Empowered by Innovation NEC

NEC's Initiatives to Build a Secure Information Society

Information Security Report 2012

Information Security Supporting an Information Society Friendly to Humans and the Earth

NEC Corporation

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

Issued July 2012

NEC Corporation

Information Security Report 2012

CONTENTS

On the Publication of This Report

This report is being published to provide a better understanding of information security initiatives in the NEC Group. The report covers related initiatives through March 2012.

For Inquiries Regarding This Report

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

NEC's Approach to Information Security

The NEC Group strives to become a leading information security company trusted by society.

Takashi Niino

Representative Director &
Senior Executive Vice President
NEC Corporation

Today's advanced information communication technologies are making our society more sophisticated by enabling us to use information and systems in many different ways. Along with this, however, information security problems such as information leaks and system disruptions due to cyber attacks are on the rise, which has a significant impact on our daily life. In this age in which the efficient and effective utilization of information within and among companies is indispensable for business success, the management of information security risks has become critical for supporting high value-added activities in the value chain.

In order to contribute to the success of our customers and the development of a better society, the NEC Group has systematized all its management activities as "the NEC Way", as we look to achieve the realization of an information society friendly to humans and the earth. In implementing the NEC Way, we pledge to pursue the sustainable expansion of society and the NEC Group by winning the support of all our stakeholders, including our customers, shareholders and investors, business partners, and local communities, while of course complying with relevant laws and regulations and fulfilling our social responsibilities as a good corporate citizen. As a global company that provides information and communication technologies indispensable for social infrastructure through the promotion of computer and communications (C&C) cloud services, the NEC Group aims to contribute to society
by protecting the information assets entrusted to us by customers and business partners, and by providing reliable products, services, and information security solutions.

To help everybody benefit from information communication technology and realize a prosperous society, the NEC Group must improve its corporate value by positioning information security as a core management activity. Specifically, we will pursue the following:

- Ensuring that the NEC Group works together as "One NEC" to promote the maintenance and enhancement of information security.
- Deploying measures to include not just the NEC Group, but our business partners as well.
- Achieving a balance between the appropriate protection of information and its appropriate sharing and use.
- Maintaining and enhancing information security on multiple levels by using a comprehensive approach that includes building information security management systems, creating an information security platform, and developing human resources for information security.
- Providing customers with reliable security solutions.

This report presents the NEC Group's information security activities. Through communication with all our stakeholders, we aim to continuously improve our corporate activities and become an information security company trusted by society. Thank you for taking the time to read this report. We appreciate your continued support and interest.

Information Security Promotion Framework

The NEC Group aims to maintain and enhance information security throughout the Group and contribute to the realization of an information society friendly to humans and the earth by creating a secure information society and offering value to customers.

Threats to information security change every day, and in today's society, which has reached a high level of sophistication through IT, information security is an important management issue that cannot be ignored. To fulfill social responsibility as a company that is trusted by society, the NEC Group has established an information security promotion framework that enables us to create a secure information society and provide value to customers, by protecting the information assets entrusted to us by customers and business partners, providing reliable products, services, and information security solutions, and conducting appropriate reporting and information disclosure to our stakeholders.

By combining the following four components, our information security activities for protecting information assets aim to maintain and enhance information security on a comprehensive basis and on multiple levels.

1. System for promoting the thorough implementation of information security throughout the organization
   "Information Security Governance"
2. System for developing policies and rules and applying PDCA cycles
   "Information Security Management"
3. IT system for protecting networks, business systems, PCs, and other corporate systems from threats
   "Information Security Platform"
4. System for raising awareness about information security and skill development training
   "Human Resources for Information Security"

These components are divided into Group-wide activities and activities carried out by each organization in the NEC Group.

Group-wide activities include the formulation of the NEC Information Security Statement and establishment of Group-wide regulations, the development of a common information security platform, the formulation, implementation, revision and improvement of policies for education/awareness building and the operation of systems such as the human resource development system, and information security governance, a system for effectively and efficiently ensuring thorough implementation of all the above throughout the entire Group.

Group-wide activities are not limited to the NEC Group and include also the development of security measures in coordination with business partners, and the establishment of development processes for providing reliable products, services, and solutions.

In addition to these Group-wide activities, each individual organization has a security management framework tailored to its own business environment and an internal organization structure for conducting activities in accordance with Group directions.

NEC Security Vision

Striving to become a leading information security company trusted by society

Information Security Governance

NEC has instituted an information security governance system for determining the direction of information security, performing monitoring and evaluation, and disclosing and reporting implementation progress. This system governs security levels for the entire Group.

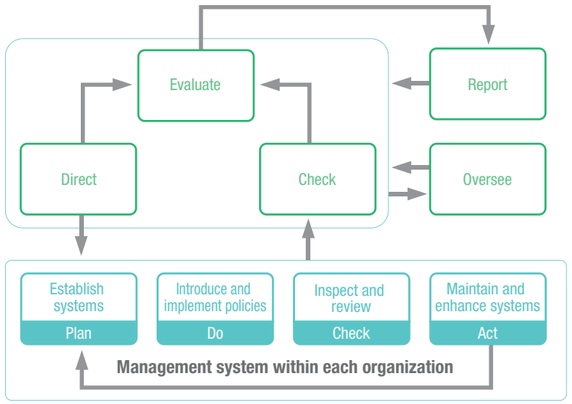
Approach to Information Security Governance

NEC has built management systems for each of the divisions and in the case of NEC Group companies, for each company (or, depending on the size of the company, for each division), and is maintaining and enhancing information security based on PDCA cycles.

The governance of information security is required in order to effectively and efficiently implement the activities of each organization and enhance the overall security level as "One NEC." Specifically, we define goals for the entire Group and determine strategies to achieve them, including establishing Group policy and organizational frameworks, as well as allocating business resources. In pursuing these goals, we check the implementation progress and achievement status of each organization, while monitoring each environment to detect information security incidents.
After evaluating the implementation progress, we provide guidance if necessary to help each organization improve its systems.

We also conduct audits to ensure that this PDCA cycle is adhered to and disclose the status of our information security activities through our Annual CSR Report and this Information Security Report to ensure transparency and business continuity.

Information Security Governance

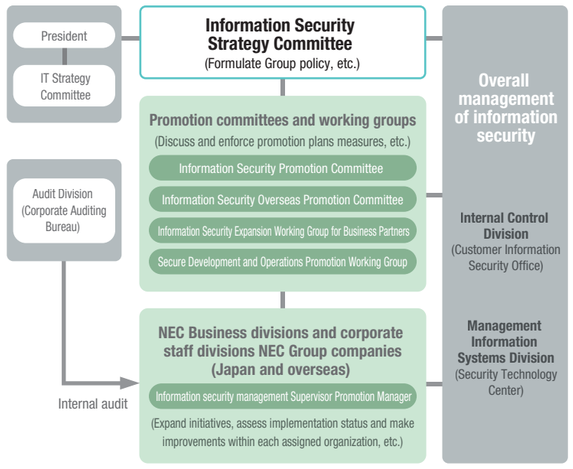


Information Security Promotion Framework Integrated with Group Management

The information security promotion framework of the NEC Group consists of an Information Security Strategy Committee and its subordinate organizations, and the promotion structure of each organization. The Information Security Strategy Committee has three main functions to completely eliminate information security incidents within the Group, namely 1) to carry out deliberations, evaluation, and improvement of information security policies, 2) to determine the causes of major incidents and determine how to prevent recurrence, and 3) to ensure the application of results to the NEC Group's information security business. Four promotion committees and working groups, which constitute the subordinate organizations of the Information Security Strategy Committee, are in charge of deliberations, coordination, thorough enforcement of instructions, and policy progress management with regard to companies in Japan, overseas companies, business partners, and the Secure Development and Operations initiative, respectively. These committees and working groups work to enhance the effectiveness, efficiency and feasibility of the various information security policies by sharing information about incidents and maintaining awareness of the security status and issues at each organization.

The information security managers of each organization have primary responsibility for information security management including Group companies under their supervision. They ensure thorough dissemination of rules within their organizations, introduce and manage policies, and conduct implementation status inspections, reviews and improvements on a continuous basis in order to maintain and enhance information security.

Information Security Promotion framework



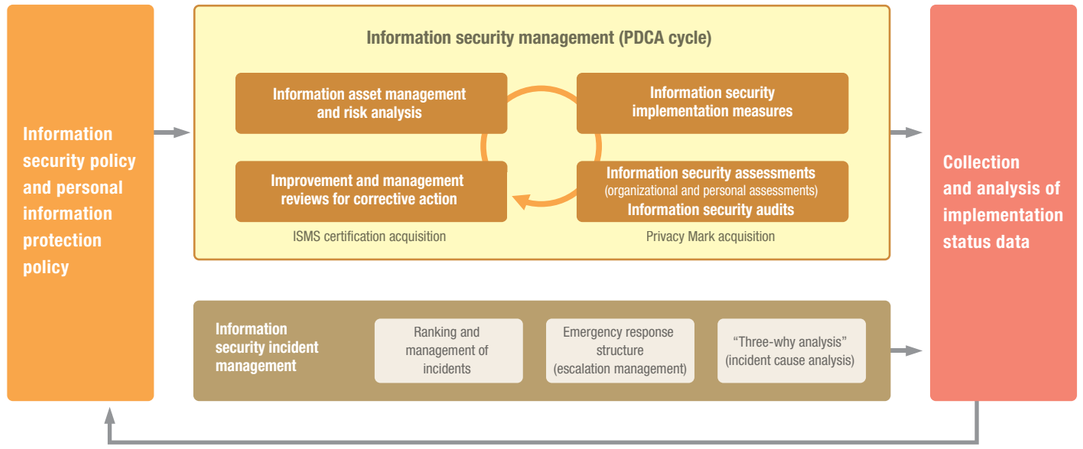
Information Security Management

In order to roll out the various NEC Group information security policies to the entire Group and get them firmly established, we have created an information security management structure and are working to maintain and strengthen information security through PDCA cycles.

Information Security Management Structure

The NEC Group is working to maintain and strengthen information security through the continuous implementation of PDCA cycles, based on policies for information security and the protection of personal information. To this end, we analyze the implementation status of information security policies based on the results of information security assessments and audits and reports on information security incidents, and revise policies as needed. Further, we encourage organizations within the Group to obtain or maintain third-party certification, such as ISMS certification and Privacy Mark certification to achieve the security level required by third-party organization standard.

NEC Group Information Security Management



Information Security Policy and Personal Information Protection Policy

The NEC Group has positioned information security and the protection of personal information as key to the proper conduct of business, and is working to strengthen management accordingly.

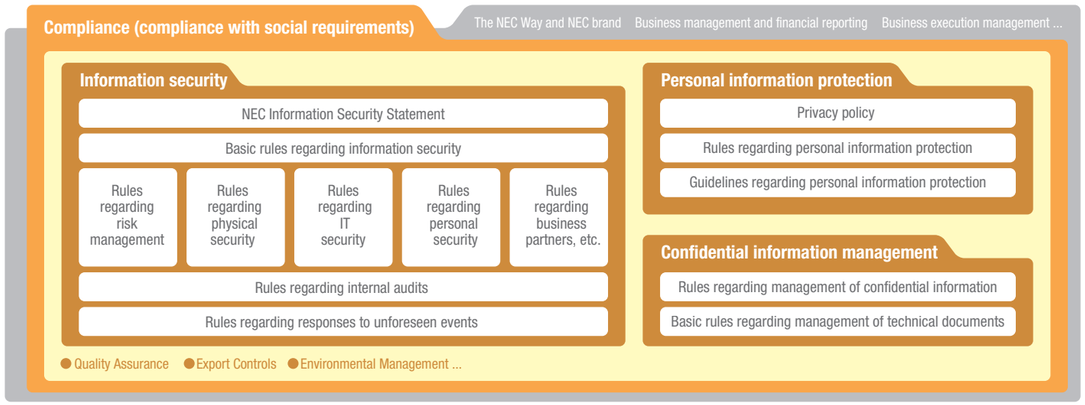
We have declared to society our commitment to information security in the form of the "NEC Information Security Statement" (established in 2000 and disclosed to the public in 2004). The concrete rules and standards for realizing these basic policies include basic information security rules, rules for information management (corporate confidential information management rules, personal information protection rules, and technical document management rules), and IT security rules. These various rules are organized into a system and form the information security policy of the NEC Group.

