Security R&D for a Safe and Secure Digital Society

Kazuhiko Okubo

Abstract

Major environmental changes and market transitions are occurring as our digital society is realized, and in line with this trend, NTT Secure Platform Laboratories is conducting research and development on security technologies to build resistance to emerging new security threats and to resolve issues involving the utilization of data. This article introduces some security issues that can arise in a digital society and security measures to deal with them, both defensive and offensive.

Keywords: cyberattack, encryption, privacy

1. Transformation to a digital society and security issues

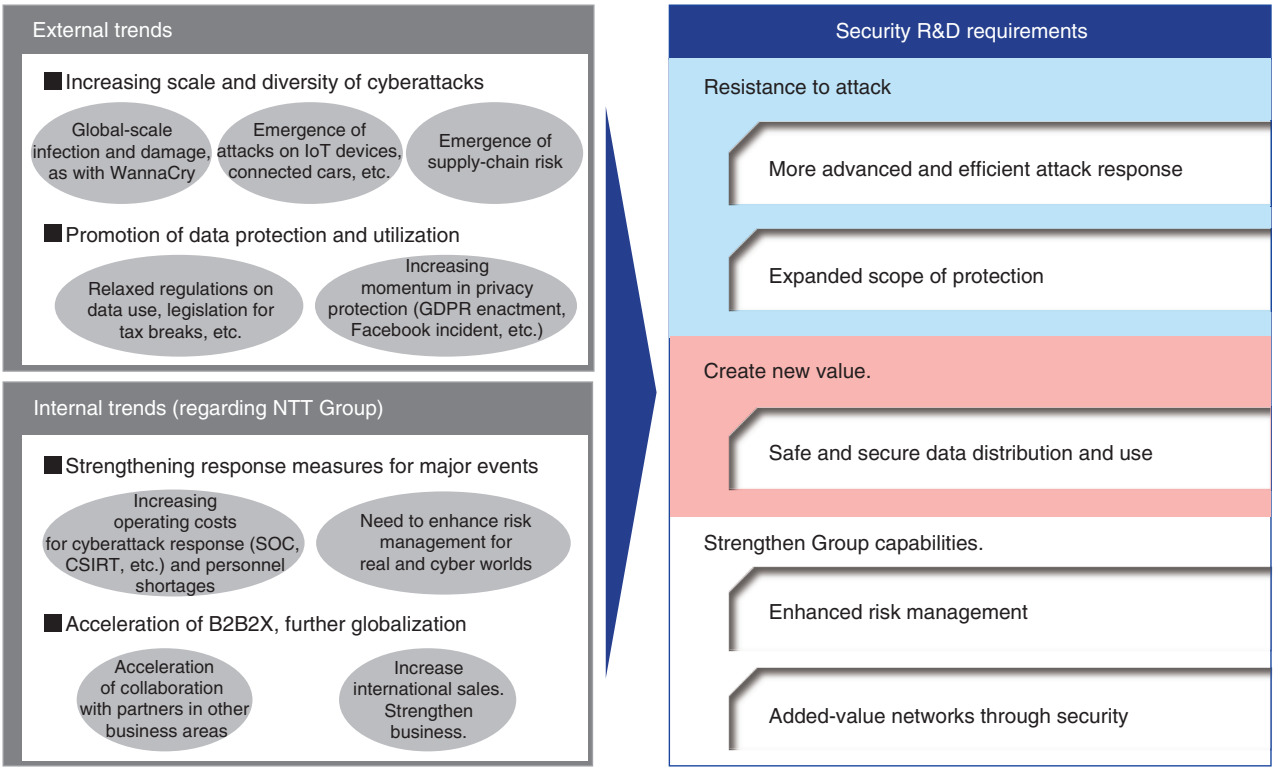
Society is going through major changes with the recent emergence of information and communication technology (ICT) and other innovative technologies. In what is being called *digital transformation*, advances in digital technology and data utilization are bringing high-level integration of cyberspace and physical space. Realization of a digital society is quickly approaching, transforming our living environments and the structure of industry and society. This promises to bring great convenience and utility to society, but there is increasing concern about the potential losses and damage that might occur in society due to previously impossible cyberattacks.

Methods of cyberattack have been advancing and becoming more sophisticated such as the recent appearance of malware with the ability to operate autonomously in cyberspace. Security threats are continuously escalating, as with WannaCry, which exploited vulnerabilities of personal computers to infect systems around the world and inflicted enormous damage. Because of this, in the information technology (IT) domain, cyberattack counter-technologies must continually advance as in an eternal game of cat-and-mouse.

