Tighter Security Operations to Help Provide Brands that are Safer and More Secure

Fumiyuki Tanemo, Ikuya Hayashi, Masaki Tanikawa, and Tsuyoshi Abe

Abstract

In this article, we review early work by NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team) and introduce the security research functions on which work has started with the aim of strengthening NTT's security response.

1. Introduction

1.1 Benefits and drawbacks of Internet growth

The Internet affects us all, and it is now closely connected to our everyday lives. With the falling cost of computers and network environments and the emergence and growing popularity of new personal devices such as smartphones, the Internet has become a means of communication that extends beyond its use merely as a tool for gathering information and providing services. For example, there are now many social networking services (SNSs) on the Internet. It is said that the 2010 Arab Spring pro-democracy movement was able to affect the governments of several countries because SNSs reach across international boundaries. This would have been inconceivable before the arrival of network technology.

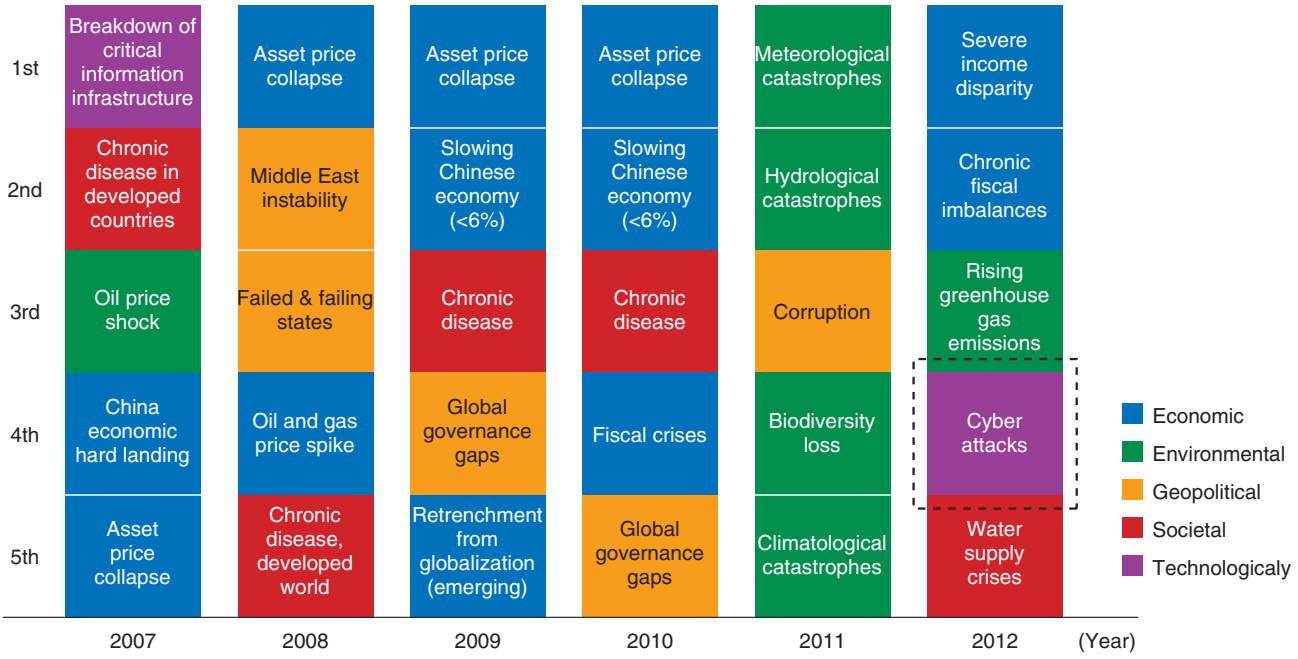
A drawback of this network development trend, however, is that it has allowed the perpetrators of cyber attacks and other malicious actions to use new methods of attack. Today, it is no longer unusual to see attackers clubbing together to launch systematic continuous attacks, and we are witnessing an increased threat of cyber attacks. The way in which the top five global risks have changed over the last few years according to the World Economic Forum is shown in **Fig. 1**. Cyber attacks were ranked fourth in 2012 despite having never appeared on this list before.

