realize a society in which people can enrich their lives.

NEC's Cyber Security

1 Overall Strategy for Cyber Security

In recent years, risks in cyberspace have become ever more serious, as typified by targeted email attacks. As the use of information and communications technology (ICT) expands, malware attacks and attacks that target system vulnerabilities are a growing concern. The targets of these attacks, which used to be limited to information systems, are also expanding to include social infrastructure such as control systems, and governments and companies are recognizing cyber attacks as a global risk.

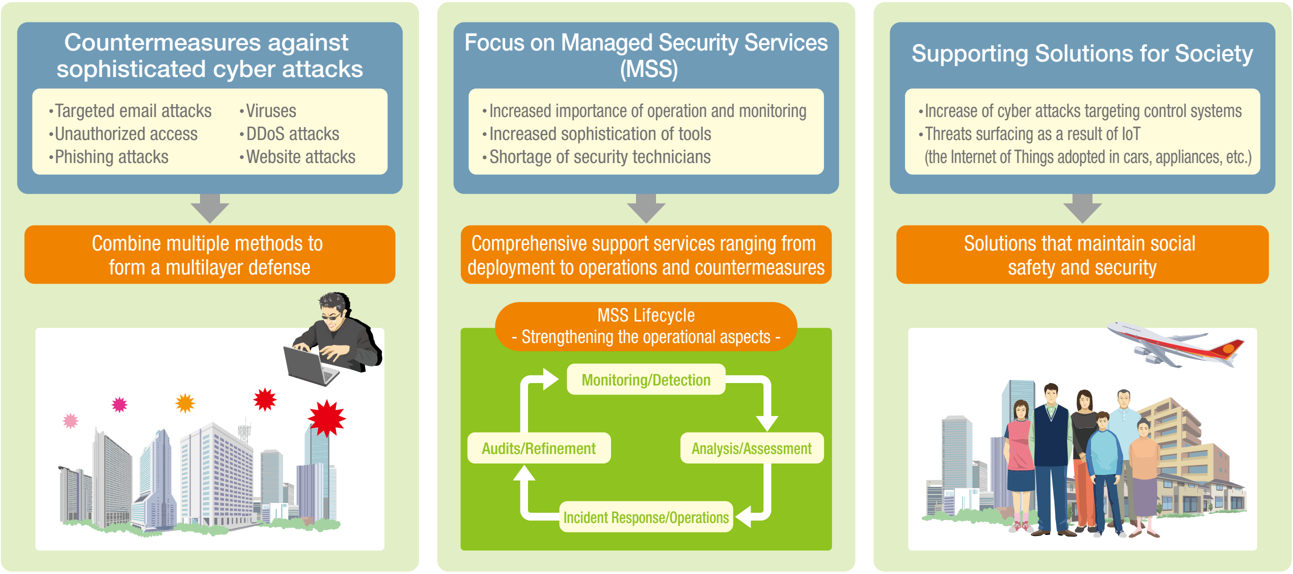
Responding to cyber attacks requires actions beyond the management capabilities of general users, and while organizations are aware of the risks, the implementation of countermeasure is still low, in spite of the fact that users expect services that provide a safe and secure environment.

What people want is a society that promotes the growth of existing industries as well as the creation of new innovative industries and services; a society where people can live safely and comfortably and in good health; a society with the world's safest infrastructure that is resilient against natural disasters; and a society where anyone from anywhere can receive one-stop services. NEC promotes its cyber security business to provide the foundation to realize an IT-driven society that is the best in the world.

2 Cyber Security Business Strategy

NEC is a Total IT Solution vendor that can provide customers with solutions at all levels, including IT business systems and networks. Our strength lies in the fact that we have extensive experience and know-how, in-house security products and unique differentiating technologies. In April 2014, NEC established the Cyber Security Strategy Division, through which it will offer total services that take advantage of these strengths, and protect customer enterprises and critical social infrastructure.

Cyber Security Business Strategy



Countermeasures against sophisticated cyber attacks
- Targeted email attacks
- Unauthorized access
- Phishing attacks
- Viruses
- DDoS attacks
- Website attacks

Combine multiple methods to form a multilayer defense

Focus on Managed Security Services (MSS)
- Increased importance of operation and monitoring
- Increased sophistication of tools
- Shortage of security technicians

Comprehensive support services ranging from deployment to operations and countermeasures

MSS Lifecycle
- Strengthening the operational aspects -

Supporting Solutions for Society
- Increase of cyber attacks targeting control systems
- Threats surfacing as a result of IoT (the Internet of Things adopted in cars, appliances, etc.)

Solutions that maintain social safety and security

Solutions to Protect Enterprises

As they face increasingly sophisticated attacks and the need for various tools and multilayer defense, customers will find themselves unable to deal with cyber attacks on their own. For customers who are facing the threat of cyber attacks, NEC provides Managed Security Service Solutions.

In addition to the existing Integrated Identity Management, Secure PC Management, Network Security Management, Server/email Security Management, and Integrated Log Management Solutions, Managed Security Services brings new standard solutions such as Cyber Attack Countermeasures: Integrated Monitoring and Operation Solutions, Smart Device Solutions, Cloud Security Solutions, and SDN Network Authentication and Access Control Solutions. These solutions go beyond simple product deployment to create the following management frameworks.

① Integrated analysis of data stream input from multiple devices
② Attack assessment
③ Swift action to combat attacks that become apparent
④ Improvement of implemented measures

Solutions to Protect Social Infrastructure

To resolve the security issues that beset the social infrastructure supporting people's lives and convenience, we aim to create solutions based on two distinct approaches: ① the integration of cyber security into systems in response to law enforcement requirements and the growing threat of cyber attacks; and ② joint development of solutions through proof of concept (PoC) and the supply of product and service security from OEMs. As an increasing number of devices are being controlled through ICT, the threat of cyber attacks is spreading. Measures against such threats include, in the area of social security/tax identification numbers, distributed management of personal information, the utilization of public personal authentication, access control, and communication encryption; in the area of the separation of electrical power production and distribution, open networks, cooperation among institutions with different policies, and access authentication; in the area of control systems, measures to combat malware such as Stuxnet, and in the area of the Internet of Things, which links all manner of things via the Internet, hacking prevention measures, and malware countermeasures.

③ Structure to Support the Cyber Security Strategy

The Cyber Security Strategy Division aims to expand NEC Group business as a whole by establishing Group strategies, performing common functions, and supporting related business divisions. In practice, by investing in human resources and core programs, the Cyber Security Strategy Division will launch service businesses that will become operation cores in the future, and develop markets by providing standard solutions for security business expansion along with consulting, sales and SE support.

Furthermore, the Cyber Security Strategy Division will develop new solutions in collaboration with related divisions, and create solutions in cooperation with customers, who will become our partners in new business areas.

④ Strengthening Cyber Security

NEC promotes various initiatives for strengthening our cyber security business for which future growth is expected. These include strengthening Group companies, research and development, human resource development, inter-organizational cooperation, and participation in industry activities.

Strengthening the NEC Group

As the threat of cyber attacks increases daily and the targets of such attacks become increasingly diversified, the provision of security measures on the part of businesses that provide governmental and social infrastructure is required. To provide advanced technological support through a strong team of cyber security professionals and offer total solutions that are unparalleled to other companies, NEC has welcomed the Cyber Defense Institute and Infosec Corporation as Group companies.

