Emergence of New Cyber Attacks and Future Directions in Security R&D

Tohru Matsuno, Toru Kawamura, Kazuhiko Ohkubo, Hidetsugu Kobayashi, Katsumi Takahashi, and Shigeru Kayaguchi

Abstract

From the viewpoint of a telecommunications operator, NTT is researching and developing new technologies for dealing with cyber attacks that are immune to existing ones. Cyber attacks have been evolving into large-scale, multifaceted attacks and their targets have grown to include clouds, smartphones, and industrial systems, raising concerns about their impact on society as a whole.

1. Introduction

1.1 ICT market trends

Corporate activities are undergoing major changes typified by keywords such as global and convergence. The information and communications technology (ICT) market is also changing as trends such as social networking, cloud computing, and multi-device lifestyles gain momentum. As the ICT market changes, so does the environment surrounding security issues (**Fig. 1**). The objectives of cyber attacks are changing and attacking techniques are becoming increasingly large-scale and multifaceted. In addition, new types of malware are continually being created, making it difficult for countermeasures to keep up with them. At the same time, cryptographic technology used for protecting data must be convenient to use from the viewpoint of users and security operations must provide a unified, advanced response both before and after the fact for various envisioned situations.

This article surveys the changes taking place in the environment surrounding security and introduces the direction of security-related research and development (R&D) in NTT to deal with these changes.

1.2 Evolution of cyber attacks

In the early days of cyber attacks, the perpetuators were mainly individuals who were simply intent on being mischievous or showing off their technical prowess. In short, their objectives were individual in nature. Recently, however, attackers and their objectives have expanded. Groups of individuals on the Internet who share the same ideology and convictions and other types of groups that may even include national institutions have become attackers. These new types of attackers also have new objectives: in addition to financial gain, they may seek to disrupt the activities of entities (companies, public institutions, etc.) having different ideas and principles from themselves or steal confidential information. This means that their objectives have become ones that can have a major impact on society and the business world.

The techniques for mounting attacks are also changing. To achieve the above objectives, a type of attack called an advanced persistent threat (APT) has emerged. It carefully prepares and executes scenarios that combine multiple approaches and methods. Corporations and organizations that have already suffered APT attacks include major search engine sites, energy-related industries, and public offices. The APT attack aims to access confidential information and corrupt systems in a way that could have a major impact on society as a whole.