1.2 Increasingly sophisticated cyber attacks

To protect against these cyber attacks, most security administrators have generally made efforts to prevent damage from occurring in the first place by taking measures such as using antivirus software and firewalls and by performing maintenance to eliminate security vulnerabilities that can be exploited in cyber attacks. In recent years, however, we have not only seen a continuing increase in the number and severity of vulnerabilities requiring conventional maintenance, but also noticed attackers using new types of attack and new attack mechanisms. It is therefore becoming harder to protect against cyber attacks by conventional methods and ways of thinking.

For example, the spread of communication tools like smartphones and SNSs has made it easy for anyone to access information that would have been difficult to obtain before, such as a user's previous actions, thoughts, locations, and relationships. By combining the information handled by multiple communication tools, an attacker can easily engineer situations where it is possible to gain the trust of target individuals or organizations. This is why targeted attacks such as advanced persistent threat (APT) attacks pose such a major threat today.

It has also been reported that a succession of intrusion and information leakage incidents in the networks of various organizations including major corporations in 2011 was committed by a new group of



Source: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf

Fig. 1. Recent changes in the top five global risks.

attackers called *hacktivists*. Unlike conventional attackers who are motivated by financial gain, hacktivists use cyber attacks as a means of asserting their views, and their attack mechanisms vary widely. Hitherto, the concept of defense has been based on the reasoning that attackers will decide that an attack is not worth pursuing if they face sufficient preventative measures such as firewalls, which require considerable technological ability and time to overcome. However, if attacks are not financially motivated, then this approach is simply no longer applicable.

1.3 Proactive and reactive security

Owing to the appearance of advanced cyber attacks and new attack motivations, our approach to preventative measures is also changing. Specifically, the diverse nature of attacks means that it may not be possible to completely prevent all attacks. On the basis of this premise, it is now more important than ever to establish organized systems that can implement reactive security measures.

With preparation, it is possible to minimize damage by taking prompt measures to prevent secondary attacks instead of hurrying to resolve issues after an attack has already taken place. It is also possible to make use of the resulting know-how to provide proactive feedback, such as preventing or detecting future incidents.

We believe that a thorough understanding of both proactive and reactive approaches is useful for handling security operations in modern Internet environments.

1.4 CSIRTs and reactive security measures

A computer security incident response team (CSIRT) is an organization that implements measures ranging from preventing security incidents to detecting them and applying countermeasures. Such organizations regard security incidents as inevitable occurrences and consider reactive measures as their main approach. They set up cooperative networks with other CSIRTs to share defense know-how and information about new attacks so that they can respond immediately to diverse attacks. Consequently, CSIRTs play a key role in reactive security measures.

To represent the NTT Group, NTT's Information Sharing Platform Laboratories (now called the Information Sharing Platform Laboratories) launched its own CSIRT called NTT-CERT (NTT Computer