As a result, NEC has gained various new functions, including the following:

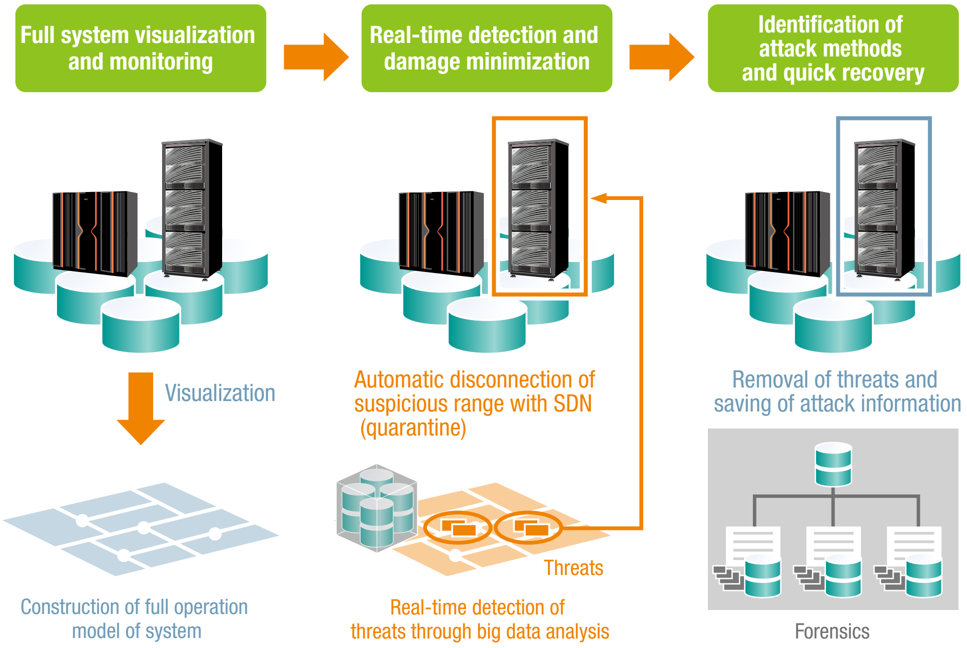
- Planning and formulation of security measures
- Design, deployment, and operations monitoring of security systems
- Security vulnerability diagnosis
- Cyber education and training
- Technical services in areas such as hacking and forensics

These additions allow NEC to provide even higher quality services by taking advantage of the wealth of experience of the above companies, including their various partnerships with overseas companies.

Security-related Research and Development

To respond quickly to increasingly sophisticated cyber attacks, NEC conducts research and development on various technologies to quickly detect anomalies, quarantine suspicious devices and networks, minimize and localize damage, and neutralize threats with the use of big data technology and SDN technology. Further, to realize ICT systems designed in principle to prevent information leaks even in the event of cyber attacks, NEC conducts research and development on advanced encryption technologies capable of processing encrypted data without decrypting it.

Security-related research and development


Full system visualization and monitoring
Real-time detection and damage minimization
Identification of attack methods and quick recovery
Visualization
Construction of full operation model of system
Automatic disconnection of suspicious range with SDN (quarantine)
Threats
Real-time detection of threats through big data analysis
Removal of threats and saving of attack information
Forensics

Participation in Industry Activities

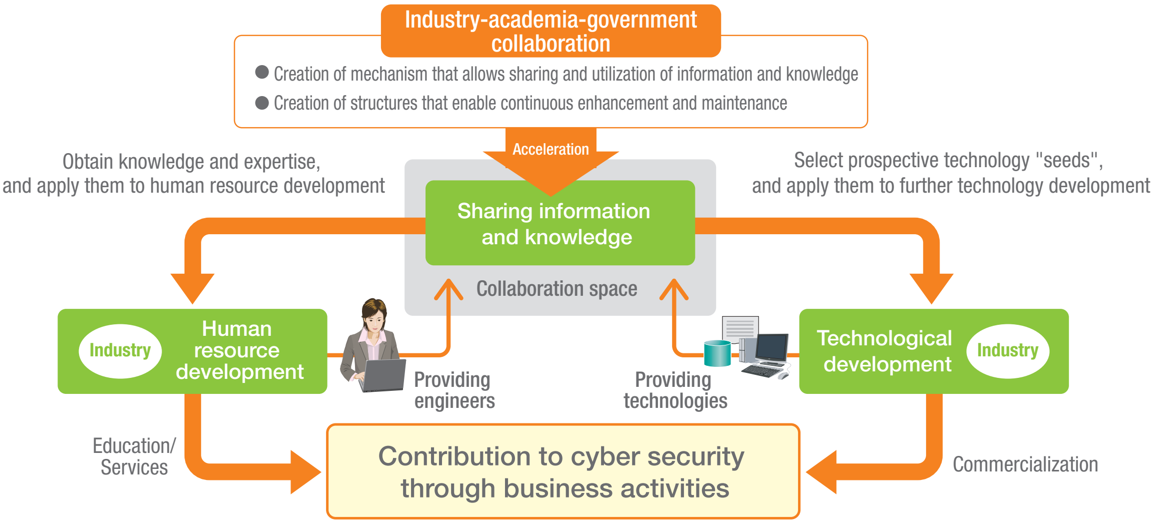
As cyber attacks become more serious, companies and institutions must work together to collaborate and share information.

NEC is actively working on making policy recommendations to the government, forming a cyber security community through collaborations with universities and participation in industry associations to expand the industry's body of knowledge and strengthen security measures.

We are helping industries that support critical social infrastructure such as information communication, public services and financial business by analyzing cyber attacks and developing countermeasures. We also contribute to research and development to ensure security in advanced technologies such as cloud computing and control systems as well as participate in international standardization activities, evaluations of system security, and security awareness-raising activities.

NEC uses the information and knowledge gained through all these activities for human resource and technological development.

Formation of a Cyber Security Community and Sharing of Information and Knowledge


Industry-academia-government collaboration
● Creation of mechanism that allows sharing and utilization of information and knowledge
● Creation of structures that enable continuous enhancement and maintenance
Acceleration
Obtain knowledge and expertise, and apply them to human resource development
Select prospective technology "seeds", and apply them to further technology development
Sharing information and knowledge
Collaboration space
Industry
Human resource development
Providing engineers
Providing technologies
Technological development
Industry
Education/ Services
Contribution to cyber security through business activities
Commercialization

Partnership with Interpol

NEC entered into a partnership agreement with the International Criminal Police Organization ("Interpol") for global cyber security measures in December 2012, under which NEC will use Interpol's international network and NEC's advanced cyber security solutions to research and analyze increasingly complex and sophisticated cybercrimes and develop state-of-the-art cyber security measures to be supplied to Interpol member countries.

Interpol established in Singapore the Interpol Global Complex for Innovation to support R&D, training, and investigation activities related to new cyber crimes. At the Interpol Digital Crime Centre ("IDCC") located at the same facility, NEC will investigate and analyze cyber security-related threat information, develop new investigative techniques, and provide systems and personnel for training purposes.

Both parties will jointly work on developing cutting-edge cyber security measures to be offered to Interpol member countries. By promoting the broad adoption of cyber security and digital security solutions through various facilities to be built at the IDCC, namely the Cyber Fusion Centre (CFC), an information dissemination and sharing operation center where threat information related to cyber crimes will be investigated and analyzed to support investigations, the Digital Forensic Lab (DFL), which will analyze malware and develop new investigative techniques, and a training room where cyber training will be conducted, activities promoting cooperation against cyber crime in neighboring countries will be carried out, leading to innovations born of the combination of global law enforcement activities, law enforcement related technologies, and safety-related technologies.

Right: Interpol Secretary General Ronald K. Noble
Left: NEC President & Representative Director Nobuhiro Endo

Image of IDCC's operations center (Cyber Fusion Centre)

Cyber Defense Institute

"Only humans can handle threats caused by humans." The Cyber Defense Institute deals with evolving cyberspace threats through globally coordinated activities. Boasting human resources endowed with professionalism and a high sense of ethics, its teams, which are active in various fields including security, hacking prevention, and forensics, provide high-quality technical services, thereby contributing to the realization of a safe and secure cyber society.

While remaining independent within the NEC Group, the Cyber Defense Institute complements and strengthens NEC's cyber security business.