In terms of protecting personal information, NEC established the NEC Privacy Policy in 2000, and obtained Privacy Mark certification in 2005. We also use management systems that are fully compliant with the Japan Industrial Standards Management System for the Protection of Personal Information (JIS Q 15001) and with Japan's Personal Information Protection Law. With regard to the handling of personal information, we ensure that strict protection is common to the entire Group, and as of March 2012, 43 companies have obtained Privacy Mark certification.

NEC Group Management Policy

The NEC Group Management Policy was established in 2009 to maximize our strength by aligning the various constituents of our Group in the same direction. The aim is to achieve a global standard based management foundation through the standardization of rules related to the conduct of business, and the unification of systems, business processes, and infrastructure. The NEC Group Management Policy also encompasses information security and personal information protection policies, and is being deployed as the common policy of Group companies worldwide.

NEC Group Management Policy



Information Security Risk Management

For information security management to be effective, information security risks need to be properly assessed and managed.

Evaluation of Information Security Risks

The NEC Group performs risk assessment and implements risk countermeasures by using two analysis methods: analysis of difference from a baseline, and detailed risk analysis. Basically, security is maintained using an information security baseline defined as the security level to be commonly implemented. When advanced management is required, we carry out analyses based on detailed risk assessment criteria and implement finely-tuned measures.

Management of Information Security Incidents

Information security incidents must be reported and data on the incident submitted for analysis. Incident information is centrally managed based on standard rules common to the entire Group that specify, for example, incident categories, report formats, criteria to determine the impact level, immediate response to stakeholders, and resolution procedures. Incident information is also input to the information security PDCA cycle.

At the macro level, we 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 knowledge thus acquired to policies common to the entire Group. We also use incident data for effectiveness measurement and as KPIs.

Moreover, in order to determine the true cause of information security incidents, we conduct three-why analysis. We have developed a framework that helps the affected sections conduct analysis on their own by using established analysis methods.

If the incident is serious, professional advisors participate in the analysis. The results are then reported to top management, and effectiveness is maximized by sharing the findings with the entire Group and reflecting them in information security measures.

Information Security Assessments

The NEC Group has been conducting information security assessments every year since fiscal 2006 to check the implementation status of information security measures and to ensure the development and execution of improvement plans for measures whose implementation is unsatisfactory. In fiscal 2011, information security assessments were conducted in 101 companies in Japan and 90 overseas companies in the NEC Group.

Information Security Assessment Details

Priority items specifically aimed at eradicating information security incidents related to information leaks have been defined and are being systematically implemented. Based on the results of information security incident analysis, the major causes were identified and measures were implemented with purpose to ensure the safe use of USB flash drives and other removable storage media, information security for work done outside the company, strict management of important personal information, proper management of confidential information when work is outsourced, and prevention of missent emails. As the result of reinforcing information leakage prevention measures since fiscal 2009, the number of information security incidents has declined to about one fourth the previous level.

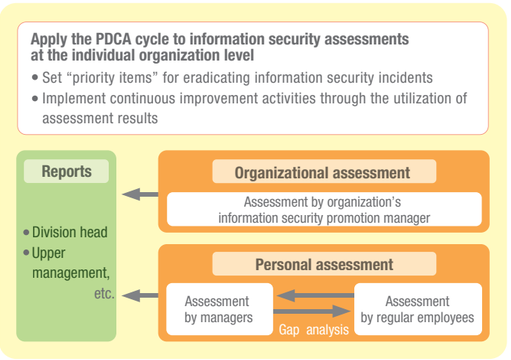
Information Security Assessment Methods

Information security assessments are conducted using two methods, namely organizational assessments, whereby the information security manager of each organization checks the status of the entire organization, and personal assessments, whereby each individual reports on the implementation status of information security measures. In the past, organizational assessments were principally implemented, but in order to finely grasp location situations and achieve more effective improvements, we have expanded the implementation scope of personal assessments. In fiscal 2012, personal assessments were conducted by approximately 82,000 people, but we plan to further expand the implementation scope in the future. Personal assessments conducted by regular employees and managers to cover both the execution and management aspects. The accuracy of information security management is improved by analyzing the gap between these aspects.

Improvements through the Utilization of Assessment Results

Based on the results of the assessments, each organization worked on problem-solving at the organizational level by determining the causes behind the inadequate implementation of information security measures and creating improvement plans accordingly. For the resolution of remaining issues and matters requiring further improvement, continuous improvements were ensured by reflecting the acquired information in the annual Information Security Promotion Plan.

Information Security Assessments (Organizational and Personal Assessments)



Information Security Audits

NEC’s Corporate Auditing Bureau plays a central role in information security management audits and Privacy Mark-related audits. The information security management situation of each organization is audited based on the ISO/IEC 27001 and JISQ 15001 audit standards. The NEC Group has established an internal audit system in which the Corporate Auditing Bureau executes thorough audits on a regular basis.

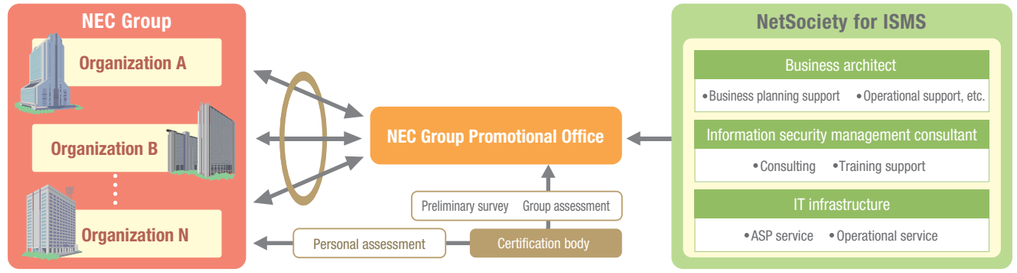
Promotion of Information Security Management System (ISMS) Certification

For organizations that need to obtain ISMS certification, the NEC Group provides a system to help them obtain the certification and operate the ISMS.

Specifically, we have designed a set of standard content for fulfilling the requirements of ISMS certification. Based on this standard content, we are offering services such as consulting, audit system development support, education and training, and support for improving auditing efficiency (such as by auditing only areas that differ from previous audits). This standard content can also be complemented with policies common to a particular corporate group as well as the individual policies of an organization. This system is also useful for sharing the know-how of organizations that have already obtained ISMS certification, and for implementing the policies of a corporate group in a unified manner.

This system, which has been used by a large number of organizations in the NEC Group and many of its business partners (about 300 companies altogether), is offered as a solution called the “NetSociety for ISMS” service.

Support for Acquiring ISMS Certification Using NetSociety for ISMS



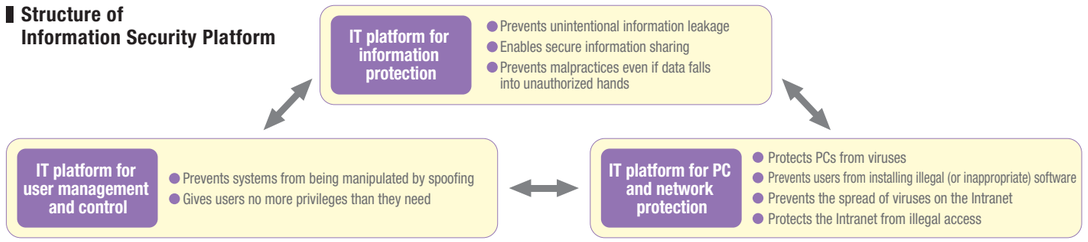
Information Security Platform

To protect customers' information and other confidential information, the NEC Group has built and operates an information security platform for the global management and administration of users and to enable the safe and efficient use of PCs, networks, and business systems.

Features and Structure of Information Security Platform

The information security platform consists of three platforms, "IT platform for user management and control," "IT platform for PC and network protection" and "IT platform for information protection," which work with and complement one another to realize the information security policies of the NEC Group.

Structure of Information Security Platform



IT Platform for User Management and Control

Authentication systems are the foundation of information security management.

The creation of a system to identify individuals makes it possible to control access to information assets and prevent identity theft using electronic certificates.

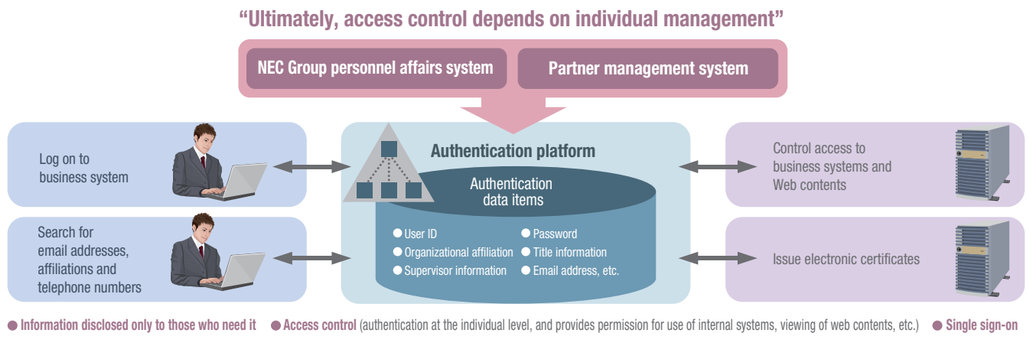
1 Suitable access control via authentication system

User identification and the granting of access authority according to the status of each user are critical in providing access to information assets.

The NEC Group has built a centrally managed authentication platform, targeting not only our own employees, but business partners as well.

In addition to user IDs, authentication data also includes organizational data, titles, and other access control information. Because these authentication data items are linked to the human resource system and information on any job changes (between companies or divisions, changes in title, retirement, etc.) is instantly reflected, the system always maintains the latest information.

NEC Group Authentication Platform



2 Encryption and electronic authentication using electronic certificates

By linking the NEC Group authentication platform with third-party certification authorities, we are able to issue electronic mail certificates, providing NEC Group employees with a means to authenticate their own person and their company. When sending important information such as customer information via email, these electronic mail certificates are used to securely exchange emails with S/MIME encoding. Email used as proof under internal controls or for compliance with Japan's Financial Instruments and Exchange Law (J-SOX) can also be signed electronically using these electronic mail certificates, reliably providing proof of the identity of the sender.

IT Platform for PC and Network Protection

The IT platform for PC and network protection is designed to maintain the security of all information devices connected to the NEC Intranet and protect the network from viruses, worms, and other attacks. Further, multi-layered protection measures against targeted attacks are required these days, and it is important to systematically apply security patch updates and anti-virus measures.

1 PC and network protection from viruses and worms

User environment support

In the NEC Group, software to monitor PC and network status is required to be running on all PCs connected to the NEC Intranet to make the status visible and ensure that the necessary security software has been properly installed. The system also automates the distribution of patches and the latest definition files for anti-virus software.

Network management

Along with a system to make PC status visible, we have set up a system for detecting intrusions on the Intranet, so that when a PC with insufficient security protection is connected to the Intranet, or a worm is detected on the Intranet, that PC or LAN is immediately disconnected from the Intranet.

Centralized management of security status

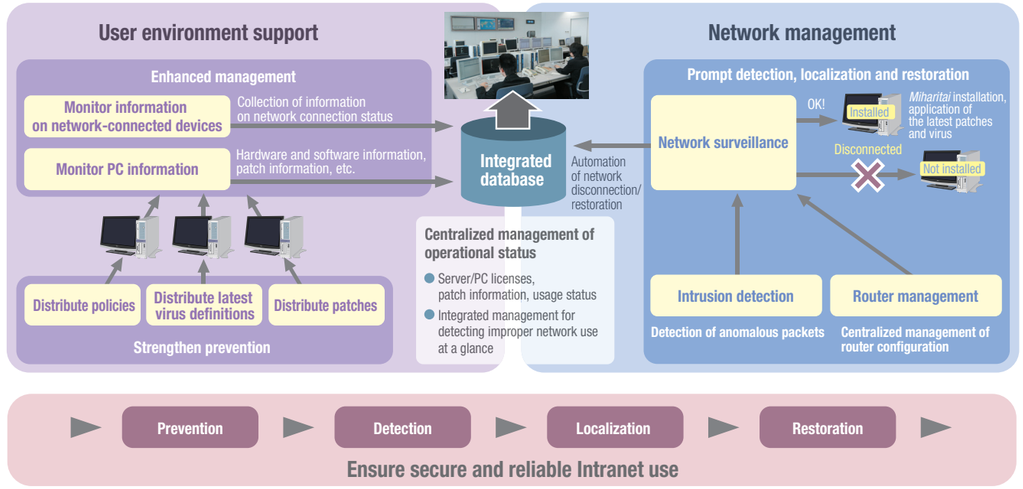
Status data associated with security measures, including software patches and anti-virus software, is collected in a centralized management system. The data is made available to Information Security Managers and Security Promotion Managers in their own divisions in a timely manner. This facilitates the smooth and thorough implementation of information security measures.

