Security as Driving Force of the Future

Shinichi Hirata and Katsumi Takahashi

Abstract

This article describes research and development (R&D) of security in the Innovative Optical and Wireless Network (IOWN) era to create a prosperous and enriching society. We seek to change the role of security to activating people and ideas. This new form of security will solve diverse problems related to security motivation in individuals, organizations, and society, convert ideas and computing resources directly into work, and ensure continuous security. We will achieve this through R&D based on the three pillars of theory, data-driven approach, and communication.

Keywords: security, IOWN, R&D

1. Driving force of the future

We have been studying communication and information security continuously for more than 30 years. During this time, the Internet came into being as a means of communicating safely no matter where one may be through cryptography; similarly, the web and cloud came into being as means of safely storing information anywhere through security measures. However, while our daily lives have thus far been protected by such security measures, it cannot be overlooked that there is still much anxiety over security threats; thus, the need for giving full attention to security measures.

The Innovative Optical and Wireless Network (IOWN) era will make life more enriching and satisfying through information and communications technology (ICT) that exceeds the limits of conventional technology. It is our goal to make security the driving force behind this transformation.

There is no debate as to the need for security. The security by design approach is being increasingly adopted, which points to the inherent need for security in achieving healthy individual and social activities. However, keywords, such as *security cost* and *security fatigue*, have appeared, reflecting the common feeling that anything that is needed to ensure healthy activities must be obligatory and troublesome. We disagree with this mode of thinking. Simply put, security should bring about a bright future.

It is our intent to change the current belief that security technology is necessary but difficult through research and development (R&D) on the basis of the following viewpoints:

- Security is widely useful for all types of work and lifestyles (*extended*).
- Security can convert ideas and computing resources directly into work (*efficient*).
- Security is ongoing (*continuous*).

In this article, we explain the concept of security R&D in the IOWN era from the viewpoints of extended, efficient, and continuous security and outline the security technologies that we will target (**Fig. 1**). The type of security discussed in this article is information security that, while not intended for maintaining public peace and order, includes peripheral fields such as privacy and ethics.

2. Extended security

It had been generally believed that security is for a particular system to be unbreakable. Since we see security as being useful for all types of work and lifestyles, we would like to drive the evolution of security R&D from the two viewpoints of security targets and security motivation.

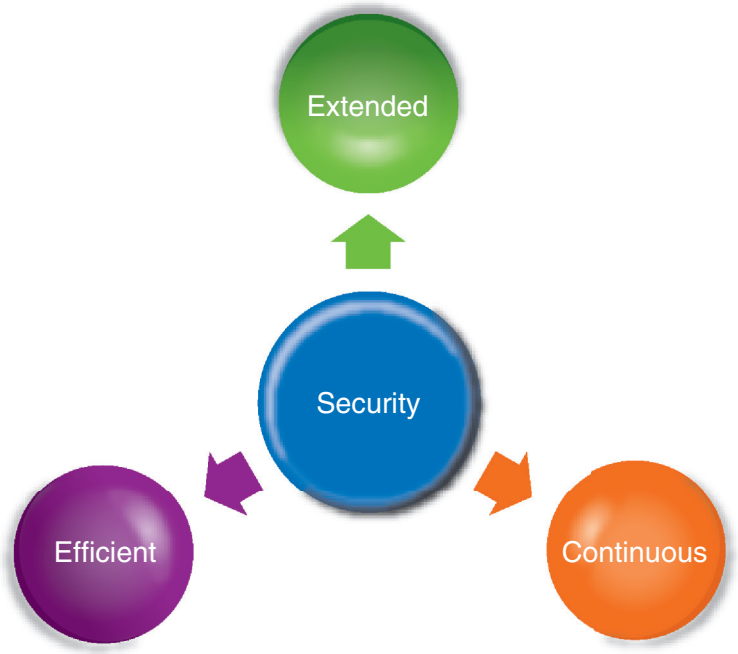

Fig. 1. Concept of security R&D in the IOWN era.

2.1 Extended 1: Security targets

In addition to particular systems (information assets) as targets of protection by security, we would like to include companies and organizations, people, and society.

2.1.1 Information assets

The target of security has been called *information assets*, which means a company's customer information, sales information, technical information, etc. The protection of information assets depends on the form of their records or storage, so the means of storing these information assets will also be a target of protection. Typical formats include files; media, such as paper; disk storage; transmission channels; hardware systems, such as smartphones and computers; and software systems, such as email, databases, and artificial intelligence (AI) services. We can add Internet of Things (IoT) devices such as drones and industrial robots.

2.1.2 Extension to companies and organizations

The targets of security are expected to change greatly in parallel with changes in the activities of companies and organizations. For example, determining the form of information assets will become difficult. Information assets may be placed in storage equipment outside the company or under the management of a separate organization through inter-company transactions. In future companies, the data generated by others in a procurement or supply chain may become an information asset of those companies. The introduction of IoT devices, however, will make the form of information assets all the more fluid.