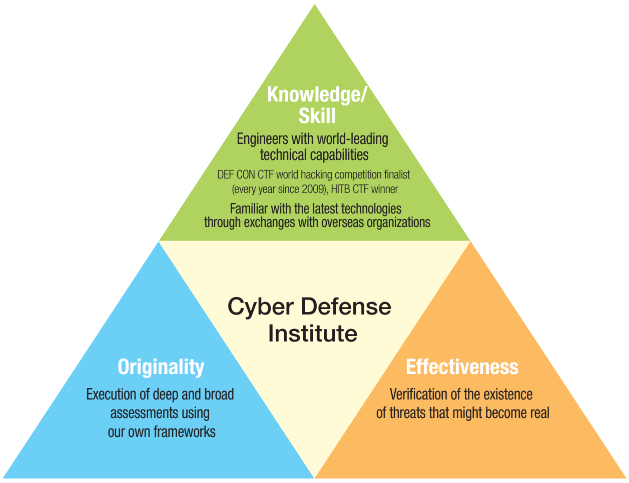
Besides making policy recommendations to the Japanese government and government offices and raising society's awareness about cyber security issues, the Cyber Defense Institute supplies security measures to providers of social infrastructure including government agencies and electric power, traffic, finance, and communications companies. Further, through coordinated activities with unique global information networks including partnerships, organizations, companies and the hacker community, we exchange the latest information about threats, vulnerabilities, security technologies, and so on, in order to implement actions to meet future security demands.

Security Assessments

Our engineers with world-leading technical capabilities carry out high-quality and original security assessments, leading to safer control systems, enterprise (organization) networks, and web applications.

Consulting and R&D

By investigating the cyber situation and developing training scenarios for assumed threats before serious incidents occur, we support activities to strengthen the functions and capabilities expected of us by related parties, as well as our inter-communication skills. In addition to incident prevention appropriate for each organization, this contributes to the minimization and localization of damage when an incident actually occurs, ensuring the prompt restoration of the affected organization's capabilities.


Knowledge/
Skill
Engineers with world-leading technical capabilities
DEF CON CTF world hacking competition finalist (every year since 2009), HITB CTF winner
Familiar with the latest technologies through exchanges with overseas organizations
Cyber Defense Institute
Originality
Execution of deep and broad assessments using our own frameworks
Effectiveness
Verification of the existence of threats that might become real

Infosec

Infosec, which was founded in 2001 as a company specialized in information security, provides a broad array of information security and cyber security related services, ranging from information security management for government agencies and companies, and consulting for the establishment of governance, to security planning for ICT systems in general, the design, construction, operation and maintenance of systems to deal with cyber attacks, and year-round 24-hour security monitoring services.

As a key member of NEC's Cyber Security Factory, Infosec also plays an important role in providing monitoring services and information analysis, and is positioned as a core player in the acquisition and fostering of human resources. Through these activities, Infosec develops NEC's cyber security business not only domestically but also overseas. It is an early adopter of leading-edge technologies and products, recruits overseas talent, accumulates operations and management know-how, and provides value-added services and intelligence.

InfoCIC Security Operations Monitoring Service

When it comes to cyber security, introducing software and hardware is just the beginning; operations management and response to emergencies following the introduction are the key to success.

Infosec Cyber Intelligence Center, or InfoCIC for short, collects logs generated from security monitoring devices and analyzes them through the eyes of professionals, continuously monitoring cyber attacks on a 24/7 basis. Moreover, true to its name of "Cyber Intelligence," it accumulates information on analyzed attacks, malware, and so on, aiming to acquire knowledge and put it to work to further improve monitoring accuracy.

Cyber Security Factory

To protect the information assets of customers from increasingly sophisticated cyber attacks, we offer advanced comprehensive services through the Cyber Security Factory, a core base that integrates our various cyber attack countermeasure functions.

NEC's Cyber Security Factory

In recent years, damage from cyber attacks, mainly from advanced persistent threats (APT), has been expanding, and sensitive information from public institutions, leading-edge technologies of companies, and personal information are being targeted by professional organized crime groups. Such attacks can make the continuation of business activities difficult as they damage the social reputation of companies and disrupt business operations, making the strengthening of countermeasures increasingly necessary.

The Cyber Security Factory is a core base equipped with the mechanisms required to support the implementation of measures against cyber attacks.

In collaboration with outside expert information security firms, the NEC Group has formed an alliance of cyber attack countermeasure specialists, which collects and analyzes cyber attack information while actually providing services such as monitoring for cyber attacks and performing detailed analysis of incidents, and creates and accumulates the technology and know-how required to respond to such attacks.

To respond to constantly evolving threats, the Cyber Security Factory works in the following five areas to implement new activities that will produce synergistic effects from the viewpoint of technological development, information sharing, and human resource development.

1 Security Monitoring

With the latest Security Operations Centers (SOC), customers' networks and websites are monitored 24 hours a day, 365 days a year, and security professionals promptly respond when unauthorized communications or malware (malicious software) infection incidents occur.

2 Cyber Range

Cyber exercises are carried out in simulated environments in which trainees practice the series of actions required when a cyber attack occurs. Evaluation and analysis of the attack resistance and usefulness of the products are also carried out. Furthermore, the results and knowledge obtained from the analysis of malware are accumulated in databases and utilized for the design of optimal cyber attack handling methods as well as for the development of new services and products, and the design and construction of systems. a

3 Cyber Intelligence

Along with collecting cyber attack trail evidence and investigating the latest attack techniques and malware trends, we cooperate with various collaboration partners, public-private sector joint councils, and Interpol, sharing information and creating new knowledge and contributing to the prediction of new cyber attack methods.

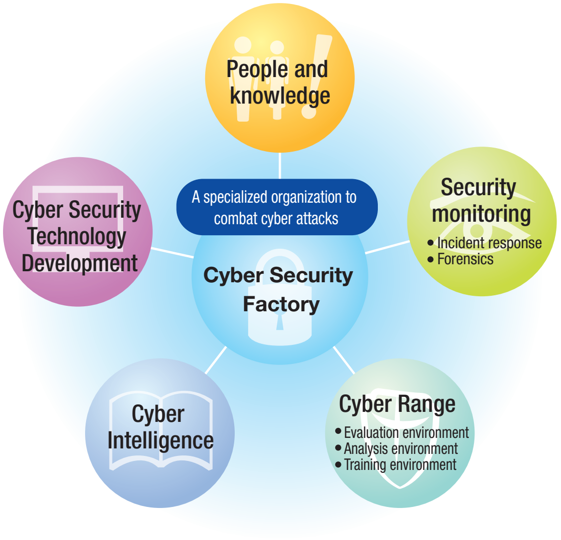
4 Cyber Security Technology Development

Leveraging our cyber range and cyber intelligence experience, we bring together new technologies such as automated analysis using big data technology, and convert cyber attack countermeasure know-how into tangible knowledge to be used to develop advanced technologies that will enable us to combat more sophisticated attacks.

5 People and Knowledge

With hands-on experience at the Factory and by sharing our accumulated knowledge, we are able to develop security professionals. Also, leveraging our Cyber Range and Cyber Intelligence activities, we will develop an effective training method and contribute to producing highly qualified engineers, who are in short supply at the moment.

Cyber Security Factory Structure



Security Operations Center (SOC)

Cyber Security Total Support Service

The Cyber Security Total Support Service is provided by security professionals and leverages the core technologies and knowledge acquired by the Cyber Security Factory. Consisting of three phases, namely a deployment phase, operation phase, and incident response and recovery phase, it offers a one-stop solution that includes the design and deployment of cyber attack countermeasure systems, the operation and monitoring of security systems, and emergency response upon detection of anomalies.

❶ Deployment Phase

During the deployment phase, optimum solutions are proposed through security consulting that includes the assessment and investigation of the security situation of the customer's systems through vulnerability diagnosis and penetration tests.

❷ Operation Phase

The operation phase is composed of operation monitoring services and routine diagnostic services. The operation monitoring services can monitor not just network entrance and exit points but also terminals to detect illegal programs such as viruses that manage to penetrate systems as the result of exploits such as targeted email attacks.

Routine diagnostic services regularly check whether software updates are being carried out properly, and whether vulnerabilities have been acquired owing to various changes during the operation of customers' systems.

