Trends in Cybersecurity and NEC's Commitment to Developing Solutions

Over the past few years, cyberattacks and cybercrime have become increasingly destructive and are now regarded as a significant social issue. Under these circumstances, the Japanese government has hammered out a number of policies aimed at boosting cybersecurity both in the public and private spheres. At NEC, we take the threat of cyberattacks very seriously and have developed a variety of technologies such as a cyberattack protection system and information leakage measurement platform to protect our own security. Most recently, we have begun to apply AI technology to detect and counter threats and are working diligently to acquire security intelligence. Drawing on the technologies we have developed and the information we have collected, as well as sophisticated security human resources, NEC is now able to offer a wide spectrum of security solutions. In this paper, we will take a closer look at trends in cybersecurity and explain in some detail the efforts NEC is undertaking in this area.

SUZUKI Mikio
Senior Expert
Business Creation Division

YAMAI Tadanori
Manager
Cyber Security Strategy Division

SUZUKI Tetsuya
Assistant Manager
Cyber Security Strategy Division

MIYAUCHI Kouji
Executive Chief Engineer
Security Research Laboratories

1. Introduction – Trends in Cybersecurity

The nature of cyberattacks is constantly in flux, always evolving to keep pace with the times. Initially, personal cyberattacks — such as email pranksters — were predominant. But as more and more of the world's business shifted online, cyberattacks grew in scope and ambition, targeting businesses, large organizations, critical infrastructure, and governments at the highest level, gradually becoming ever more sophisticated and complex. These attacks range from economically motivated to politically motivated and can include targeted attacks aimed at specific subjects who have expressed social or political opinions that differ from those of the attackers. These often take the form of distributed denial of service (DDoS) attacks in addition to the hacking of websites. On the more prosaic side, theft of credit card information and other personal information has become an almost daily occurrence, along with illegal remittances via Internet banking. As a consequence, cyberattacks have come to be recognized as an issue that society as a whole must confront.

Against this background, the Japanese government enacted the Basic Act on Cybersecurity in 2014. This move highlighted the importance of cybersecurity measures in governmental administrative organs and critical infrastructure and the necessity for voluntary commitment to enhanced security by private businesses and academic/research institutions, as well as the importance of developing human resources.

Recent years have witnessed the accelerating dissemination of new technologies such as IoT and the expanding utilization of information communication technology. Massive DDoS attacks have been launched using vulnerable IoT devices as springboards, while large-scale power outages have occurred due to attacks on critical infrastructure. In May 2015, the Cybersecurity Strategic Headquarters announced its "Guidelines for the Establishment of Safety Standards of CIIP (4th Edition)," pointing out the importance of minimizing the impact of cyberattacks as much as possible through early detection and quick recovery, as well as prevention of their recurrence.

Around the same time, the Ministry of Economy, Trade and Industry (METI) formulated its own "Cybersecurity Management Guidelines," with a view to bringing corporate management around to the notion that the promotion of cybersecurity measures should be at the core of their corporate strategy. As for developing and training the cybersecurity personnel needed to cope with cyberattacks, METI estimated that there was a shortage of 132,000 workers in this area and that number was expected to increase to 193,000 by 2020. Recruitment and training of cybersecurity personnel is critical to the promotion and implementation of effective cybersecurity strategies.

In this regard, efforts are now underway in all areas of industry, government, and academia to train up cybersecurity personnel. Thanks to METI's promotional projects, universities throughout Japan are now offering cybersecurity-related courses in cooperation with businesses. In the industrial sector, an organization called the Cross-Sector Forum for Cybersecurity Workforce Development was launched with a view to achieving an "ecosystem" that fosters, employs, and utilizes cybersecurity personnel. Significant results are expected from this organization's activities.

2. NEC's Commitment

NEC has been a leader in the war against cyberattacks and cybercrime ever since they first began to manifest.

In the early 2000s, computer worms called Code Red and Nimda created havoc by self-propagating by infecting everything around them. Based on our experience combatting these viruses, we developed the concept of "count management" and put it into practice. "Count management" assumes that what we cannot count cannot be managed. Applying this concept to actual practice, we developed the Cyber Attack Protection System (CAPS). CAPS comprehensively collects and visualizes a wide range of data such as the types and versions of OSs installed on PCs and servers, details of programs, application conditions of security measures, and infection conditions of viruses. By promptly applying appropriate patches based on that information, CAPS eliminates vulnerabilities and establishes proactive defensive measures against attacks. This concept forms the foundation of NEC's security measures.

