\Orchestrating a brighter world

NEC

# Information Security Report 2018

# NEC's Approach to Information Security

NEC positions information security as an important management foundation for business continuity and aims to continue to be a trusted company.


## Kazuhiro Sakai

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


Under the company's corporate message of "Orchestrating a brighter world," NEC aims to use ICT to solve global issues to realize a safe, secure, efficient, and equal society where people are able to live prosperous lives.
Another development is that the world is currently at a major turning point as new business models and schemes are being created as the result of Digital Transformation.*1 NEC regards Digital Transformation not as a simple trend but as a movement with sufficient influence to change even the industrial structure. In order to realize new value creation and business transformation, the utilization of ICT is more important than ever.

Information security is indispensable for the realization of a safe, secure, efficient and equal society as well as for the promotion of Digital Transformation, and as such, NEC positions information security as an important management foundation for business continuity.

In addition to implementing measures against ingenious and sophisticated cyber attacks, ensuring highly secure products, systems and services, and promoting information security measures in cooperation with business partners, we aim to continue to be a trusted company by proactively developing information security management, information security infrastructure, and information security personnel. NEC's information security initiatives are based on the following basic concepts.

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

This report introduces the NEC Group's information security activities. We invite you to read this report and find out more of what the NEC Group is doing in the field of information security.

*1 Digital Transformation (DX): Concept of creating new value and changing economic and living conditions for the better through the use of information technology that connects the real world with the cyber world.

# Information Security Report 2018



## On the Publication of This Report

The purpose of this report is to provide stakeholders with information on the information security activities of the NEC Group. The report covers our activities up to June 2018.





For inquiries regarding this report, please contact:

**Chief Information Security Officer**
**Management Information Systems Division**
**NEC Corporation**
NEC Headquarters, 7-1 Shiba 5-chome, Minato-ku,
Tokyo 108-8001
Phone: 03-3454-1111 (main line)

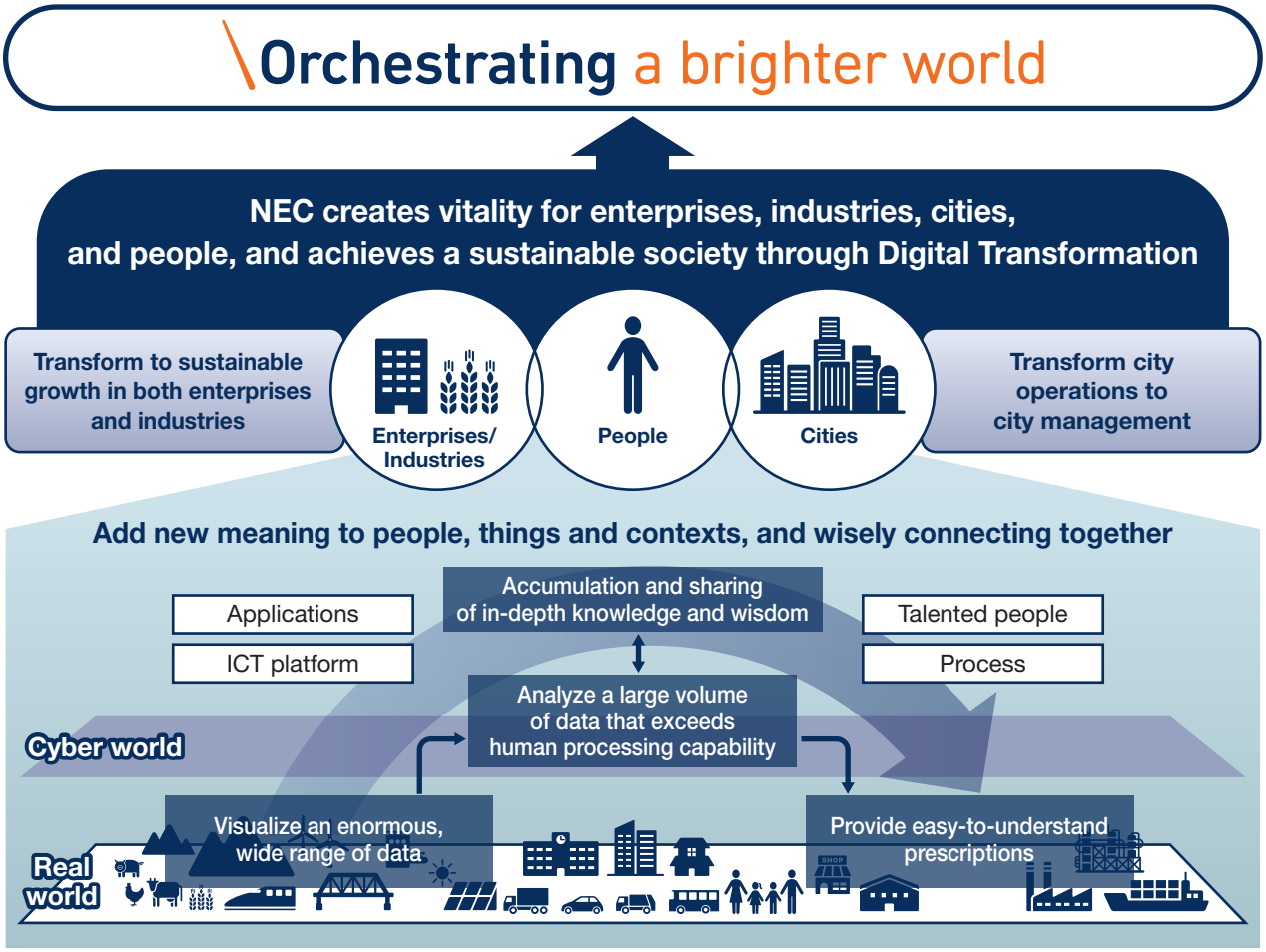
# Security Supporting Digital Transformation (DX)

NEC envisions digital transformation as “digitalizing events in the real world, incorporating them into the cyber world, and creating new value by connecting people, things, and contexts to change lives and businesses for the better.”

There are three major processes in the use of digital data. The first process is digitizing the real world and visualizing it in the cyber world. The second is to perform a sophisticated analysis of the vast amounts of data. The third is to apply prescriptions to the real world based on the analysis results. A highly secure platform that can support digital transformation is imperative for driving these processes. AI technology, IoT technology, network technology, computing technology capable of processing high volumes of data at high speed, and security technology are indispensable to making this platform a reality.

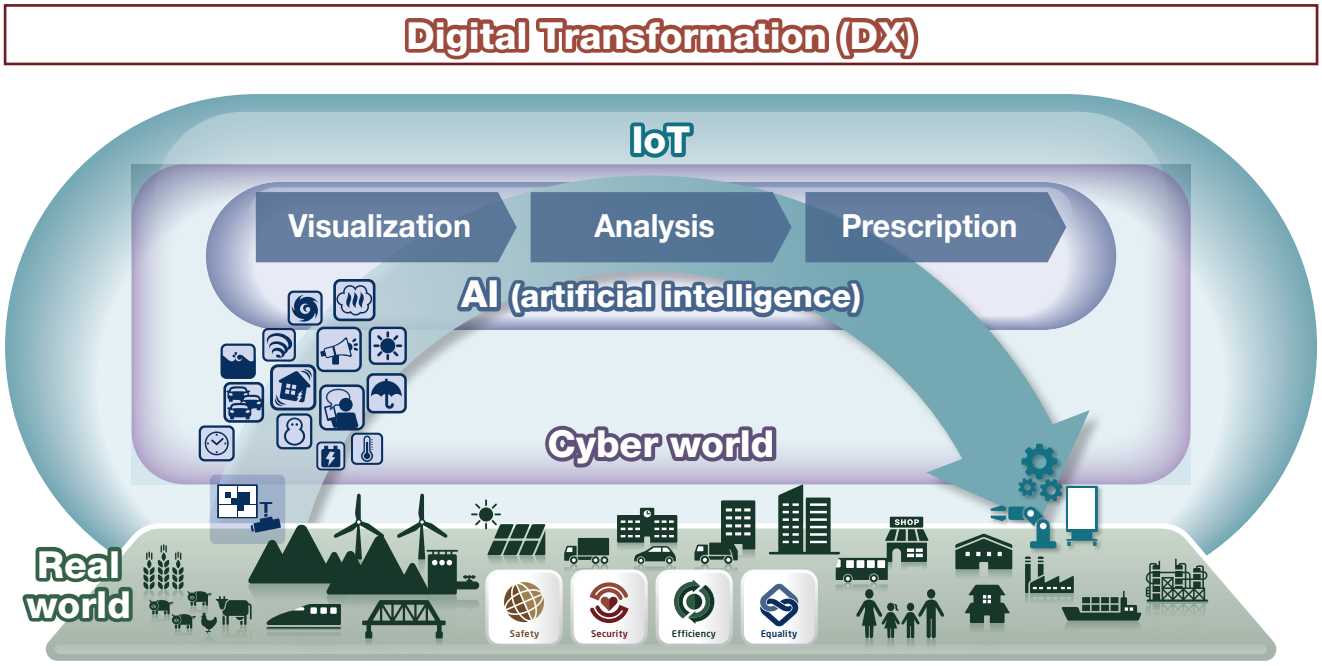
Through the use of these technologies, NEC is expanding its suite of “NEC DX Solutions” that contribute to making digital transformation possible, and reinforcing proposals of these solutions to customers.

Furthermore, NEC is also working to bring about its own digital transformation in areas such as sales, marketing, design and development, production, and work style. In this way, NEC is engaged in building and operating a secure infrastructure that ensures safe and secure business operations in an aim to realize digital transformation within the NEC Group.




Digital Transformation (DX) as envisioned by NEC

## 1 NEC the WISE IoT Platform




Digital Transformation (DX) and IoT

With the use of AI and IoT, Digital Transformation can be realized in areas such as transforming work style, transforming the value chain, transforming organizations and ecosystems, and transforming the operation model.
IoT is a tool that can be used for creating connections with the real world. AI is a tool that can be used for quick and sophisticated analysis of the data collected from the real world. These technologies can be used to create new value by driving the cycle of visualizing and analyzing real-world information then identifying prescriptions and reapplying it back to the real world.

In the area of transforming work style, we will shift from operations based on experience and expertise to operations executed based on real data and analysis. This will lead to the creation of new value in such forms as stable operations, the creation and sharing of explicit knowledge, and work style without the constraints of location or time.
In the area of transforming the value chain, we will create new value by shifting from traditional value chains (for example, manufacturing ⇒ sales ⇒ consumers), to a consumer-centric structure that is characterized by more efficient production planning and product development, product planning that meets needs in a timely manner, and the provision of a completely different purchasing and user experience.
In the area of transforming organizations and ecosystems, we will achieve overall optimization by connecting various departments involved in IT, marketing, development, and support, and create new value by moving away from local optimization and transforming organizations and ecosystems to ones centered on consumers, partners, and residents.
In the area of transforming the operating model, we will utilize digitally connected products and services to increase operational efficiency and produce innovation.

NEC offers the NEC the WISE IoT Platform, integrated with advanced AI technology and IoT, as a platform to drive digital transformation. This platform features a highly efficient data collection infrastructure and a building block structure that allows quick system creation and migration from demonstration to production, making it possible to build secure and robust systems in a short time.
In addition, NEC provides total support ranging from business know-how cultivated in various industries to common business functions that provide value, common applications that support corporate business activities, infrastructure, development/execution environments, cloud usage environments, networks, security, and operations.

**NEC the WISE IoT Platform Lineup**

**Integrated IoT platform**

Integrated IoT utilization environment that covers from the collection of IoT data to its analysis using AI and the operation of the entire system

**Components of integrated IoT platform and other services/products**

**AI and analytics**

Environment that allows quick and flexible use of NEC the WISE's various AI engines and BIs

**Common business functions**

Early launch support for new businesses

**Application development/execution functions**

Support for rapid application development

**Infrastructure**

Cloud platforms supporting DX

Unique products supporting DX

**Security**

IoT environment security enhancement

**Networks**

Networks supporting IoT environment

**Operation**

Enhancement of operational efficiency of IoT environment

NEC the WISE IoT Platform

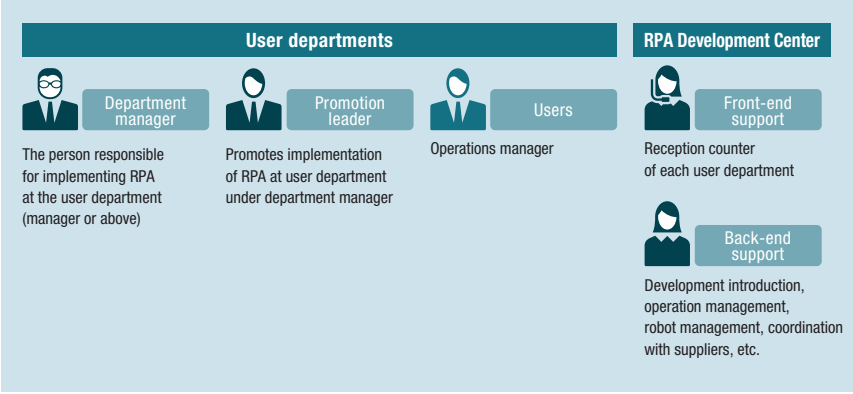
## 2 Business Automation through RPA*1

RPA technology is expected to greatly contribute to productivity improvement by automating routine tasks that were done by people until now, such as data entry into business systems. RPA is expected to be actively used for bringing about digital transformation in areas such as sales and marketing, design and development, production, work style, and so on. NEC implements RPA security measures to cope with risks such as unauthorized use of unmanaged RPAs and bugs during RPA system updates.

