Security R&D Initiatives for Creating a Safe and Secure Society

Shinichi Hirata

Abstract

To talk about the future vision of security research and development (R&D) that NTT is working on, it is important to think not only about the problems in front of us but also about the future of society and security. This article introduces security R&D initiatives for the future.

Keywords: security, cyber attacks, data utilization

1. Introduction

The novel coronavirus has had varying impact on our society and lives. Various events, including the Olympic and Paralympic Games, were postponed due to the transition of social activities and lifestyles premised on the securing of social distance.

As the impact of the coronavirus has spread worldwide and the situation is expected to continue for a long time, the world's transformation (adoption of a new way of life and reconstrucion of social order in a post-coronavirus world) is being accelerated; accordingly, various efforts towards digitization and enhancement of connectivity to the Internet are rapidly advancing. The supply chain, which was based on conventional social activities, has become dysfunctional, and major changes are occurring not only at the individual level but also at the social-framework level.

Security and privacy concerns are spreading, and the damage caused by cyber attacks aimed at telework/telecommuniting, which is increasing rapidly, and attacks that take advantage of people's anxiety are becoming increasingly serious. Sufficient consideration must also be given to privacy in monitoring and behavior tracking to identify infected persons and those suspected of being infected for preventing the spread of coronavirus infection.

In the supply chain, wide-area attacks taking advantage of the rapid digitization and enhancemnet of connectivity are intensifying, and reconstruction of secure supply chains is necessary.

NTT is conducting research and development (R&D) on security to contribute to a safe and secure society. As the world changes drastically, it is important to think about the future of society and security to engage in security R&D looking ahead not only to the problems that are occurring in front of us but also to the future.

To create a safe and secure society, we will consider future visions, specifically the Smart World [1] 10 years from now, through changes in the social environment and development of technologies surrounding information and communication technology.

2. What will be the Smart World 10 years from now?

The society in which innovative technologies, such as artificial intelligence (AI), Internet of Things, robots, and big data, have penetrated is the fifth new society (Society 5.0 [2]) in the history of social development, following the development into an industrialized society due to the industrial revolution and into an information society due to the development of computer technology, and is expected to be a future ideal way (Smart World) to enrich lives.

In the Smart World, where cyberspace (virtual space) and the physical space (real space) are highly integrated by various innovative technologies, an enormous amount of data, such as sensor information

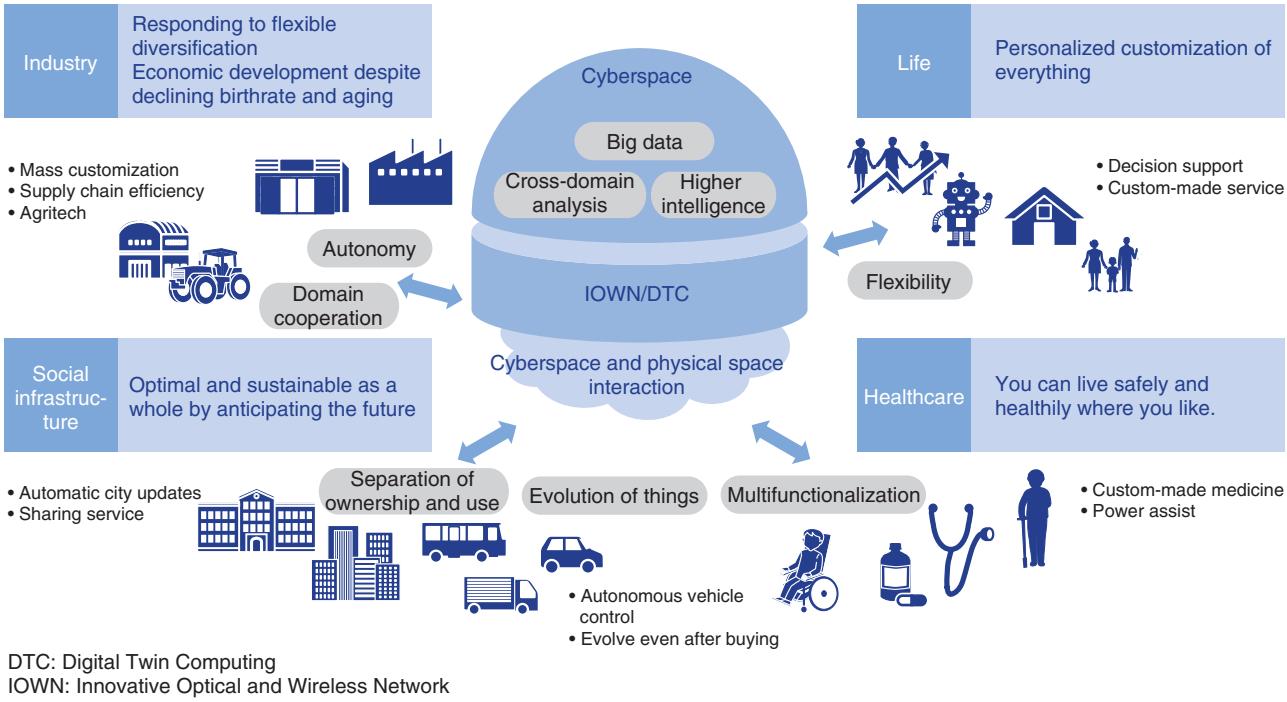

Fig. 1. The Smart World 10 years from now.

accumulated from physical space, is used for data analysis and prediction in highly intelligent cyberspace and fed back autonomously to the physical space. As a result, both the optimization of individual users and that of society as a whole will progress in various services and social infrastructures, and a society in which everyone can live safely and independently (a true Smart World) will be possible.