The Internet of Things (IoT) is an important factor in the integration of cyberspace and physical space. From a security perspective, though, there are many IoT devices connected to the Internet that have unpatched vulnerabilities, and these are being used as a platform for distributed denial of service (DDoS) and other large-scale cyberattacks. IoT devices generally do not have the computing resources of other IT devices (CPU (central processing unit) power, memory/disk space, power capacity, etc.), so security functions conventionally used in IT devices cannot be used. As such, establishing new security technologies for IoT devices is an urgent task.

With the accelerating digitization in the fields of operational technology (OT) and critical infrastructure, which provide essential services for everyday life and social activity, control systems of factories and plants are being connected directly to the Internet for the first time. This is leading to growing concern about security threats such as previously unheard of cyberattacks on these facilities, and about the inadequate preparations to prevent such incidents and to deal with them if they occur. Consequently, technical development to improve the security of OT and critical infrastructure, strengthen risk management for both the cyber and the physical worlds, and to optimize operations using technologies such as artificial intelligence are becoming increasingly urgent.

Another issue in realizing a digital society, besides opposing cyberattacks, is to stimulate the use of data. Using digital technologies to obtain and use various



B2B2X: business-to-business-to-X

Fig. 1. Environmental changes and security R&D requirements.

types of detailed data promises to yield new business opportunities such as accurately predicting events that could not previously be predicted, or refining targeting for marketing. Laws are also being revised to accommodate safe and secure businesses utilizing data, while closely examining developments in the digital transformation. Examples of this include revisions to the Act on the Protection of Personal Information introduced in Japan in May 2017, and the enactment of the European Union's General Data Protection Regulations (GDPR). However, there are still obstacles to using data, such as inadequate or incomplete technologies and environments for safe and secure circulation of personal and private information, confidential corporate information, and other sensitive data. Psychological and social acceptance of these technologies is also still quite low. For these reasons, data security technologies such as encryption with advanced features to mitigate risks are in great demand for the creation of new value and economic stimulation.

As an enterprise providing communication infrastructure and supporting ICT businesses, the NTT Group faces conditions with high expectations placed on us as well as requests to us to strengthen efforts to ensure the success of international events. In terms of security in particular, we have to deal with the increasing operational costs of organizations such as security operations centers (SOC) and computer security incident response teams (CSIRT), as they respond to increasingly advanced and sophisticated cyberattacks. There is also a shortage of security personnel to support these organizations and a need to improve the management of risks that accompany such major events.

2. Initiatives at NTT Secure Platform Laboratories

The large environmental changes and market transitions happening in the process of realizing a digital society led to three major research and development (R&D) requirements in order to find solutions to the security issues discussed above (**Fig. 1**).

(1) Promote the advancement, increased efficiency, and automation of responses to cyberattacks