1.3 Expansion of countermeasures through technical innovation

In the past, the targets of cyber attacks were mainly

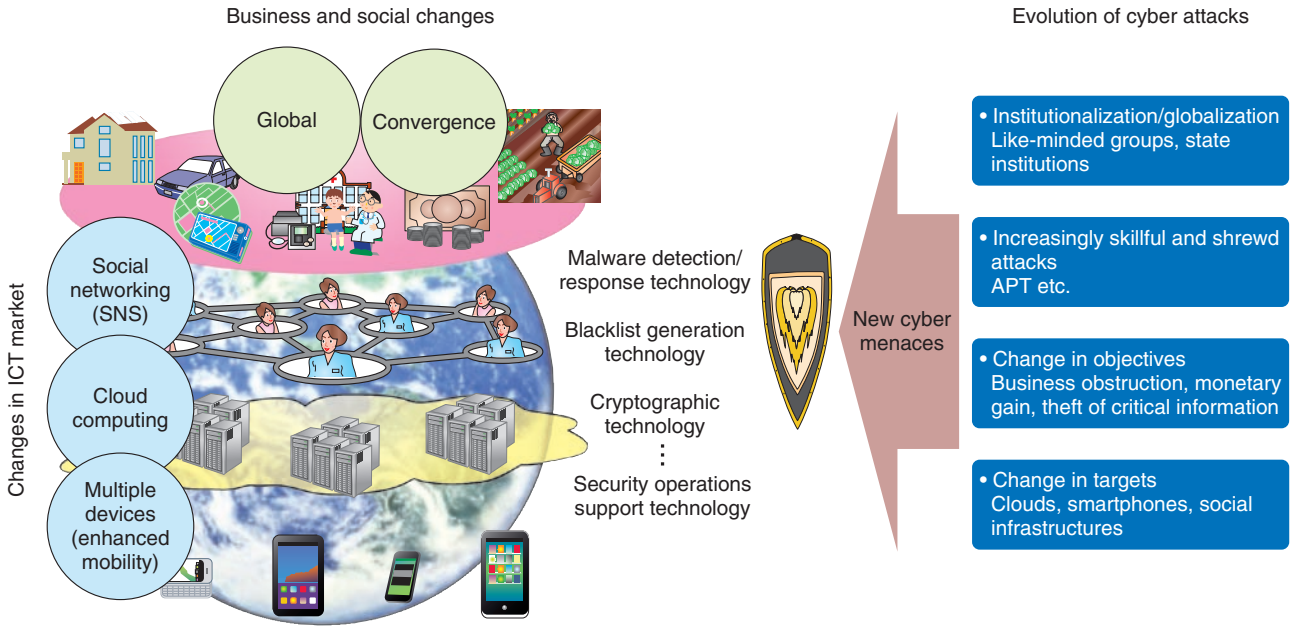

Fig. 1. Changes in ICT market trends and security environment.

the servers of computer systems and the personal computers of individual users. Nowadays, however, a wide variety of terminals including smartphones and tablets are connected to the network while operating systems and other operation platforms are becoming increasingly generalized and information distribution is becoming more open in nature. For example, mobile phones in Japan traditionally operated on separate operation platforms specified by different makers. Smartphones, however, are being provided on globally standardized operation platforms such as Android as a shift takes place from closed content distribution unique to each carrier to content distribution on an open market. These developments are creating an environment similar to the past situation with personal computers that makes it easy for attackers to devise attack methods and to increase the number of targets susceptible to an attack.

The number of cases of smartphones affected by malware is on the increase, suggesting that serious problems like the leakage of personal information will only intensify as smartphone users increase in number.

New issues are now coming to the fore as the cloud service operators make changes to the technologies that they use. Cloud computing is a technology that has significant benefits such as prompt system development and significant cost reductions because users have no need to actually own the facilities they need. The use of clouds, though, can generate concern about security because users must entrust their confidential information to cloud service operators.

Up to now, each company has owned and managed its own corporate systems, but advances in cloud computing are prompting the shift of some management processes—such as the checking of operating conditions and the operation history of systems owned and managed by companies (customers)—to cloud service operators. However, as the cloud resources provided by cloud service operators can change dynamically, it is becoming increasingly difficult for companies (customers) to fully grasp the configuration of the systems they own and manage. To carry out security audits in a manner similar to that of conventional corporate systems, cloud operators need to provide a trail that can sustain an audit (**Fig. 2**).

In addition, even control systems for public and corporate infrastructures that have traditionally been closed using proprietary technology are introducing general-purpose technology because of its cost benefits, thereby creating new targets of attacks. For example, the malware called Stuxnet can penetrate certain industrial control systems even in environments segregated from the Internet. Its use to mount a cyber attack on a nuclear complex has made the