*1: RPA: Robotic Process Automation

### (1) RPA Development Center Management Framework

At NEC, the RPA Development Center Management Framework has been established to properly manage the robots used within the NEC Group and to support the improvement of productivity through RPA. This framework consists of the RPA Development Center, which centrally manages RPA, promoters in departments implementing RPA, and the actual RPA users. Using this framework, we centrally manage the robots to be used within the NEC Group and implement security measures.




System

### (2) RPA Infrastructure Environment

When introducing RPA, it is necessary to take adequate measures to cope with the risks caused by differences between humans and robots. We operate the robots used within the NEC Group in an RPA infrastructure environment with security measures, and manage them through monitoring. Through this environment, users can use RPA safely and securely to improve productivity.

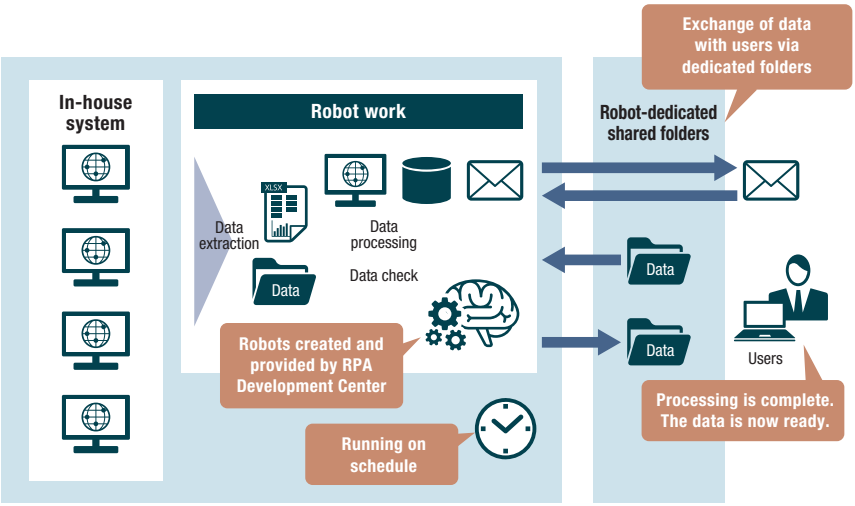



Illustration of RPA Use

### (3) Establishment of Guidelines

Robots can be used to perform all routine tasks that people perform on PCs, but depending on the application and the structure of the robot, the risk of security incidents may increase. At NEC, the RPA Development Center conducts risk assessment for the use of RPA, and provides countermeasures as guidelines.

## 3 Cloud Service (SaaS: Software as a Service) Security

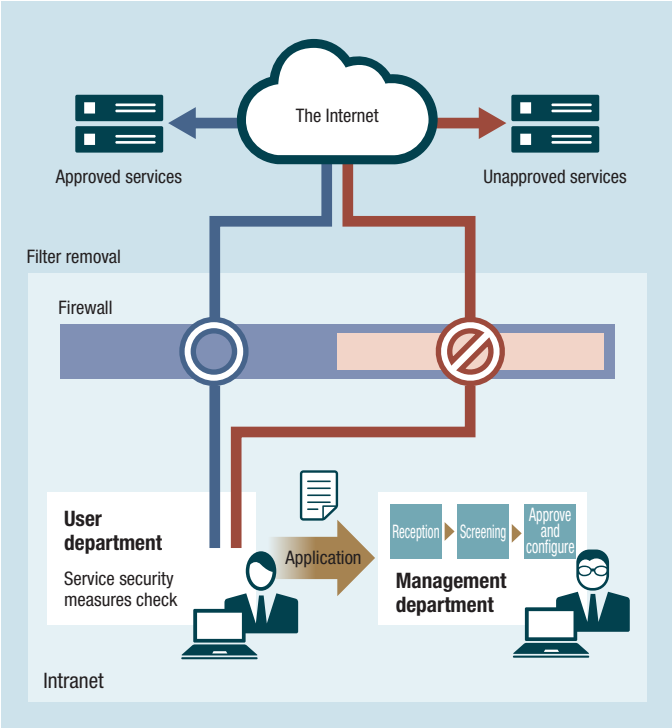
Since cloud services (SaaS) can be deployed quickly, they can help improve business speed and offer many other benefits that make them indispensable for realizing Digital Transformation.
NEC offers unprecedented value by combining NEC's technology, platforms, and cloud services, and connecting multiple cloud services to one another. Within the NEC Group, we implement measures to actively use cloud services in a safe and secure environment.

### (1) Framework to Promote Company-wide Usage of Cloud Services

NEC has established a Cloud Utilization Center to ensure the proper management of the use of cloud services in the NEC Group. The Cloud Utilization Center provides cloud services for use by the entire NEC Group, and it also carries out security checks.
Further, it shares security-related information on cloud services according to the Information Security Promotion Framework.

### (2) Security Policies and Rules

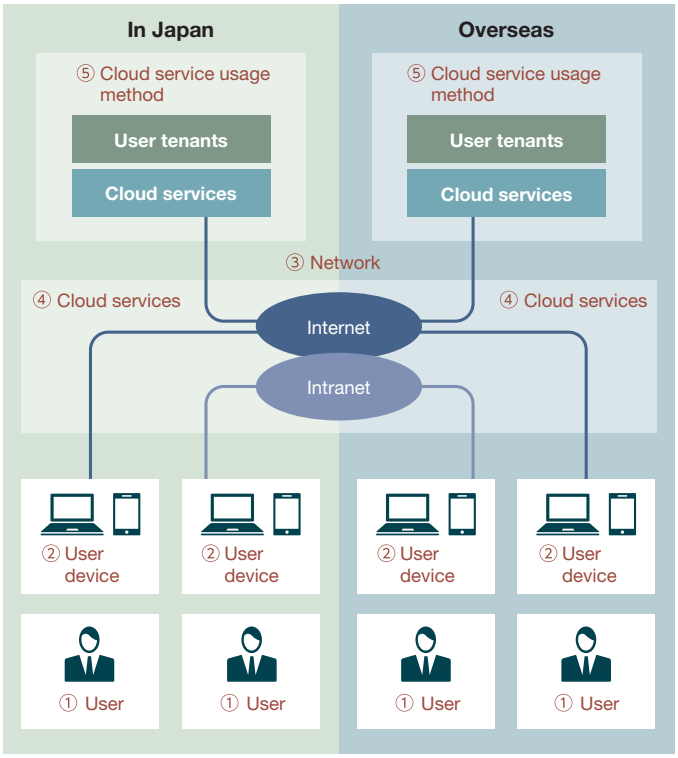
NEC stipulates security policies that must be complied with when using cloud services within the NEC Group. Prior to using the cloud services, users must check that security measures are in place then submit an application and receive approval from the Cloud Utilization Center.




**Security Policies Regarding the Use of Cloud Services**

### (3) Security Measures When Using Cloud Services

In the past, the security level was secured by constructing a system within the intranet where security measures were implemented. However, when using cloud services on the Internet, traditional security measures do not suffice.
At NEC, we divide the environment for using cloud services into five categories: users, devices, network, cloud services, and cloud service usage methods, and we ensure the required security level by implementing security measures in these environments.




**Security Measures When Using Cloud Services**

### (4) Classification of Cloud Services

To ensure the safe, secure and efficient use of cloud services, NEC categorizes and manages cloud services according to: cloud services used by the entire NEC Group, cloud services whose use is conditional upon approval of the application submitted by the organization that wishes to use them, and cloud services whose use is prohibited.

# Measures against Cyber Attacks

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

*1 CSIRT: Computer Security Incident Response Team

## 1 Cyber Security Risk Analysis

NEC implements cyber attack countermeasures based on the results of four types of risk analysis of cyber attacks such as targeted attacks, ransomware, BEC*2, and indiscriminate email attacks*3.

*2 BEC: Business E-mail Compromise, a type of email fraud
*3 Indiscriminate email attack: An attack that targets an unspecified, large number of people

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

**Monitoring operations analysis**
We perform reviews of our current monitoring processes as needed, study operations in line with changing cyber threats, and identify operational issues.

**Solution and IT analysis**
We also evaluate PoCs*4 and, through internal IT environment surveys of the NEC Group, analyze matters including the applicability of countermeasure products and services to the Group's internal IT environment.

*4 PoC: Proof of Concept

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

## 2 Global Measures against Cyber Attacks

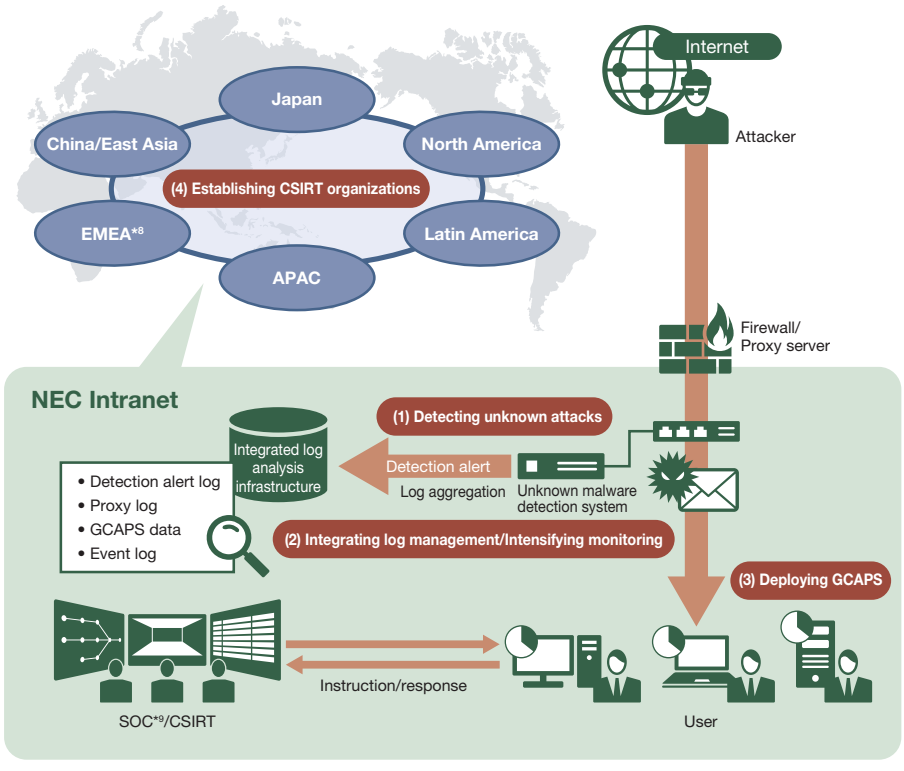
NEC formulates plans for countermeasures based on cyber security risk analysis, and implements the countermeasures with the approval of the CISO*5.
As a company that deploys Solutions for Society on a global scale, NEC understands that adopting a globally unified approach to cyber security risks is vital for business continuity.
Our global cyber security measures broadly focus on four areas:
1) Detecting unknown attacks
2) Integrating log management/Intensifying monitoring
3) Deploying GCAPS*6
4) Establishing CSIRT organizations

*5 CISO: Chief Information Security Officer
*6 GCAPS: Global Cyber Attack Protection System

### (1) Detecting Unknown Attacks

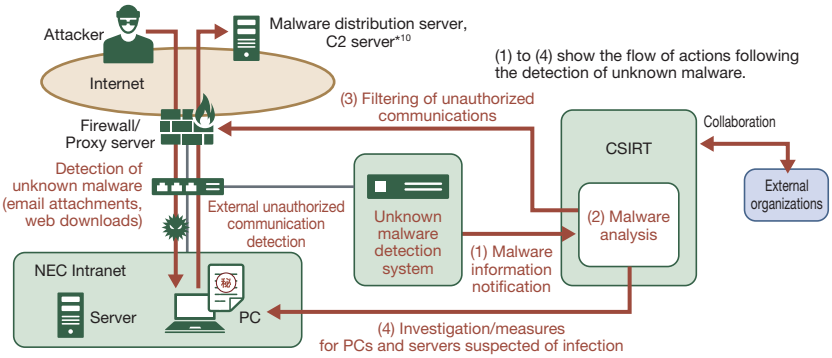
As entrance and exit countermeasures, we implement unknown malware detection systems, monitor web communications and in-coming emails, and, based on information about detected unknown malware, filter out improper communications and take measures to handle PCs and servers suspected of infection.
Together with SDN*7 we also use these technologies to realize 24/7 automatic blocking of unauthorized communication from infected devices, thus preventing the spread of secondary infection and minimizing security risks.

*7 SDN: Software-Defined Networking



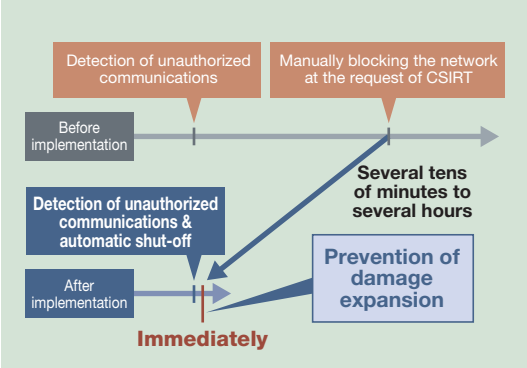

*8 EMEA: Europe, the Middle East and Africa *9 SOC: Security Operation Center

**Overview of Countermeasures against Global Cyber Attacks**




*10 C2 server: Command & Control server - a server taking unauthorized control over the devices infected by malware

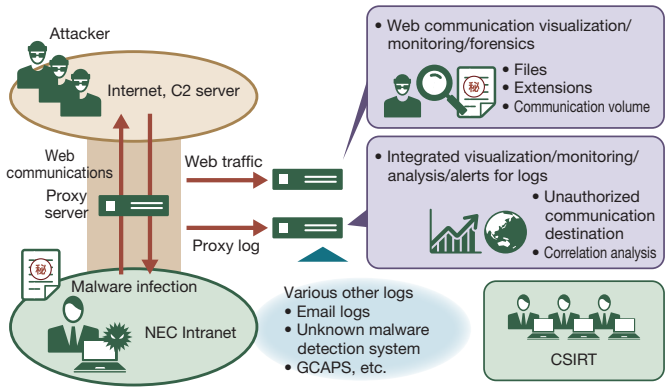
**Detection of Unknown Malware and Unauthorized Communications**




**Benefits by Linking the Unknown Malware Detection System with SDN**

## (2) Integrating Log Management/Intensifying Monitoring

Through comprehensive and integrated management of the communication and operation log data of 180,000 PCs/servers across the NEC Group, we are making our monitoring and analysis more efficient and sophisticated.
We also conduct relational analysis of multiple logs to identify possible risks, which will enable us to reduce the risk of information leakage.




