

**Information Security**

NEC recognizes that it is our duty to protect the information assets entrusted to us by our customers and business partners as well as our own information assets in order to provide better products and services and contribute to the development of society. Accordingly, we have codified this commitment in the NEC Information Security Statement.

**NEC Information Security Statement**

**Policy**

The NEC Group has established an "Information Security Promotion Framework" by which we endeavor to realize a secure information society and offer value to our customers through the protection of the information assets entrusted to us by our customers and business partners; the provision of reliable products, services, and information solutions; and the proper reporting and disclosure of information to our stakeholders.

As part of our information security initiatives to protect information assets, we combined the four elements of "Information Security Management," "Information Security Platform," "Information Security Staff," and "Information Security Governance" to comprehensively maintain and enhance information security on multiple levels. (For details, please refer to the Information Security Report 2016 "Information Security Promotion Framework."

[Diagram of Information Security Promotion Framework]

**Information Security Report**
Promotion Framework

NEC’s information security promotion organizational structure consists of the Information Security Strategy Committee and its subordinate organs, as well as the promotion structure at each organization. To handle information security risks, which include cyber security risks, the Information Security Strategy Committee, chaired by the Chief Information Security Officer (CISO), deliberates important issues such as the decision, assessment, and improvement of information security reinforcement measures, the clarification of the causes of severe incidents and decision on measures to prevent reoccurrence, and the reflection of achieved results into NEC’s own information security business. The three subordinate organs (a sub-committee and two working groups) under the Information Security Strategy Committee perform various tasks that include discussion and coordination of implementation plans and measures to be executed, as well as enforcement of directives and monitoring of progress of various measures for Group companies worldwide, for business partners, and for driving the Secure Development and Operations initiatives.

Information security managers of each organization have the primary responsibility for managing information security for their organization, including the Group companies under their supervision. They are tasked with maintenance and improvement of security by continually ensuring the dissemination of rules within the organization, implementing security measures, inspecting and reviewing implementation status, and improving measures as necessary.

Main Activities and Results for Fiscal 2016

| Strengthening Global Information Security Infrastructures |

NEC has completed the global deployment of the integrated management platform that enables the visualization*1 of the status of information security measures for PCs (e.g. installation of security patches, malware countermeasures, and PC encryption) at overseas subsidiaries.

We have initiated preparations towards the adoption of the Global Cyber Attack Protection System (GCAPS), which is aimed at reinforcing measures against PC and server vulnerabilities and optimizing responses to security incidents, in some subsidiaries in the APAC region and subsidiaries in the Latin American region.

“Visualization”*1 in this context refers to systems for quantitatively confirming the status of information security measures at overseas subsidiaries, which includes, for example, security patch installation and implementation rates for PC encryption measures. Information Security Managers at the Management Information Systems Division, at regional headquarters, and at local subsidiaries confirm the status of their measures and take specific actions to further improve their information security.
Targeted attacks, which are a form of cyberattack targeted at a specific company or organization, are increasingly becoming more advanced and sophisticated each year. To counter this threat, we developed the Global Cyber Attack Protection System (GCAPS), which provides a mechanism for proactively identifying vulnerable areas within our Intranet in advance (proactive measures), as well as a rapid incident response framework for promptly assessing the status of an intranet attack, for blocking the spread of intrusion, and for restoring affected systems (rapid Computer Security Incident Response Team [CSIRT] action). For fiscal 2017, we plan to deploy GCAPS within NEC Group companies in Japan.

Also, to improve technical skills of incident response personnel (CSIRT), NEC conducted exercises, drills, and in-house security contests (Capture the Flag [CTF]). As with the previous year, we also conducted targeted attack drills to sharpen employees’ awareness against suspicious emails.

We also started the global deployment of measures against cyber attacks (detection of unknown malware, log/packet analysis, CSIRT establishment) first for the APAC region and for overseas research laboratories. Going forward, we will expand the coverage area for deployment and establish CSIRTs in other overseas subsidiaries.
Promoting and Enforcing Secure Development and Operations

Aiming to reduce the burden for dealing with vulnerability threats in development project sites, we started operating a service for verifying operation and effects to systems of patches aimed at fixing vulnerabilities related to customers’ systems. Currently, we are making sure that measures for fixing vulnerabilities are being implemented in each project by sharing results of vulnerability tests within the NEC Group.

Also, in accordance with the Cybersecurity Management Guidelines formulated in 2015 by the Ministry of Economy, Trade and Industry (METI) and the Information-Technology Promotion Agency, Japan (IPA), we issued documents that support the preparation of customer system proposals (includes implementation guidelines for compliance with the said Cybersecurity Management Guidelines). Going forward, we will aim to expand business by adopting these documents in on-site projects.

Further, in order to reinforce and promote global implementation of our Secure Development and Operations initiatives, we prepared mechanisms for confirming, through pre-order acceptance screening for overseas projects, that security requirements were surely presented to the customer, and for lending tools and providing services for vulnerability assessment. Going forward, we will deploy these mechanisms horizontally beginning at the APAC region, eventually expand to other regions, and enhance capabilities of assessment team members.