To combat the type of cyberattacks that we face today, we conduct risk analysis of threats and implement protection measures accordingly. We are particularly focused on detection of unknown attacks, integrated management and monitoring of logs, the introduction of the Global Cyber Attack Protection System (GCAPS), and establishment of the structure of the Computer Security Incident Response Team (CSIRT). In addition to incident response, we also perform value validation of leading-edge technology developed by NEC. These efforts have helped us achieve a successful and proactive cybersecurity management.

In cybersecurity measures, security intelligence — or knowledge about attacks — also plays an important role. Attackers do not necessarily use the same method each time they make an attack; rather, they implement new methods. This makes it necessary for the defenders to watch for and study new methods as soon as they appear and to develop effective countermeasures. Close study of these methods will also reveal the attributes of the attackers because each attacker has their own particular habits and characteristics, making it easier to predict future attacks and to take steps to prevent them. At NEC, our CSIRT collects information on attacks and incident cases relating to our company. In addition to this in-house data collection, we also work in conjunction with organizations that maintain surveillance over international cybercrimes, while sharing information and conducting joint research with the Japan Cybercrime Control Center (JC3) and various security vendors that promote aggregation, analysis, and containment of cybercrimes. Furthermore, NEC is the first Japanese company to participate in the framework to quickly share threat information on cyberattacks between government and corporate entities — an effort promoted by the U.S. Department of Homeland Security (DHS). We analyze data collected both internally and externally, as well as domestically and internationally, and use that knowledge to build a cyberintelligence database.

These are just a few examples of the NEC Group's commitment to cybersecurity. This means that the solutions we have developed and now offer to our customers have been actually tested and validated at NEC, and their effectiveness, convenience, and safety have also been verified in-house. Our experience with in-house operation has also given us the know-how to better support our customers and to constantly upgrade the quality and serviceability of system operation and maintenance.

3. Cybersecurity Solutions Offered by NEC

The increasing sophistication and diversification of cyberattacks means that it is no longer sufficient to implement targeted security measures; instead, measures must be put in place that focus on multiple points from different perspectives — multi-layered defense, in other words. Consequently, like the attacks themselves, security measures are becoming increasingly diversified.

Unfortunately, the shortage of experienced cybersecurity personnel makes it difficult for many of our

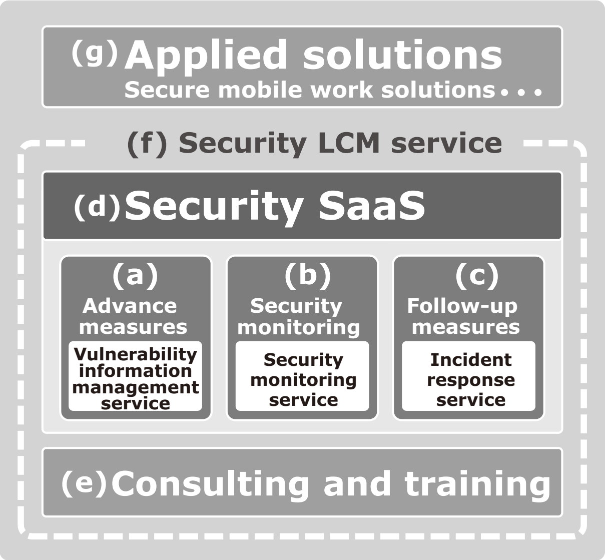
(g) Applied solutions
Secure mobile work solutions • • •
(f) Security LCM service
(d) Security SaaS
(a) Advance measures
Vulnerability information management service
(b) Security monitoring
Security monitoring service
(c) Follow-up measures
Incident response service
(e) Consulting and training

Fig. NEC's cybersecurity solutions.

customers to implement complex security measures on their own, increasing demand for support from external experts. For this reason, NEC not only offers these cybersecurity measures as products, but also as services (some measures are only available as services).

NEC's cybersecurity solutions are comprised of several services as shown in **Fig**.

The services that offer countermeasures mainly against cyberattacks include: (a) advance measures, (b) security monitoring, and (c) follow-up measures. Also offered is NEC's unique solution called (d) security SaaS where a security measure is operated by NEC.

(a) Advance measures

We provide a vulnerability information management service that visualizes risks in a customer's organization such as unaddressed vulnerabilities and enables the customer to deal with them.

(b) Security monitoring

We offer a security monitoring service that detects the occurrence of an incident. Conventional security monitoring services have been individual-dependent, thus making it difficult to provide many customers with high-precision services. For this reason, NEC is making efforts to monitor the environments of our customers using AI technology and a tripolarity system.

(c) Follow-up measures

When a security incident occurs, we offer an original incident response service to help customers deal with it. In ordinary incident response services, staff are dispatched to the site to investigate — which takes time. At NEC, we conduct preliminary research from a remote site and, if the case is relatively simple, we can make an immediate assessment.