**Integrated Analysis of Logs and Investigation of Packets**

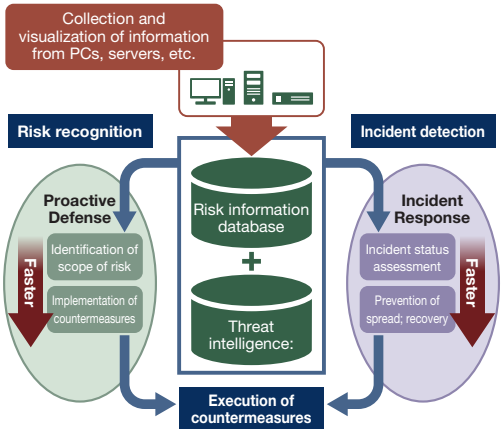
## (3) Deploying GCAPS

NEC is rolling out the GCAPS (sold externally as a solution under the name NCSP*11) to the entire Group, for the purposes of strengthening measures related to PC and server vulnerabilities and increasing the efficiency of incident response.
To prevent attacks that exploit vulnerabilities, we are globally strengthening measures related to PCs and servers with GCAPS from two standpoints: "Proactive Defense" performed on the basis of risk recognition, and "Incident Response" when an incident has been detected.

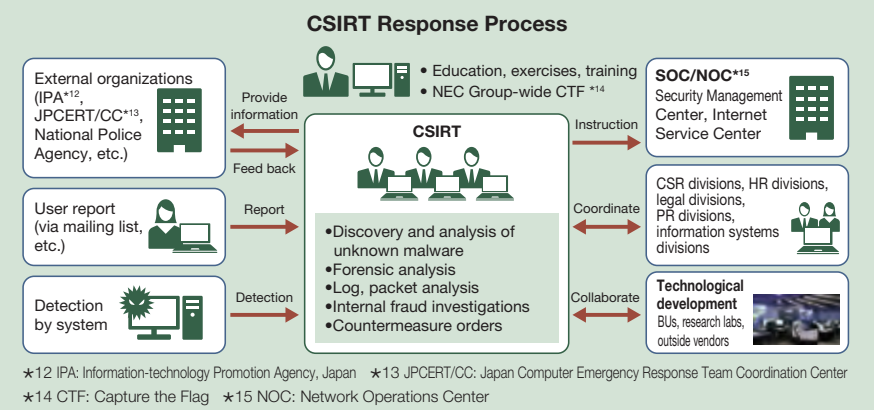
*11 NCSP: NEC Cyber Security Platform

## (4) Establishing CSIRT Organizations

NEC has established a CSIRT, headed by the CISO. The CSIRT monitors for cyber attacks, analyzes the features of discovered attacks and malware, and shares the information with related departments. If an incident occurs, the CSIRT takes immediate steps to protect the company's systems and find out what type of attack they are facing. The team then analyzes the cause of the incident and implements measures to bring the attack to an end. The NEC Group also shares threat intelligence based on detected cyber attacks and unauthorized communications among group companies across the globe, thus enabling the CSIRTs of the entire group to work together smoothly.




**Concept of GCAPS**




*12 IPA: Information-technology Promotion Agency, Japan *13 JPCERT/CC: Japan Computer Emergency Response Team Coordination Center
*14 CTF: Capture the Flag *15 NOC: Network Operations Center

**Overview of CSIRT**

# 3 Utilization of AI for Protection against Cyber Attacks

NEC has incorporated Artificial intelligence (AI) to realize leading-edge cyber security. By operating our advanced solution in an actual environment as proof of concept, NEC is making efforts on the growth of its focused area as well as the development of an advanced internal reference model.
We have implemented ASI*16, NEC's AI-based self-learning technology that detects abnormal behaviors of a system, into the IT environment of NEC Asia Pacific (Singapore), and enabled CSIRT to monitor the environment more effectively. Requirements and points for improvement obtained through actual operations are provided to the development division as feedback, contributing to the improvement of ASI quality.

*16 ASI: Automated Security Intelligence – a self-learning technology that detects abnormal behaviors of a system

# Information Security Promotion Framework

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

Information security threats change every day in our society, which has become highly sophisticated through IT. Information security is therefore a critical issue for all businesses. NEC has established an information security promotion framework to fulfill our responsibilities to society as a trusted company. This framework enables us to realize a secure information society and provide value to our customers by protecting the information assets entrusted to us by our customers and business partners.

To protect information assets, NEC is implementing cyber attack measures, providing secure products, systems and services, and promoting information security in collaboration with business partners. At the same time, we have positioned information security management, information security infrastructure, and information security personnel as the three pillars of the information security governance framework within the NEC Group, thereby maintaining and improving our comprehensive and multi-layered information security.

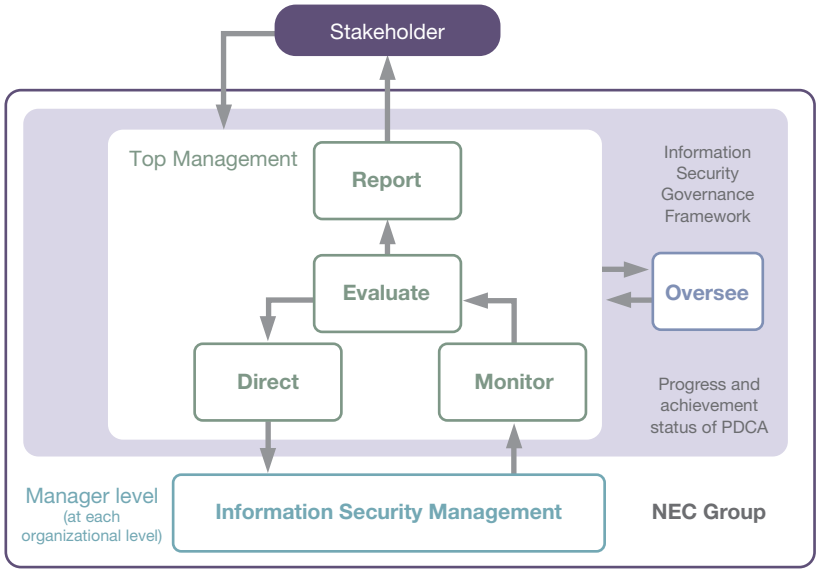
The information security governance framework enables us to effectively and efficiently deploy activities across the NEC Group. Activities include the establishment of the NEC Information Security basic policy and group-wide rules, and the development of a common information security infrastructure. Activities conducted by top management include establishing security targets; determining Group policies, system architecture, and the policy for allocating management assets; and monitoring and improving the system.

# Information Security Governance

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

## 1 Information Security Governance in the NEC Group

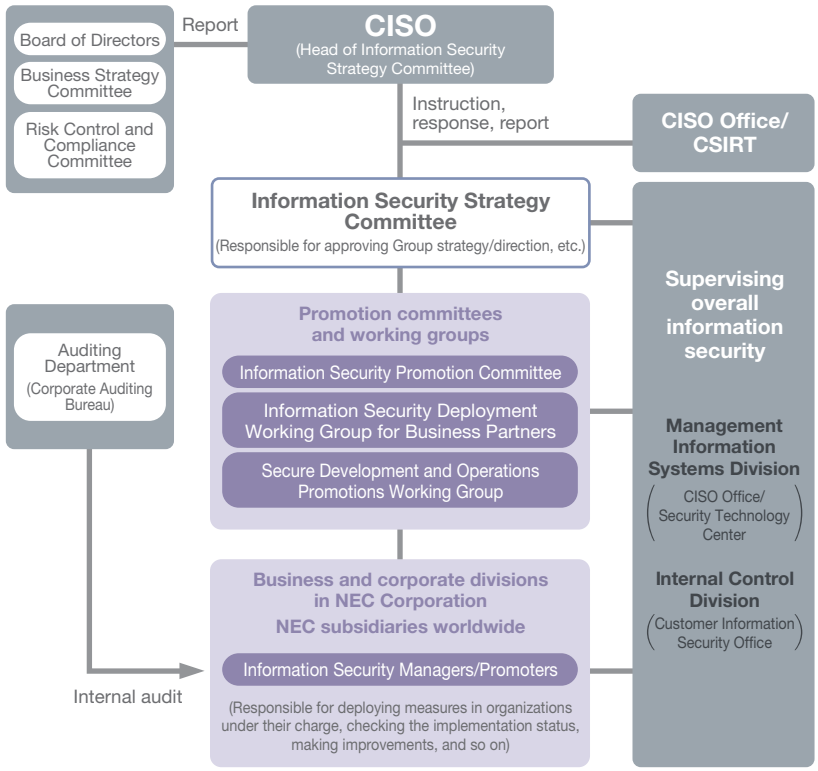
NEC has established the NEC Group Management Policy, a set of standardized rules related to the conduct of business, unified systems, business processes, and infrastructure to create a foundation from which to achieve standard global management so that the whole Group can make a comprehensive contribution.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




**Information Security Governance**

## 2 Information Security Promotion Organizational Structure of the NEC Group

The information security promotion organizational structure of the NEC Group consists of the Information Security Strategy Committee, its subordinate organs, and the promotion structure at each organization level.
The Information Security Strategy Committee, headed by the CISO*1, 1) evaluates and discusses how to improve information security measures, 2) discusses the causes of major incidents and the direction of recurrence prevention measures, and 3) discusses how to apply the results to NEC's information security business to address information security risks, including risks related to cyber security. The CISO also heads the CISO office, whose job is to receive direct instructions from the CISO and promote cyber security measures, and the CSIRT*2, whose job is to monitor for cyber attacks, and when an attack is detected, immediately analyze it, identify the cause of the incident and implement measures to bring the situation to normal.
The Information Security Strategy Committee and working groups discuss and coordinate security plans and implementation measures, enforce instructions to achieve them, and manage the progress for group companies worldwide, for business partners, and for driving the Secure Development and Operations initiative, respectively.
The information security manager in each organization has primary responsibility for information security management including the group companies under their supervision. They continuously enforce information security rules within their organizations, introduce and deploy measures to assess the implementation status, and implement further improvement measures to maintain and enhance information security.




**Information Security Promotion Structure**

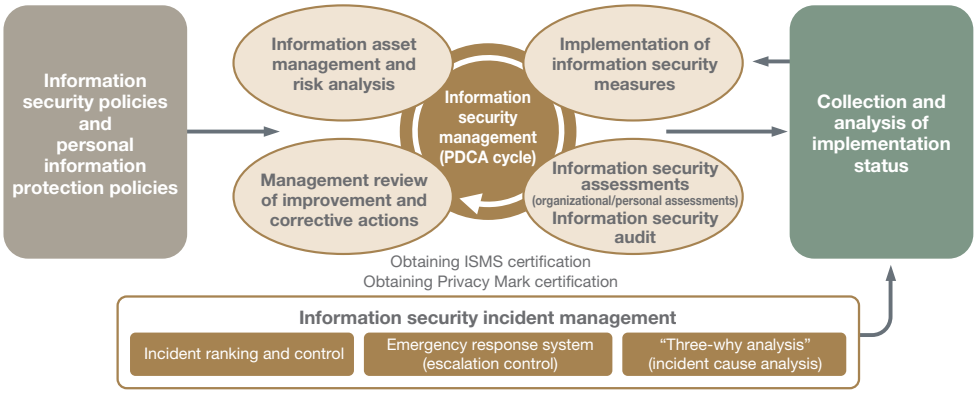
*1 CISO: Chief Information Security Officer *2 CSIRT: Computer Security Incident Response Team

# Information Security Management

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

## 1 Information Security Management Framework

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




**NEC's Information Security Management**

## 2 Information Security Policies

NEC has rolled out the NEC Group Management Policy as a set of comprehensive policies for NEC Group companies all over the world. This includes information security and personal information protection policies. The NEC Group has been strengthening management with information security and personal information protection positioned as important matters in conducting business.

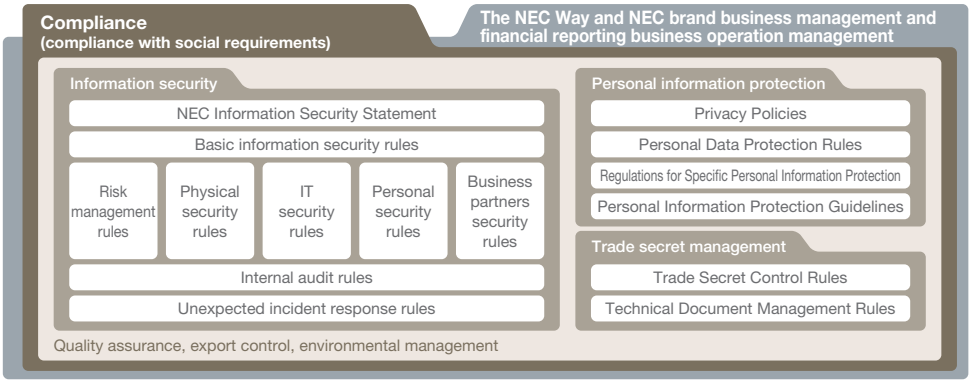
For information security, NEC has released the "NEC Information Security Statement" and established and streamlined a variety of rules and standards including basic information security rules, rules for information management (Trade Secret Control Rules, Personal Data Protection Rules, Regulations for Specific Personal Information Protection, and technical document management rules), and IT security rules to enforce these basic policies.