2 Checks using vulnerability detection tools

Using vulnerability detection tools, we check vulnerabilities in the information devices connected to the NEC Intranet.

Detected vulnerabilities are centrally managed by the system, and managers in each division are able to view the status of their division and fix any vulnerabilities using specified methods. The status of vulnerabilities (i.e., whether they have been fixed or not) is also centrally managed by the system, enabling us to monitor the status of the entire NEC Group.

Protection of PCs and Networks from Viruses and Worms



IT Platform for Information Protection

To prevent information leaks, it is necessary to identify the illegal channels through which information is leaked and to take appropriate measures based on risk analysis. As the NEC Group manages not only our own Group information but information entrusted to us by customers and information disclosed to business partners, we implement comprehensive and multilayered measures for each channel based on the characteristics of networks, PCs, electronic media, and other IT components.

1 System to prevent information leaks in the NEC Group

We have built an internal system to prevent information leaks using our own InfoCage products. Specifically, the system encrypts hard disks and files, restricts use of USB flash drives and other external storage media, and logs and monitors PC operations. The system has proved to be enormously effective in preventing information leaks.

Hard disk encryption

All business PCs in the NEC Group have InfoCage PC security software installed. This ensures that all the data on the PCs is stored in an encrypted state. This prevents the leakage of critical information in case of theft or loss, thereby minimizing damage.

Restrictions on the use of external storage media

In the NEC Group, USB flash drives and other external storage media used in business must be standard models with a forced encryption feature that applies to all the data stored on the device. To prevent information from being taken outside the company, stolen, or lost through the use of personal, off-the-shelf media, PCs are also configured to write data only to designated media.

Logging of PC operations

When an information leak occurs, it is necessary to accurately understand the circumstances surrounding the incident, minimize the impact of the leak, and enact measures to prevent recurrence. By saving PC operation logs, it is possible to investigate the impact of the leak and analyze the incident with accuracy.

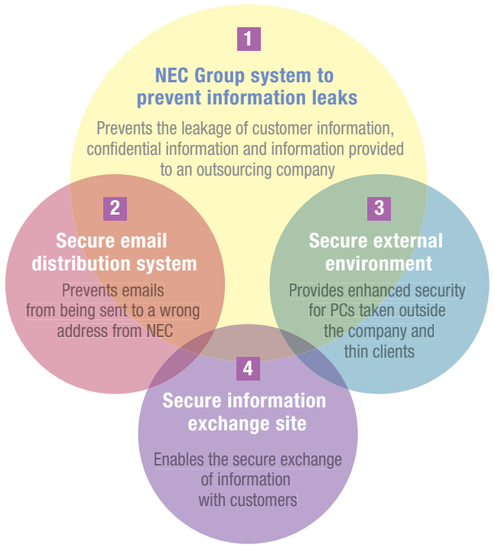
Policy Receipt Client

The InfoCage PC security policies for controlling the use of external storage media and collecting operation logs are centrally managed. Preset policies are applied on a mandatory basis to each PC, making it possible for managers in each company or division to easily control of the usage environment of authorized PCs.

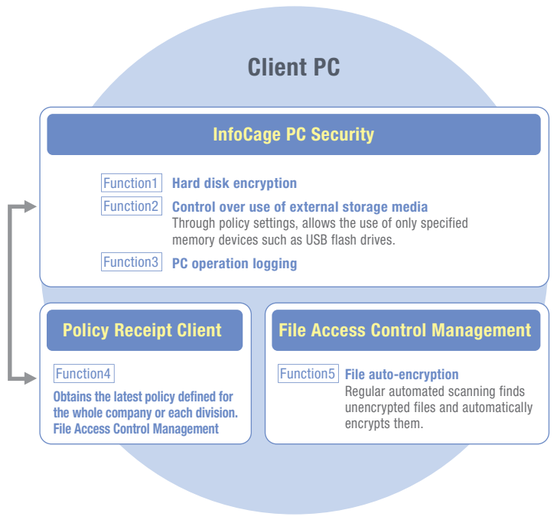
Automatic file encryption

We have implemented a file access control system at Group companies and business partners. This system automatically encrypts files exchanged within the Group and restricts access to those files only to authorized users. Since files can be viewed and edited even if they have been encrypted and are always handled in an encrypted state, information cannot be leaked even if the files fall in the hands of an unauthorized third party.

Overview of IT Platform for Information Protection



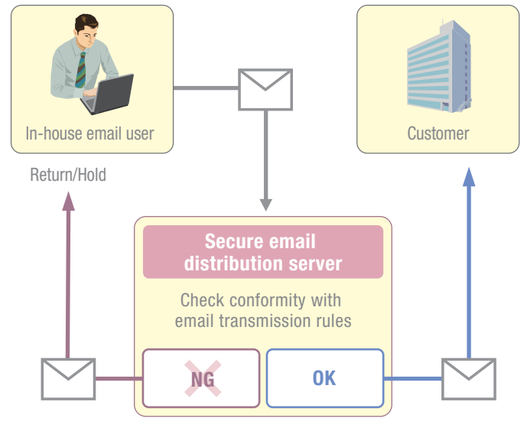
Overview of System to Prevent Information Leaks



2 System to prevent misdelivery of emails

Information leaks can arise from minor mistakes an incorrectly entered email address, or a file attached in error. We have therefore implemented a system to prevent misdelivery of emails. It ensures that the addressee and attachment information for all emails sent from NEC Group companies to external companies are checked prior to sending. 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 addressee and contents. This leads to an even further reduction in errors, as well as the prevention of information leaks due, for example, to the unauthorized forwarding of emails.

Secure Email Distribution System



3 Secure external environment

To reduce the number of information security incidents, the NEC Group has built its own secure external business environment, which a large number of Group members use.

Strengthened security for PCs taken outside the company

Using company PCs outside the office increases threats compared to in-house use.

To strengthen the protection of the information in PCs in case of theft and loss when taken outside the office, we have developed secure PCs equipped with strong encryption of the entire HDD, pre-boot authentication prior to OS launch, and remote data deletion/PC locking functions. These PCs also feature a function to mitigate attacks against unknown vulnerabilities and an auto-run antivirus function, to protect them against increasing cyber attacks.

Thin Clients

The thin client system employs a virtual PC approach for more efficient operational management and for environmental considerations. Security patches are applied in batch to all the virtual PCs by the system administrator, allowing countermeasures to be applied in a short time even in the case of targeted attacks that exploit new vulnerabilities. Users are freed from the hassle of daily security measures and can concentrate on business.

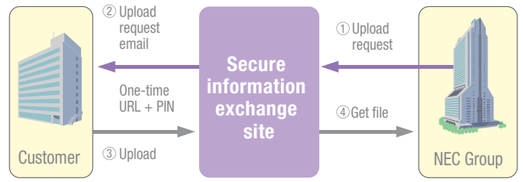
The system uses thin client terminals that realize advanced security features such as unknown vulnerability countermeasures while maintaining the convenience of the Windows operating system. Further, a type that can be started from a CD has also been developed, allowing employee-owned PCs to be converted into secure thin client terminals that can be connected to the company's networks. Intended for use during disasters such as earthquakes or super-flu epidemics, this type played a major role in maintaining social infrastructure operations during the Great East Japan Earthquake of March 2011.

4 Secure information exchange site

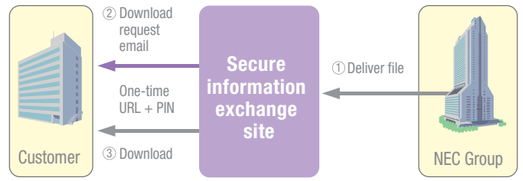
The NEC Group operates a secure information exchange site, which enables us to exchange of important information with customers and suppliers safely and securely. The system uses a one-time URL (an address that can be connected to only once) and password system to allow the secure exchange of files. This eliminates the need to carry USB flash drives and other external storage devices, reducing the risk of information leaks arising from the theft or loss of such devices.

Secure Information Exchange Site

Upload (transmission) diagram



Download (reception) diagram



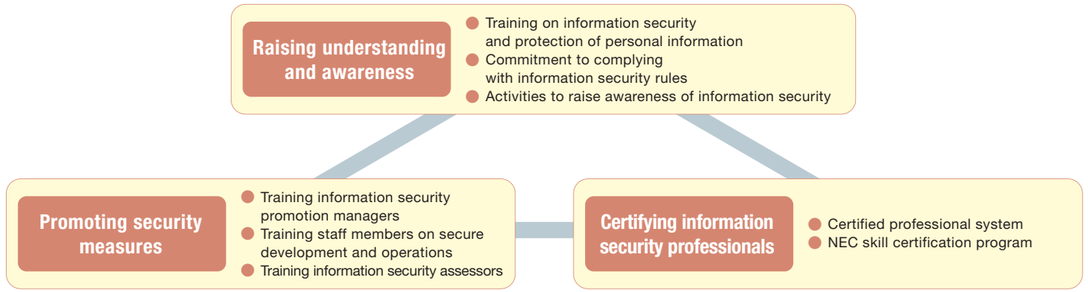
Human Resources for Information Security

The NEC Group carries out ongoing training and development of human resources with expertise and skills relating to information security to meet the expectations of customers, business partners, the market, and general society.

Developing Human Resources for Information Security

The NEC Group's system for developing human resources for information security targets all employees and focuses on the following three areas: 1) raising understanding and awareness; 2) promoting security measures; and 3) certifying information security professionals.

System for developing human resources for information security



Raising Understanding and Awareness

To maintain and improve information security, the NEC Group runs training programs and implements awareness-raising activities to ensure that all employees know how to handle information appropriately and have a thorough understanding of information security.

1 Training on information security and protection of personal information

All employees take a web-based training (WBT) course on information security and the protection of personal information to raise awareness and improve their information handling skills. The content of this training course is reviewed every year and updated to include the latest information on security measures and descriptions of actual security incidents so that the course remains relevant to the current business environment. The WBT system is linked with the NEC Group's HR database to ensure that the list of employees subject to training is kept up to date.

2 Commitment to complying with information security rules

The NEC Group has compiled 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. All NEC Group employees are obliged to read and understand these rules, and pledge to observe them. This is carried out efficiently and effectively by using NEC's Electronic Pledge System.

3 Activities to raise awareness of information security

Raising awareness of information security is an effective way to reduce the possibility of information security incidents caused by the loss or theft of confidential information or the transmission or distribution of information to the wrong person. Awareness-raising activities conducted by the NEC Group include using videos about information loss incidents and potential miss-sending accidents to highlight security risks and make employees consider their own approach and behaviors.

By providing effective methods tailored to each Group company, such as workplace discussions, three-why analysis, and video presentations, the NEC Group helps employees raise their security awareness through active dialog and hone their analysis and judgment skills.

Promoting Security Measures

The NEC Group has created an information security promotion framework in each business unit of NEC and in each business department or administrative office at Group companies. Managers assigned in this framework play an important role in implementing security measures and receive skills training to ensure they can carry out their role properly.

1 Training information security promotion managers

The NEC Group carries out information security management (ISM) leader training to provide information security promotion officers in each organization with the necessary practical knowledge and skills to ensure that information security measures are implemented properly. Instructors with extensive practical experience teach promotion strategies using videos and case studies. The training also provides security promotion managers with a good opportunity to share information on their experiences and any issues they have encountered when implementing security measures in their organization.

2 Training staff members on secure development and operations

To raise the level of security of products and services supplied to customers, the NEC Group has enhanced its framework for promoting secure product development and operations. Responsible security promotion managers and developers receive secure development training to acquire and maintain the knowhow required to carry out secure product development and operations.

3 Training information security assessors

The NEC Group carries out onsite inspections to assess and improve information security at business partners. The assessors who conduct these onsite inspections are trained using standardized methods and curricula. NEC has conducted many training sessions since the system started and has certified more than 300 assessors. Plans are also in progress to expand this framework.

Certifying Information Security Professionals

The NEC Group is developing information security professionals with a high level of expertise to provide customers with added value by supplying reliable products and services and offering information security solutions.