For example, when it comes to personal life and living, people will be able to enjoy ultimate customized services tailored to their individual circumstances. In terms of social infrastructures, AI predictions will enable us to take proactive measures to optimize the entire society and provide sustainable services. In terms of economy and industry, it will be possible to flexibly respond to diversification and develop the economy even in a society with a declining birthrate and aging population (**Fig. 1**).

There is also concern that the exposure to cyber attacks and the extent of such damage will intensify due to the increase in higher intelligence, autonomy, flexibility, and domain cooperation of technologies and infrastructures that support such an ideal world (**Fig. 2**). When analyzing or using huge amounts of data, privacy may not be sufficiently considered, unethical use may occur, or information may be unintentionally leaked.

The threat of malicious tampering with data-analysis algorithms is also becoming more real. In the past, it was difficult to tamper with a program that was created in accordance with a pre-designed algorithm without directly modifying or replacing it. However, in a situation in which AI has become widespread, there are risks of attacks that do not involve direct tampering, such as causing malfunctions in AI learning and AI decisions. Specifically, we can think of new attacks, such as an attack in which an attacker makes an intended decision by mixing illegal values into data learned by AI or an incorrect decision by crafting data recognized by AI or a new attack in which data that could violate privacy are illegally obtained by inferring data learned from AI operations.

Alteration of the algorithm can not only result in the intentional leakage of data but can also change the analysis results to malicious ones. Malicious analysis results are fed back into the physical space, which has a significant impact on various services and social infrastructures.

To achieve a true Smart World, it is necessary to consider that a new threat will be created by the advanced fusion of cyberspace and the physical space

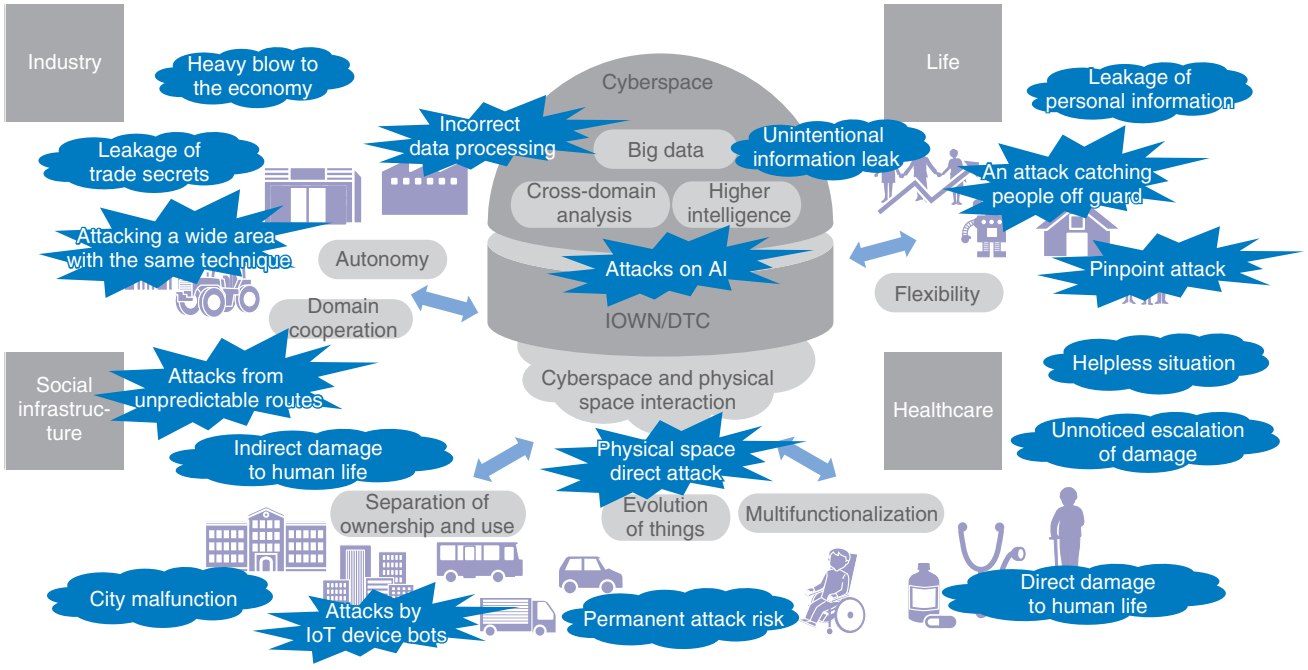

Fig. 2. Security threats in Smart World 10 years from now.

and focus on security R&D that can simultaneously improve convenience while resisting attacks that grow in size and sophistication.