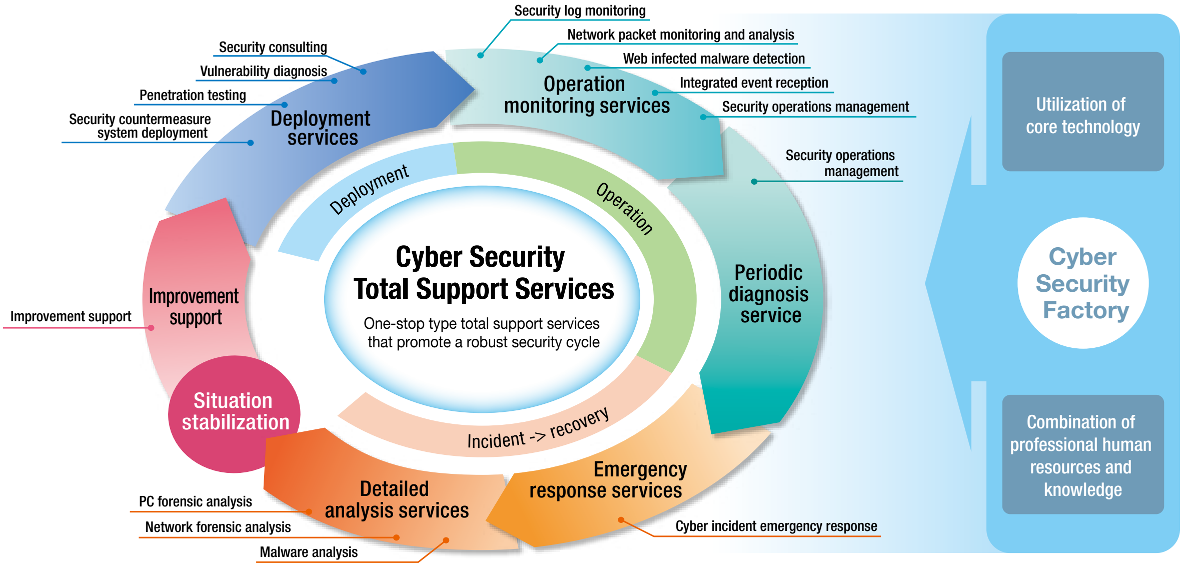
❸ Incident Response and Recovery Phase

This phase consists of emergency response services and detailed analysis services. Emergency response services include Cyber Incident Onsite Services whereby, if a customer's system is deemed highly likely to suffer a security incident, professional staff will rush to the site and implement appropriate initial response and on-site protection maintenance. The actions taken include the preservation of evidence and system stoppage and recovery in coordination with analysts at the Cyber Security Factory.

Detailed analysis services consist of PC, network, and malware analysis, determination of the specific source of infection and what information was leaked, and analysis of the nature of the damage done.

After the problem that caused the incident is studied and suitable solutions are proposed, support is provided for the necessary improvements.

Total Support Services Menu


Security log monitoring
Network packet monitoring and analysis
Web infected malware detection
Integrated event reception
Security operations management
Security consulting
Vulnerability diagnosis
Penetration testing
Security countermeasure system deployment
Deployment services
Operation monitoring services
Security operations management
Deployment
Operation
Cyber Security Total Support Services
One-stop type total support services that promote a robust security cycle
Improvement support
Improvement support
Periodic diagnosis service
Situation stabilization
Incident -> recovery
Detailed analysis services
Emergency response services
PC forensic analysis
Network forensic analysis
Malware analysis
Cyber incident emergency response
Utilization of core technology
Cyber Security Factory
Combination of professional human resources and knowledge

Other Activities

The Cyber Security Factory is actively involved in promoting the understanding of cyber security and the identification of talented human resources, and it is engaged in creating a lively cyber security event scene in Japan, including SECCON, Hardening, and CODE BLUE. Further, in addition to promoting collaborations with partners by taking advantage of the opportunities that arise at the Cyber Security Factory, we are actively engaged in activities to share new information from bodies such as CRIC (Cyber Risk Information Center), and continuously apply the knowledge accumulated at the Factory.

* SECCON : Japan's largest security competition (hacker convention). Sponsored by the Japan Network Security Association (JNSA).
* Hardening : A competition for discovering and honoring engineers who have advanced protection ("Hardening") technology skills. Sponsored by WAS Forum.
* CODE BLUE : An international information security conference in Japan. The first conference was held in February 2014.
* CRIC : A private organization that shares risk cases in cyberspace and handling-related information, and also conducts research activities.

Examples of Information Security Activities ③

Focus on Solutions for Society

The NEC Group is focused on Solutions for Society, promoting a more sophisticated social infrastructure through the use of ICT. We aim to become a Social Value Innovator that resolves social issues worldwide and promotes safety, security, efficiency, and equality.

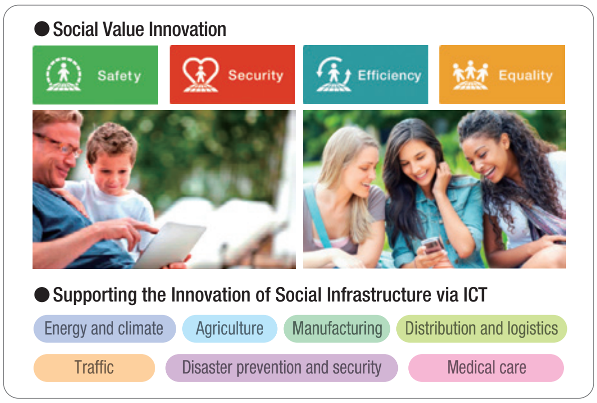
NEC's Innovative Social Infrastructure Concept

NEC's Innovative Social Infrastructure concept is an infrastructure that will provide for "All People, an Abundant Life".

Specifically, NEC defines four business domains as targets of its Solutions for Society. These domains consist of the conventional public domain, which includes disaster prevention and security, electronic administration, and financial, telecom carrier domain, which includes information networks and related service businesses, and enterprise domain, which includes distribution and logistics infrastructure and traffic, with the addition of smart energy, which is expected to grow in the future. We aim to further advance ICT, which includes cloud infrastructure and broadband networks, a strength of the NEC Group, and by concentrating management resources in these areas, we are contributing to the realization of an affluent and equitable society which makes efficient use of resources and whose members are safe and personally secure.

Solutions for Society that NEC Focuses on

Providing infrastructures for an abundant society for all people via ICT



●Social Value Innovation
Safety
Security
Efficiency
Equality
●Supporting the Innovation of Social Infrastructure via ICT
Energy and climate
Agriculture
Manufacturing
Distribution and logistics
Traffic
Disaster prevention and security
Medical care

With regard to the advancement of social infrastructure through ICT, the NEC Group already has a rich track record of solutions, including traffic control and fire and disaster prevention systems, water management systems, as well as seafloor seismographs and electronic medical records. These systems are built upon all kinds of sensors, ranging from seabed to space, and next-generation network technology, and each of these systems supports people's lives as infrastructure that is indispensable to society. Even if invisible to the eye, the infrastructure for living, which is truly indispensable for our daily lives, is supported by NEC's ICT to this day.

The use of information, a domain called big data, will become particularly important in the future for ICT use.

The NEC Group holds a large number of proprietary ICT assets of competitive value, including the following:

① Advanced sensors and human interface technologies for gathering information

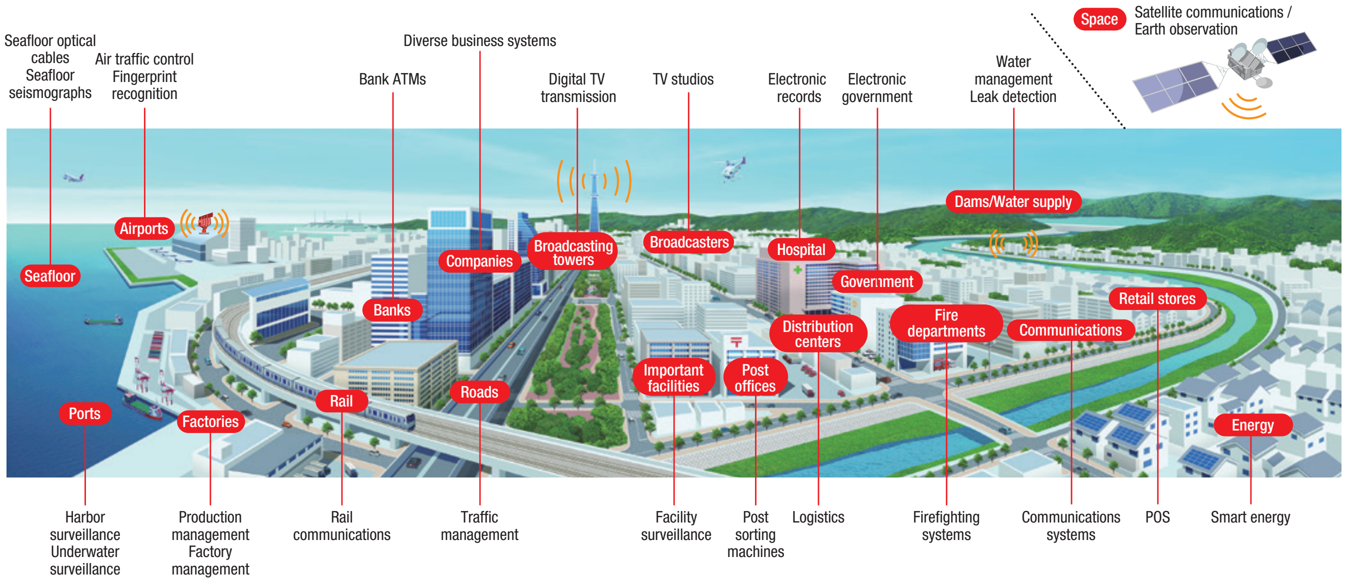
② Highly reliable high-performance IT platform technologies for analyzing the information gathered

③ Software-Defined Networking (SDN) that will serve as the foundation of next-generation network platform technologies for supporting the distribution of huge volumes of information

④ Cyber security, which is becoming a major social issue.

We are actively engaged in the creation of new value to resolve various social issues by taking full advantage of these ICT assets.

To formalize our engagement in Solutions for Society, NEC announced NEC Cloud IaaS and NEC Big Data Solutions in 2013.



Our Approach to Cloud Security

NEC is working to strengthen its cloud business, an area of major focus, as part of its Solutions for Society business offering advanced social infrastructures that use ICT, based on the latest data center technology and NEC Cloud IaaS, a cloud infrastructure service.

Features of NEC Cloud IaaS

NEC Cloud IaaS is a cloud infrastructure service that, in addition to offering high cost performance and high-performance, high-reliability service menus, allows integrated operations management including other companies' clouds and the existing systems of customers.

This service uses Software-Defined Networking (SDN) technology, which allows flexible and dynamic control by software of network configurations and settings. With this technology, networks can be visualized and safe environments where the communication environment of each customer is logically separated can be realized. Furthermore, the existing systems of customers can be ported to a cloud environment without having to change private addresses, and changes in the network configuration can be freely implemented from operation portals.

NEC Cloud IaaS is engaged in the following activities to improve the safety and reliability of cloud-based operations.

① Realization of both convenience and security
② Strict operation that conforms to relevant standards
③ Provision of security services
④ Effectiveness evaluation by auditors and publication of the results

❶ Realization of Both Convenience and Security

The Kanagawa Data Center where NEC Cloud IaaS is located uses face authentication and circle gates in addition to IC card authentication as the mechanism for machine room access control, thereby preventing spoofing and tailgating. NEC's NeoFace® face detection and face matching engine was found to be the world's most accurate during a technical benchmark test conducted by the National Institute of Standards and Technology (NIST) in the United States. Unlike other biometric authentication, face authentication can be done by simply facing the camera, resulting in greater convenience for machine room users.

❷ Strict Operation that Conforms to Relevant Standards

NEC Cloud IaaS performs strict access management that complies with the various cloud security standards issued by CSA*1, FISC*2 and other organizations, thereby improving reliability.

To ensure service security for service operations, operations personnel must submit work applications for each task. Upon task approval by an administrator, the worker in question is issued a one-time ID, and he or she uses that account to carry out the assigned task. Upon completion of the task, the one-time ID expires. The entire work history is recorded and monitoring that checks task application contents against the work history is performed, resulting in a mechanism that guarantees the legitimacy of access and operations.

Further, thanks to ISMS certification and compliance with FISC safety standards, NEC Cloud IaaS can be used with confidence even by financial institution customers.

❸ Provision of Security Services

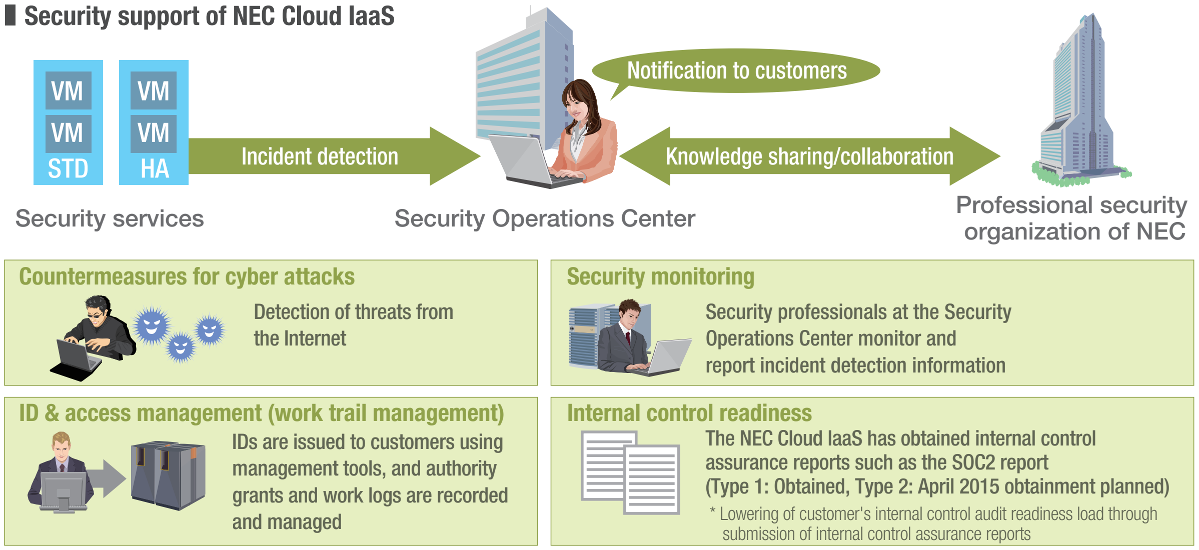
With regard to external threats, NEC Cloud IaaS provides an unauthorized access monitoring service through the Security Operations Center, which performs monitoring 24 hours a day, 365 days a year and solves problems that arise in collaboration with NEC's internal professional security organizations. NEC Cloud IaaS also provides services to enhance the reliability of customer operations such as ID and access management. Through security technology and internal controls, the safety of customer systems is improved.

❹ Effectiveness Evaluation by Auditors and Publication of the Results

NEC Cloud IaaS will undergo an audit by an auditing firm to ensure that it complies with policies and procedures related to security, availability, business continuity, and compliance. Obtainment of the verification reports (SOC1, SOC2*3 Type 2 reports) of the auditing firm is expected in April 2015. (The SOC2 Type 1 report, which is a single-time evaluation, has already been obtained by the Kanagawa Data Center.)

*1 CSA:The Cloud Security Alliance *2 FISC:The Center for Financial Industry Information Systems
*3 SOC1,SOC2:Service Organization Control1,2

Security support of NEC Cloud IaaS


VM
VM
STD
VM
VM
HA
Incident detection
Notification to customers
Knowledge sharing/collaboration
Security services
Security Operations Center
Professional security organization of NEC

Countermeasures for cyber attacks
Detection of threats from the Internet

Security monitoring
Security professionals at the Security Operations Center monitor and report incident detection information

ID & access management (work trail management)
IDs are issued to customers using management tools, and authority grants and work logs are recorded and managed

Internal control readiness
The NEC Cloud IaaS has obtained internal control assurance reports such as the SOC2 report (Type 1: Obtained, Type 2: April 2015 obtainment planned)
* Lowering of customer's internal control audit readiness load through submission of internal control assurance reports

Big Data Solutions and Security Technologies

NEC works on resolving various social issues by developing state-of-the-art media processing technology and unique analysis techniques, and leveraging this know-how through co-creation with customers.