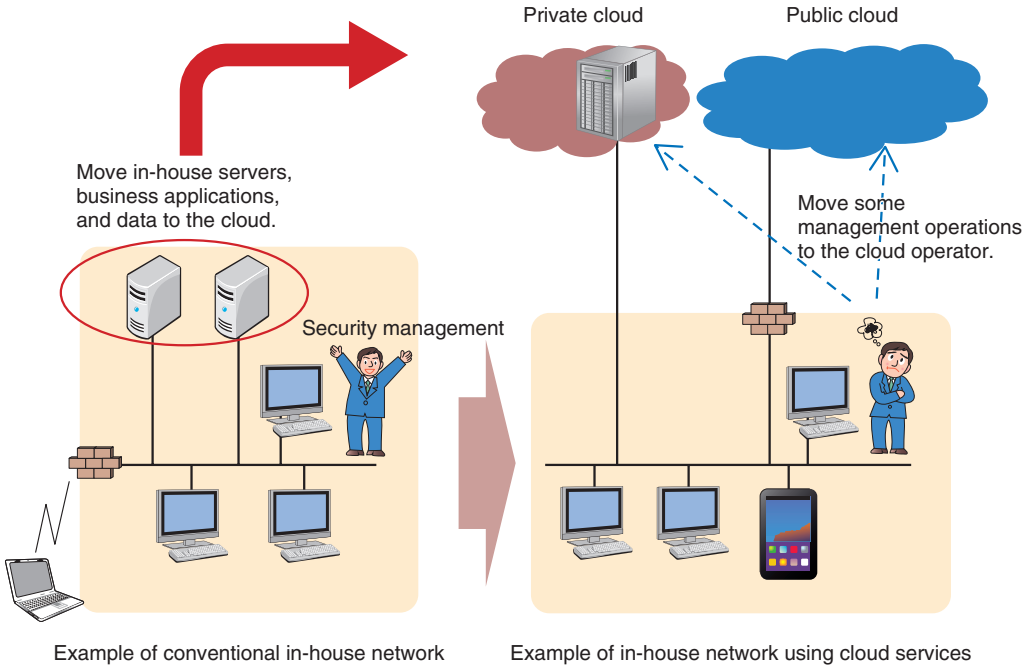

Fig. 2. Concerns about security in the cloud.

name Stuxnet notorious.

But public and corporate infrastructures are also social systems, and as such, they simply cannot come to a halt. The effects of an attack on such a system can be very great, but, as is the case with ordinary information systems, it is difficult to implement security countermeasures after a system has been brought down.

2. Countermeasures to new cyber attacks

The targets of ever-evolving cyber attacks are expanding on a daily basis, so attempting to tackle them with a conventional mindset is ineffective. There is an urgent need to fortify the development and deployment of anti-attack technologies on the basis of a new way of thinking and to enhance all security-related operations from the early detection of attacks and abnormal events that portend attacks to the restoration of a system damaged by an attack [1].

As new attack techniques appear in rapid succession and continue to evolve, it is essential to be able to detect a wide variety of attacks, including ones that are currently unknown, at an early stage. Up to now, it has taken much time to discover an attack, and the response to an attack has often been implemented only after much damage had been caused. Dealing with attacks has therefore incurred much time and cost. If attacks and their indicators can be detected early and if early detection can be combined with effective countermeasures, it should be possible to curb the spread of damage.

In the cloud era in which data is routinely deposited and processed in the cloud, encryption is an absolute necessity. However, this is not just a matter of developing cryptographic technology that focuses on only confidentiality as in the past. It is also essential to develop cryptographic technology that places importance on the use and application of that data. If efforts were to be centered on only security at the sacrifice of convenience in everyday business and life, then security technologies would not be well received by users and corporate security administrators, and the level of security would actually drop as a consequence. From here on, there will be even greater demand for cryptographic technology that does not reduce usability from the user's viewpoint.

For telecommunications operators like the NTT Group, accountability in relation to security events is also important. They must be able to give appropriate explanations to all business-related stakeholders including users, auditors, and even other operators.