To protect personal information, NEC established the NEC Privacy Policy and obtained Privacy Mark certification in 2005. We also established a management system that conforms to the Japan Industrial Standards Management System for the Protection of Personal Information (JIS Q15001) and Japan's Act on the Protection of Personal Information. Additionally, in 2015, the NEC added a My Number (personal identification number) management framework to its information security management system to ensure compliance with the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure ("My Number Act").

Furthermore, in 2017, NEC took the required steps to comply with the Amended Act on the Protection of Personal Information, such as by making revisions to manuals. To comply with revisions made to the JISQ15001 standards in 2017, NEC also revised the regulations and manuals pertaining to protecting personal information, and to the GDPR*1-compliant NEC guidelines.

The NEC Group requires employees to handle personal information at the same protection management level throughout the entire Group. As of the end of June 2018, 28 companies have acquired Privacy Mark certification.

*1 GDPR: The EU General Data Protection Regulation




**NEC Group Management Policy**

## 3 Information Security Risk Management

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

### (1) Information Security Risk Assessment

The NEC Group assesses risk and takes measures by analyzing the difference from a baseline or by analyzing detailed risk on a case-by-case basis. We

maintain security by using an information security baseline defined as the fundamental security level to be implemented across the Group. We perform analysis according to detailed risk assessment standards and take detailed measures based on the Information Security Risk Assessment Standards if advanced management is required.

### (2) Management of Information Security Incident Risk

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

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

## 4 Information Security Assessments

NEC conducts information security assessments every year to check the implementation status of information security measures and to create and execute improvement plans for measures not completed.

### (1) Details of Information Security Assessments

We analyze information security incidents and set priorities, mainly to eliminate information leaks. Assessments are aimed to help respondents realize what is required to secure their environment and raise their awareness on security; respondents are asked to answer if they are implementing required security measures and if not, they have to answer their current status to be improved.

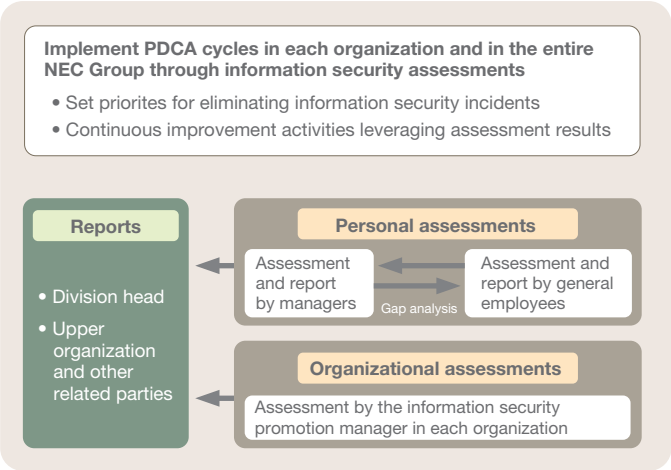
Specifically, assessments are conducted on such subjects as management of information taken outside of the company's premises, management of confidential and personal information, management of external contractors (business partners), secure email distribution, measures against targeted attack emails, and Secure Development and Operations.

### (2) Information Security Assessment Methods

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

### (3) Improvements Leveraging Assessment Results

Based on the assessment results, we have solved problems systematically by identifying measures that were required but not sufficiently implemented, finding the reasons why they were not implemented properly, and making improvements. At the same time, we analyze trends in the entire NEC Group, and establish the information security promotion plan for the following fiscal year to solve the remaining problems and to enhance our security for continuous improvement.




**Information Security Assessments (Organizational and Personal Assessments)**

## 5 Information Security Audits

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

## 6 Acquiring the ISMS Certification

NEC provides services such as consultations, creation of a structure for audit, training, and allowing users to get ISMS Certification screening efficiently (e.g., evaluated only by the difference) for organizations that must acquire ISMS certification for their business based on standard contents designed to reliably fulfill the requirements of ISMS certification. These services are packaged and offered as a solution called "NetSociety for ISMS." This solution has been successfully used by many organizations in the NEC Group as well as our business partners.

# Information Security Infrastructure

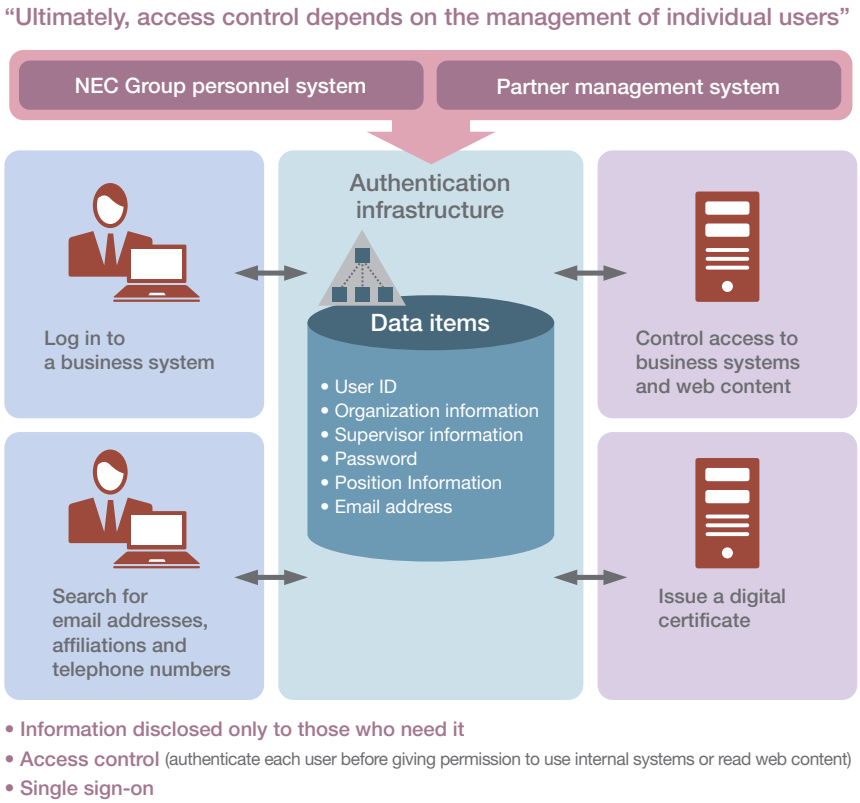
NEC has built and operates information security infrastructure to manage and control users and to allow them to safely, securely and efficiently use PCs, networks, and business systems in order to protect customer and confidential information.

## 1 Features and Configuration of Information Security Infrastructure

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

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

The basis of information security management is the user authentication infrastructure. Using a system to identify individuals enables proper control of access to information assets and prevents spoofing by using digital certificates.
It is important to identify and authenticate users and assign them correct privileges so that information assets can be managed appropriately. NEC has built an authentication platform to centrally manage information used for authenticating users and assigning privileges (authorization), covering not only our employees but also some business partners and other related parties if needed for business.
The information used for authenticating and authorizing users consists of access control information such as the user's ID and password, as well as information about their organization and position. This information is used to control access to business systems and other company infrastructure on an individual basis. We also centrally manage which system and for what purpose the information for authenticating and/or authorizing users managed by each Group company is being used.
With respect to controlling access to systems that handle critical information, besides the use of the user's ID and password (memory-based authentication), we are also promoting the use of certificate-based individual authentication (token-based authentication). In addition, plans are in place to adopt face recognition (biometrics authentication) in the future.
The cloud service authentication system has been connected to the internal authentication platform, enabling a seamless system of authentication for internal and external services. The system ensures that users can safely, securely, and comfortably share information with external parties when using cloud services.




**NEC Group Authentication Infrastructure**

## 3 IT Platform for PC and Network Protection

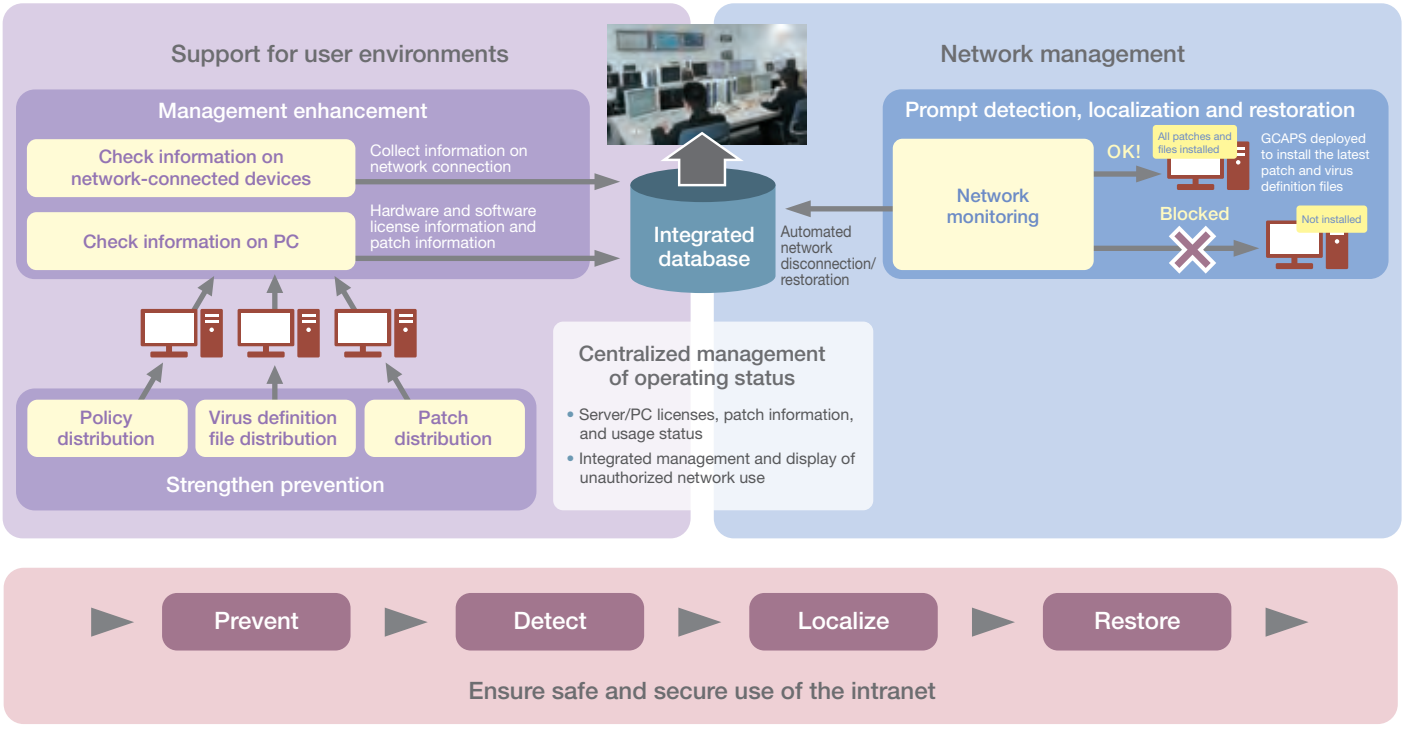
NEC has constructed a global IT platform to protect the Group's PCs and networks from viruses, worms, and other attacks and maintain the security of information devices connected to the NEC Intranet. In addition, as multi-level measures are recently required to address increasing risks of targeted attacks,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

### (1) Protecting Our PCs from Viruses and Worms

**[Support for user environments]**
NEC Group employees using the NEC Intranet are required to install software to check the status of their PCs and the network. Being able to visualize the current state allows us to instantly check whether all the necessary security software is installed on all PCs. In addition, there is a system in place to automatically distribute security patches and updates of definition files for antivirus software.
We also define prohibited software and monitor whether users are using software properly.

**[Network management]**
In addition to visualizing PC status, when a PC for which security measures are not sufficiently implemented is connected to the NEC Intranet or a worm is detected on the NEC Intranet, that PC or LAN is disconnected from the NEC Intranet. We also control communications to people or organizations outside NEC by using web access filtering based on prohibited categories, prohibiting the use of free email accounts, using SPF authentication (sender domain authentication), and other methods.