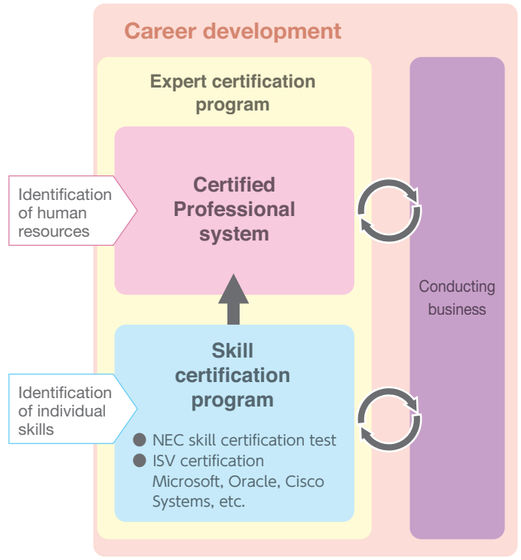
1 NEC Certified Professional system

NEC has built the Certified Professional System to develop experts with the specialist skills required to carry out different types of business in the NEC Group. In this system, an expert with in-depth knowledge of information security is certified as a Technical Specialist (Security). Advanced information skills are also required for employees to be certified as IT service management or network solution specialists. These experts with advanced skills or public qualifications in information security and who have been trained and certified as NEC Certified Professionals (NCPs) play a key role in ensuring the security of NEC Group products and services and help provide customers with optimized information security solutions.

2 NEC skill certification program

The NEC skill certification program consists of computer-based qualification examinations to certify employees' technical expertise and operational skills with products and services from NEC and independent software vendors (ISVs). Several subjects are related to information security. This program provides employees with specific goals in improving their skills, which increases their motivation and ultimately leads to the enhancement of customer trust and the growth of critical businesses.

Certification system for information security professionals



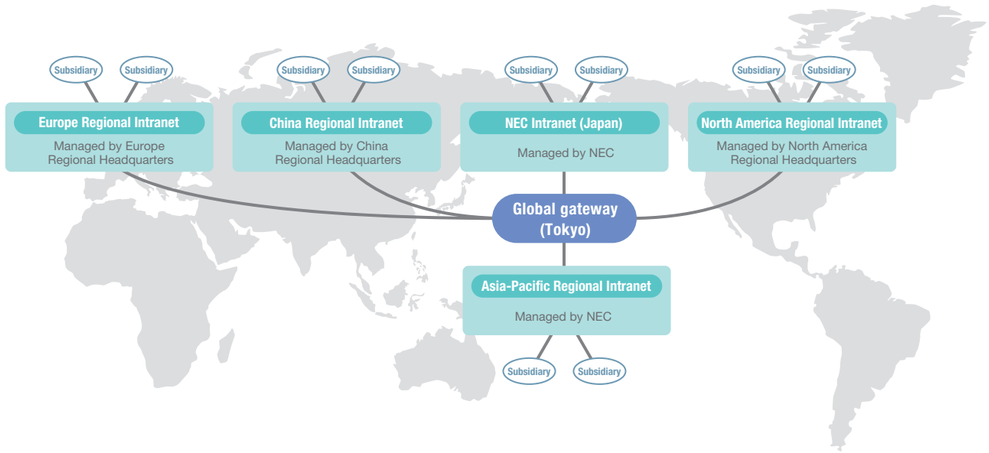
Information Security at Overseas Subsidiaries

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

Global NEC Intranet

The NEC Group uses regional intranets to connect its more than 150 offices worldwide, creating a global NEC Intranet. The regional intranets are managed by the company responsible for general administration in each region, while global operations such as connections between regional networks are centrally administered by NEC.

Global NEC Intranet



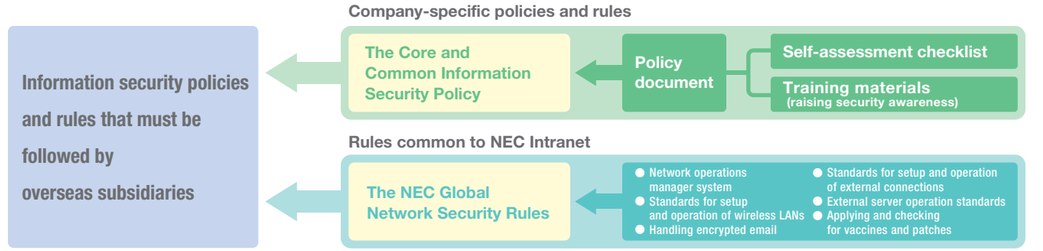
Information Security Policies and Rules

NEC defines common information security policies and rules that must be followed by all overseas subsidiaries in the NEC Group.

NEC has developed the Core and Common Information Security Policy template for Group companies so that they can establish their own policies and rules on information security and so that security measures implemented by Group companies can be shared throughout the entire Group. The NEC Core and Common Information Policy template is based on the ISO/IEC 27001 standard and can easily be applied to the organization of Group companies worldwide. Each company can simply map roles in their organization onto the template, while maintaining compliance with laws and regulations applicable to their region and their own company, and create policies and rules in the same format and using the same details as the template. Additions and modifications made by overseas subsidiaries must be verified and approved by NEC.

In addition, the NEC Group implements The NEC Global Network Security Rules, a set of common rules regulating the use of the global NEC Intranet. The rules cover operations such as establishing a management system, connecting to the Internet, and managing office networks. All overseas subsidiaries must follow these rules when using the Intranet.

Global information security policies and rules



Information Security Management

NEC has created information security training programs for employees of overseas subsidiaries. Subsidiaries carry out regular information security training using these contents.

Overseas subsidiaries also carry out regular information security assessments to ascertain their own information security status. NEC reviews the results of these assessments and makes recommendations for improvements if required.

NEC headquarters in Tokyo also monitors the status of network security at each subsidiary based on the standard security rules of the global NEC Intranet.

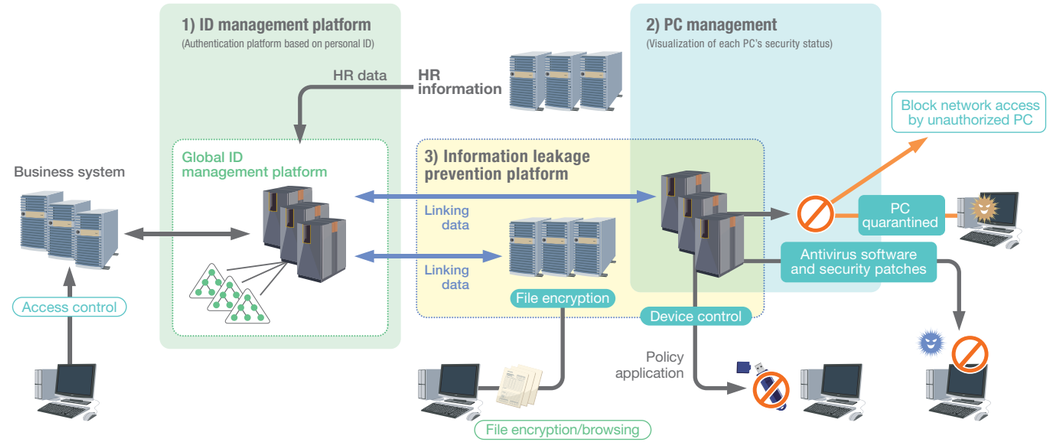
Information Security Platform

A unique ID has been allocated to every employee of each NEC Group company in the world. These IDs are managed centrally by the global ID management platform, making it possible to have NEC office documents encrypted worldwide.

NEC is also in the process of implementing a system to make the security status of all personal computers used by overseas subsidiaries visible and easy to confirm and to provide antivirus software and security patches. NEC can then use this information to roll out security measures to further limit access to removable media such as USB flash drives (device control) or to quarantine unauthorized computers.

* As an information leakage prevention platform, NEC has also established system that automatically encrypts files transferred between Group companies and allows only authorized users to open the files, preventing the leakage of information to unauthorized parties.

Global information security platform



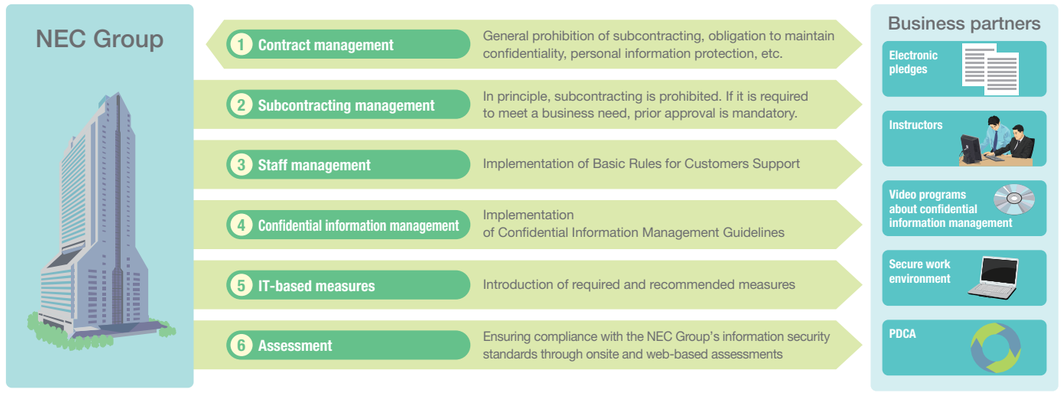
Information Security Measures Coordinated with Business Partners

To protect customer information, the NEC Group works in close coordination with business partners through the rollout of security measures and security assessments, followed by improvement actions, with the aim of raising the level of information security at business partners.

Framework

NEC Group business activities are conducted in partnership with business partners. We recognize that it is extremely important for business partners not only to have technical ability but also to maintain information security. The information security measures that we require of our business partners are classified into the following six major categories: 1) contract management, 2) subcontracting management, 3) staff management, 4) confidential information management, 5) IT-based measures, and 6) assessment.

Information Security Measures for Business Partners



1 Contract management

All contracts between the NEC Group and business partners are comprehensive agreements that include confidentiality obligations (core agreement).

2 Subcontracting management

Subcontracting by business partners to other companies is prohibited under the core agreement. If subcontracting is required, the business partner must obtain written permission from the original contractor in the NEC Group.

3 Staff management

The NEC Group has established "Basic Rules for Customers Support", which indicates the security measures to be followed by people engaging in work outsourced from the NEC Group. Workers are requested to submit an "oath" to the company they are working for as an evidence of their commitment to these security requirements.

4 Confidential information management

Management of confidential information handled under NEC Group contracts is covered by the Confidential Information Management Guidelines, in which NEC requires confidential information to be labeled, the taking of information outside the company to be strict managed, and confidential information to be disposed of or returned after the work is completed. Vendors' commitment to these requirements is a precondition for ordering.

5 IT-based measures

To ensure our business partners implement critical technical measures without fail, we have two levels of requests: "Required" (e.g., the entire encryption of a mobile device) and "Recommended" (e.g., using the Information Prevention System and the Secure Information Sharing Platform).

6 Assessment

Based on Information Security Standards for Suppliers (issued in fiscal 2009), which defines the required levels of information security for the NEC Group's business partners, we carry out an annual assessment program using an organizational and procedural framework common throughout the Group in order to check the security status of each business partner and provide improvement guidance if necessary.

Promotion of Measures for Business Partners

1 NEC Information Security Initiatives Seminars

NEC Information Security Initiatives Seminars are held (at eight bases throughout Japan) once a year for business partners nationwide (approximately 2,300 companies, including approximately 700 ISMS certified companies), to ensure that business partners understand and implement the NEC Group's security measures.

2 Training sessions to develop instructors

Suppliers are requested to appoint in-house instructors to teach the aforementioned Basic Rules for Customers Support. Training sessions to certify instructors or renew their certification (certification is effective for one year) are held every year. In fiscal 2012, a total of approximately 1,700 people attended the sessions.

3 Distribution of videos about confidential information management

Based on the results of analyses of security incidents, we show educational videos at NEC Information Security Initiatives Seminars, and we distribute these videos to business partners and encourage their use for in-house education. Thus far, the themes of these videos have included compliance matters, the management of confidential information, information leaks through Winny, virus infections, and the loss of information caused by drinking.

From fiscal 2013, we will offer our business partners existing video content through a streaming service.

4 Distribution of guides to implementing information security measures

To enable business partners to more smoothly implement the information security measures of the NEC Group, we offer guides to implementing these measures. Thus far, we have issued various kinds of guides including those for the execution of antivirus measures and for secure development and operation of Web systems, to ensure the required level is achieved. In addition to these, a guide on security of smart devices is planned to be released.

