The Measures Applied Internally by the NEC Group to Forestall and Prevent Cybersecurity Incidents

YOSHIDA Atsumasa

Abstract

The NEC Group currently deploys proactive cybersecurity measures both inside and outside Japan in order to protect companies from the cyberattacks that are becoming increasingly sophisticated and advanced. Our security resources have been developed based on expertise accumulated over more than two decades, as well as on information sharing with external organizations including expert international security agencies and police forces. The group is also promoting the practical implementation of a system for localizing cyberattack damage by applying AI (Artificial Intelligence) and SDN (Software Defined Networking) technologies. This paper introduces the cybersecurity measures enhanced globally across the NEC Group, together with details of the existing information security infrastructure that the group is applying to protect customer information and other confidential data[1)].

Keywords

cybersecurity, AI, SDN, ASI, GCAPS, NCSP, CSIRT, malware, cloud authentication linkage, multi-factor authentication, InfoCage, OMCA

1. Enhancement of Cybersecurity Measures

Under the recent sophistication and advancement of cyberattacks, the NEC Group positions the enhancement of cybersecurity as the most important measure for it and deploys various activities in the NEC Group inside and outside Japan under the leadership of the CISO (Chief Information Security Officer). The following sections introduce some of the main activities.

1.1 Cybersecurity Risk Analysis

The NEC Group analyzes the risks of cyberattack threats that occur in daily business operations, including targeted attacks, ransomware (a kind of malware that encrypts files and then demands a ransom in exchange for decryption), and indiscriminate email attacks (attacks aimed at unspecified, large numbers of people), and implements measures against cyberattacks based on the analysis results. NEC sorts risk analysis into four types including the "cyber threat analysis" (assessment of the status and characteristics of cyberattacks on the NEC Group and consideration of responses in accordance with the threat risk), "monitoring operations analysis" (appropriate reviews of the current monitoring processes), "solution and IT analysis" (analysis of the applicability of countermeasure products and services to the Group's internal IT environment) and "countermeasure analysis" (investigation of the countermeasures required by the NEC Group).

1.2 Global Measures against Cyberattacks

The NEC Group formulates annual plans for countermeasures based on cybersecurity risk analysis, and implements the countermeasures with the approval of the CISO.

As a company that deploys Solutions for Society on a global scale, the NEC Group understands that adopting a globally unified approach to cybersecurity risks is vital for business continuity.

The global cyber security measures of the NEC Group broadly focus on four areas; 1) detecting unknown attacks; 2) integrating log management/Intensifying monitoring; 3) deploying GCAPS and; 4) establishing CSIRT organizations (**Fig. 1**).

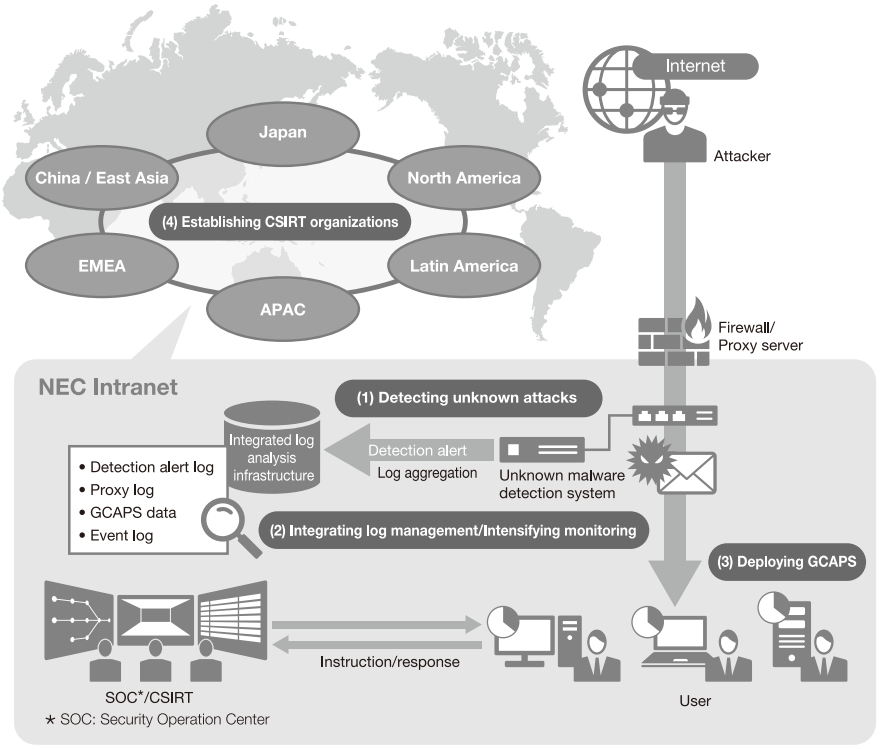

Fig. 1 Overview of countermeasures against global cyberattacks.