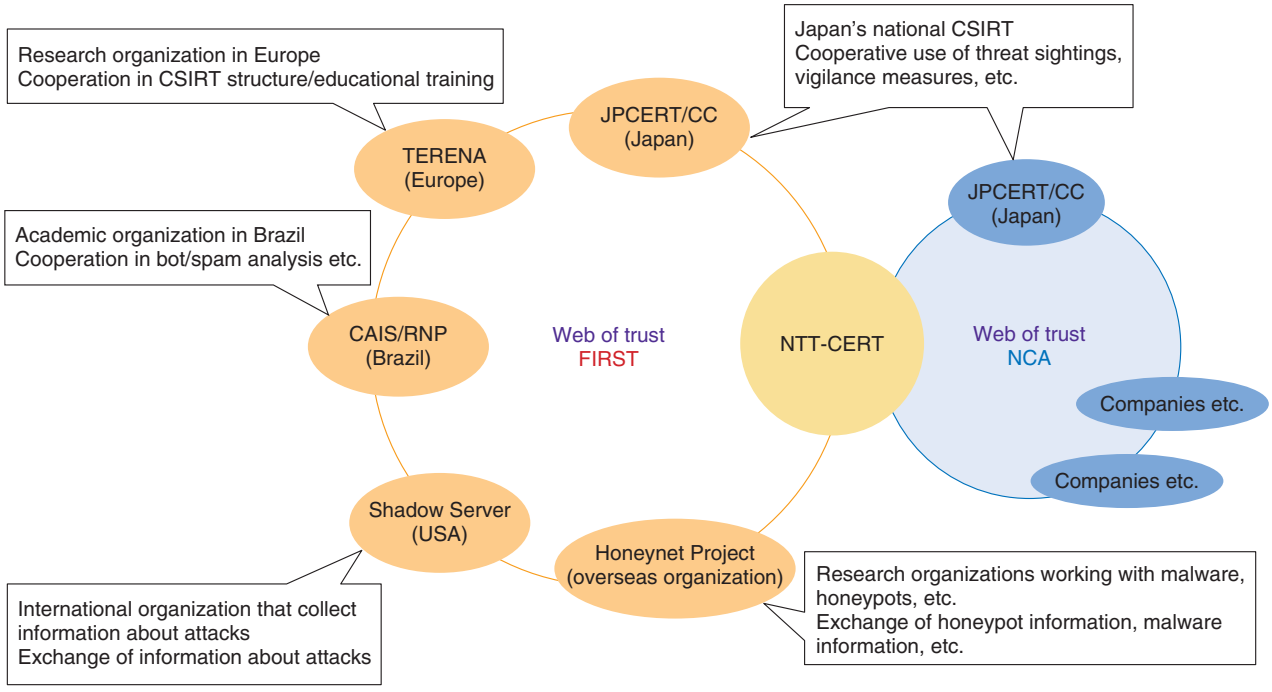


Fig. 2. Cooperation between NTT-CERT and other representative CSIRTs in Japan and overseas.

Security Incident Response and Readiness Coordination Team), which has been active since 2004 [1], [2].

CSIRTs originated from the CERT Coordination Center set up in the USA in 1988 to deal with a global malware pandemic [3]. Today, there are CSIRTs that have been set up by countries, businesses, and organizations all over the world, including Japan. In 1990, the CSIRT international forum FIRST (Forum of Incident Response and Security Teams) was set up by the principal CSIRTs at that time because of the need for a response to international concerns [4]. FIRST's members include over 200 CSIRTs from all over the world, including NTT-CERT (as of April 2012). NTT-CERT is also an active founding member of the Nippon CSIRT Association (NCA), which was established in 2007 as a collection of Japanese domestic CSIRTs [5] (**Fig. 2**).

2. NTT-CERT

2.1 Activities

At NTT-CERT, we are building a worldwide cooperative circle of CSIRT organizations from different countries and organizations by taking advantage of communication forums such as FIRST and NCA (**Fig. 3**). We also provide the following functions for the NTT Group:

(1) Offering the trustworthy point of contact
(2) Collecting, analyzing, and providing security-related information
(3) Supporting the construction of CSIRTs
(4) Providing training and educational activities
(5) Conducting security-related research and development

Specifically, we provide support and information to all companies in the NTT Group, such as support for incident countermeasures and the discovering/reporting of vulnerabilities, and we collect information from external organizations including other CSIRTs as a point of contact with the NTT Group.

In addition to providing documentation such as reports on vulnerabilities verified at NTT and security configuration guidelines used when configuring servers, we actively provide information to each company in the NTT Group in an easily understood form, including holding workshops on various security-related themes.