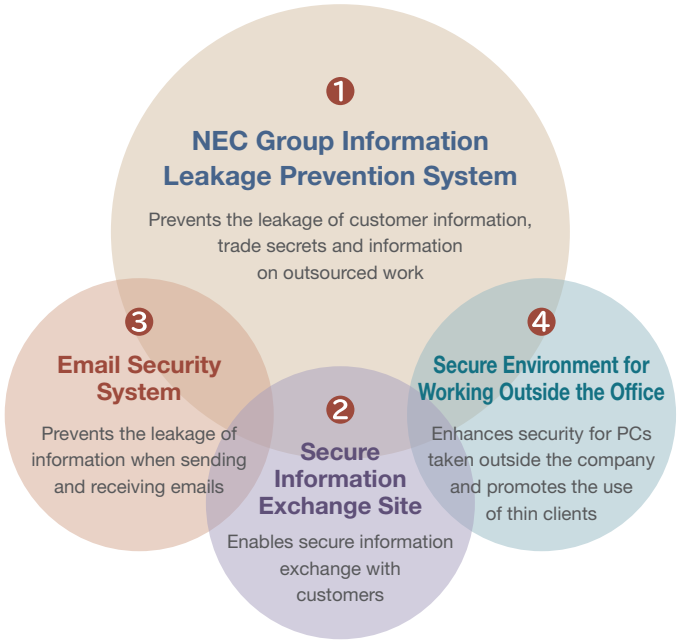
**[Centralized management of operating status]**
Data on the implementation status of security measures, including installation of patch programs and antivirus software, is collected in a management system so that information security managers and security promotion managers can see the implementation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




**Protection of PCs and Networks from Viruses and Worms**

## 4 IT Platform for Information Protection

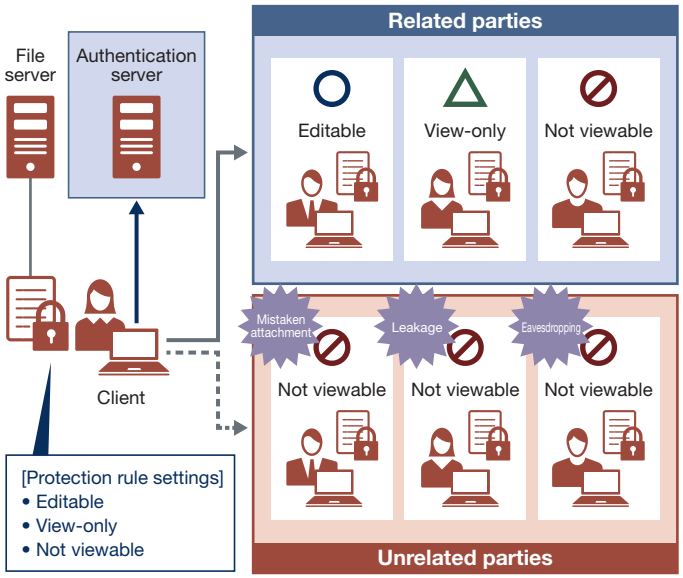
It is necessary to identify channels that can lead to information leaks, analyze risks and take appropriate measures to prevent leaks.
As NEC manages not only our own information but information entrusted to us by customers and information disclosed to business partners, we implement comprehensive and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




**Overview of IT Platform for Information Protection**

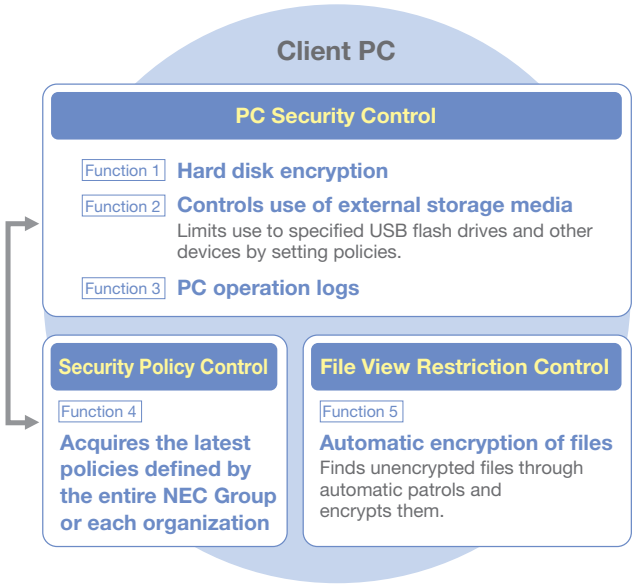
### (1) NEC Group Information Leakage Prevention System

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




**File Encryption Using InfoCage FileShell and Usage Restrictions**

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

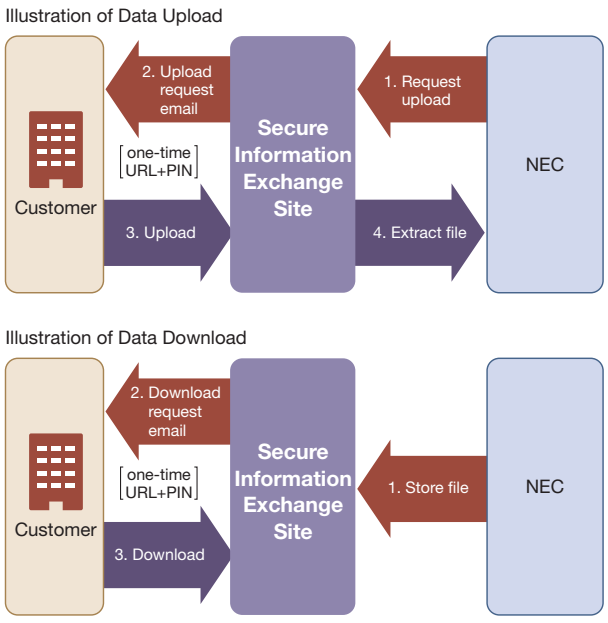



**Overview of Information Leakage Prevention System**

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

## (2) Secure Information Exchange Site

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

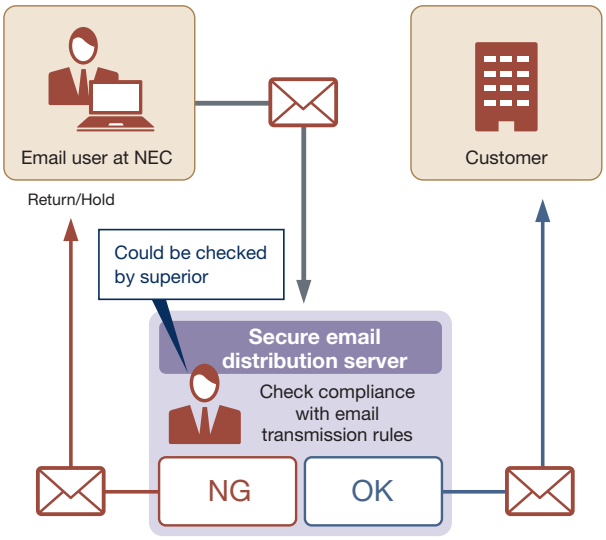



**Secure Information Exchange Site**

## (3) Email Security System

NEC has implemented a secure email distribution system to prevent incidents of information leakage caused by mistaken email address entry or mistaken email attachments.
To increase the usability, the system provides a feature that allows users to check the email address and attached file(s) on the Web screen. The system is also equipped with a function for an appropriate person (not the user himself/herself but, for example, his/her superior) to check details of an email including its destination, which serves to prevent the intentional leak of information through email transmission.
Our efforts to increase email security also include the rollout of OMCA*1 within NEC. OMCA provides functionality to alert users about a suspicious email that may be a targeted attack and to display a popup window prompting users to check the destination address and attached file(s) before sending an email.

*1 OMCA: Outlook Mail Check AddIn




**Secure Email Distribution System**

## (4) Secure Environment for Working Outside the Office

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

# Information Security Personnel

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

## 1 Developing Information Security Expertise

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

## 2 Strengthening Knowledge and Awareness of Information Security

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

### (1) Training on Information Security and Personal Information Protection

NEC provides a web-based training (WBT*1) course on information security and personal information protection (including protection of people's personal identification numbers ["My Numbers"]) for all NEC employees to increase knowledge and skills in the information security field. The content of this training course is reviewed every year to reflect the latest trends in security threats and other security-related information. Specifically, the course aims to raise awareness about new security threats and required responses, and ensure that employees thoroughly understand NEC Group policy in important areas such as information handling, internal fraud prevention, contractor management, and Secure Development and Operations.

*1 WBT: Web Based Training

### (2) Commitment to Following Information Security Rules

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

### (3) Activities to Raise Awareness of Information Security

NEC performs awareness-raising activities using video dramas about cyber attacks, information loss incidents, and other possible mistakes mainly caused by human actions so that employees gain a sense of crisis concerning information security risks and learn how to think, decide and act by themselves. Workplace discussions encourage employees to raise their awareness through talking about security issues with colleagues and to improve their analysis and judgment skills.

## 3 Developing Personnel to Promote Information Security Measures

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

### (1) Training Information Security Promoters

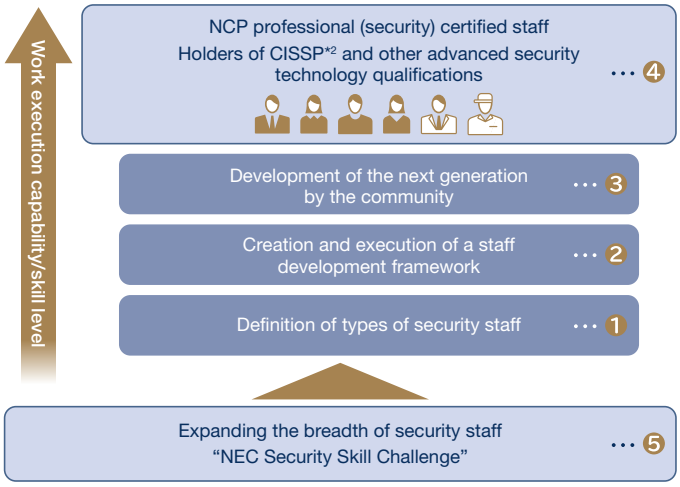
NEC has established a system for newly assigned information security promoters in each organization to learn about the security management structure, roles and responsibilities, specific security measures, details of promotion initiatives and other topics required to promote information security whenever it is necessary. We also provide training programs using videos based on actual incidents to develop practical skills to cope with considerable risks which differ depending on the organization, as well as to enhance capabilities in risk control and proactive thinking/action-taking.

### (2) Auditor Training

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

# 4 Developing Experts

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

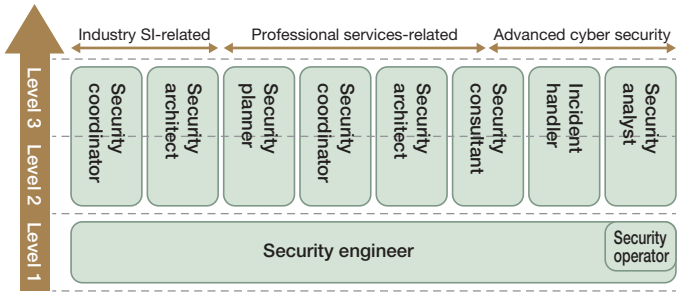



*2 CISSP: Certified Information Systems Security Professional

**Professional Staff Development**

## (1) Definition of Types of Security Staff

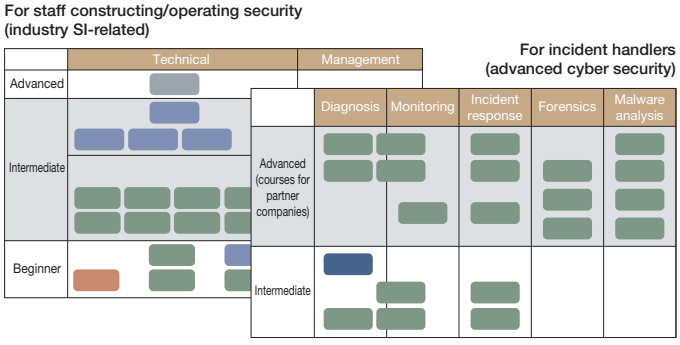
We define the security staff necessary for NEC and work to develop staff in each category. We also ensure that our definitions are aligned with the types of staff required by our customers, and continue to adjust our definitions as required.




**Types of Security Staff**

## (2) Creation and Execution of Staff Development Framework

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



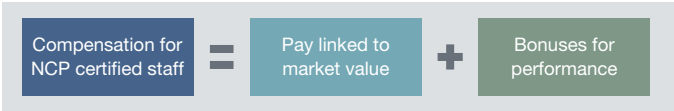

**Training Courses**

## (3) Development of the Next Generation by the Community

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

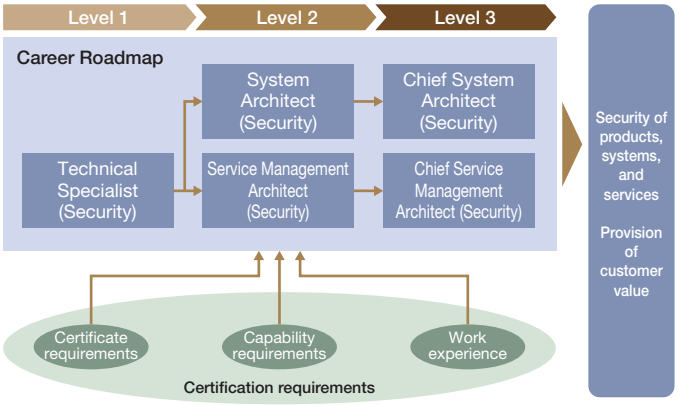
## (4) Certification System and Compensation Packages to Maintain Top Staff

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




**NCP Senior Professional Compensation Framework**

NEC also strongly encouraging our staff to acquire official qualifications for security including CISSP, an international certification, and "Registered Information Security Specialist," a certification by the Japanese government. Employees who have advanced skills, work experience and/or certification in the information security field take the lead in providing customers with optimal solutions.




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

**Professional Certification System (Security)**

## (5) Implementation of CTF across the Group

The NEC Group conducts the NEC Security Skill Challenge, an internal CTF*3 event aimed at all of our employees. In fiscal 2017, about 1,200 staff members took part in the competition, which leads to expanding the breadth of our security personnel.

*3 CTF: Capture the Flag

# Information Security in Cooperation with Business Partners

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

## 1 Framework

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

| Level (risk level) | Contractor acceptability |
|---|---|
| A (low risk) | Acceptable contractor. |
| B (middle risk) | Acceptable contractor.<br>However, only if the contractor completes the required security improvements. |
| Z (high risk) | Unacceptable contractor. |

**Information Security Levels**

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

### (1) Contract Management

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

### (2) Subcontracting Management

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

### (3) Staff Management

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

### (4) Information Management

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

### (5) Introduction of Technical Measures

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

### (6) Secure Development and Operations

NEC created the Secure Development and Operation Guidelines for Business Partners concerning the development and operation of products, systems, and services for customers to ask business partners to consider security during development and operation. These guidelines include conducting development


**Information Security Measures for Business Partners**

according to secure coding protocols and performing vulnerability diagnoses before releasing products, systems, and services.