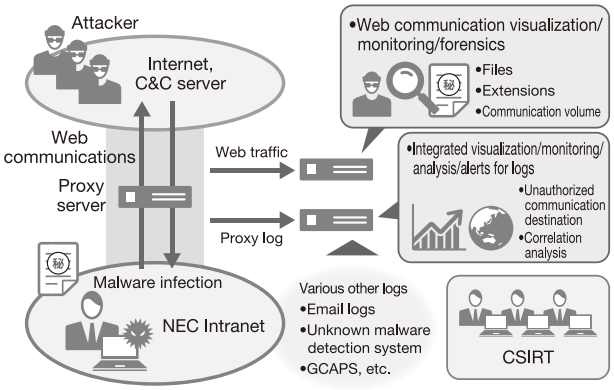

Fig. 2 Integrated analysis of logs and investigation of packets.

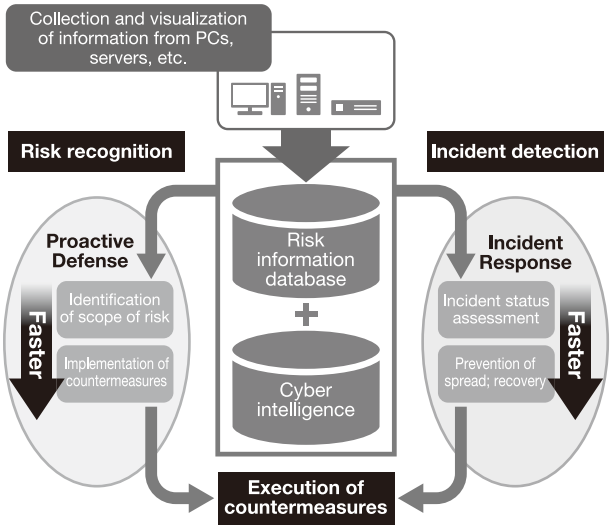

Fig. 3 Concept of GCAPS.

(1) Detecting unknown attacks

As entrance and exit countermeasures, the NEC Group implements unknown malware detection systems, monitors web communications and in-coming emails, and, based on information about detected unknown malware, filters out improper communications and take measures to handle PCs and servers suspected of infection.

(2) Integrating log management/intensifying monitoring

The NEC Group performs integrated log management over the Group's 180,000 PCs and servers and the logs collected from security products, thus making the log analysis more effective and comprehensive. The group also conducts relational analysis of multiple logs to identify possible risks, which will enable us to reduce the risk of information leakage (**Fig. 2**).

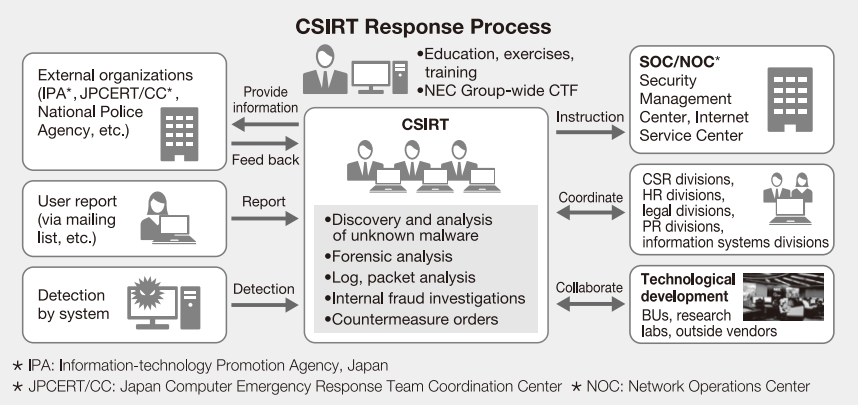

Fig. 4 Overview of CSIRT.

(3) Deploying GCAPS

NEC is rolling out the GCAPS (sold externally as a solution under the name NCSP, or NEC Cyber Security Platform) to the entire Group, for the purposes of strengthening measures related to PC and server vulnerabilities and increasing the efficiency of incident response.

With GCAPS, the NEC Group will globally strengthen measures related to PCs and servers from two standpoints: "Proactive Defense" performed on the basis of risk recognition, and "Incident Response" when an incident has been detected (**Fig. 3**).