We are also actively contributing to a wide range of outward-facing activities such as cooperating with the preparation of annual reports at the Information-technology Promotion Agency of Japan (IPA) and

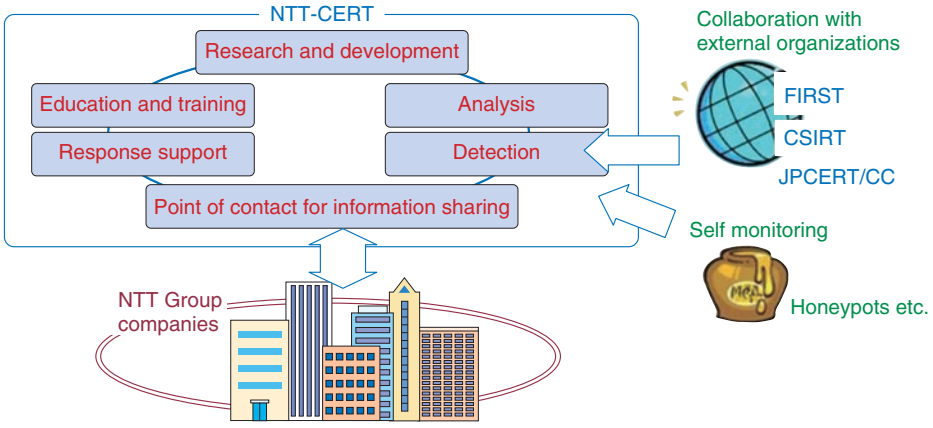


Fig. 3. Overview of NTT-CERT's activities.

Fig. 4. Our presentation at the FIRST meeting in March 2012.

giving various presentations and issuing research papers via FIRST and NCA (**Fig. 4**).

2.2 Challenges of security operations

As mentioned above, attacks against information systems and services are becoming more and more sophisticated, and they are likely to continue changing in the future. It is therefore important that our security operations keep in step with these changes with both proactive and reactive security measures.

In proactive security, measures for detecting and preventing attacks need to be appropriately reviewed according to changes in attack trends. From the viewpoint of APT attack countermeasures, it is now more important than ever to analyze log files as a way of detecting attacks.

In reactive security measures, there is an increasing need for advanced techniques and know-how to analyze the traces of attacks and correctly perceive what has happened in order to minimize the damage.

2.3 Security research functions

To meet the challenges faced by security operations, we launched a security research function that builds on the activities of NTT-CERT, and we started efforts to support the security operations of each company in the NTT Group (**Fig. 5**). We are working to support the NTT Group companies and improve our security operations technology across the following seven missions, ranging from proactive incident prevention measures to reactive damage mitigation measures.

1) Security product evaluation

Various security products and technologies target increasingly sophisticated attacks. We subject these products to technical appraisal before they are