3. Approach to security R&D from a long-term perspective

Security risk depends on the threat of an attack (in a broad sense involving people and society), vulnerability of the system, and size of the assets that must be protected (including not only information and money but also human life). As cyber attacks grow in size and sophistication and we become more exposed to various threats due to the advanced fusion of cyberspace and the physical space, security risks will increase dramatically.

There is a limit to how much a company can spend on security measures because it is expensive to strengthen security measures. It is difficult to implement countermeasures against all threats only by extending or simply enhancing existing security measures. Therefore, it is necessary to drastically improve defense and countermeasures against cyber attacks.

Security R&D from a long-term perspective must (1) focus on technologies that respond to new threats and protect the environment to support the creation of value in the Smart World; and (2) create technologies that change the situation in which attackers dominate, such as technologies that reduce the vulnerability risk to zero and that predict and proactively respond to attacks.

The NTT Group will strengthen its response systems to major sporting and cultural events, and the development of new fields (urban development, energy, and healthcare) on the basis of its medium-term management strategy will require the safe use of data and the security necessary to implement the Innovative Optical and Wireless Network (IOWN). Therefore, the following points will be important in security R&D (**Fig. 3**).

(1) Development and deployment of data distribution and utilization technologies that secure the value-creation process

Develop technology for flexible and safe sharing and analysis of data and capable of using data across fields to solve problems of data encirclement, privacy infringement, and illegal use of data [3].

(2) Development of technologies to solve operational-cost problems and minimize damage

Develop technology to autonomously and automatically respond to cyber attacks while responding to new threats so that humans will be able to focus on confirming responses and responding to new threats that require creativity, thereby strengthening their

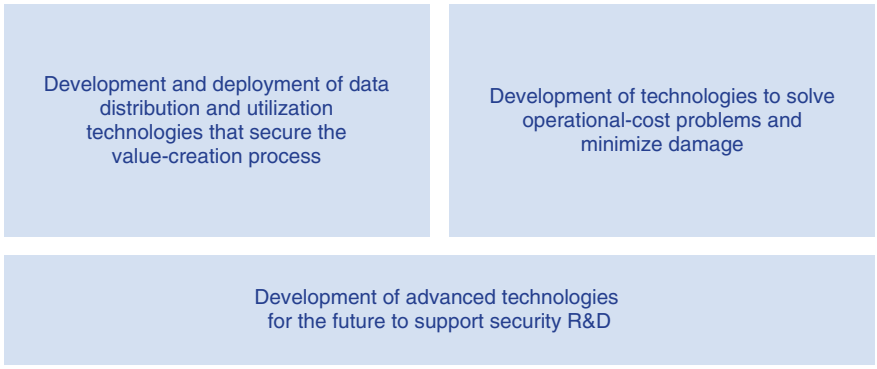

Fig. 3. Viewpoints required for security R&D.

comprehensive response capabilities [4].

(3) Development of advanced technologies for the future to support security R&D

As a security Center of Excellence, develop basic technologies for the future such as cryptography and information theory and quantum information security technology [5].

To sustain the safe and secure communication demanded by the NTT Group into the future, we will engage in R&D to meet the medium- and long-term objectives of safe data distribution and utilization and minimize damage including cutting-edge technologies for the future and those that make use of IOWN.

References

[1] NTT Technology Report for the Smart World, https://www.rd.ntt/e/techreport/

[2] Cabinet Office, Government of Japan, "Society 5.0," https://www8.cao.go.jp/cstp/english/society5_0/index.html

[3] T. Washio, Y. Orime, T. Morita, K. Chida, K. Morimura, and Y. Oshima, "Data Sharing and Utilization Technologies for Safe and Secure Value-creation Processes," NTT Technical Review, Vol. 19, No. 6, pp. 75–80, June 2021. https://ntt-review.jp/archive/ntttechnical.php?contents=ntr202106fa12.html

[4] Y. Koga, Y. Nakajima, N. Chiba, J. Miyoshi, T. Koyama, H. Shito, and A. Miyajima, "Establishment and Development of Cybersecurity Technologies to Solve Problem of Increasing Operation Costs and to Minimize Damage," NTT Technical Review, Vol. 19, No. 6, pp. 81–87, June 2021. https://ntt-review.jp/archive/ntttechnical.php?contents=ntr202106fa13.html

[5] Y. Tokunaga, Y. Suzuki, S. Endo, R. Nishimaki, F. Kitagawa, and S. Tamechika, "Security Based on Quantum Information Technology and Data Protection of Quantum Information," NTT Technical Review, Vol. 19, No. 6, pp. 88–93, June 2021. https://ntt-review.jp/archive/ntttechnical.php?contents=ntr202106fa14.html

Shinichi Hirata
Vice President, Head of NTT Secure Platform Laboratories.
He received a B.S. from Hokkaido University in 1990 and joined NTT in the same year. He has been engaged in R&D of cryptography, smart card technology, and authentication systems.