(4) Establishing CSIRT organizations

The NEC Group has established a CSIRT in Japan, headed by the CISO. This CSIRT monitors for cyberattacks, 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 cyber intelligence based on detected cyberattacks and unauthorized communications among group companies across the globe, thus enabling the CSIRTs of the entire group to work together smoothly (Fig. 1 and **Fig. 4**).

Members of the CSIRT undergo training and exercises to improve their technical skills, as well as participate in the Group-wide CTF (Capture The Flag) security contest. The NEC Group also conducts comprehensive exercises with top management to enhance the ability of the entire organization to respond appropriately to security incidents.

1.3 Proving the Value of NEC's Advanced Technologies

The NEC Group is validating and ensuring the value of its cutting-edge cybersecurity solutions that adopt SDN and AI by testing and using them in actual IT environments, thereby driving the progress of NEC's focused technology areas and building internal reference cases of advanced technologies.

(1) Incorporating SDN into measures against cyberattacks

The NEC Group validated the value of its automated cyberattack protection system that uses SDN to quickly localize the damage from malware infection caused by a ransomware or targeted attack. The test was completed and the system is currently in production in the NEC Group environment.

(2) ASI (Automated Security Intelligence)

The NEC Group is working together with its laboratories to validate the value of NEC's Automated Security Intelligence (ASI) solution that detects abnormal situations of systems by leveraging machine learning AI technology. The solution is currently being evaluated in the actual IT environment of NEC Asia Pacific in Singapore about the accuracy and performance in detecting unknown attacks at endpoints and tracing the source of attacks. Results of the evaluation are used as a feedback for taking the ASI solution to the market.

2. Information Security Infrastructure

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

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

2.1 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. The NEC Group is currently strengthening its authentication infrastructure for user management and control. Main strengthening measures including the "linkage between authentication infrastructure and cloud services" and "multi-factor authentication" are described in the following.

(1) Linkage between authentication infrastructure and cloud services

In today's diverse business environment, there is a growing need to share information with people outside the company and utilize cloud services. The NEC Group has therefore created a system whereby cloud services are linked to the Group's internal authentication infrastructure, enabling cloud services to be used safely and securely (**Fig. 5**).

(2) Multi-factor authentication

To strengthen measures against internal fraud and cyberattacks (targeted attacks), the NEC Group not only implements user IDs and passwords (knowledge-based authentication) for controlling access to systems handling critical information, but also promotes the employment of personal authentication using digital certificates (possession-based authentication). The group intends to further combine this with face recognition (biometric authentication).

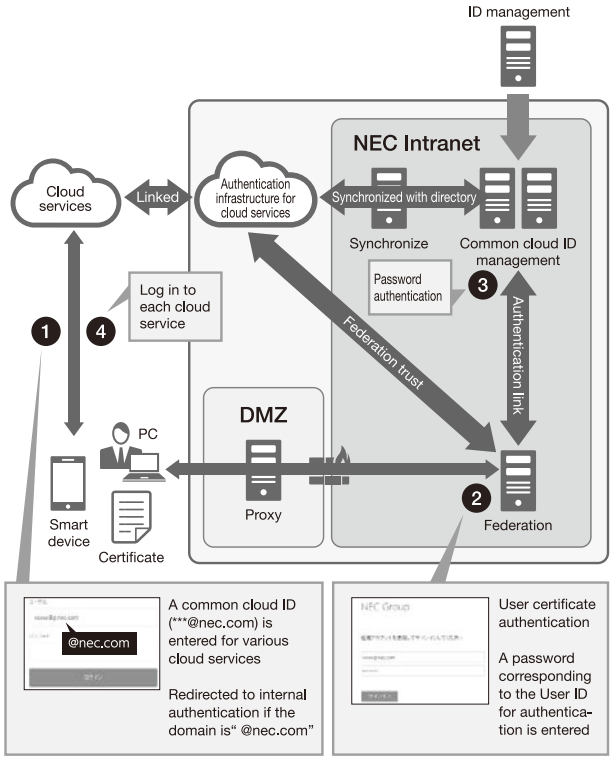

Fig. 5 Cloud authentication linkage.

2.2 IT Platform for PC and Network Protection

NEC has constructed an IT platform to protect the group's PCs and networks from viruses, worms, and other attacks and maintain the security of information devices connected to the NEC Intranet. In addition, in order to address increasing risks of targeted attacks, it is important to install all necessary security updates and antivirus software.

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 them makes possible monitoring of appropriate software use by the users.

When a PC for which security measures are not sufficiently implemented or a LAN infected by malware is connected to the NEC Intranet, that PC or LAN is automatically disconnected from the NEC Intranet. The NEC Group also controls communications to people or organizations outside the group by using web access filtering, prohibiting the use of free email accounts, using sender domain authentication, and other methods.