2.1.3 Extension to people

If people were to be regarded as a medium of information assets, they could be called a medium requiring a very high degree of confidentiality. While it is said that facial expressions reflect a person's feelings, it is not the case that customer information could be leaked from facial expressions. People can be easily deceived, and in some cases, they can betray others. Corporations deal with such situations by training their employees and establishing rules and regulations. There is also posting in social networking services (SNSs) as a medium of people's activities not limited to those of corporations. Information security incidents via SNSs include information leaks, copyright infringements, and flaming. However, such incidents are mostly left as a matter of personal responsibility. When it comes to security targeting people, there is a limit as to what safety management that treats people as systems can accomplish.

2.1.4 Extension to society

There is currently no established opinion on whether society can be set as a target of security. Autonomous

car and surveillance-camera systems, for example, are in the process of becoming systemized at a social level. In a smart city, such systems will have basic conventions (policies) with regard to security, so this can be thought of as an extension of a conventional security target, though it depends on the system scale. A specific example is how a pandemic should be dealt with. Measures, such as contact-tracing apps, operate under clear policies, but the rules of behavior behind the operation of many other measures tend to be agreed upon by consensus through voluntary and spontaneous exchanges of information. It is thought that society as a whole operates in this manner. Such rules of behavior are sometimes referred to as ethics or customs, and dealing with them requires a new approach.

2.2 Extended 2: Security motivation

We believe that the reasons (motivation) security is necessary are wide-ranging going beyond preventing information leaks. They also include the existence of incidents, system quality, laws, ethics, customs, and social objectives.

2.2.1 Incidents

The most known motivation for security is preventing information leaks. It is common knowledge that this motivation drives measures for blocking a variety of threats such as unauthorized access, malicious software, and unauthorized entry and exit. However, we believe that it is important not to think of such incidents as infringing upon confidentiality, integrity, and availability. For example, incidents involving privacy (flaming) should also be given attention. Instead of being a matter of information leaking, they have been thought of as a peripheral security problem that arises due to inadequate explanation of information access, purpose of use, etc. or violation of rules. We should also think about whether abnormal AI operations are peripheral security problems. The results of AI operations have not traditionally been considered a security problem. We consider that problems requiring attention should not be treated within the conventional security framework but be extended to include any problems brought about by computers or problems related to privacy, AI, etc.

2.2.2 System quality

In fields such as critical infrastructures, a high level of security is required beforehand in system development. This need produces some of the motivation for security. Yet, there are also systems in which security is just a tacit requirement. In such a case, the level of security required is also tacitly expressed, and providing for security is simply regarded as a development cost. This is a problem that cannot be ignored. Security is an inherent requirement of a system, so any deviation from that requirement due to a lack of motivation must be fundamentally solved starting with its cause.

2.2.3 Laws

Observing laws and regulations is also a security motivation. In Japan, the Basic Act on Cybersecurity calls for the people of the nation to make security-related efforts. For companies, this means security premised on such laws as the Act on the Protection of Personal Information and Unfair Competition Prevention Act. We believe that it is not simply a matter of scrutinizing the security-related legal system and applying it to R&D but something that must be actively participated in through discussions on what the legal system should be.

2.2.4 Ethics, customs, and social objectives

There are cases in which security would still be felt necessary even if there were no fear of incidents, quality was kept constant, and laws were complied with. This feeling is based on values and fears that people hold within themselves that can be expressed in terms of ethics, customs, and social objectives. We believe their existence should be treated as elements providing some of the motivation for security.

3. Efficient security as a driving force

Unfortunately, security has the possibility of being treated as a business cost, but we would like to change this perception by introducing the concept of security efficiency. Efficiency relates to (1) ideas and (2) computing resources. Maximizing both these aspects will maximize the efficiency of security.

3.1 Efficiency 1: Converting ideas directly into work

We are investigating security that does not hinder the implementation of ideas and supports people in challenging themselves. When implementing an idea, security requirements and methods of achieving them must be determined. Minimizing this process leads to efficiency, and ideally, the security required at the time of system development would be built-in without having to worry about it.

Determining requirements normally consists of analyzing all the elements described above under security motivation, legal compliance assuming the occurrence of incidents, etc. Next, in determining a method for satisfying these requirements, it should be

noted that constructing security measures from scratch is seldom done. The typical approach is to survey available components (in a library) and use the security functions needed.

We are now investigating minimizing and automating both processes. The automation of security is extremely difficult, but the problems involved can be solved through a theoretical approach and the data-driven approach described later. In addition, if *best coupling* of security requirements and implementation methods can be provided through a development environment and user interface, a shortcut to solving these problems should be achieved.

3.2 Efficiency 2: Converting computing resources directly into work

In current web applications, for example, no one is really concerned about the fact that security processing generates overhead and slows down communications and screen displays. However, in the IOWN era in which a massive amount of devices in urban, transport, and other social infrastructures are connected to the network, this cannot be ignored. In the context of carbon-neutral initiatives, security processing that can make full use of computing and communication resources is desirable. For this reason, we are investigating security that can exploit the special features of advanced hardware represented with the All-Photonics Network of IOWN and maximize our experience with information communications.