### (7) Assessments

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

## 2 Promotion of Security Measures for Business Partners

### (1) Information Security Seminars

The supply chain management and information security divisions work together to organize information security seminars at 10 places across Japan from Hokkaido to Okinawa every year for nationwide business partners (approximately 1,500 companies, including approximately 800 ISMS certified companies) to ensure that business partners understand and implement NEC's information security measures.

### (2) Skill Improvement Activities for Core Business Partners

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

### (3) Use of Videos to Maintain Awareness

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

### (4) Operation of Examination System

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

### (5) Distribution of Measure Implementation Guidebooks

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

### (6) Standardization of Contractor Management Process

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


**Standardized Contractor Management Process**

## 3 Assessments and Improvement Actions for Business Partners

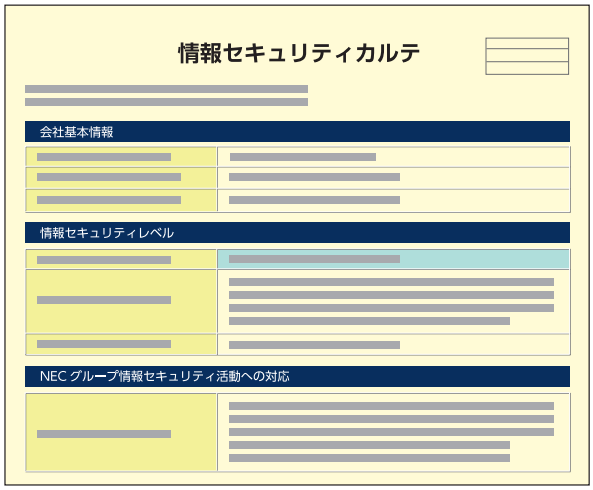
Assessments of our business partners mainly consist of web-based self-assessments and on-site assessments, but besides periodic assessments, assessments are also conducted irregularly and on a per need basis.

Web-based self-assessments are performed at approximately 1,500 companies that deal with NEC every year. New business partners receive a document assessment when opening their account. Business partners carry out self-assessments of their implementation status of security measures based on assessment items revised every year that take into account the status of information security incidents and other factors. NEC creates a report of these assessment results and provides it as individual feedback to each company. The business partners can see their security level among all the business partners of NEC, realize the challenges they face, and make efficient improvements. The business partners can then update their registered information, which allows NEC to always have updated security status information.

On-site assessments are carried out at about 100 companies that frequently deal with NEC every year. Assessors authorized by NEC (approximately 100 assessors) visit the business partners and carry out assessments onsite and uncover issues that were not found in the business partner's own assessment (i.e., web-based self-assessment).

NEC follows up all assessments by checking the extent of improvement in business partners to which improvement was required, so that business partners can achieve the required level of security.

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




**Information Security Assessment Sheet**

# Providing Secure Products, Systems, and Services

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

## 1 Promotion of Secure Development and Operations

### (1) Group-wide Promotion Structure

In order to enable Secure Development and Operations for the products, systems, and services we offer our customers, the NEC Group has created a “Secure Development and Operations” promotion structure. This promotion structure consists of the Secure Development and Operations Promotion Working Group, made up of representatives from the various NEC organizations and Group companies, and Secure Development and Operations promoters appointed throughout the NEC Group (approximately 500 people). The working group discusses proposed measures for Secure Development and Operations directed at the eradication of information security incidents caused by product, system, and service vulnerabilities, configuration mistakes, and system failures, and shares information on the implementation progress of adopted measures. The Secure Development and Operations measures adopted by this working group are communicated to the promoters at the various divisions through the Secure Development and Operations Promotion Liaison Group and other groups. The promoters then ensure that the measures are fully disseminated within their respective division, carry out implementation status inspections, and continuously work on improvements.

### (2) Group-wide Standards and Guidelines Established Based on These Standards

The Secure Development and Operations Management Rules were established as part of the NEC Corporation Industrial Standards, which are the Group-wide standards of NEC. These rules define fundamental matters such as NEC’s secure development and operations promotion structure, the tasks to be carried out by various divisions, and related standards.

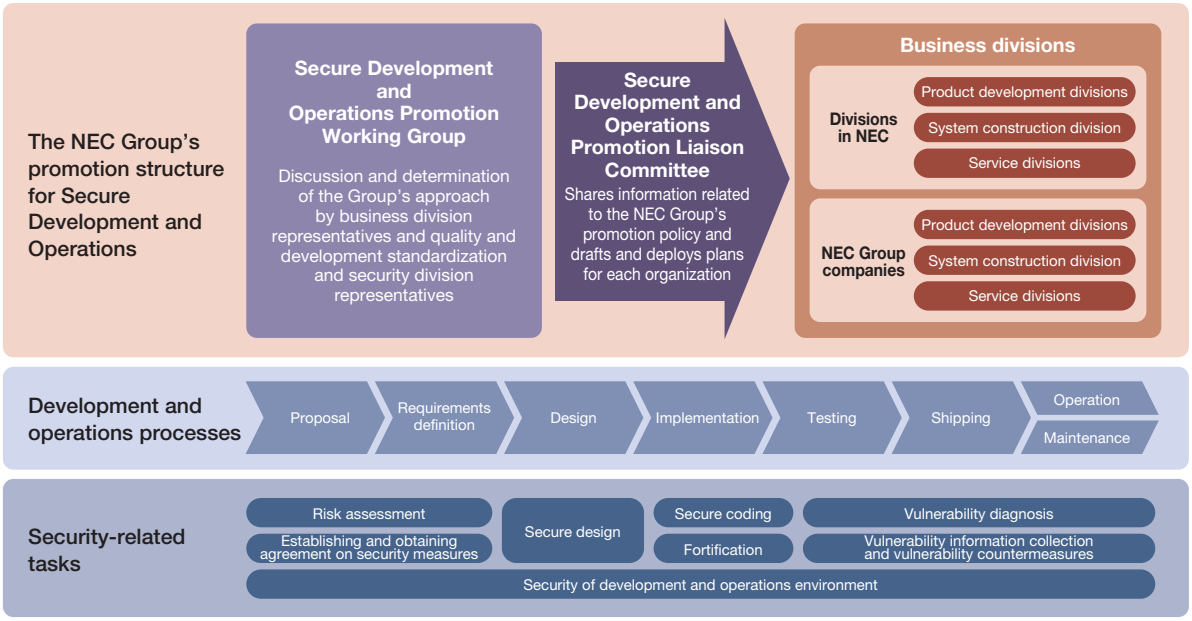
Additionally, practical matters such as tasks and standards to ensure security are established as guidelines and templates. As IoT-related security risks are increasing, risk assessment methods for IoT systems, specific security measures required for each model case (e.g., authentication, encryption), and other IoT security are being standardized.

### (3) Ensuring Security Quality

To ensure the security quality of our products, systems, and services, we use the “Secure Development and Operations Checklist” to ensure that security tasks (risk assessments, secure design, fortification, vulnerability assessments, etc.) have been implemented in each phase of development and operations. The check list has been designed with consideration given to various requirements such as ISO/IEC 15408 and other international security standards, the security standards of government agencies, and industry guidelines. The check list also reflects security measures to counter new threats in a timely manner.
Based on the check list, we have developed a tool to visualize the security situation. Approximately 7,000 business projects are managed under this system, allowing managers to efficiently assess and audit the security situation of their project.

### (4) Strengthening Security through Risk Assessments

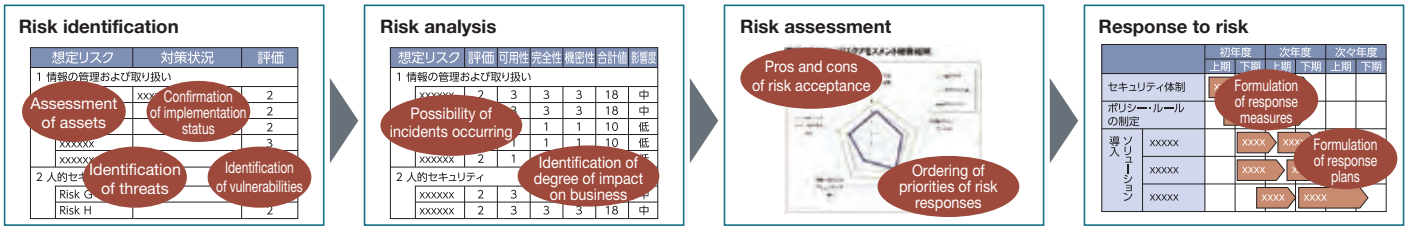
In recent years, it has been pointed out that management needs to take leadership in understanding and implementing measures against security risks.




**Secure Development and Operations Processes**

"Cybersecurity Management Guidelines Ver. 2.0", a revised guideline issued in November 2017, indicates that security measures are not limited to ensuring business continuity and improving defense capability against cyber attacks, but as it also plays an important role in improving profitability through the utilization of IT, investing in security is an essential responsibility of management. In order to properly invest in necessary security measures, it is believed that the ability to correctly judge target risks is vital, and with this in mind, NEC is focusing on the implementation of risk assessment. Risk assessment is the process of identifying and evaluating risks to the business, assets and other factors, and prioritizing risk measures accordingly. In general, risk assessment earlier on in the development process, such as during the customer system planning and proposal stages, makes it possible to select cost-effective security measures that maintain a balance between cost and safety. For this reason, NEC implements risk assessment from the beginning of the development process, ensuring the security of the products, systems, and services offered to customers.

Besides carrying out risk assessment within the company, NEC provides risk assessment services to customers. With the rise in the number of cyber attacks on control systems in recent years, we are also focusing efforts on offering risk assessment services for control systems that comply with security standards such as ISO/IEC 27001 and IEC 62443.




**The Flow of Risk Assessment**

## 2 Rapid Response to Vulnerabilities

### (1) Vulnerability Information Sharing Framework

To protect products, systems and services from cyber attacks, it is important to acquire vulnerability information as soon as possible and to take necessary measures. NEC implements a PSIRT*1 that manages vulnerabilities in order to quickly respond to the vast majority of vulnerabilities that are discovered on a daily basis. The PSIRT collects and analyzes vulnerability information and functions as POC*2 for communications with external organizations such as IPA*3 and JPCERT/CC*4. A framework for sharing vulnerability information, which is collected principally by the PSIRT, is being built for deployment throughout the NEC Group. Especially for vulnerabilities of a serious nature and having a particularly broad scope of influence, an early warning system has been installed to quickly detect such vulnerabilities and widely disseminate the information throughout the NEC Group.

NEC is a member of the Information Security Early Warning Partnership*5, and has set up an operation framework with close cooperation of IPA and JPCERT/CC. This enables us to be informed of vulnerabilities possibly affecting our products before the vulnerability information is publicly disclosed, allowing the product division to take necessary measures such as developing security patches and other countermeasure programs, and providing them to customers in conjunction with the announcement of the vulnerability.

*1: PSIRT: Product Security Incident Response Team
*2: POC: Point of Contact
*3: IPA: Information-technology Promotion Agency
*4: JPCERT/CC: JPCERT Coordination Center
*5: A public-private partnership for the smooth dissemination of vulnerability information on software products and web applications

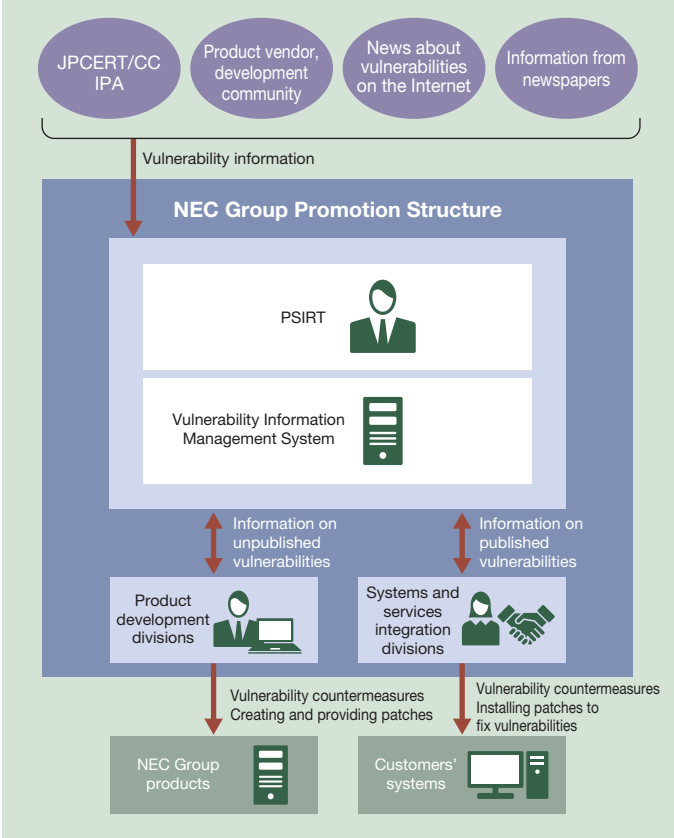
### (2) Collection and Dissemination of Vulnerability Information

NEC deals with vulnerabilities in two business areas: product development and services integration.

In the product development business, we obtain and handle vulnerability information related to NEC products through the aforementioned Information Security Early Warning Partnership.