The NEC Group checks vulnerabilities in the information devices connected to the NEC Intranet by using a vulnerability detection tool and manages the found vulnerabilities centrally by the system. The vulnerabilities are corrected by each department but the correction status is also centrally managed by the system, allowing the status of the entire NEC Group to be easily ascertained.

2.3 IT Platform for Information Protection

It is necessary to identify channels that can lead to information leaks, analyze risks and take appropriate measures to prevent leaks. As the NEC Group manages not only its own information but information entrusted

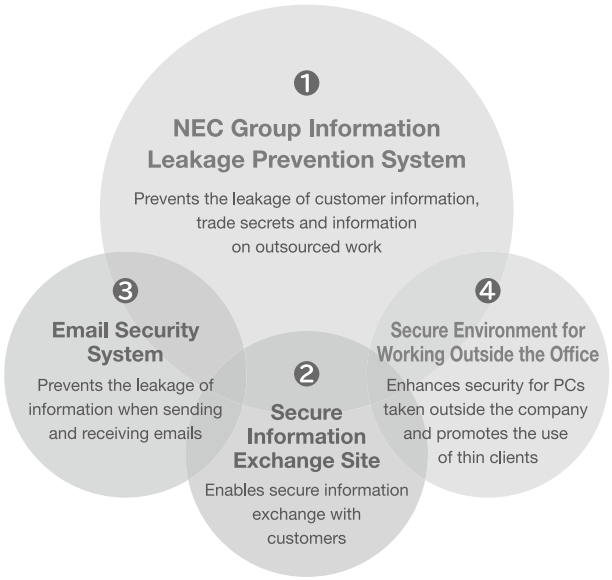

Fig. 6 Overview of IT platform for information protection.

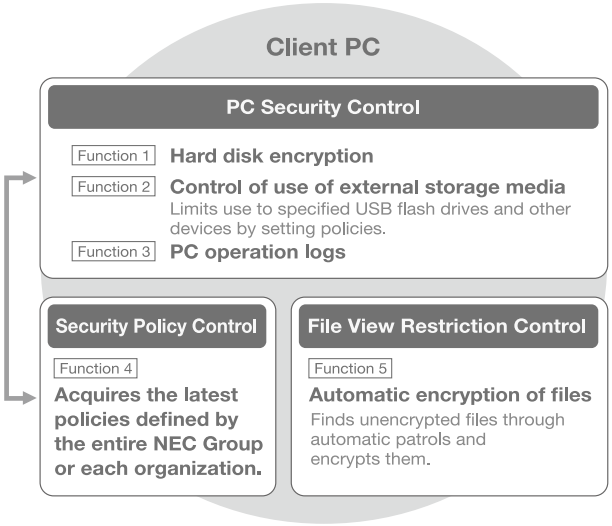

Fig. 7 Overview of information leakage prevention system.

to it by customers and information disclosed to business partners, the group implements comprehensive and multilayered measures for each channel that might lead to an information leak (malware infection, email exchange, external storage media, devices taken outside the company) while considering the characteristics and risks of networks, PCs, external storage media, and other IT components (**Fig. 6**).

(1) NEC group information leakage prevention system

The NEC Group has constructed an information leakage prevention system that uses its InfoCage series of products. By implementing "encryption (through adoption of InfoCage FileShell)," "device control" and "log recording/monitoring," the group counters the risk of information leakage caused by external attacks or internal misconduct (**Fig. 7**).

(2) Secure information exchange mechanism

The NEC Group operates a secure information exchange site to safely and reliably exchange important information with customers and business partners. NEC conducts the exchange of information in access-restricted areas of the secure information exchange site. Access to these areas requires the use of one-time URLs and passwords. 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.

The NEC Group has implemented a secure email distribution system to prevent incidents of information leakage caused by mistaken email address entry, mistaken email attachments or intentional email transfer.

Other efforts to increase email security include the rollout of OMCA (Outlook Mail Check AddIn) within the NEC Group. 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.

(3) Secure environment for working outside the office

The NEC Group has 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. "Trusted PCs" employ technologies such as "fully encrypted HDD" and "remote data deletion/PC locking" in order to protect the information stored inside the PC.

Reference

1) NEC: Information Security Report 2017
http://www.nec.com/en/global/csr/security/index.html

Authors' Profiles

YOSHIDA Atsumasa
Manager
Management Information Systems Division

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.12 No.2 Cybersecurity

- Building Futureproof Security to Support Business Safety and Reliability -

Vol.12 No.2
January 2018

Special Issue TOP