1 NEC's Big Data Solutions

NEC performs semantic analysis of the various types of information in the real world, using world-leading media processing technology and advanced data analysis techniques, in order to discover new laws and predict and forecast the future. The effectiveness of these technologies has been verified in various areas such as the following.

❶ Enhancement and Optimization of Operations

As social systems increase in scale and complexity, the burden of maintaining stable operations is ever growing.

By visualizing correlations of sensor data and using invariant analysis techniques that allow early detection of abnormal behaviors, NEC constantly monitors correlations and balances among collected sensor data, allowing the practical use of predictive failure monitoring of plants and networks, quality management of constituent equipment, and anomaly detection of infrastructures.

❷ Enhancement and Improvement of Product and Service Value

Predicting the future from vast amounts of data and implementing appropriate responses requires the skills of highly experienced professionals.

NEC has developed heterogeneous technology capable of highly accurate extrapolation by deriving a plurality of rules from diverse data sets, and selecting rules suitable for each situation.

This technology allows future forecasting based on correlations among actual data and current related information.

❸ Strengthening Information Management and Detection of Crime and Fraud

Grasping information comprehensively to find risks that will affect business and public security requires a tremendous amount of work.

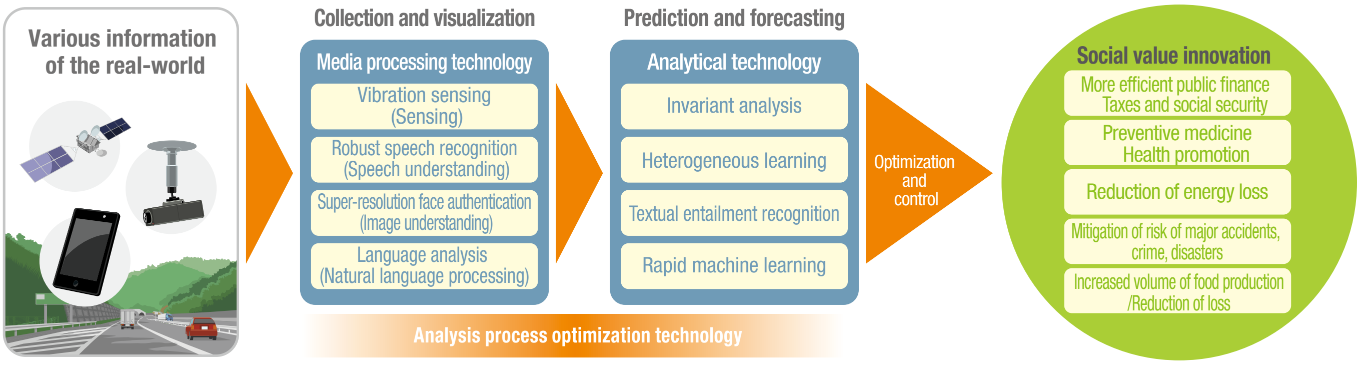
NEC has developed a new technology for recognizing textual entailment (RTE) that automatically determines if information subject to control is included in the text. With this technology, content requiring special attention is automatically extracted, enabling users to manage only the specified information more strictly, thereby enhancing corporate information governance and improving the efficiency of web and SNS trend analysis.

❹ Customer Management (Trend Analysis)

To properly grasp trends from a wide variety of data, preliminary hypothesis and rulemaking are important.

NEC has developed a technology to verify the validity of a hypothesis based on behavior analysis and/or profiling through machine learning technologies that automatically create processes analogous to human thinking.

Creation of value through media processing technology and analytical technology

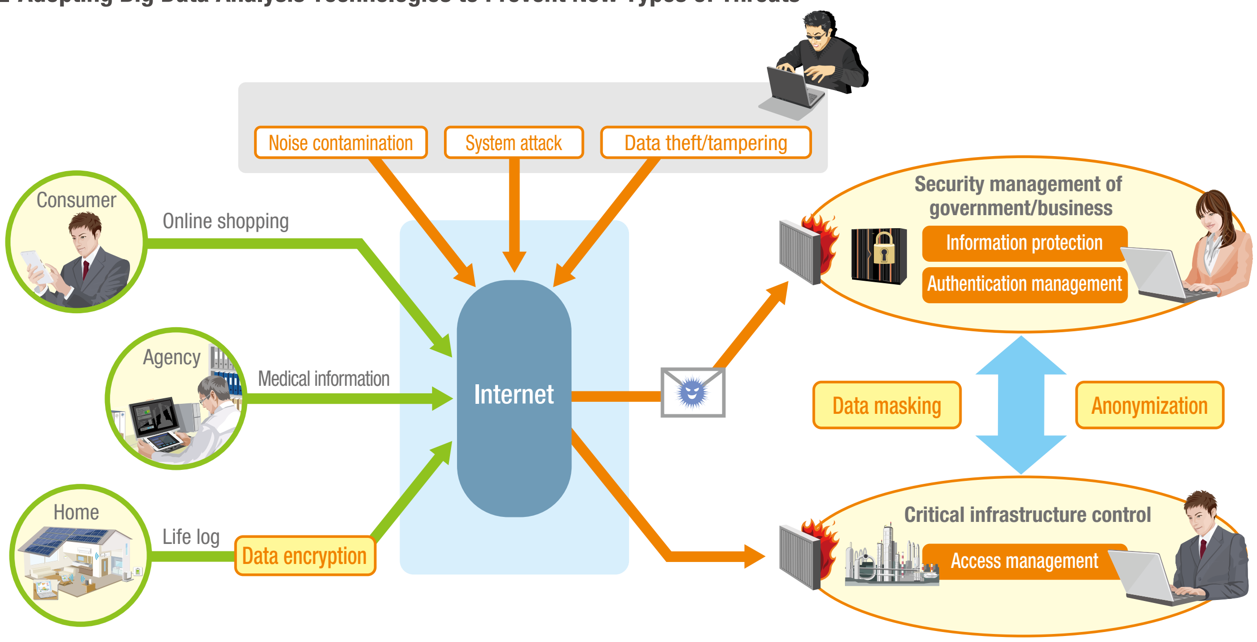

Various information of the real-world
Collection and visualization
Media processing technology
Vibration sensing (Sensing)
Robust speech recognition (Speech understanding)
Super-resolution face authentication (Image understanding)
Language analysis (Natural language processing)
Prediction and forecasting
Analytical technology
Invariant analysis
Heterogeneous learning
Textual entailment recognition
Rapid machine learning
Optimization and control
Analysis process optimization technology
Social value innovation
More efficient public finance Taxes and social security
Preventive medicine Health promotion
Reduction of energy loss
Mitigation of risk of major accidents, crime, disasters
Increased volume of food production /Reduction of loss

2 Security Challenges and Actions to be Taken in Big Data Environments

The data analysis technology provided by NEC is also effective for swiftly handling unknown attacks. For example, in the case of attacks on industrial systems, invariant analysis of the operational status for early detection of signs of an unknown attack can minimize damage. Further, when a security incident occurs, log data and event information can be automatically classified and analyzed without relying on the intuition or experience of experts, allowing efficient extraction of hypotheses based on correlations of data and occurring events. In addition, by regularly collecting and analyzing intelligence information on cyber attacks from the Internet and community websites, it is possible to catch early on signs of cyber crime and fraud and respond appropriately.

On the other hand, as the use of big data from social systems grows more widespread, new threats and issues might arise. In conjunction with value creation through the practical use of big data analysis techniques, NEC promotes the development of technology to deal with potential security incidents. For example, in addition to system operation interruptions caused by illegal access to systems, it is necessary to deal with issues such as ① the theft and/or tampering of sensor data, and ② the theft of specific personal data.