Monitoring and Improvement

Information Security Assessment Activities

Every year, NEC confirms the status of implementation of security measures through information security assessments and conducts activities to propose and execute improvement plans.

In fiscal 2016, information security assessments were conducted at 62 NEC Group companies in Japan. Assessments were conducted both by general employees as well as by managers of specific security measures to confirm the status of measure implementation based on their respective roles (personal assessment). We were able to improve effectiveness by accurately assessing the actual on-site security situation.

These ongoing activities ensure that information security measures for the entire NEC Group are continually being implemented and improved. There remains, however, room for improvement for some of these measures, and we issued reminders for their thorough implementation within the NEC Group.
Personal assessments were also conducted at 40 overseas subsidiaries, which enabled a detailed grasp of their security measures, and further raised awareness and recognition among them.

### Assessment of Business Partners

On the basis of the "Information Security Standards for NEC Group Business Partners", the "Basic Rules for Customer-Related Work for Business Partners" and other related guidelines, we conducted assessments and evaluations of the implementation status of information security measures in business partners (through on-site assessment and Web-based self-assessment by business partners themselves). We provided business partners with feedback on evaluation results, and thoroughly implemented improvements.

In fiscal 2016, Web-based self-assessment was carried out in approximately 1,600 companies and on-site assessment in approximately 100 companies.

These ongoing activities ensure that information security measures for business partners are continually being implemented and improved. There remains, however, measures that have relatively low implementation rates compared to other measures, and we requested concerned business partners to conduct thorough implementation of such measures.

### Assessment of Security Measures for Products and Systems Provided to Customers

By promoting a system that visualizes the progress of security measures for customer projects within the NEC Group, we were able to identify projects for which measures for secure development, operation, and maintenance were inadequate, and continued to make the necessary improvements.

### Objectives and Achievements

#### Objectives for the Medium Term (From fiscal 2014 to fiscal 2016)

As a global company that provides ICT essential to social infrastructures, NEC will contribute to society by protecting information assets entrusted to it by customers and business partners and its own information assets, as well as by providing even more secure, reliable and trusted products and services, and information security solutions.
### Fiscal 2016 Objectives, Achievements and Progress, and Degree of Completion

(Degree of completion: achieved ○ /mostly achieved ○ /some progress △ /no progress ×)

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Achievements and Progress</th>
<th>Degree of completion</th>
</tr>
</thead>
</table>
| 1. Strengthening global information security infrastructures             | • In addition to revision and implementation of information security rules for overseas subsidiaries, we identified the actual situation (device regulation and use of smart devices) of information security measures in each subsidiary, and gave instructions for improvement.  
  • We initiated preparations for the introduction of the Global Cyber Attack Protection System (GCAPS) in some subsidiaries in APAC and Latin America. | ○                    |
| 2. Strengthening measures against cyber attacks                           | • We developed the platform for deploying GCAPS, which is capable of countering the latest cyber attacks, in NEC Group companies in Japan.  
  • We implemented various activities (drills, exercises, in-house CTF contests, etc.) aimed at improving skills of CSIRT personnel.  
  • We initiated the global deployment of cyber attack countermeasures (unknown malware detection, log/packet analysis, CSIRT establishment) beginning with APAC and overseas research laboratories. | ○                    |
| 3. Promoting and enforcing Secure Development and Operations             | • We started operating a service for verifying security patches for customer systems, and ensured the leveraging of results in local projects and thorough implementation of measures against vulnerabilities.  
  • We issued documents based on the "Cybersecurity Management Guidelines" to support the preparation of customer system proposals.  
  • We prepared mechanisms for confirming, through pre-order acceptance screening for overseas projects, that security requirements were surely presented to the customer, and for lending tools and providing services for vulnerability assessment. | ○                    |
### Objectives for the New Medium Term (From fiscal 2017 to fiscal 2019)

As a global company that provides ICT essential to social infrastructures, NEC will contribute to society by protecting information assets entrusted to it by customers and business partners and its own information assets, as well as by providing even more secure, reliable and trusted products and services, and information security solutions. Also, NEC will fast-track the global implementation of human resource development and construction of mechanisms to counter cyber attacks that are expected to increasingly become more advanced and sophisticated.

### Fiscal 2017 Objectives

<table>
<thead>
<tr>
<th>1</th>
<th>Strengthening measures against cyber attacks (Japan, overseas)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Deploy GCAPS within Japan and expand global deployment of cyber attack countermeasures, in order to strengthen measures against increasingly sophisticated and advanced cyber attacks</td>
</tr>
<tr>
<td>2</td>
<td>Strengthening global security infrastructures</td>
</tr>
<tr>
<td>2.1</td>
<td>Increase the level of information security at overseas subsidiaries to the level in Japan</td>
</tr>
<tr>
<td>3</td>
<td>Promoting and enforcing Secure Development and Operations</td>
</tr>
<tr>
<td>3.1</td>
<td>Implement the mechanisms for efficiently providing customers with secure products, systems, and services to local projects, train leaders to enable them to drive Secure Development and Operations initiatives in the field, and expand business growth</td>
</tr>
</tbody>
</table>