Assessments and Improvement Actions for Business Partners

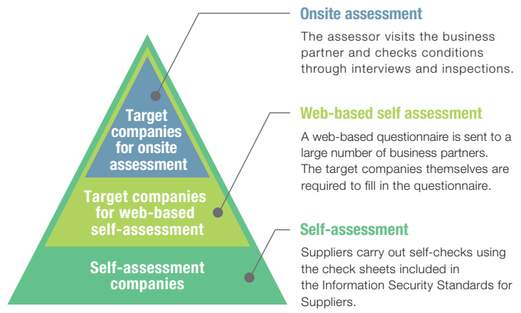
Assessments of the security of our business partners consist mainly of onsite assessments and web-based self-assessments.

Onsite assessments are carried out every year at about 100 companies that have frequent dealings with the NEC Group. As the assessors designated by the NEC Group (there is a total of approximately 300 assessors) visit the business partners and carry out assessments on site, they are able to uncover issues that were not found in the business partner's own web-based assessments.

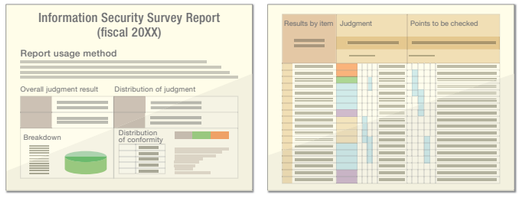
Web-based self-assessments are carried out annually by approximately 2,300 companies that deal with the NEC Group. These business partners carry out self-assessments of how they are currently implementing measures according to a list of assessment items that change every year according to the status of information security incidents and other factors, and enter the assessment results into a Web-based system. These assessment results are compiled into reports by the NEC Group and provided as individual feedback to each company. Along with being able to compare their company's security implementation level with the other business partners of the NEC Group, these assessments enable each business partner to grasp the issues it is facing and effectively carry out improvements.

All the assessments are followed up based on improvement plans for business partners who need improvement, thereby ensuring the achievement of higher levels of security.

Categories of Assessment for Target Companies



Onsite Assessment Report



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.

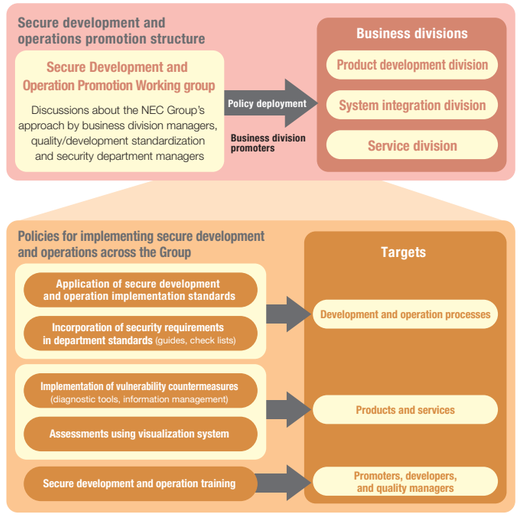
Initiative to Ensure Secure Development

Establishment of a framework for secure development and operations

Cyber attacks targeting specific companies and organizations have been increasing, and the protection of information assets such as personal information and trade secrets has become a major concern.

To supply safe and secure products and services to customers, the NEC Group has established the Secure Development and Operations Promotion Working group to discuss and determine the Group's approach, and implements specific measures in business divisions through the approximately 300 secure development and operations managers appointed throughout the NEC Group.

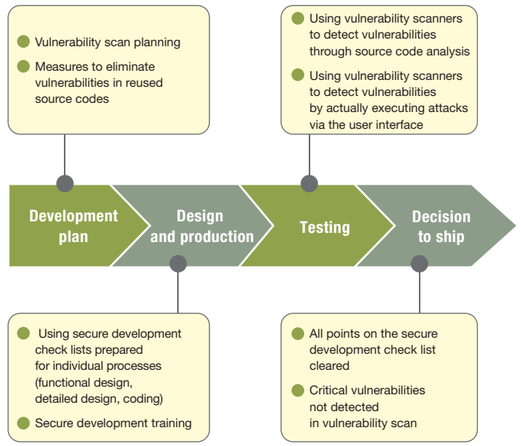
Secure Development and Operation Promotion Structure and Policies



Incorporating security requirements in development and operation processes

We have established a Secure Development and Operation Implementation Standard that sets concrete baselines for security measures required for development and operations, and ensure that business divisions and Group companies adhere to this standard. Further, we have defined development processes that incorporate the concepts of the ISO/IEC 15408 international standards on IT security evalution, and indicate the security requirements in the quality and safety guidelines common to the entire NEC Group and the development standards of the major business units.

Secure development measures incorporated into standard processes (example of Platform Business Unit)



Making Products and Services Secure

The NEC Group has developed various guides and check lists for development divisions to enable them to implement secure design, coding, and server hardening of NEC Group products and services. We are also actively working to eliminate vulnerabilities by collecting the latest vulnerability information and making diagnoses using vulnerability scanners.

Further, to grasp the implementation status of security measures, the NEC Group has built and runs a visualization system. This system is used to manage approximately 1,700 projects, enabling us to monitor current statuses and respond quickly to improve any problematic situations that might arise in a monitored project.

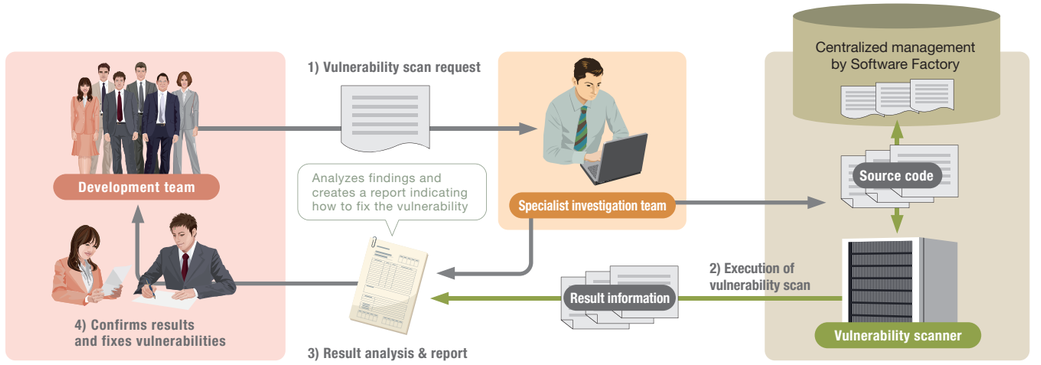
Human Resource Development

The NEC Group is strengthening human resource development for secure development and operation by conducting training for secure design, server hardening, and secure coding for secure development/operations promoters, product/service developers, and product quality managers. (A total of 1,570 staff members received such training in fiscal 2012.)

Centralized management and vulnerability diagnosis by Software Factory

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

Centralized Management and Vulnerability Diagnosis by Software Factory



Addressing Vulnerabilities Urgently in Daily Operations

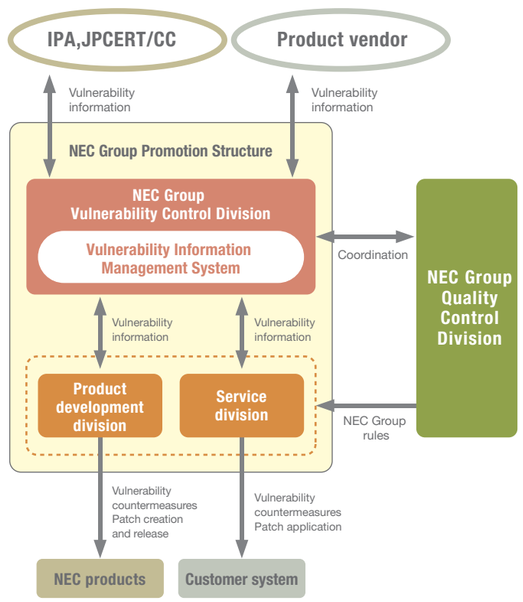
By taking security into consideration while carrying out development, we can eliminate many vulnerabilities that create security risks. However, as new vulnerabilities are discovered every day in currently used operating systems and software products, these vulnerabilities must be fixed quickly and thoroughly.

To this end, the NEC Group operates its own vulnerability information management system that has approximately 600 staff members to facilitate the sharing of vulnerability information throughout the entire Group. Further, the implementation of anti-vulnerability measures is required according to the quality protection rules of the entire Group, which ensures that the system is used conscientiously.

With regard to the NEC Group's products, we have constructed a management system for the rapid release of vulnerability information and patches. 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 announced publicly.

Moreover, 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 a 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 Measure Promotion System



Security Solutions Trusted by Customers

To resolve the information security issues of customers, NEC offers SecureSociety, an integrated security management solution that provides customers with core NEC expertise gained through the development and operation of our internal systems.

NEC's Security Solution

In conducting business, companies are exposed to various information security threats every day, and how to assure business continuity in a safe and stable environment has become a critical issue. To resolve this, NEC offers SecureSociety as a total solution to satisfy the specific security requirements of the customer.

1 Concept of SecureSociety

SecureSociety provides a visual representation of the security environment by using a "quantification management" function that enables managers to grasp threats and vulnerabilities in IT systems and networks in quantitative terms. Quantification management also clarifies security risks and the priority level of countermeasures, creating a platform for integrated security management through the coordination of different security products and services.

2 Benefits of SecureSociety

SecureSociety provides a variety of benefits to help customers succeed, including 1) solutions based on expertise obtained through the operation of our internal systems; 2) total services ranging from planning to implementation; 3) cost reductions through overall optimization; and 4) continuous improvement of security measures.

NEC has established an internal security platform used by tens of thousands of employees. We are now helping customers by planning safe and secure solutions that satisfy their needs based on the solutions used and verified in our own environment. This is one-stop solution ranging from establishment of security policies and definition of information security platform requirements to platform development and construction. By eliminating redundant security measures and management inefficiencies, we clearly define what should be implemented, how, and with what resources, to realize a company-wide security environment that promotes total cost optimization. And by using quantification management, we can maintain a clear view of the existing challenges and points to be improved, thus continuously implementing higher levels of security (using PDCA cycles) and responding to constantly emerging new threats.

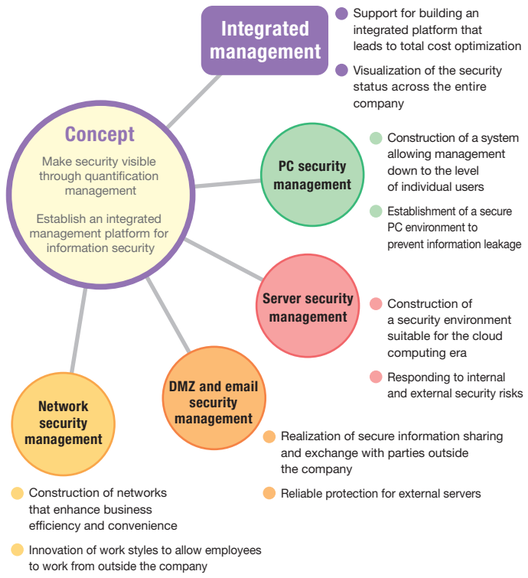
3 Categories of solutions

SecureSociety solutions consist of the following major categories: integrated management, server security management, DMZ and email security management, and network security management. A variety of products, services, and related solutions are available in each of these categories, of which we especially focus on the prevention of information leaks and protection against cyber attacks.

4 The seven management points of information security

To prevent information leaks and cyber attacks, it is important to implement reliable measures for the "seven doors" through which information passes. The "seven doors" concept has been developed by NEC based on the know-how it has acquired through the actual implementation of information security measures. Specifically, it refers to the management of 1) PCs and USB memories, 2) internal servers, 3) fax machines and printers, 4) network equipment, 5) wireless LAN access points, 6) external servers, and 7) remote access points. The concept widely covers the IT domain, network domain, and physical domain, enabling us to propose solutions that successfully and comprehensively strengthen the customer's management system.