Adopting Big Data Analysis Technologies to Prevent New Types of Threats



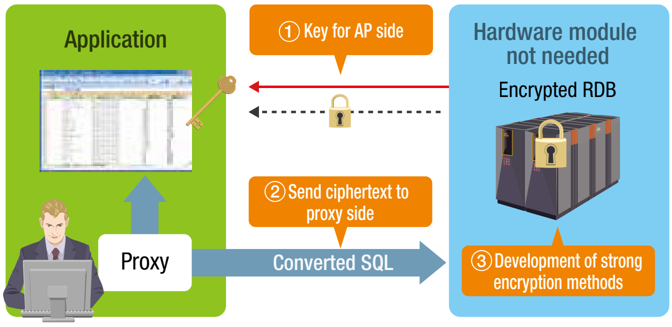
❶ Dealing with Data Theft and Tampering

When using big data, predictions are made solely based on the data itself by focusing trends and correlations, without relying on the experience and knowledge of people. For this reason, methods to verify the confidentiality and reliability of the data itself are required in addition to the enhancement of the current strict authentication infrastructure.

If the data that is collected and analyzed is confidential information, that data, even if it is encrypted in the database, will be decrypted in the database during data processing, so the risk exists that the data might be stolen or tampered with by someone who has usurped the privileges of the database manager or administrator.

NEC has developed the world' s first data masking computation technology that allows collected and analyzed data to be reused while remaining encrypted. As a result, any risk of unauthorized browsing of data by database managers or people entrusted with database administrator privileges is eliminated. Further, even if an attacker steals database manager privileges through a targeted attack or other illegal means, it is possible to prevent theft or tampering of the data itself on the database side.

Data masking computation technology


Application
Proxy
① Key for AP side
② Send ciphertext to proxy side
Converted SQL
Hardware module not needed
Encrypted RDB
③ Development of strong encryption methods

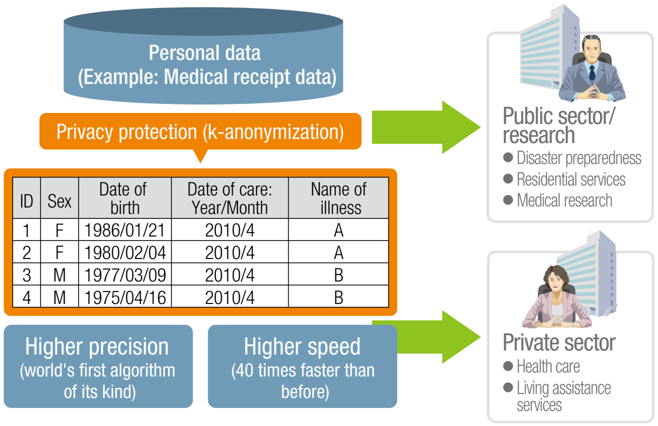
❷ Dealing with Theft of Specific Personal Data

Information collected as big data is often used for analysis to achieve various business tasks or purposes. Strict safety management is required for handling the collected data, especially if the data includes private data such as life-log information, because the data can be used to specify a person by linking it with other related information.

NEC has developed a mechanism that allows faster processing for anonymization technology that reduces the risk of personal identification without losing the information needed to understand individual tendencies and characteristics. As a result, personal data such as medical and healthcare information, as well as behavior history, can be safely and effectively utilized.

Along with working to create new value for customers, NEC contributes to the realization of a safe and secure social system, in which information is shared actively and securely, by making big data-related technologies suitable for practical use.

Anonymization technology (k-anonymization)


Personal data
(Example: Medical receipt data)
Privacy protection (k-anonymization)
Higher precision
(world's first algorithm of its kind)
Higher speed
(40 times faster than before)
Public sector/ research
● Disaster preparedness
● Residential services
● Medical research
Private sector
● Health care
● Living assistance services

ID	Sex	Date of birth	Date of care: Year/Month	Name of illness
1	F	1986/01/21	2010/4	A
2	F	1980/02/04	2010/4	A
3	M	1977/03/09	2010/4	B
4	M	1975/04/16	2010/4	B

Examples of Information Security Activities 4

Global Safety Business Activities

As one of the pillars of its growth strategy, NEC is accelerating the expansion of SI capabilities at overseas locations, the strengthening of its customer base, and the global deployment of its locally led "safety business" by leveraging the technologies we have accumulated thus far.

NEC's Global Safety Segment

Background and Concept of Safer Cities

"Safer Cities" is a new concept in public safety solutions deployed on a global scale by NEC. We provide advanced technologies and solutions for the prevention of crises and stronger response capabilities when crises occur to realize a world in which people are able to live, work, and play in safety and comfort.

To strength the global deployment of Safer Cities, NEC established the Global Safety Division in Singapore in 2013. Based outside of Japan, this division is achieving expansion into key markets through strategic planning and development of new technologies and solutions based on global market trends and needs, by fully leveraging the solutions experience and capabilities gained overseas so far. Further, as a new research base, NEC established in the same year NEC Laboratories Singapore, also located in Singapore. NEC Laboratories Singapore handles numerous projects in Singapore to resolve various urban problems in collaboration with government agencies and universities, studying and performing demonstrations of new technologies and solutions. These technologies and solutions will be deployed not only in Southeast Asian countries, but also in emerging countries in South America and Africa.

The Seven Business Areas of Safer Cities

Numerous challenges, such as the increase of urban populations and the risk of terrorist attacks, threaten safety at the state and city levels, and NEC provides solutions by combining various technologies, products, and services for the possibility of events that might cause significant danger and damage. Safer Cities offers solutions in seven areas.

1 Citizen Services and Immigration Control

Solutions in this area include national ID systems, voter ID management systems, and immigration systems that leverage biometric verification technologies, including the world's most accurate fingerprint matching and face recognition technologies.

2 Law Enforcement

Solutions in this area support peace-keeping activities by enabling person detection and criminal investigations based on surveillance footage. These solutions leverage NEC’ s biometrics technologies boasting the world's highest accuracy.

3 Critical Infrastructure Management

Solutions in this area include area monitoring centered on video surveillance and high-performance sensing systems, as well as security warning systems to proactively prevent threats to important facilities such as airports, ports, power plants, gas facilities, manufacturing plants, and stadiums, damage to which would significantly impact social life.

4 Emergency & Disaster Management

Solutions in this area consist of systems to predict the occurrence of natural disasters such as earthquakes, tsunamis, floods, fires, and typhoons and to minimize the damage caused by them in order to allow quick restoration of normal conditions.

5 Public Administration Services

Solutions in this area support public administration services for public safety and security, such as the prevention of infectious diseases and the promotion of e-government, using the technologies we have built up over the years.

6 Information Management

Solutions in this area enable the realization of safety in cyberspace, an essential requirement for our information society and one that has a major impact on people's lives.

7 Inter-Agency Collaboration

Solutions in this area provide network infrastructure to allow sharing of information among various organizations such as municipalities, government agencies, and other related organizations. They also provide data analysis and visualization to enable the extraction and presentation of useful data from collected big data.

The seven business areas of Safer Cities

Inter-Agency Collaboration
Critical Infrastructure Management
Emergency & Disaster Management
Information Management
Citizen Services & Immigration Control
Law Enforcement
Public Administration Services

Safety Solutions Case Studies

NEC has introduced over five hundred safety-related solution systems in forty countries around the world, and based on the extensive experience it has gained in the process, is developing technologies, products, and services, forming various partnerships, and actively submitting proposals to customers as it rolls out its offerings across the globe, creating new value and contributing to the creation of advanced social infrastructures.

❶ Citizen Services and Immigration Control Solutions

NEC offers public safety infrastructure solutions to realize a safe and secure social life, ranging from the national level such as national ID systems, to the local level in the form of public institutions and companies.

Biometric Authentication

Face recognition technology has the advantage of allowing the acquisition of authentication information from a distance, unlike other biometrics technologies, and NEC is strengthening its capabilities in this area, from research and development to product commercialization, as a foundation technology that will allow it to develop new markets. Further, NEC is also carrying out development of multimodal finger authentication technology that allows the acquisition of not only fingerprints but also other information such as vein patterns all at once, and portable DNA analyzers that enable DNA analysis with portable devices, something that was heretofore impossible as this required a number of large analytical equipment units in a laboratory.