In terms of strengthening security operations,

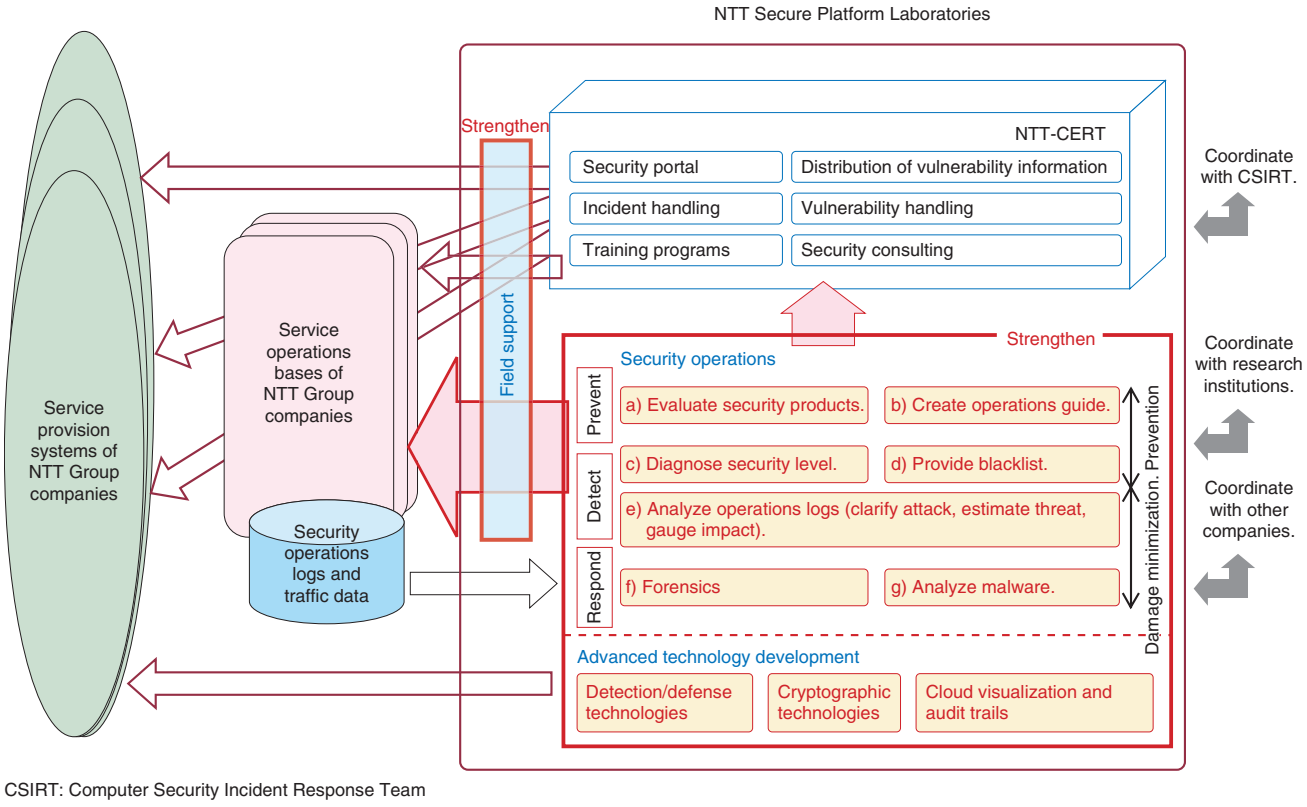

Fig. 3. Technology development and strengthening of security operations.

complete prevention of ever-evolving cyber attacks is difficult, which makes it important to prepare systems, accumulate know-how, and construct tools that can help discover and respond to attacks at an early stage. In this regard, importance should be placed on accumulating and systematizing know-how through daily security operations.

3. NTT's approach to cyber attacks

In NTT, researchers are taking a two-sided approach to dealing with new cyber attacks. First, they are developing advanced, security-related technologies, and second, they are developing techniques and accumulating know-how that can be put to immediate use in strengthening current security operations (**Fig. 3**).

In the development of advanced technologies, researchers are focusing their efforts in areas in which telecommunications operators feel that existing technologies are incapable by themselves of defending against new cyber attacks (**Fig. 4**). Specifically, the targets of these efforts can be divided into (1) detection, analysis, and countermeasure technologies; (2) cryptographic technologies; and (3) cloud visualization and audit trails, as summarized below.

Detection, analysis, and countermeasure technologies for new cyber attacks have much to do with early detection of attacks and the ability to mount a prompt response. Two key points here are the large-scale collection and advanced analysis of attack-related data and the execution of countermeasures using the analysis results. NTT's laboratories coordinate with NTT Group companies to collect diverse types of security-log information from attack sensors located throughout the world. In the analysis of this information, those items deemed serious and requiring attention must be quickly extracted and passed on to the relevant system administrators. In the past, deciding what items required a response often depended on the judgment of skilled and experienced personnel. The aim now, however, is to use advanced technologies developed by NTT to automate the analysis of information about malicious applications, malicious websites, sources of attacks, etc. and to provide blacklists so that feedback can be provided promptly to operations. More details about these technologies are given