(d) Security SaaS

Our SaaS solutions offer various security functions such as email security, file encryption, and web application firewalls (WAFs) on clouds to help reduce the management burden.

(e) Consulting and training

Security measures must be introduced and upgraded systematically with a view to simplifying management. NEC offers a consulting service based on the "Cybersecurity Management Guidelines," formulated by the METI. To enforce effective security measures, it is also important that customers make efforts in training up personnel. At NEC, we also provide training to support cybersecurity human resources.

(f) Security LCM service

In order to help our customers maintain up-to-date cybersecurity measures, we now offer a life cycle management (LCM) service that covers a wide spectrum of services, ranging from consulting to system construction, monitoring, and incident response.

(g) Applied solutions

We are also planning and developing various new secure solutions that incorporate the cybersecurity measure products and services we have already discussed. For example, we have started offering a secure mobile work solution.

In addition to the cybersecurity solutions offered directly to customers, we strive to ensure the security of our own development and operations so that our customers can be assured of the safety and security of the systems, products and services we provide. At the same time, we are working on the acquisition of personnel and development of technology to offer security solutions to our customers.

4. Backing up Cybersecurity Solutions with Cutting-Edge R&D

The threat posed by cyberattacks is multi-fold. Not only are these attacks constantly evolving — becoming ever more sophisticated and diverse, but they are also occurring more and more frequently. As the ability of conventional security experts to deal with them is limited both qualitatively and quantitatively, AI technology is now regarded as the best hope for managing this challenge in the years ahead.

By automating some of the operations which security experts typically handle, such as detection and analysis of cyberattacks, as well as planning of countermeasures, NEC is pushing forward with research into new security technology that solves the problem of the shortage of experts, while making it possible to cope with sophisticated cyberattacks that humans might find difficult to discover and counteract.

One of the aspects of today's cyberattacks that is most troubling is that it is difficult to even detect an attack with current security technology. At NEC, we are using AI to develop technology that can detect unknown attacks and determine appropriate countermeasures through constant analysis of detailed system conditions. Once an attack has been detected, our security experts can draw on their deep knowledge and experience to draw up an overall picture of the attack using its fragmentary traces, elucidate the method of attack, assess the extent of the damage, and plan an appropriate response. Although today's AI-based cybersecurity technology can identify counter methods by searching through an enormous database on past attacks, it still cannot take over the advanced operations handled by security experts. At NEC, we hope to develop security technology that will be capable of taking over these operations by leveraging our proprietary logical inference AI technology.

In the meantime, one of the best ways to minimize the damage caused by cyberattacks is to predict cyberattacks that are likely to occur imminently and to implement countermeasures in advance. Here, what is called security intelligence — or knowledge about cyberattacks — plays a crucial role. At NEC, we use AI to analyze massive amounts of data obtained from social media networks that attackers use to exchange information. Building on these results, we have developed and are now evaluating technology to generate security intelligence automatically, as well as technology to predict cyberattacks and plan counter measures.

In addition to these efforts, we are also endeavoring to develop state-of-the-art encryption technologies to support critical infrastructure which is also under increasing threat from these kinds of attacks. These technologies are introduced in "Lightweight Cryptography Applicable to Various IoT Devices" (NEC Technical Journal, Special Issue on IoT That Supports Digital Businesses, Vol. 12, No. 1, October 2017: pp. 67–71) and "Enhancing FinTech Security with Secure Multi-Party Computation Technology" (NEC Technical Journal, Special Issue on FinTech That Accelerates Digital Transformation, Vol. 11, No. 2, June 2017: pp. 46–50).

5. Conclusion: Futureproof Society — Beyond a Sense of Security

The NEC Group is focusing on the advancement of social infrastructure to achieve the four social values of safety, security, efficiency, and equality — which are indispensable for the achievement of a global society of abundance. At NEC, we have developed technology and expertise to support the infrastructure critical to an efficiently functioning modern society. Under the slogan "Futureproof Security — Beyond the frontlines of cyber security" we are committed to the development of cybersecurity systems that will provide individuals and society with the safety and security they need to move forward into a better future.

The details about this paper can be seen at the following.

Related URL:

Cyber Security Solutions
http://www.nec.com/en/global/solutions/cybersecurity/index.html

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 -

\Orchestrating a brighter world NEC
NEC Technical Journal
Cybersecurity
- Building Futureproof Security to Support Business Safety and Reliability -
Vol.12 No.2

Vol.12 No.2

January 2018

Special Issue TOP