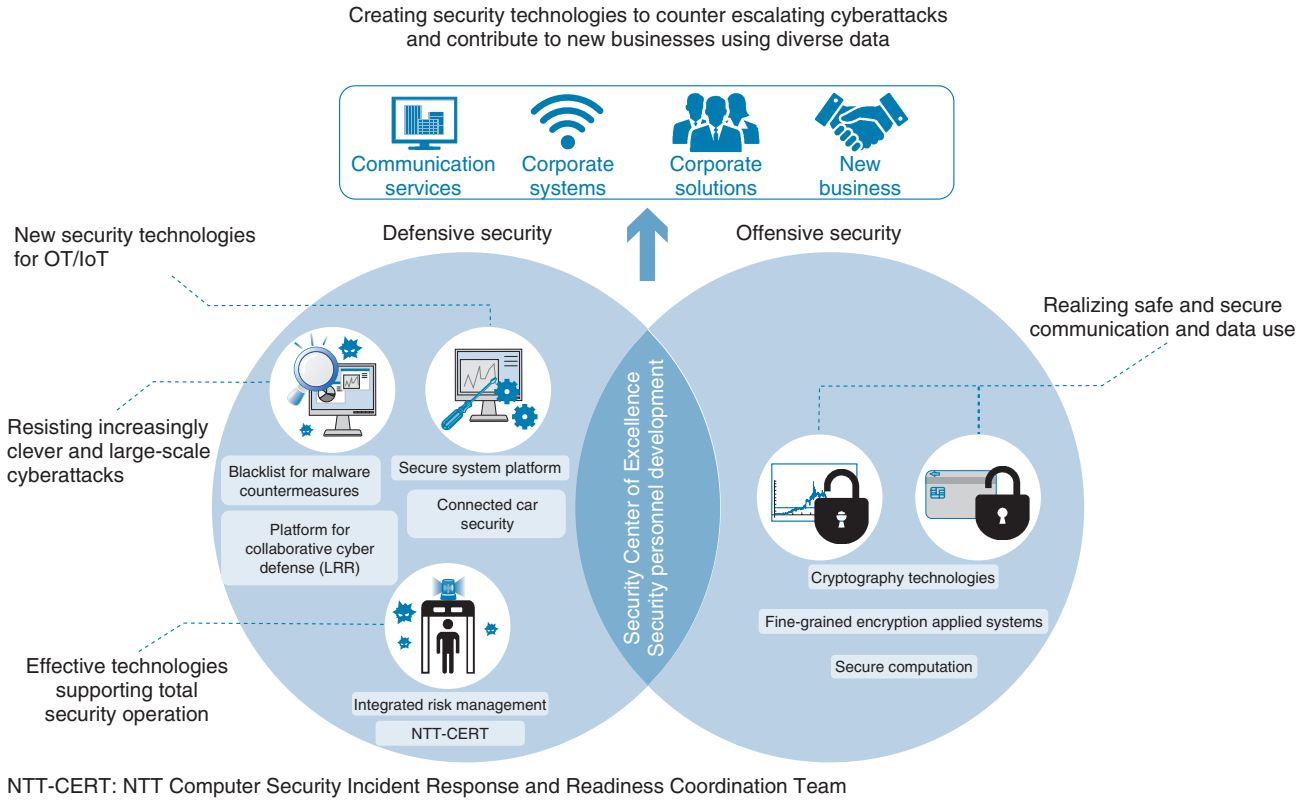


Fig. 2. Security R&D initiatives.

as these attacks increase in sophistication and scale, and expand the scope of protective measures to new domains requiring security, such as IoT and OT.

(2) Realize a safe and secure flow and use of information so that new value can be created.

(3) Advance risk management and create high added-value networks through security in order to enhance the capabilities of the NTT Group.

NTT Secure Platform Laboratories conducts R&D covering these requirements, with the objective of achieving a safe and secure digital society. Specifically, we promote R&D on various security technologies that can be categorized as defensive security, which is focused on opposing the intensifying cyberattacks, offensive security, which uses diverse information to help create new business, and basic research, which is the source of new technologies for the other categories. Our research is organized around a Security Center of Excellence (CoE) and security personnel development (**Fig. 2**).

2.1 Defensive security

In defensive security, we take into account recent changes in environments and market requirements related to cyberspace and conduct world-class R&D on security technologies to eliminate threats and security problems that are materializing in several domains, including conventional IT as well as IoT, OT, and critical infrastructures. The latter require protection from cyberattacks because unlike earlier systems, they connect directly to the Internet.

(1) IT

In the IT domain, to oppose the increasingly large-scale and sophisticated cyberattacks, we continue monitoring corporate, home, and ISP (Internet service provider) networks for attacks as before, and also work to improve countermeasure technologies such as detection of malicious websites [1] and malware infection, bot profiling, and domain reputation. The scope of monitoring must also be expanded, from both micro and macro perspectives, to include both end points and backbone networks. For end points, we are working on malware analysis using technologies such as memory forensics and taint analysis, and

using it to generate advanced IOCs (indicators of compromise). These are then used in effective MDR (managed detection and response) products. For backbone networks, high volume data flow analysis can highlight the overall structure of a botnet and be used for high-performance DDoS detection, and such measures are being used where appropriate.

(2) IoT and OT

In the areas of IoT and OT, a set of security technologies including authentication and authorization, configuration management, detection, and incident handling must be established. For authentication and authorization, we are working on a next-generation authentication technology that does not require password management on the server. With this method, devices submit secret information when first registered as clients, and authentication is performed using encryption with this information and a unique device ID (identification). This technology has the benefits of not requiring individual passwords for each IoT device, or the additional costs of issuing and handling authentication certificates.

In the areas of configuration management, detection, and incident handling, we are developing a technology able to identify or infer devices and ascertain the configuration accurately, in conditions where multiple and diverse IoT devices are connected under a gateway, even in LAN (local area network) environments with severe operational conditions. This is done by analyzing the output characteristics and canceling noise in Address Resolution Protocol frames, which are commonly used. Other technology is able to detect anomalous traffic conditions using methods such as graph theory to identify communication with unusual (not white-listed) counterparts due to cyberattacks or other anomalous causes, and to apply appropriate controls to communication using means such as alerts or blocking.

(3) Critical infrastructure

In the area of critical infrastructure, it is important to consider the increasing risks due to changes in environments, such as the tendency for systems to expand in scale and become more complex and interlinked, and to use new, open, and generic technologies. Regarding the former, it is not unusual for infrastructure facilities to have thousands of server devices and tens or hundreds of thousands of control devices, so the effects of a successful cyberattack on even one of these devices could be widespread. As such, authenticity and integrity monitoring technology that continually checks for compromised or altered devices and prevents anomalous behavior is needed to ensure that components are operating properly.