SecureSociety Concept and Solution Categories



Case Study of Quantification Management and Integrated Management

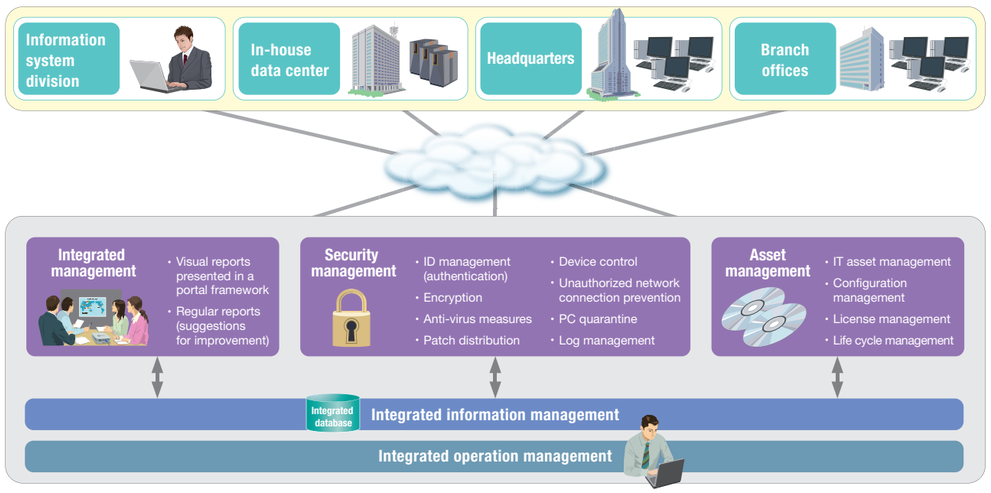
With the increasing popularity of cloud computing, the need for the PCs we use every day to be offered as a service rather than as an asset is rising.

Against this backdrop, NEC has built and deployed the "PC Integrated Management Service," which maximizes the use of SecureSociety solutions.

The simultaneous offering of standard PCs and PC integrated management in this service realizes a total service for the entire PC environment. Users can run PCs flexibly any time and at a reasonable cost even if the number of PC users increases or decreases drastically, or if some of the PCs are malfunctioning. Furthermore, this service provides a framework to integrate information via a special portal for PC asset management (configuration management, license management and lifecycle management) and for security management.

This service also provides various security features such as encryption, anti-virus measures, device control, unauthorized network connection prevention, PC quarantine, ID management, and log management, at the equivalent of information security level 4 (FISC/COBIT global standards).

Integrated PC Management Service



"Seven Doors" and Solution Categories

			"Seven doors" through which information passes						
			PC/USB memories	Internal servers	Fax machines and printers	Network equipment	Wireless LAN access points	External servers	Remote access points
Integrated management	"SecureSociety/PS" Information security construction planning	Support of security planning extending to operation and deployment	●	●	●	●	●	●	●
	"SecureSociety/DS" Integrated ID management system construction	Realization of speedy and low-cost integrated ID management	●	●	●		●		●
	"SecureSociety/LM" Integrated log management system construction	Construction of a system for centrally managing various logs	●	●	●	●		●	
	"SecureSociety/IR" Security dashboard construction	Central management of security failures in real time	●	●	●	●	●	●	●
PC security management	"SecureSociety/SP" Secure PC management system construction	Total management of network connections with all kinds of PCs	●						
	"SecureSociety/IC" Employee ID IC card issuance and operation management system construction	Total support of IC card operation improving security and usability	●		●		●		●
Server security management	"SecureSociety/CU" Datacenter security management system construction	Centralized management of data center security measures	●	●		●		●	●
	"SecureSociety/IM" Privileged ID management	Strengthening internal controls by thorough management of IDs and access	●	●					●
DMZ and email security management	"SecureSociety/WA" Web application security	Protection of web and other external servers from various threats						●	
	"SecureSociety/SS" Secure exchange site construction (secure information distribution)	Protection of PC and server files and prevention of information leaks						●	
	"SecureSociety/ML" Email security	Reduction of information leak risks by checking and saving emails						●	
Network security management	Wireless LAN authentication	Realization of secure network connection preventing unauthorized access					●		
	Remote access	Realization of in-house security level in external environment							●
	Entrance and exit management	Realization of improved security and more efficient operation	●	●	●	●	●	●	

Information Security Case 1

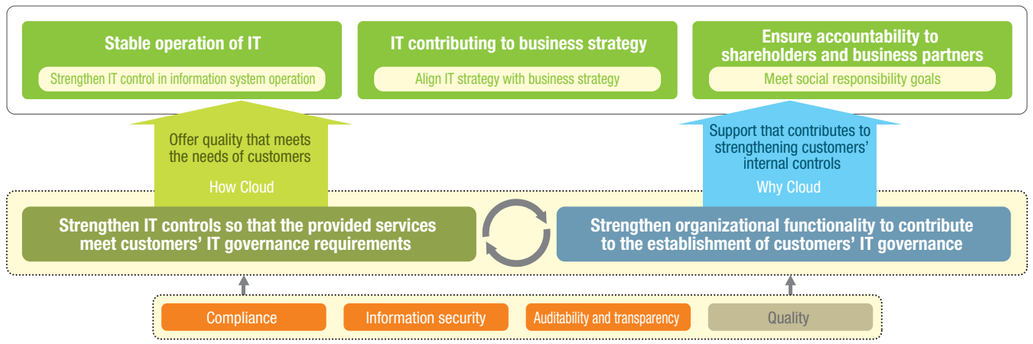
Cloud Security Activities

Cloud computing has begun to deliver new value, but along with this, the information security of cloud services is becoming a major issue. Here, we introduce our efforts to deliver customers information safety and reliability through our cloud services.

NEC's Cloud Service Concept

NEC's cloud services offer IT support to help customers improve management quality and strengthen internal control by making the operation of their IT systems more stable, thereby contributing to strategic management and increasing accountability to shareholders and to their own customers. To realize this, NEC has been focusing on quality, information security, compliance, auditability and transparency to raise the level of management through continuous improvement.

NEC's Cloud Service Concept



Features of Cloud Security

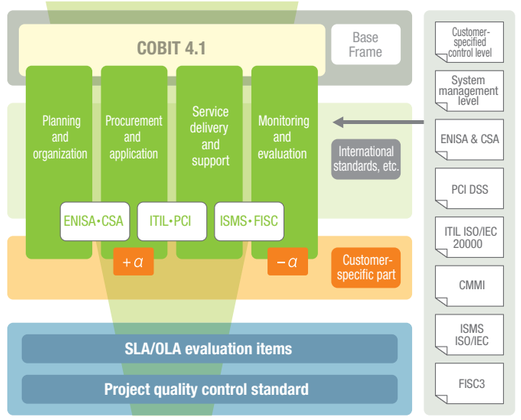
NEC has been driving activities that focus on 1) compliance, 2) information security functions, and 3) auditability and transparency as the elements required to establish and maintain cloud security.

1 Compliance (cloud security framework)

In order to offer transparency of service levels for cloud security and provide a means of communication to meet diverse customer requirements for compliance and security, NEC has built a cloud security framework that complies with applicable cloud security-related standards. This framework incorporates the cloud-related security guidelines of the Ministry of Economy, Trade and Industry, the security requirements of ENISA*1, the guidance of CSA*2, and the safety standards of FISC*3, thereby reducing the information security risks of cloud computing in coordination with NEC's management cycle.

*1 ENISA: European Network and Information Security Agency
*2 CSA: The Cloud Security Alliance
*3 FISC: The Center for Financial Industry Information Systems

NEC's Cloud Security Framework



2 Information security

NEC's cloud services focus on six core security features for realizing cloud security: 1) organization level control that enables continuous improvement and implementation of measures against new risks, 2) segregation of duties and an inter-process check mechanism to prevent illegal activities and errors, 3) protection of customers' information assets in a multitenant environment, 4) autonomous defense against emerging threats, 5) secure and authorized access to and operations of critical assets by administrators and operators, and 6) secure interconnection with the Internet or external networks and robust infrastructure and network topology.

3 Auditability and transparency

To ensure customer compliance and make the IT performance visible, NEC uses international external assurance reports (SOCR) for cloud services. Moreover, NEC guarantees the safety and security of its cloud platform by using audit reports that follow the Japanese-version SOX regulations. Customers can use these external assurance reports, for example, to ensure their company's compliance with SOX.

Implementation of Cloud Platform Services

RIACUBE is NEC's cloud platform service that implements the above-described concept and features. The RIACUBE Series currently consists of RIACUBE, which provides a physical server environment, and RIACUBE-V, which provides a virtualized server environment. The RIACUBE Series meets various cloud security requirements worldwide.

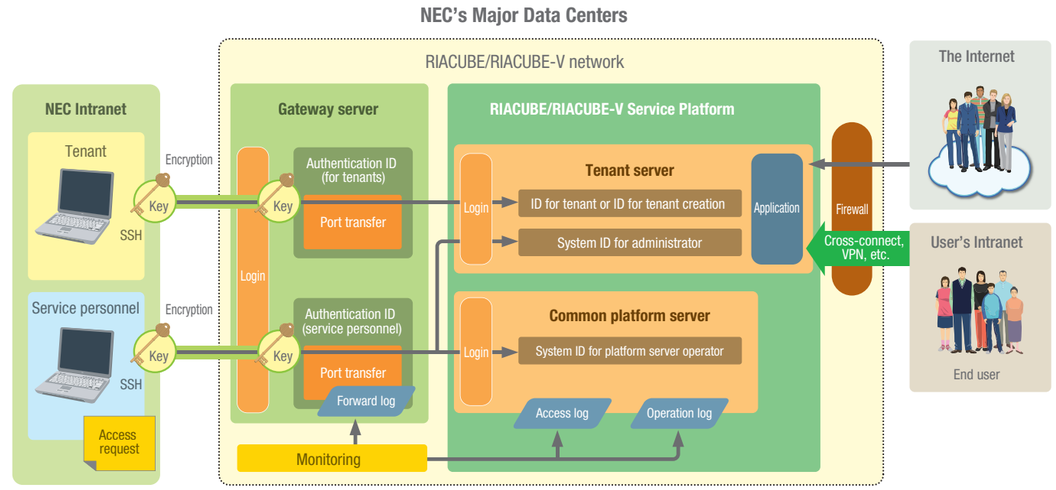
For example, in the area of access management, unauthorized accesses from both the inside and the outside can be detected by collecting the connection logs of internal management servers in real time and automatically comparing them with the submitted access requests details in coordination with the change management work flow. Similarly in a virtual environment in which a customer's information assets are stored, the system guarantees the legitimacy of accesses and operations of administrators and operators by recording and monitoring operation commands. Moreover, access to servers, storage devices and networks is permitted via a secure remote network environment in which a variety of encryption technologies are incorporated, and IDs used for such access are efficiently managed by an ID management system that automates ID creation, allocation, inventory, and password management.

The NEC Kawasaki Data Center, one of the major data centers that use the RIACUBE Series, clarifies the implementation status and proves the validity of its equipment management and physical security control through internal control assurance reports (SSAE16*4, ISAE3402*5). The RIACUBE and RIACUBE-V systems in this data center have been validated by an internal control assurance report pursuant to Auditing Standards Board Report No. 18 supporting Japanese-version SOX regulations.

NEC's cloud platform service thus supports the customer's business and IT strategies through enhanced IT controls in operations (stable information systems) and the fulfillment of social responsibility (accountability to shareholders and business partners).

*4 SSAE16: Statement on Standards for Attestation Engagements No.16
*5 ISAE3402: International Standard on Assurance Engagements No.3402

Operation Management Configuration for RIACUBE Series



Information Security Case 2

Research and Development of Security Technologies to Support Cloud Computing Environment

To achieve stronger security and lower operating costs for a cloud computing environment in which numerous servers and network devices are supposed to run harmoniously, we are working on R&D and commercialization of security technologies using the OpenFlow protocol.

Development of Integrated Access Control Technology

In a cloud computing environment where a large number of servers and network devices operate in an integrated fashion, it is critical to allocate access privileges to general users and system administrators correctly and efficiently. NEC has developed the world's first integrated access control technology, which automatically generates detailed information to set access privileges for each server and network device by just entering a simple access privilege policy on a Web screen, and then issues access privileges to all the target users at once. In addition to reducing the burden on system administrators, this technology prevents security vulnerabilities caused by improper settings and realizes the robust and secure network environment required by businesses for cloud operations in a short period of time and at a low cost.

Furthermore, privileges to access virtual servers and networks in the cloud computing environment can be managed centrally by using this technology in OpenFlow networks.