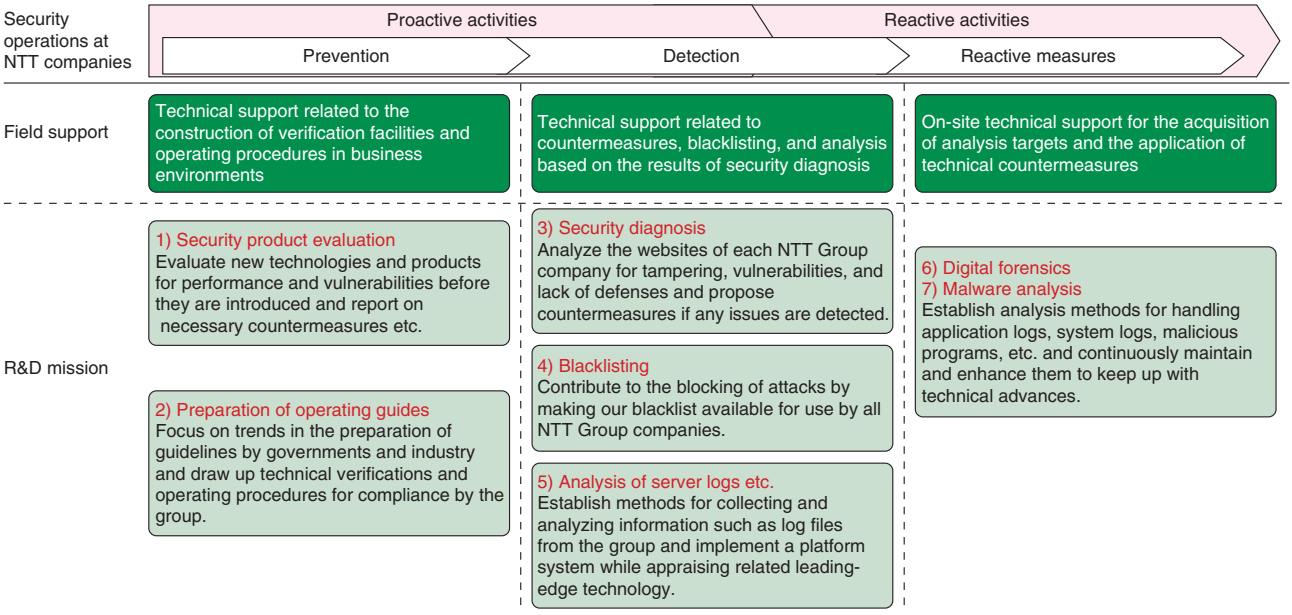


Fig. 5. Security research functions.

introduced for business use, and we are continuing to develop more advanced product evaluation techniques for this purpose.

2) Preparation of operating guides

While keeping abreast of trends in the formulation of guidelines (e.g., cloud security guidelines) by government and industry bodies, we prepare guidelines for use within the NTT Group for the defense of servers, Android platforms, and so on.

3) Security diagnosis

On the websites of NTT Group companies, we periodically search for tampering, vulnerabilities, and lack of defenses, and we issue reports on the trend of any problems discovered and the countermeasures taken.

4) Blacklisting

Using advanced malware detection technology developed at NTT, we are creating a blacklist of higher quality than those of existing providers, such as antivirus vendors, and we are providing this blacklist to companies in the NTT Group.

5) Analysis of server logs etc.

We collect information such as large-scale server logs and security news from sources such as network equipment, servers and operating systems, and we are using a large-scale data processing platform to establish techniques for analyzing log files in order to streamline our operations, including automatic extraction of incident-related information based on machine learning and automatic classification of security logs.

6) Digital forensics

To understand what occurred on compromised computers, we deeply investigate by examining system logs and other records on the computers and related systems.

7) Malware analysis

We also deeply analyze malicious programs that we can get from compromised computers or other sources.

It is difficult to implement items (6) and (7) at all NTT Group companies. To support them, we are working on detailed analysis methods for application and system logs, malicious programs, etc.

References

[1] NTT-CERT. http://www.ntt-cert.org/index-en.html
[2] M. Nagashima, Y. Sugiura, T. Abe, T. Yoshida, and A. Mukaiyama, "CSIRT Activities at NTT," NTT Technical Review, Vol. 8, No. 7, 2010. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201007sf5.html
[3] CERT. http://www.cert.org/
[4] FIRST. http://www.first.org/
[5] Nippon CSIRT Association. http://www.nca.gr.jp/en/

Fumiyuki Tanemo

Senior Research Engineer, Supervisor, Security Management & Operations Project, NTT Secure Platform Laboratories.

He received the B.E. and M.E. degrees in information engineering from Nagoya University, Aichi, in 1991 and 1993, respectively. He joined NTT in 1993. He is engaged in network security R&D as the leader of NTT-CERT. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of the Information Processing Society of Japan and the IEEE Computer Society.

Ikuya Hayashi

Senior Research Engineer, Security Management & Operations Project, NTT Secure Platform Laboratories.

He received the B.S. degree in earth science from Hokkaido University in 1998. He joined NTT in 1988. He is currently engaged in network security R&D as a member of NTT-CERT. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories.

Masaki Tanikawa

Senior Research Engineer, Security Management & Operations Project, NTT Secure Platform Laboratories.

He received the B.E. and M.E. degrees in systems science from Tokyo Institute of Technology in 1993 and 1995, respectively. He joined NTT in 1995. He is engaged in network security R&D as a member of NTT-CERT. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

Tsuyoshi Abe

Senior Research Engineer, Security Management & Operations Project, NTT Secure Platform Laboratories.

He received the B.E. and M.E. degrees in mechanical engineering from Waseda University, Tokyo, in 1993 and 1995, respectively. He joined NTT in 1995. He is engaged in network security R&D as a member of NTT-CERT. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of IEICE.