Regarding the latter, open source software such as Internet technologies and Linux are being widely adopted, and it is getting easier to obtain information regarding vulnerabilities, so it is a basic assumption that cyberattacks will emerge. For anomaly detection, a bolt-on behavior-monitoring and analysis technology is needed that can monitor systems for anomalies, including networks and devices such as IoT, where it cannot be built-in. We have been conducting R&D on some of these technologies from fiscal years 2015 to 2019 as part of the Cross-ministerial Strategic Innovation Promotion Program (SIP), “Cybersecurity for Critical Infrastructure” (funding agency: the New Energy and Industrial Technology Development Organization (NEDO)). This work is supported by the Council for Science, Technology and Innovation (CSTI).

2.2 Offensive security

In offensive security, we conduct R&D on technologies that contribute to the safe and secure utilization of data. The enactment of the revised Act on the Protection of Personal Information has drawn attention to advanced anonymization methods such as k-anonymization. This method processes data using operations such as rounding to coarse-grain the information, based on an index of security called k-anonymity (no fewer than k number of persons with the same information can be distinguished from the data). However, it is difficult to preserve both safety and usability at the same time, so there is concern that data processed in this way will not be usable.

We are developing a technology called Pk-anonymization, which rewrites data introducing randomization. This technology can ensure security equivalent to k-anonymization while maintaining the utility of the data. There is a need in society to handle detailed data that cannot be released outside an organization, even in an anonymized state, such as genome data. In such cases, secure computation can be used to process data directly in its encrypted form. There are many methods that can be considered secure computation, but the technology from NTT Secure Platform Laboratories is based on secret sharing [2], which is a standard from the International Organization for Standardization (ISO). It is a very practical system from the perspectives of a safety definition, general purpose computations, reasonable performance, and international standards, and we will continue R&D and deployment efforts to spread this technology in the future [3].

2.3 Security CoE, security personnel development

The Security CoE provides personnel with the high-level-specialist skills of our laboratories, both within and outside the NTT Group, in wide-ranging fields such as the scientific and high-level specialist communities. In the field of cybersecurity, in addition to operating a well-known contest, we are involved in activities to nurture security personnel, such as writing educational and introductory books [4] that are accessible to non-specialists and giving lectures at universities. In the field of data security, we are conducting world-leading research in fields such as encryption theory and working to create differentiating technologies that will be a source of competitiveness ten or twenty years in the future. Concrete examples include research on fully homomorphic encryption, which could be the next generation of secure computation, and quantum-resistant encryption [5], which will remain safe, even after quantum computers are achieved.

3. Future prospects

For defensive security, technologies for analyzing sites that are under cyberattack, and effective countermeasures that connect directly with business are needed. For offensive security, technologies and environments for using data safely and securely need to be expanded, and initiatives to increase social acceptance, from the perspective of the legal system will be important. NTT Secure Platform Laboratories is working to improve security for the companies in the NTT Group as a whole, to collaborate with external stakeholders, and to realize a safe and secure digital society.

References

[1] T. Watanabe, "Discovery of Silhouette—a New Threat to Privacy—and Our Efforts to Counter It," NTT Technical Review, Vol. 17, No. 3, pp. 11–15, 2019.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201903fa2.html

[2] ISO/IEC 19592-2: Information technology – Security techniques – Secret sharing – Part 2: Fundamental mechanisms

[3] H. Kitajo, T. Yamaguchi, S. Nishiyama, G. Takahashi, A. Miyajima, K. Hirota, S. Nishida, and J. Hashimoto, "Trial Service of Secure Computation System San-shi™," NTT Technical Review, Vol. 17, No. 3, pp. 16–21, 2019.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201903fa3.html

[4] A. Nakajima, "Cyberattack! Happening behind the Scenes in the World of the Net," Kodansha Blue Backs, 2018 (in Japanese).

[5] K. Xagawa, "Research Trends in Post-quantum Cryptography," NTT Technical Review, Vol. 17, No. 3, pp. 22–26, 2019.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201903fa4.html

Kazuhiko Okubo
Vice President and Head of NTT Secure Platform Laboratories.
He received a Master of Science in Management of Technology from the Massachusetts Institute of Technology Sloan School of Management, MA, USA, in 2000. He joined NTT in 1989. At NTT Secure Platform Laboratories, he divides his efforts between protecting the online activity of customers with security technology that can withstand even state-of-the-art cyberattacks, and conducting R&D of technology that can strengthen our competitive edge by ensuring information can be used securely in businesses facing new threats.