In the services integration business, we obtain vulnerability information daily from various sources including product vendors, development communities and the Internet, and inform business projects of the vulnerabilities regarding the software they are using, thus ensure reliable and comprehensive security for customer systems.

We operate our own vulnerability information management system as infrastructure for deploying and managing the acquired information within the NEC group. Using this system, we are steadily disseminating and managing vulnerability information.




**Vulnerability Measures Promotion Framework**

# NEC's Cyber Security Strategy

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

## 1 Basic Policies

In a keynote speech titled "Shaping the Communications Industry to Meet the Ever-Changing Needs of Society" in October 1977, the NEC Group put forth C&C (Computer & Communication)" as its slogan for achieving the integration of computers and communications. In line with this declaration, by connecting the world's computers, we have been able to connect people with things and things with things, contributing to societal development that meets many of society's needs.

The NEC Group has built up and leverages many technologies that have supported infrastructure vital to society, from domestic traffic control systems, firefighting and disaster prevention systems, water management systems, ATMs, and logistics systems, to systems used in various fields from the ocean floor to outer space. In doing so, we are engaged in global development of total security that fuses the physical and the cyber.

Looking ahead, with the appearance of the IoT*1, automobiles, smart meters, and other objects will connect over cyber space to make our lives more convenient. At the same time, however, the threat of cyber attacks is becoming a global social issue, and the problem of "cyber-physical attacks"—attacks from cyber space that have an impact on the real world—is becoming more severe.

The scope of cyber security, too, is expanding beyond existing defense and detection, driven by research and development of new security technologies such as automatic prediction and protection using big data analysis, SDN*2, and cloud computing.

Among them are intelligence-based support for decision making (i.e., a machine learning solution) and an AI-based anomaly detection that localizes damage to the minimum by automatically disconnecting the affected system and appropriately responding to the event. We are making efforts toward the practical use of these technologies.

With regard to the physical, too, we are undertaking testbed demonstrations that analyze signal data from sensors and make use of cyber space in a variety of areas, including achievement of failure prediction, a solution to locate lost children by analyzing human behavior from surveillance camera footage, and tracking of stolen automobiles or items.

NEC will advance the fusion of the physical and the cyber, create secure cyber spaces, achieve a society and lifestyles rich with bright hope, and connect these to a better future.

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


**NEC's Business Domains That Support Social Infrastructure**

## 2 Investments in Cyber Security

### (1) Personnel and Technology

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

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

**Strengthening the Personnel Base**

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

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

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

**Establishment of endowed lecture series at the Japan Advanced Institute of Science and Technology (JAIST)** (November 2014) (October 2017)
Name of lecture series: "Cyber Range Organization and Design (CROND): Cyber Security Education and Training"

**24-hour monitoring system based on a follow-the-sun model** (October 2016) (March 2017)
Established Infosec Austria and Infosec America. Established a 24-hour security monitoring system (follow-the-sun model) using the time differences of three locations around the world.

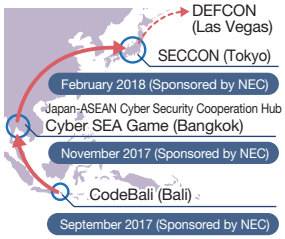
**Held NEC Security Skills Challenge** (February 2016)
Security technology contests held continuously since 2016 for the discovery and development of security talent with practical ability within the NEC Group

**Hired Mr. Kimiya Kimura, a pioneering cybercrime investigator, in Japan** (April 2017)
NEC hired Mr. Kimura, who has been active at the frontlines of cybercrime investigation. Mr. Kimura's duties include cyber-security-related solution planning and development, sales advice, personnel development, lectures, etc. He is also in charge of JC3 personnel development.

**Participation in IPA Industry Cyber Security Center** (April 2017)
NEC participates in the Center's personnel development program aiming to create the personnel, organizations, systems and technologies required for responding to cyber security risks to critical/social infrastructure.

**Acquired UK's IT service company NPS*5** (January 2018)
Accelerating overseas expansion of the safety business. ★5: Northgate Public Services Limited

**Global Personnel Development**
Through CodeBali*6 and the Japan-ASEAN Cyber Security Cooperation Hub*7, NEC holds CYDER exercises and security contests in various countries. The winning team participates in SECCON*8.




★6: An international conference hosted by Id-SIRTII/CC (a core organization of cyber security in Indonesia)
★7: A project of Japan-ASEAN Integration Fund 2.0 (JAIF) promoted by the Ministry of Internal Affairs and Communications
★8: Japan's largest security contest sponsored by Japan Network Security Association (JNSA)

In 2015, the Ministry of Economy, Trade and Industry and the IPA*9 released "Cybersecurity Management Guidelines" aimed at small-to-medium companies. Cyber security measures are now being advanced by many of our customers. However, faced with the pressing issue of a lack of cyber security personnel, NEC is making efforts to develop personnel in cooperation with a large number of customers, business partners, and related organizations.
The education programs offered by NEC contain a variety of programs such as training for targeted email attacks. Among these, in our cyber attack training program persons in charge of security in information system departments learn through actual experience with the flow of actions in incident handling, including incident discovery, reporting, identification of problem areas, isolation, analysis, and confirmation of damage status. Through this experience, we hope that the program will offer a venue for improvement of customers' technical capabilities and for confirming the sufficiency of cyber security measures for the ICT platforms that support customers.
This program is being adopted by more and more CSIRTs*10, helping customers not only in Japan but widely across the globe.

★9 IPA: Information-technology Promotion Agency, Japan
★10 CSIRT: Computer Security Incident Response Team

### (2) Strengthening Information Platforms

To strengthen information platforms against increasing cyber crimes, we collaborate with related organizations in Japan and overseas.

**Strengthening Information Platforms**

**Participation in Control System Security Center (CSSC)** (November 2013)
CSSC is a public-private partnership project of the Ministry of Economy, Trade and Industry for ensuring the security of critical infrastructure equipment and control systems

**Participation in Japan Cybercrime Control Center (JC3)** (November 2014)
This is an organization that gathers experience in dealing with threats in cyberspace across industry, academia, and law enforcement agencies. It aims to neutralize the root of cyber threats and mitigate damage.
NEC senior officer Takaaki Shimizu was appointed as representative director

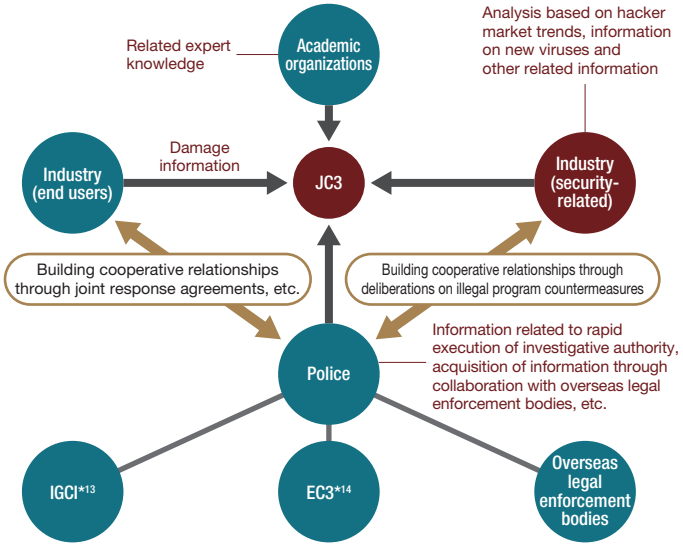
**Participation in the U.S. Department of Homeland Security AIS*11 initiative for public-private sector intelligence sharing** (March 2017)
NEC became the first Japanese company to join the AIS initiative of the U.S. Department of Homeland Security (DHS) for swiftly sharing intelligence on cyber threats between the government and the private sectors.
★11: Automated Indicator Sharing

**Participation in ICT-ISAC launch** (March 2017)
NEC participates in ICT-ISAC, which was established to enable a diverse group of operators to share information regarding the collection and analysis of information and countermeasures, and to counter threats as a collaborative and concerted organization, transcending the boundaries of the industry.
(NEC had been a participant of Telecom-ISAC, the predecessor of ICT-ISAC.)

**Participation in the Cross Sector Forum for Cybersecurity Workforce Development** (January 2016) (April 2017)
Together with NTT and Hitachi, Ltd., we established a study group for the development of cyber security personnel. In 2017, this study group transferred over to Cyber Risk Information Center (CRIC) and launched an initiative for information sharing.

In addition to participating in the Control System Security Center, in 2014 we participated in the Japan Cybercrime Control Center (JC3*12), and are contributing to the creation of a safe, sound, and comfortable environment by promoting government-industry-academia collaboration with domestic academic research organizations, industry, and legal enforcement bodies, by enhancing cyber crime response, and by returning the gains from these activities to society.

★12 JC3: Japan Cybercrime Control Center




★13 IGCI: The INTERPOL Global Complex for Innovation ★14 EC3: European Cybercrime Centre

**Framework Centered on the Japan Cybercrime Control Center**

In a bid to strengthen the global fight against cybercrime, NEC signed a partnership agreement with INTERPOL in 2012 to fight cybercrime in the INTERPOL Global Complex for Innovation (IGCI) in Singapore. NEC delivered a digital forensic platform and various other technical resources for IGCI, which began full operations in 2015. IGCI offers essential assistance for national authorities in terms of investigating and identifying cyber crimes and criminals, research and development in the area of digital crime, and digital security.


**Operation Center (Cyber Fusion Centre)**

## 3 Global Expansion

### (1) Trends in Cyber Security around the World

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

### (2) Global Safety

NEC has long supported critical social infrastructure in Japan by providing safe, secure, and comfortable environments. Looking ahead, we will continue to leverage our personnel and high technological capabilities to provide total security in both the physical and cyber worlds, including the world's most accurate face and fingerprint recognition systems, national ID management systems, and payment networks. Already, NEC is rolling these out in the U.S., South Africa, Brazil, and Asian countries, while in the APAC (Asia Pacific) region, we are increasing our presence each year as a top-class security consultant and MSS*15 vendor. To meet the expectations of customers around the world, in January 2016 NEC opened a cyber security center in Singapore and will continue to accelerate the global rollout of security solutions.

*15 MSS: Managed Security Service

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

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


**Rollout of Global Safety Around the World**

## 4 Globalization of Security Operations Centers (SOCs)

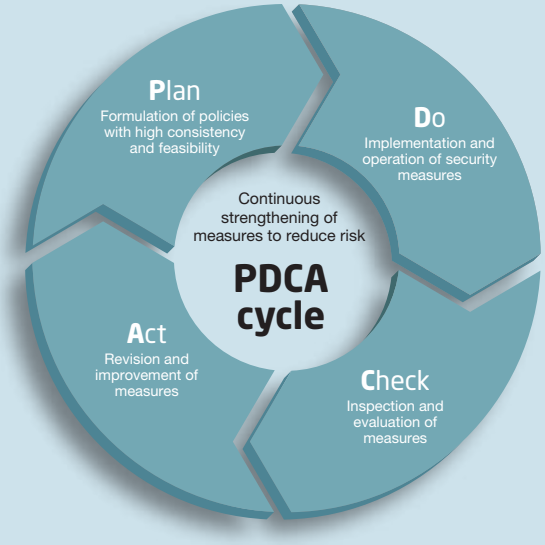
To protect critical infrastructure and our many customers' ICT infrastructures in Japan from the threat of cyber attacks, NEC is exerting the Group's collective power to roll out Security Operations Centers (SOCs).
Among our multiple SOCs in Japan, we established the Cyber Security Factory that started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

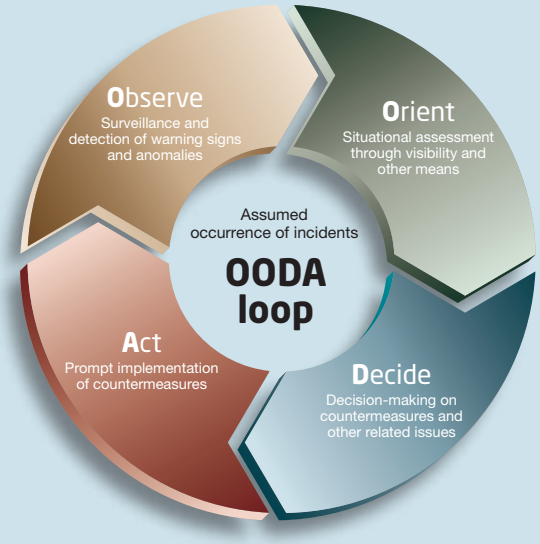

**Cyber Security Factory**

## 5 Support for Strengthening Security Based on In-House Operational Expertise

### NEC keeps on strengthening proactive measures to reduce risk from cyber attacks and achieve stronger security across the entire group.

Merely implementing required measures does not complete our cyber security. In order to counter increasingly advanced and sophisticated cyber attacks comprehensively, it is important to continuously enhance security measures in a planned and systematic manner. In addition to strengthening the security of the entire group through effective combination of various security measures, NEC supports ongoing activities for fixing vulnerabilities based on a PDCA cycle, which consists of formulating policies, implementing measures, assessing the results, and considering improvement.




### Supports appropriate situational assessment and prompt response in the event of an incident

In addition to security risk management through a PDCA cycle, it is particularly important in preparation for cyber attacks to consider measures in case incidents such as unauthorized intrusions and/or malware infections actually occur. Rapid detection of anomalies and prompt decision making/response in case of emergencies can reduce the damage. To support appropriate and immediate incident response, NEC incorporates the concept of the OODA loop that consists of recurring "Observe" "Orient" "Decide" and "Act" phases.