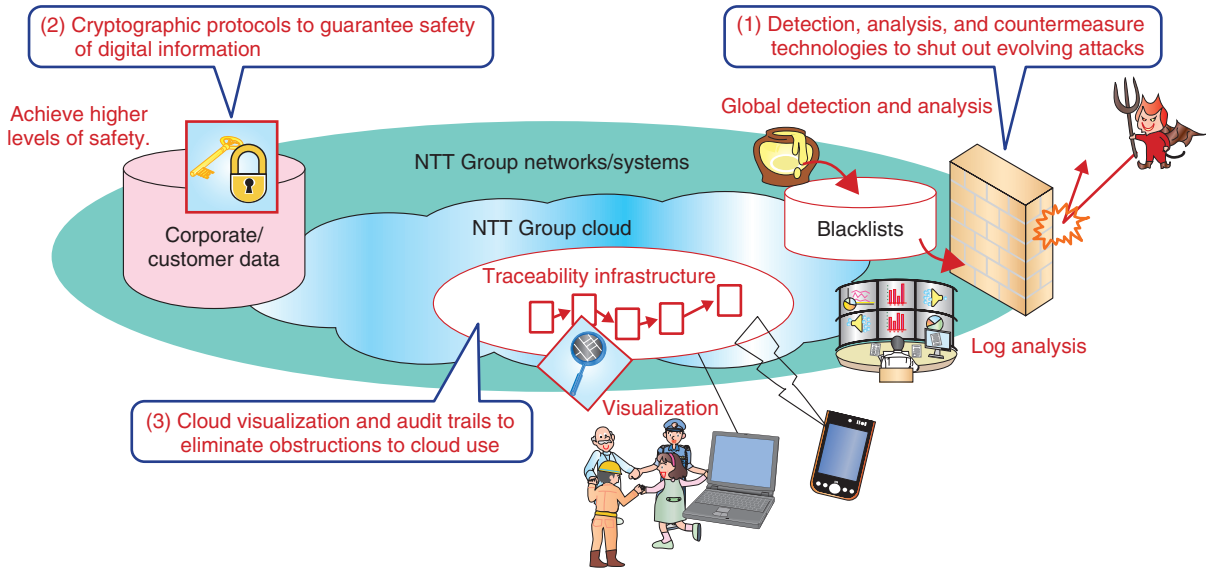

Fig. 4. Key fields in the development of advanced technologies.

in the Feature Article "Detection, Analysis, and Countermeasure Technologies for Cyber Attacks from Evolving Malware" [2] in this issue.

Next, in anticipation of the migration of data to a cloud infrastructure as systems convert to a cloud format, progress is being made in cryptographic technologies. NTT is promoting the formulation of new cryptographic theories, the creation of new cryptographic protocols, the application of cryptographic technologies to various types of systems, and the standardization of those technologies. More details about the development of new cryptographic technologies that take into account the environment surrounding security are given in the Feature Article "Cryptographic Techniques that Combine Data Protection and Ease of Utilization in the Cloud Computing Era" [3] in this issue.

The introduction of cryptography into a system does not guarantee safety from attacks on a permanent basis. Over time, the techniques used by attackers improve and attacks become more powerful, thereby making the cryptographic technology relatively vulnerable (cryptographic compromise). This means that cryptographic technologies that are currently in use must be reviewed periodically. NTT also provides information about the appropriate use of cryptography.

Finally, in the area of cloud visualization and audit trails, the plan is to develop a cloud-forensics function that can correctly interpret a history of operations and events on the basis of operations information collected from the cloud. Such a function will help establish accountability in the provision of cloud services.

One more approach in addition to the development of advanced technologies is the development of techniques for strengthening security operations in the present. The NTT Computer Security Incident Response and Readiness Coordination Team (NTT-CERT) [4], [5] has been promoting methods for handling incidents and vulnerabilities, developing training programs, and supporting techniques for preventing the recurrence of attacks. Looking forward, NTT-CERT plans to develop a system for evaluating security technologies, create and disseminate an operations guide, and establish preventive measures such as security-diagnosis techniques for NTT Group websites. It also plans to provide information about malicious websites obtained from the abovementioned advanced technologies and to disseminate security-related know-how such as how to make early responses based on security-log analysis and how to collect and analyze Android malware. More details about techniques for strengthening security operations are given in the Feature Article "Tighter Security Operations to Help Provide Brands that are Safer and More Secure" [6] in this issue.