Immigration Control Solutions

More than 200,000 people travel every day across the border between Singapore and Malaysia via the Causeway Bridge. In collaboration with Singapore's Immigration & Checkpoints Authority (ICA), NEC has delivered an eIACS system that allows rapid processing of travelers at the border. The new system, which uses electronic passports called BioPass that hold the fingerprint data of passport holders, automatically issues a security alert if a passport number or fingerprint does not match at the security gates. The misidentification rate of this fingerprint authentication system is an extremely low 0.001 percent, making it the world's most accurate fingerprint authentication technology

Citizen services and immigration control

● Main solutions

- National ID system
- Voter ID management system
- Immigration control system
- e-Passport/e-visa system

● Introduction track record

- South Africa: National ID system
- Singapore: e-Passport / e-visa system
- Macau: Automated immigration control system

❷ Critical Infrastructure Management and Inter-Agency Collaboration Solutions

NEC has a long track record of providing security solutions for social infrastructure facilities using various sensors and analysis technologies.

Singapore Safe City Testbed Demonstration

NEC participated in the Singapore Safe City Testbed initiative spearheaded by the Ministry of Home Affairs (MHA) and the Singapore Economic Development Board (EDB), performing R&D and testing of new technologies to be used to maintain a safe and secure society. This experiment was aimed at realizing inter-agency collaboration (IAC) across government agencies in a bid to solve urban problems. NEC collected data through integration of the sensors and networks held by various government agencies, and used analytical techniques based on big data analysis, correlation modeling, risk characterization and other techniques, to detect the occurrence of accidents and incidents as well as warning signs thereof, and develop and demonstrate solutions for the safe and speedy transmission of information to the relevant government agencies. Among NEC's many successes are the development of new technologies such as the "Media Analysis Platform," which realizes large-scale real-time monitoring by connecting an analysis engine, whether from NEC or another company; "e-Evidence Technology," which increases reliability by checking the validity of surveillance cameras and their video data through the use of digital signature technology, and "Shared Digital Signage," which displays warnings and provides guidance on evacuation routes in the public space when an emergency occurs.

Argentina: City of Tigre Monitoring System

NEC has supplied the City of Tigre in Argentina with the world's fastest and most accurate face recognition technology for its urban monitoring system. This system compares the real-time surveillance data of network cameras mainly located at railway and ship terminals with a huge collection of photographic images stored in a database. This highly efficient monitoring assists the public prosecutor's office, judicial agencies, public welfare organizations to search for missing persons as well as to achieve other goals.

NEC has also supplied the city with various other original technologies, including the detection of double-riding on motorcycles, which is often linked to crimes such as purse-snatching, the detection of motorcyclists riding without helmets for road safety enforcement, suspicious behavior recognition for detecting the suspicious behavior of pedestrians or vehicles, and license plate recognition for detecting suspicious vehicles. Our solutions also include advanced features such as "crime maps" that display past crime areas. By integrating these latest technologies with the city's monitoring systems, we can contribute to enhancing security measures throughout the city.

Critical infrastructure management and inter-agency collaboration

● Main solutions

- High-performance sensing systems
- Video surveillance solutions
- Visualization solutions
- Plant monitoring systems
- Big data analysis systems

● Introduction track record

- Brazil: Stadium monitoring system
- Singapore: Singapore Safe City Testbed
- Argentina: Urban video surveillance system

Third-party Evaluations and Certifications

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

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
- NEC Engineering, Ltd.
- NEC Solution Innovators, Ltd.
- NEC Soft Okinawa, 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, Ltd.
- NEC Platforms, Ltd.
- NEC Management Partner, Ltd.
- NEC TOSHIBA Space Systems, Ltd.
- NEC TOKIN Corporation
- NEC Capital Solutions Limited
- Nittsu NEC Logistics, Ltd.
- NEC Aerospace Systems, Ltd.
- NEC Communication Systems, Ltd.
- NEC Saitama, Ltd.
- NEC Nagano, Ltd.
- NEC Shizuokabusiness, Ltd.
- Forward Integration System Service Co., Ltd.
- KIS Co., Ltd.
- N&J Financial Solutions Inc.
- NEC Informatec Systems, Ltd.
- Cyber Defense Institute, Inc.
- Infosec Corporation
- Sunnet Corporation
- NETCOMSEC Co., Ltd.
- Yokohama Electronic Computing & Solutions Co., Ltd.
- Showa Optronics Co., Ltd.
- Nippon Avionics Co., Ltd.
- ABeam Consulting Ltd.
- ABeam Systems Ltd.

(Companies listed in random order)

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
- NEC Engineering, Ltd.
- NEC Soft Okinawa, Ltd.
- NEC Solution Innovators, Ltd.
- NEC TOKIN Corporation
- NEC Nexsolutions, Ltd.
- NEC Networks & System Integration Corporation
- NEC Net Innovation, Ltd.
- NEC Personal Computers, Ltd.
- NEC Business Processing, Ltd.
- NEC Fielding, Ltd.
- NEC Facilities, Ltd.
- NEC Platforms, Ltd.
- NEC Management Partner, Ltd.
- NEC Magnus Communications, Ltd.
- NEC Livex, Ltd.
- NEC Fielding System Technology, Ltd.
- NEC Shizuokabusiness, Ltd.
- Forward Integration System Service Co., Ltd.
- Toyo Networks & System Integration Co., Ltd
- VALWAY121Net, Ltd.
- KIS Co., Ltd.
- N&J Financial Solutions Inc.
- NEC Informatec Systems, Ltd.
- Sunnet Corporation
- Yokohama Electronic Computing & Solutions Co., Ltd.
- LIVANCE-NET Ltd.
- ABeam Consulting Ltd.

(Companies listed in random order)

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.

NEC products and systems with ISO/IEC 15408 certification

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

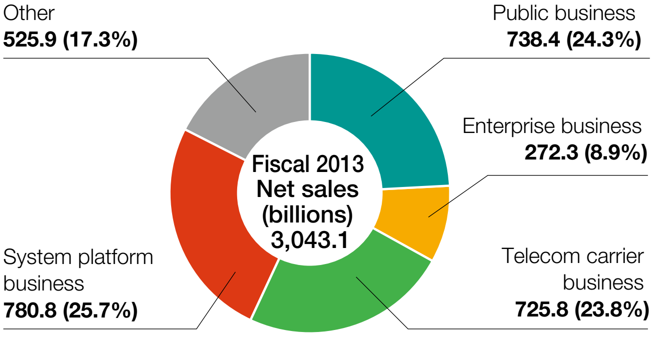
Number of employees (Consolidated):
100,914*

Consolidated subsidiaries:
258*

* As of March 31, 2014

Segment Information

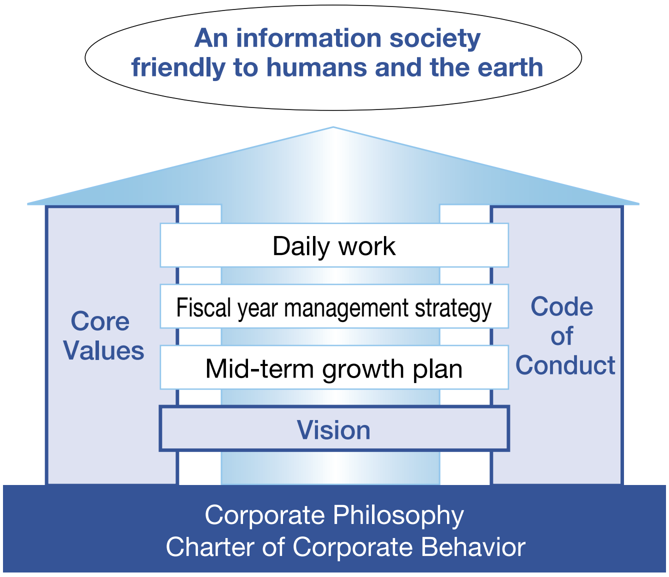
Net Sales by Segment (Percentage)



* As of March 31, 2014

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

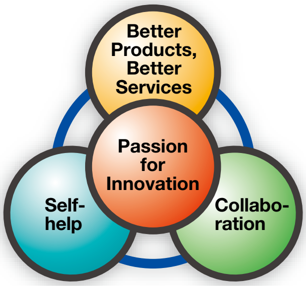
NEC Group Vision 2017

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 an open mind ● Collaborate beyond organizational boundaries
For our customers **Better Products, Better Services**	● Think from the 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 August 2014