**PDCA Cycle and OODA Loop**

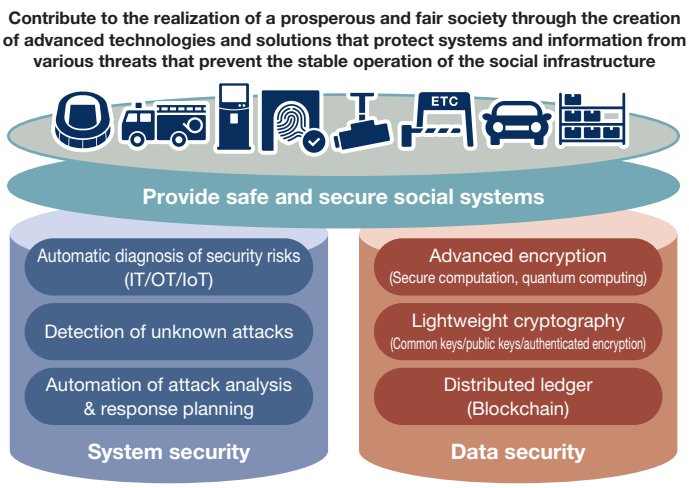
# R&D at the Leading Edge of Cyber Security Technology

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

## 1 Concepts for Research Themes

Under the slogan “Futureproof security -- Beyond the frontlines of cyber security,” NEC conducts research and development in both system security and data security suitable for increasingly advanced social infrastructure, and provides customers with safe, secure, and comfortable environments by establishing social infrastructure that does not stop, break, or malfunction.
In the area of system security, NEC is developing cutting-edge security technologies to counter increasingly advanced and sophisticated cyber attacks. Among them are automatic diagnosis of security risks using AI, detection of unknown cyber attacks, automatic analysis of attack methods and their impact on systems, automatic planning of effective countermeasures, and so on.
In the area of data security, NEC is working to eradicate information leakage incidents through the development of “Secure Computation” that allows data to be processed while remaining encrypted, and “Lightweight Cryptography” to implement an encryption function on IoT*1 devices.

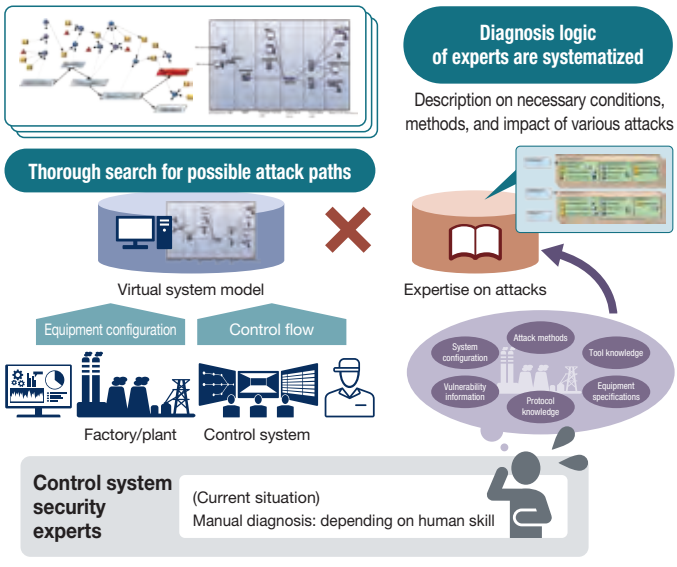
*1 IoT: Internet of Things




NEC’s Security Research

## 2 Automatic Security Risk Diagnosis Technology

This technology comprehensively identifies the security risks latent in “unstoppable” systems such as those in factories and plants. By modeling a complex control system in a virtual space, it explores the possibility that an attack might reach the target that requires protection (an attack path), and identifies physical damage that might be caused by the attack. Further, in collaboration with control system security experts, the technology configures computers to automatically perform diagnosis based on the concentrated knowledge and experience of the experts about various attacks. As a result, security diagnosis can be carried out at any time using the latest attack knowledge without affecting the operation of the system.




Automatic Security Risk Diagnosis Technology

## 3 Security Using AI

### (1) AI for Analyst Support

While techniques of targeted attacks are becoming more and more diversified and personalized, AI is starting to be used as a countermeasure and turning out to be effective by automatically detecting malware and its behavior. Unlike conventional methods based on signatures and rules, AI using machine learning technology can detect variants and unknown malware, presenting a solution to deal with the diversification of attacks. However, while AI based on machine learning does not require manual input of knowledge, it needs a large amount of training data. In the case of targeted attacks directed at specific victims, it may not be possible to collect sufficient amount of data for training. Moreover, it is

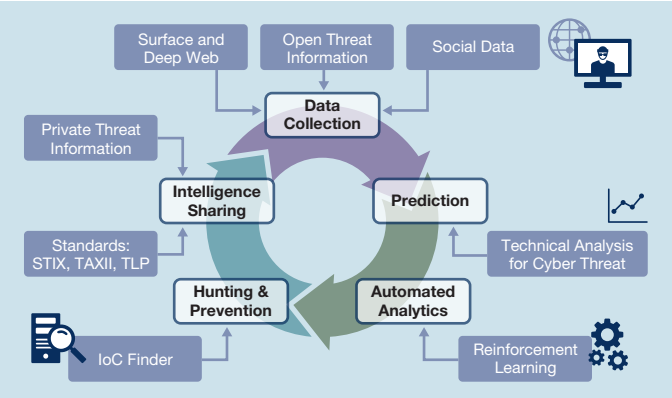
not easy for security analysts to verify or partially change the judgment criteria the AI learned.
To overcome these limitations, NEC is conducting research on new AI technology based on logical thinking. In responding to an incident, for example, this new type of AI tries to estimate the situation of the attack by understanding the context, and solve the problems in collaboration with humans. AI based on logical thinking has advantages over its machine-learning counterpart: it can present the result derivation process in a manner understandable to humans, and easily add/modify knowledge for analysis. With this technology, we are focusing on development of new IoT security. In this new process, it collects fact data relating to anomaly detected by sensors as much as possible, and estimates the behavior of the malware and/or even the attacker. Through analysis, it constructs a flow to the estimated final goal of the attack, and verifies the entire attack process by comparing assumed operations in each phase with the obtained facts. After the identified attack flow is determined to be almost correct, then it identifies the procedures to block the attack and submits the results to the human analysts for confirmation.
By combining the benefits of two different technologies, machine learning and logical thinking, AI will be able to support human analysts in responding to sophisticated cyber attacks more efficiently. NEC believes this is the future of security utilizing AI.

### (2) AI for Threat Analysis Using Open-source Intelligence

The importance of open-source intelligence in cyber threat analysis is increasing as attackers frequently post their intentions on social media that they are planning to target critical facilities and major companies in the world, and as attacking tools and services are traded on the deep web*2.

Under such circumstances, NEC is developing new technologies for detecting signs that a threat trend is close to its peak by applying technical analysis methodologies used in financial engineering, as well as technologies for grasping the whole picture of a cyber attack through analysis based on deep reinforcement learning, a type of machine learning. By combining these technologies, we will be able to use a huge amount of open-source information for rapid and appropriate automatic prevention against cyber attacks.
NEC is as committed as ever to advancing its research and development on cyber attack prevention technologies in order to realize a safe, secure and sustainable society.

*2: Websites that are inaccessible by conventional search engines




**Security Management**

## 4 Cryptography and Secure Computation

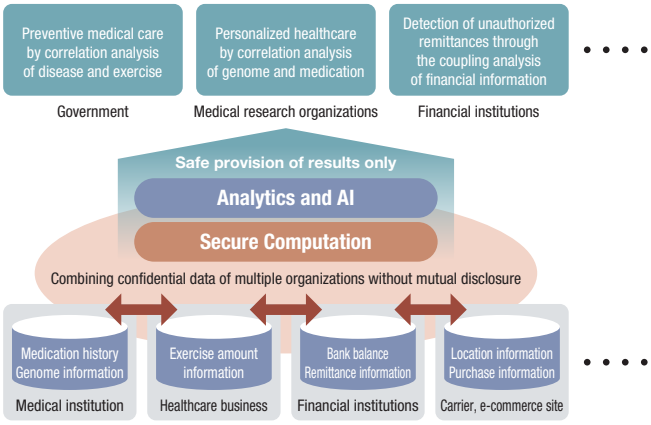
### (1) Lightweight Cryptography

In 2012, NEC announced TWINE, a lightweight block cipher which realizes world-class lightness and high processing performance even on resource-constrained IoT devices, and in 2015, OTR*3, an authenticated encryption method that cuts the conventional data processing volume in half (a theoretical limit). These cryptosystems make it possible to safely connect sensor devices placed in a variety of environments to cyberspace.

*3 OTR: Offset Two-Round

### (2) Secure Computation

Secure computation allows data to be processed while remaining encrypted, thereby strongly protecting data from malware or internal abuse.
Performance has been the bottleneck of this technology, but in 2016, NEC succeeded in developing a method that dramatically improves performance through multiparty computation, which allows multiple servers to jointly compute distributed data while keeping it secret. In the demonstration conducted on an authentication system, it achieved more than 10,000 authentication processes per second, proving that the technology can be practically used even in large organizations. In addition to information leakage prevention, multi-party computation allows multiple organizations to share their confidential data while keeping it private, enabling participants to obtain insight from data more easily. We will carry out further research and development of multi-party computation to bring this technology to the market as a core of data utilization platforms.




**Data Utilization by Secure Computation**

## 5 Cloud Technologies

### Secure Storage Archives

With the proliferation of cloud storage services, important data is increasingly stored in the cloud. NEC is undertaking research and development into a technology to safely store and utilize this data so that it can be put to greater use.

With this technology, we encrypt data using a technology for secret sharing, apply distributed storage and redundancy, and perform periodic high-speed inspections, automatically restoring data even in the case of loss.
This technology assures confidentiality, integrity and availability, and creates new value that allows customers to use cloud services safely, securely, and efficiently.

# Third-party Evaluations and Certifications

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

## 1 ISMS Certification

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

### NEC Group Companies with ISMS Certified Units

- NEC Corporation
- ABeam Consulting Ltd.
- ABeam Systems Ltd.
- NEC VALWAY, Ltd.
- NEC Space Technologies, Ltd.
- NEC Solution Innovators, Ltd.
- NEC China Soft (Japan), Ltd.
- NEC Nexsolutions, Ltd.
- NEC Networks & System Integration Corporation
- NEC Network and Sensor Systems, Ltd.
- NEC Fielding, Ltd.
- NEC Fielding System Technology, Ltd.
- NEC Platforms, Ltd.
- Infosec Corporation
- KIS Co., Ltd.
- Cyber Defense Institute, Inc.
- Sunnet Corporation
- brees corporation
- YEC Solutions Inc.
- Q&A Corporation
- NEC Shizuokabusiness, Ltd.
- Showa Optronics Co., Ltd.
- NEC Aerospace Systems, Ltd.
- NEC Communication Systems, Ltd.
- Forward Integration System Service Co., Ltd.
- LanguageOne Corporation

## 2 Privacy Mark Certification

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

### NEC Group Companies with Privacy Mark

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

## 3 IT Security Evaluations and Certifications

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

### NEC products and systems with ISO/IEC 15408 certification

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

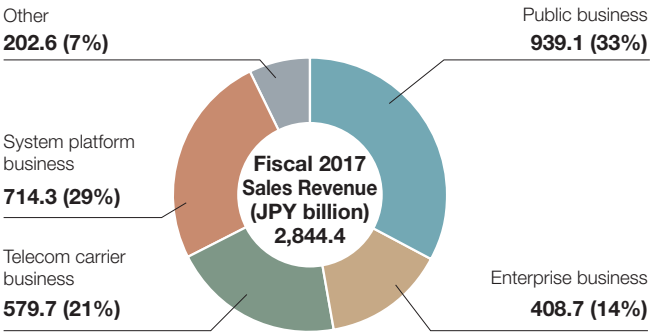
## Corporate Profile

| | |
|---|---|
| Company name: | NEC Corporation |
| Address: | 7-1, Shiba 5-chome, Minato-ku, Tokyo, Japan |
| Established: | July 17, 1899 |
| Capital: | ¥397.2 billion* |
| Number of employees: (Consolidated) | 111,200* |
| Consolidated subsidiaries: | 303* |

*As of March 31, 2018

## Segment Information

### Sales Revenue by Segment (Percentage)




*As of March 31, 2018

## NEC Way

### The NEC Way:

NEC has established the "NEC Way" that represents a frame of mind and commitment to work that is necessary for each person in the NEC Group.
The basis of practicing or implementing a corporate philosophy is found in the behavioral guidelines such as the sense of ethics, the "Charter of Corporate Behavior" or the "Code of Conduct" as defined by the NEC Group.
To achieve the "NEC Group Vision", the ideal corporate model, and "Orchestrating a brighter world", the ideal model of society that NEC wants to realize, each employee works daily by following the four "NEC Group Core Values" (passion for innovation, self-help, collaboration, better products and better services), behavioral principles and code of conduct. In 2016, NEC defined the personnel required for the social value creation initiative as those who have a heightened and broad perspective and are able to successfully challenge boundaries and achieves goals ("HR philosophy").


### 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

The NEC Group Vision states what we envision as a company, and the society which we will strive to realize in pursuing our Corporate Philosophy.

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, 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<br>• Question the existing ways and develop new ways<br>• Unite the intelligence and expertise around the world |
| [ As an individual ] **Self-help** | • Act with speed<br>• Work with integrity until completion<br>• Challenge beyond own boundary |
| [ As a team member ] **Collaboration** | • Respect each individual<br>• Listen and learn with open mind<br>• Collaborate beyond organizational boundaries |
| [ For our customers ] **Better Products, Better Services** | • Think from a user's point of view<br>• Impress and inspire our customers<br>• Continue the pursuit of "Global Best" |


## NEC Corporation

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


Issued July 2018