4. Concluding remarks

One question that is often asked in relation to security is "To what extent should I take measures to feel safe?" As described in this article, attacker expertise and attacking techniques are evolving quickly and the countermeasures to those attacks are expanding on a daily basis. In such an environment, there is no way that such evolving attacks can be dealt with effectively if today's countermeasures are considered to be satisfactory. The technology infrastructure supporting information systems is also undergoing severe change together with the social environment, business environment, and technology trends. NTT Secure Platform Laboratories is moving forward with the development of cutting-edge technologies and seeks to contribute to enhanced system safety and the secure provision of services through the development of technologies that can strengthen security operations.

References

[1] "Special Feature: Trend of Network Security Technologies," NTT Technical Review, Vol. 8, No. 7, 2010.
https://www.ntt-review.jp/archive/2010/201007.html

[2] T. Hariu, M. Akiyama, K. Aoki, T. Yagi, M. Iwamura, and H. Kurakami, "Detection, Analysis, and Countermeasure Technologies for Cyber Attacks from Evolving Malware," NTT Technical Review, Vol. 10, No. 10, 2012.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa2.html

[3] H. Fuji, A. Fukioka, T. Kobayashi, K. Chida, F. Hoshino, T. Miyazawa, and K. Suzuki, "Cryptographic Techniques that Combine Data Protection and Ease of Utilization in the Cloud Computing Era," NTT Technical Review, Vol. 10, No. 10, 2012.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa3.html

[4] 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

[5] NTT-CERT. http://www.ntt-cert.org/index-en.html

[6] F. Tanemo, I. Hayashi, M. Tanikawa, and T. Abe, "Tighter Security Operations to Help Provide Brands that are Safer and More Secure," NTT Technical Review, Vol. 10, No. 10, 2012.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa4.html

Tohru Matsuno
Chief producer, NTT Research and Development Planning Department.
Since joining NTT in April 1990, he has contributed to the development of digital exchanges, systems engineering, human resource management, global sales, and the datacenter business. He is currently leading NTT's security R&D activities.

Toru Kawamura
Producer, NTT Research and Development Planning Department.
Since joining NTT in April 1988, he has contributed to R&D-related data communication traffic control, a recommendation engine, and a 3D-GUI system for web browsing and some applications using cryptographic technology. He is currently promoting security R&D activities for the NTT Group.

Kazuhiko Ohkubo
Vice President, Project Manager, Security Management & Operations Project, NTT Secure Platform Laboratories.
He was engaged in operation system developments for intelligent networks and interactive multimedia systems in the 1990s. After receiving the MBA from MIT Sloan in 2000, he promoted R&D renovations by introducing exhaustive commercialization functions called the *producer system*. Recently, he has generalized security management related R&D such as CSIRT, SIEM, and cloud security platforms.

Hidetsugu Kobayashi
Project Manager, Network Security Project, NTT Secure Platform Laboratories.
Since joining NTT in April 1987, he has contributed to the development of a range of network-security-related products such as firewalls for IP-VPNs and authentication servers for the NGN. His research interests include network security and information networks.

Katsumi Takahashi
Project Manager, Information Security Project, NTT Secure Platform Laboratories.
He received the B.S. degree from Tokyo Institute of Technology in 1988 and the Ph.D. degree from the University of Tokyo in 2006. Since joining NTT in 1988, he has been working on information retrieval, data mining, cryptographic protocols, information security, privacy protection, and security social science.

Shigeru Kayaguchi
Senior Research Engineer, Supervisor, Security Management & Operations Project, NTT Secure Platform Laboratories.
Since joining NTT, he has been engaged in operation system development for ISDN services, new business development, and the management of an Internet media venture company. His research interests include cloud security, smartphone security, and methods of compromising cryptosystems.