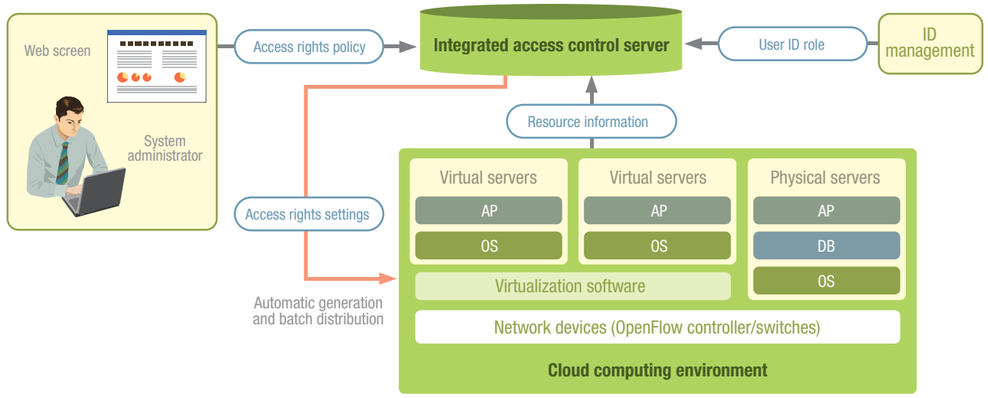
Network Access Control with OpenFlow

OpenFlow is a collective term for technologies and interface specifications proposed by the OpenFlow Consortium, which was established in 2008 and is hosted at Stanford University. OpenFlow is a new technology that allows a centralized controller to control every OpenFlow switch.

NEC has been actively engaged in promoting the broad adoption of OpenFlow, and in March 2011, we launched the world's first OpenFlow switches on the market. These switches have begun to be used in data center business as well as in private networks of companies worldwide.

In systems adopting OpenFlow, an OpenFlow controller centrally manages a large number of OpenFlow switches based on access control information, realizing flexible network access control according to user IDs and roles (organization, duty, etc.). By using this system, network access control settings that usually take about a week can be completed in just a few minutes, thus dramatically reducing the cost of security operations and management while enhancing network security.

Integrated Access Control Technology that Supports OpenFlow



Standardization Activities

To enable the widespread use of these new technologies, their interoperability with various software and network devices provided by third-party vendors is extremely important. NEC participates in international standardization bodies such as the Distributed Management Task Force (DMTF) and Open Network Foundation (ONF), and actively engages in standardization activities for integrated access control technology and OpenFlow technology.

(a) Distributed Management Task Force (DMTF)

DMTF is an international organization for the standardization of systems management in a multi-vendor environment, and includes major virtualization software, OS, and database vendors as members. NEC proposed a specification for software to automatically set access control (an adapter) to the DMTF, which was officially adopted in September 2011 (DSP-1106, "Integrated Access Control Policy Management").

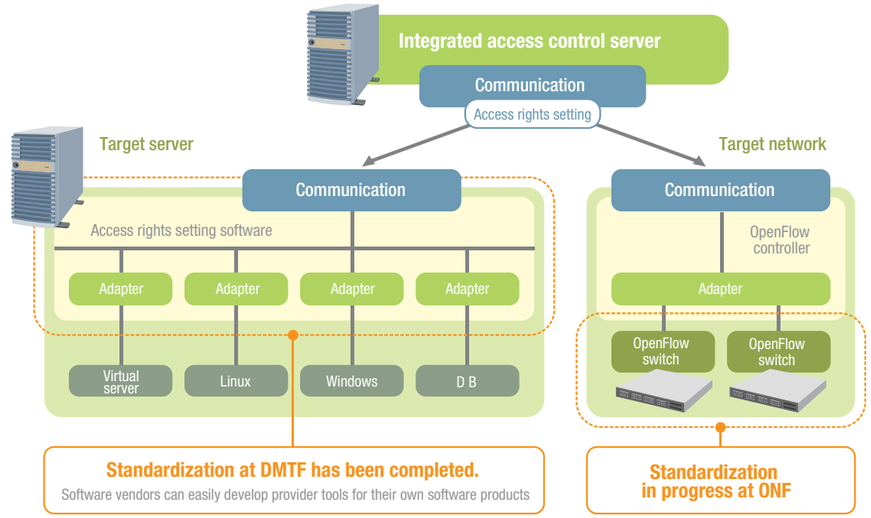
(b) Open Network Foundation (ONF)

The ONF is an international organization for the standardization of OpenFlow specifications. Its participants are major Internet service providers and network device vendors.

As one of the OpenFlow Consortium founding members, NEC participates in the formulation of control protocols for network switches, and is currently developing a proposal for configuring future network access control.

We will continue working for the improvement and global standardization of this technology, and carry out further research and development to create commercial products that contribute the success of our cloud computing platform and cloud service businesses.

Integrated Access Control Technology/OpenFlow Technology Standardization Activities



Information Security Case 3

Information Security Initiatives by NEC Soft

As a company that plays a central role in the IT service business of the NEC Group, NEC Soft, Ltd., provides value and reliability that satisfies customers. NEC Soft places high priority on information security and takes a proactive approach to it.

Information Security Policy of NEC Soft

As a core company for IT services in the NEC Group, NEC Soft works on innovating systems integration, providing highly reliable IT services, systems, and solutions to customers.

In order to offer customers outstanding systems and services with high reliability, the company focuses not only on development technology but also on security to meet the specific needs of each customer's business and establish a secure development process. To this end, based on the information security policies of the NEC Group, NEC Soft carries out organizational control of ISMS and personal information management under the Group-wide information security management system. The company also strictly manages individual projects for developing and constructing IT services and systems to keep the information secure.

Information Security Measures of NEC Soft

The main measures supporting information security are: 1) security management in projects, 2) secure development and vulnerability management, and 3) information security education and personnel training.

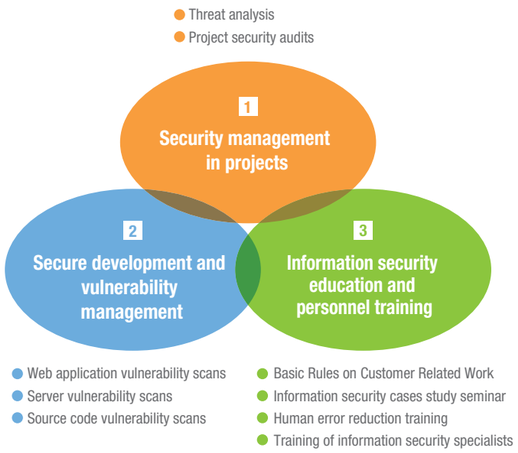
1 Security management in projects

All projects in the company are managed based on processes stipulated in corporate rules and guides, but in addition to that, risk management tailored to the project and a scheme to check the status of the defined management processes are also required. NEC Soft has constructed systems for threat analysis and project security audits to ensure security quality in individual projects.

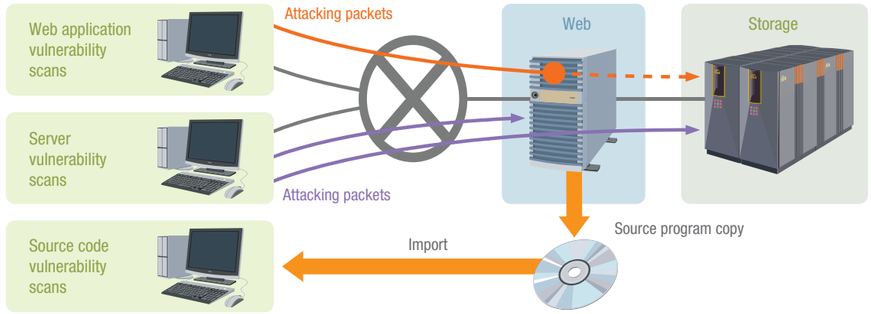
In threat analysis, the company clarifies the needs of the customer, identifies potential threats based on an outline of the service or system at the proposal phase and determines appropriate countermeasures. In conducting the analysis, NEC Soft uses a worksheet with about 30 checkpoints that are considered to be most critical, which enables the company to grasp in the early stage of designing what security functions are needed for the customer and implement effective security measures.

Project security audits are conducted to monitor the security implementation status in projects. Through the combined use of document-based audits and onsite audits, the burden of the audited party is reduced and improvement measures can be implemented accurately and quickly. These activities began in 2006 and over 100 audits are conducted every year. As the number of projects on which audits have been carried out is increasing, not only improvements required for a specific business but also common challenges and best practices for the entire company have been identified through monitoring.

Information Security Measures of NEC Soft



Product, System and Service Vulnerability Scans



2 Secure development and vulnerability management

Recently, there is an increasing number of information security incidents in which services and systems made open to the public are attacked, resulting in significant damage and even liability issues. As more critical information is posted online and attacks are becoming more sophisticated, information security incidents impact a wider range of business activities.

To enable customers to use NEC Group services and systems safely and securely, NEC Soft has been building an organizational scheme and providing employee guidelines (for configuration, programming, etc.) to ensure secure development within the company.

Especially, the company conducts vulnerability scans of developed systems and products in three main areas: vulnerability scans of web applications, which started in 2007, and scans of server and source code vulnerabilities, which are currently executed as well. Hardware and software is prepared in addition to personnel assigned for the scans. In fiscal 2012, the number of systems and products shipped after receiving vulnerability scans exceeded 130. The scans eliminate vulnerabilities that are difficult to detect in a manual (human) check or assessment, while correcting the incorrect knowledge of developers and helping them rapidly acquire the knowledge and experience they need. The vast knowledge and experience gained in this process lead to more efficient development and a system or product with higher quality. This knowledge and experience is also accumulated as expertise and shared within the Group through education and training.

3 Information security education and personnel training

To maximize the effectiveness of each security information measure, NEC Soft conducts education and training based on an annual plan. To prevent information security incidents from happening, NEC Soft shows its employees the Basic Rules on Customer Related Work that has been provided to companies throughout the entire NEC Group and ensures they implement the rules as their fundamental code of behavior. Taking an education course on the rules is a requirement for employees to take a part in a project. The company offers the course six or more times every month throughout the year, so that employees can take the course any time.

In addition, every business unit holds an information security cases study seminar (face-to-face learning) at the beginning of each term, where participants share cases of information security incidents and are urged to remind each everyone in their division to be careful in terms of security, thus gaining a better understanding and awareness of their own situation and responsibilities for information security.

Furthermore, considering the fact that information security incidents are for the most part caused by human error, training to reduce human error has been implemented since fiscal 2011. In this training, the participant is required to select errors he/she tends to commit from among 14 different error categories, and learn how to reduce these errors. Over 2,600 employees have taken this training so far and its effectiveness has been demonstrated.

Employees, including those engaged in project security audits and vulnerability scans, are encouraged to obtain a qualification for information security, and are trained to be specialists so that they can effectively use their knowledge and experience, which has been validated by certification from organizations such as IPA*1, JASA*2 and SAAJ*3, which raises the security level of the entire NEC Group.

*1 IPA: Information-technology Promotion Agency
*2 JASA: Japan Information Security Audit Association
*3 SAAJ: Systems Auditors Association of Japan

Information Security Case 4

Activities of NEC (China) Co., Ltd.

NEC (China) Co., Ltd., has established an information security policy based on NEC's global standards, created an information security management system (ISMS), and implements information security measures in an integrated and comprehensive manner.

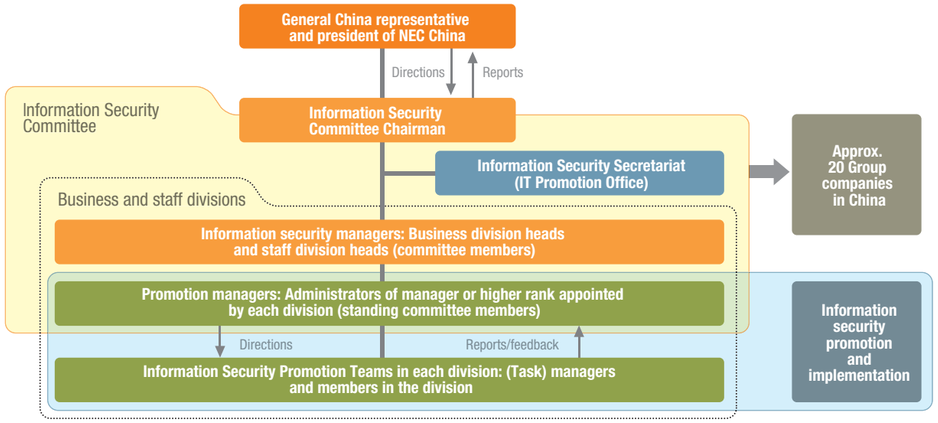
Structure for Information Security Management

In the China region, enforcing information security in the systems integration business and offshore development is becoming more and more critical, and measures to ensure systematic implementation are required.

Considering this need, NEC (China) Co., Ltd. (hereafter, "NEC China") has set up an Information Security Committee composed of an Information Security Chairman appointed by the president of NEC China, an Information Security Secretariat (IT Promotion Office), and committee members and standing committee members from business and staff divisions. This committee, which holds regular sessions, makes decisions on measures to ensure employees follow information security policies and rules, how policies and rules should be deployed, and on technology-related measures, while implementing activities to eliminate information security incidents.