4. Continuous security

Security must be continuously maintained. Security attacks and defensive measures evolve along with ongoing progress in information processing technology, so our R&D efforts in this area are ongoing to be prepared for that evolution. There is another reason continuity in security R&D is necessary. The core of security technology is theory and data. An example of the former is cryptography and an example of the latter is whitelisting/blacklisting in which theory and data, respectively, must be continually built up. In contrast to the continuity of security technology, the arrival of discontinuous changes in the form of quantum computers is predicted. We are therefore investigating the development of technology based on continuity that can withstand even major changes.

5. Three new pillars of security R&D

To achieve extended, efficient, and continuous security, we are promoting R&D focused on the following three pillars (**Fig. 2**).

5.1 Guaranteeing security through theory

Cryptography guarantees the confidentiality of applied data through theory. Given a software module that is theoretically guaranteed to be safe, there is no need to worry about the security of that module. If a system should be constructed by correctly interconnecting only theoretically safe modules, that system can be evaluated as being entirely secure. Increasing the number of theoretically safe modules will clearly contribute to achieving system security. While cryptography is typical of theory that can guarantee security, mathematics, including cryptography, cryptographic protocols, and formal methods, forms the foundation of this theory. Attention is also being given to physics. If quantum information processing becomes possible, we can expect the prevention of new forms of eavesdropping and data alteration to be found not only in communications but in data processing.

5.2 Guaranteeing security by using a data-driven approach

Theoretically guaranteeing the security of all targets is difficult, so it is necessary to guarantee certain items in a data-driven manner. For example, given an infrastructure system consisting of multiple devices, one approach is to record the state of all constituent devices and evaluate risk. This work would be carried out throughout a supply chain and its operations. The records of these states constitute data, and their evaluation is called a data-driven approach. Those parts of an evaluation result that can be used at other times and in other environments can be reformatted and reused. This data-driven approach can be applied to any security target in addition to infrastructure systems. We call such data for conducting re-evaluations *trust data*, which includes both positive and negative evaluations with regard to safety. Using trust data enables a data-driven type of security guarantee. Trust data are not intended to be absolute overall but rather local and fair.

5.3 Communication for a consensus of security level

In addition to the theoretical and data-driven continuous approaches, there is the communication approach in relation to forming agreements that we have come to recognize as being extremely necessary. We noticed that we have to consider how to establish

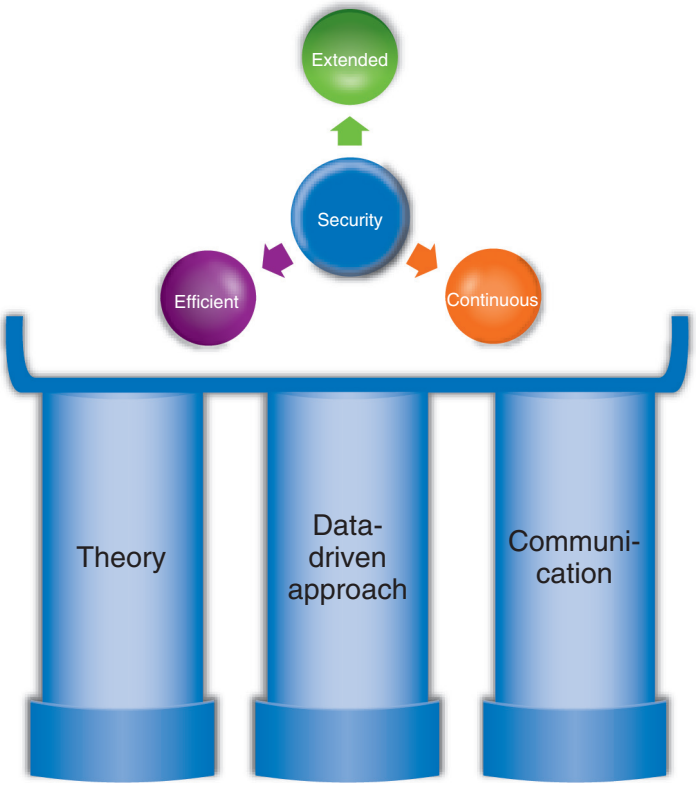

Fig. 2. Three pillars of security R&D.

a security policy, which is a precondition of executing security measures, by considering what is safe to do, and what should be done so that people can live their lives to the fullest without anxiety. To establish a policy that confirms a *security motivation*, we believe that forming agreements through communication between the parties concerned becomes important while extending security in the narrow sense to ethics, customs, and social objectives. We are studying a mechanism for forming agreements on security decisions by concerned parties and a mechanism for evaluating whether operations can actually be carried out according to the agreed-upon decision.

6. Conclusion

In this article, we reorganized the direction of security R&D in the IOWN era from the viewpoints of extended, efficient, and continuous security and outlined the security technologies that we will target by the three pillars of theory, data-driven approach, and communication. We aim to create a society without anxiety regarding security with high ethical standards and technologies.

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

Katsumi Takahashi
Executive Research Scientist, Chief Security Scientist, NTT Social Informatics Laboratories.
He received a B.S. in mathematics from Tokyo Institute of Technology in 1988 and Ph.D. in information science and technology from the University of Tokyo in 2006. He joined NTT in 1988 and has studied information processing technologies including security and privacy.