As the regional HQ in the China region, NEC China also promotes information security measures for 20 NEC Group companies in China, and monitors their implementation.

Structure for Information Security Management in NEC China



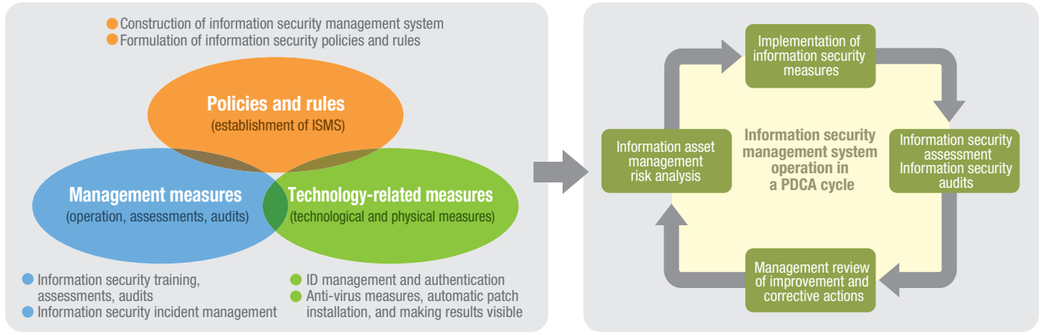
Information Security Management System (ISMS)

NEC China performs information security management by combining three elements: policies and rules, management measures, and technology-related measures. In these activities, the company makes efforts to ensure that information security policies and rules are adhered to while revising them when necessary, and provides regular security training to all employees as well as special education to new members (for both new employees at entry level and in mid-career).

For technology-related measures, the company has adopted the ID management platform, document encryption, and PC management, which are functions of the NEC Global Standard Security Platform.

NEC China also carries out information security assessments on a regular basis, monitors the implementation status of various security measures and takes improvement and corrective actions as needed, implementing security measures by applying the PDCA cycle.

ISMS Operation in NEC China



Third-Party Evaluation and Certification (ISO/IEC 27001:2005)

In July 2007, NEC Advanced Software Technology (Beijing) Co., Ltd., became the first company in China to obtain the ISO/IEC 27001:2005 certification. It was followed by NEC China, which obtained the same certification in July 2011.

Various obstacles lay in the way of obtaining these certifications as the company had to verify the implementation status of the security measures and harmonize risk analysis activities among organizations scattered across China. To overcome these obstacles, NEC China used video-conferencing, e-learning, and other technologies to share information in a timely manner. Furthermore, by grading risks at three levels, the company set criteria for risk acceptance and specified acceptable levels for risks, which enabled the company to carry out risk analyses. Even after obtaining certification, NEC China continues to execute a series of reinforcement activities including risk analysis, information security education, internal audits, and management reviews to adhere to these standards.

*1: NEC Advanced Software Technology (Beijing) Co., Ltd.: Engaged mainly in development and sales of server- and storage-related platform software products

Information Security Measures at Business Partners

Deployment and implementation of policies

A large number of business partners in China are software developers and systems integrators for outsourcing. NEC China promotes the deployment and implementation of information security measures among these business partners in China at a level equivalent to that in Japan, in cooperation with NEC and its Japanese subsidiaries as well as the four major group companies in China: NEC Advanced Software Technology (Beijing) Co., Ltd., NEC Solutions (China) Co., Ltd., NEC Soft (Jinan) Co., Ltd., and NEC System Technologies (Hangzhou), Ltd.

These activities target a total of approximately 150 companies, consisting of offshore companies that directly take orders from NEC and its Japanese subsidiaries, and business partners of NEC China and the four major local group companies. The activities aim to introduce at the target business partners 1) contract management, 2) subcontracting management, 3) staff management, 4) information management, and 5) IT-based measures similar to Japan.

Regarding 2) subcontracting management in particular, only primary subcontracting is permitted in the case of offshore contracts between a developer in China and a Japanese company. In this case, the business partner who outsourced their ordered work is required to submit information about the subcontractor once a year and obtain approval from the client. If the contract is between a developer in China and one of the major subsidiaries in China, subcontracting is totally prohibited.

Education Support and Dissemination to Suppliers

Since fiscal 2011, NEC China has been holding seminars on information security initiatives for business partners at major locations in China.

In these seminars, NEC China defines information security incidents for the business partners and reminds them that it is mandatory to report such incidents when they occur, as well as presents information security measures. The company also holds training workshops for instructors in charge of information security education at business partners and disseminates education tools and NEC's original videos created to raise information security awareness to support information security education at business partners and to build awareness among the workers there.

NEC Information Security Initiatives Seminars

Assessments and Improvement Actions for Business Partners

NEC China began assessing the implementation status of security measures at business partners in fiscal 2012. There are about 50 assessment items mainly related to information management and compliance matters, and partners are requested to conduct self-checks for contracted work and projects. NEC China also conducts onsite visits at major business partners, checking conditions and providing guidance as needed. Also, when selecting a new partner, NEC China visits the candidates for preliminary verification of the information security management status.

Third-Party Evaluation and Certification

The NEC Group proactively promotes third-party evaluation and certification 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	Chugoku Sunnet Corporation
NEC AccessTechnica, Ltd.	NEC Software Chubu, Ltd.
ABeam Consulting Ltd.	NEC Communication Systems, Ltd.
ABeam Systems Ltd.	NEC Design & Promotion, Ltd.
NEC Infrontia Corporation	NEC TOSHIBA Space Systems, Ltd.
N&J Financial Solutions Inc.	NEC TOKIN Corporation
NEC Engineering, Ltd.	NEC Nagano, Ltd.
Auraline Corporation	Nippon Avionics Co., Ltd.
NEC CASIO Mobile Communications, Ltd.	NEC Nexsolutions, Ltd.
NEC Capital Solutions Limited	NEC Networks & System Integration Corporation
NEC Software Kyushu, Ltd.	NETCOMSEC Co., Ltd.
KIS Co., Ltd.	NEC Network and Sensor Systems, Ltd.
NEC Aerospace Systems, Ltd.	NEC Network Products, Ltd.
NEC Computertechno, Ltd.	NEC Purchasing Service, Ltd.
NEC Saitama, Ltd.	NEC Business Processing, Ltd.
NEC Shizuokabusiness, Ltd.	NEC BIGLOBE, Ltd.
NEC System Technologies, Ltd.	NEC Fielding, Ltd.
NEC Informatec Systems, Ltd.	Forward Integration System Service Co., Ltd.
Showa Optronics Co., Ltd.	NEC Software Hokuriku, Ltd.
NEC Soft, Ltd.	NEC Software Hokkaido, Ltd.
NEC Software Tohoku, Ltd.	NEC Logistics, Ltd.
NEC Soft Okinawa, Ltd.	

Privacy Mark Certification

The following companies have been licensed by Japan Institute for Promotion of Digital Economy and Community (JIPDEC) to use the Privacy Mark.

NEC Group Companies with Privacy Mark	
NEC Corporation	NEC Nexsolutions, Ltd.
NEC AccessTechnica, Ltd.	NEC Networks & System Integration Corporation
ABeam Consulting Ltd.	Toyo Networks & System Integration Co., Ltd.
NEC Infrontia Corporation	NEC Net Innovation, Ltd.
N&J Financial Solutions Inc.	NEC Personal Computers, Ltd.
NEC Engineering, Ltd.	VALWAY121Net, Ltd.
NEC Software Kyushu, Ltd.	NEC Business Processing, Ltd.
KIS Co., Ltd.	NEC BIGLOBE, Ltd.
NEC Control Systems, Ltd.	NEC Facilities, Ltd.
NEC Computertechno, Ltd.	NEC Fielding, Ltd.
CyberWing Corporation	NEC Fielding System Technology Ltd.
G-PLAN INC.	Forward Integration System Service Co., Ltd.
NEC Shizuokabusiness, Ltd.	NEC Professional Support, Ltd.
NEC System Technologies, Ltd.	NEC Software Hokuriku, Ltd.
NEC Informatec Systems, Ltd.	NEC Software Hokkaido, Ltd.
NEC Soft, Ltd.	NEC Magnus Communications, Ltd.
NEC Soft Okinawa, Ltd.	NEC Mobiling, Ltd.
NEC Software Tohoku, Ltd.	NEC Livex, Ltd.
Chugoku Sunnet Corporation	NEC Learning, Ltd.
NEC Software Chubu, Ltd.	LIVANCE-NET Ltd.
NEC Display Solutions, Ltd.	NEC Logistics, Ltd.
NEC Design & Promotion, Ltd.	Yokohama Electronic Computing & Solutions Co., Ltd.

IT Security Evaluation and Certification

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

Basic Data

Corporate Facts

Company Name:
NEC Corporation

Address:
7-1, Shiba 5-chome, Minato-ku, Tokyo, Japan

Established:
July 17, 1899

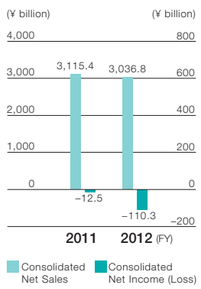
Capital:
¥397.2 billion*

Number of Employees (consolidated):
109,102*

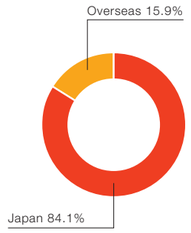
Consolidated Subsidiaries:
265*

*As of March 31, 2012

Consolidated Net Sales and Net Income (Loss)

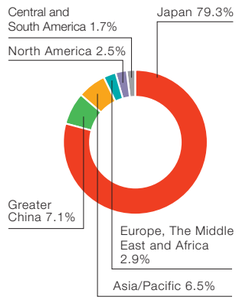


Composition of Consolidated Net Sales by Region



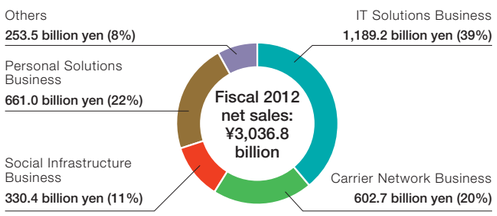
Fiscal year ended March 31, 2012

Composition of Employees by Region



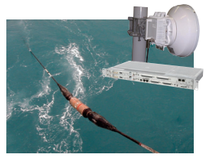
Segment Information

SEGMENT SALES (COMPOSITION)



IT Solutions Business

This business provides IT services, such as systems implementation and cloud services, and platform products essential to the implementation of IT systems and enterprise network systems, for government agencies and private-sector companies.



Carrier Network Business

This business provides network equipment to telecom carriers, along with network control platform systems, operating services and other products and services. It helps to realize highly reliable communications infrastructure based on its extensive track record and advanced technological capabilities.

Social Infrastructure Business

This business helps to realize a safe, secure and comfortable society by harnessing information and communications technology (ICT) to enable the advanced operation of various social infrastructure systems. These range from broadcasting and video distribution systems to transportation and public network systems, fire and disaster prevention systems, and aerospace and defense systems.

Personal Solutions Business

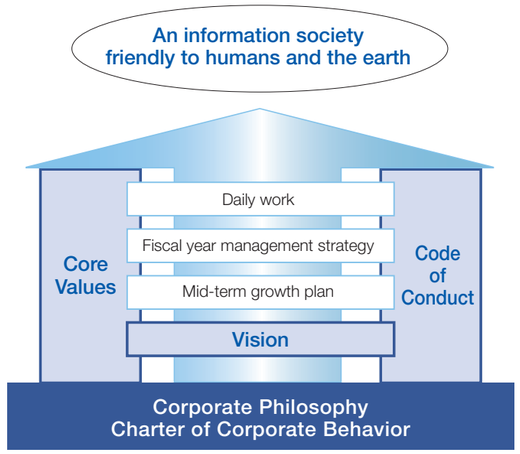
This business provides smartphones, mobile phones, personal computers for enterprises, Internet services, display solutions and other products. It also works to develop products that serve as interfaces between the cloud and users.

Others

This business strives to contribute to the realization of a low-carbon society through the provision of lithium-ion rechargeable batteries, electrodes for automobiles, and home energy management systems. It also provides lighting equipment that creates comfortable and refined living environments.

The 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

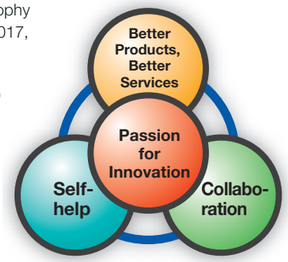
NEC Group Vision 2017

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”