Invited Paper

Cybersecurity Technologies Essential in the Digital Transformation Era

Kazuhiko Ohkubo

NTT Secure Platform Laboratories, NTT Corporation, Japan
kazuhiko.ookubo.sw@hco.ntt.co.jp

Abstract - An age of digital transformation is currently pressing. New fundamental technologies are penetrating in fields of IoT (Internet of Things) and OT (Operational Technology) in addition to a conventional IT field. Also, a paradigm shift of the ICT environment is producing many advanced economic activities of data use in society. This paper summarizes increasing security risks in such a condition and security technologies we should promptly develop for reducing the risks. Regarding IT security, threat monitoring targets need to be expand to more micro and macro, specifically to endpoint and backbone network. Regarding IoT and OT including critical infrastructure, breakthrough countermeasure functions need to be developed all over functions of the NIST Cybersecurity Framework. Then, we should take into consideration IoT and OT features such as poor computer resources, peculiar industrial protocol, variations of system configuration, etc. Toward development of data use in society, an up-to-date environment needs to be offered by making full use of cryptographic techniques. In other words, both data holders and data users can distribute and handle even privacy and confidential information safely and securely.

Keywords: Cyberattack countermeasure, NIST Cybersecurity Framework, Critical Infrastructure Protection, Secure Computation, Anonymization

1 INTRODUCTION

Digital transformation is the idea that “IT will penetrate every aspect of people’s lives to transform it for the better,” proposed in 2004 by Professor Erik Stolterman of Umea University, Sweden [1]. In the first phase of digitization, work processes were improved through use of IT; in the second phase work is being replaced by IT; and in the third phase work is being transformed seamlessly to IT, and IT to work. In the past, mechanisms such as artificial intelligence and robotics belonged to the world of science fiction, but they are now being realized, partly through innovations in IT technology, to develop a cyberspace society that distinguishes less and less between real and virtual worlds.

Security threats are rapidly escalating. Malware that can act more and more autonomously have begun to appear, cyberattacks are increasingly intelligent. Moreover, Internet of Things (IoT) devices, which are already vulnerable in terms of security, are being connected to the Internet but providing a platform for large-scale DDoS cyberattacks. For these reasons, technologies to counter cyberattacks must continually advance in a game of cat-and-mouse. Also, technologies to counter new anticipated security threats are needed as economic activity develops and ICT environments undergo further paradigm shifts.

On the other hand, the approach of the 2020 Tokyo Olympics and Paralympics is prompting serious concern regarding increasing threats to security in the Operational Technology (OT) domain. This covers control systems and even critical infrastructure, and the concern is whether or not activity surrounding incident prevention and operational responses is adequate if an incident should occur. As such, urgent issues have already become technical development to maintain security for OT domain and strengthening security risk management to improve efficiency of various operational responses.

In addition to "defensive" security measure described above, there is also an increasing need for so-called "offensive" security measure. It enables to ensure safe and secure data utilization businesses that keep pace with the progress of digital transformation. Especially, it will play an important role in light of the enactment of revisions to the personal information protection laws made in May 2017 and the General Data Protection Regulations (GDPR) in May 2018. As such, there is much anticipation for efforts toward risk mitigation using encryption and other information security technologies, and toward new value creation that will contribute to economic revitalization.

Considering these changes in the cyberspace environment and economy, this article discusses threats and security issues being realized in the areas of IT, Non-IT (IoT/OT) including critical infrastructure, and data use in society. Then, it studies on technical development needed to be accelerated for elimination of these issues in the future. Finally, we discuss current conditions and future prospects for security related to AI, which is still advancing today, and anticipates the so-called Singularity, when it is believed AI will exceed human intelligence.

2 CAT-AND-MOUSE IT SECURITY

For the PyeongChang Winter Olympics in February 2018, targeted attacks on Olympics-related organizations occurred from the beginning of the year, and several incidents caused damage around the time of the opening ceremony. Specifically, the public Web site, the press center network connection and the stadium wireless LAN all went down temporarily, and the drones intended for use during the opening ceremony did not fly. We conducted an independent investigation, acquiring and analyzing malware used in the cyberattacks, called Olympic Destroyer. As a result, we found that the malware caused destructive activity in PCs and other devices, and that the attack was clearly intended to disrupt the event. Besides, recent cyberattacks

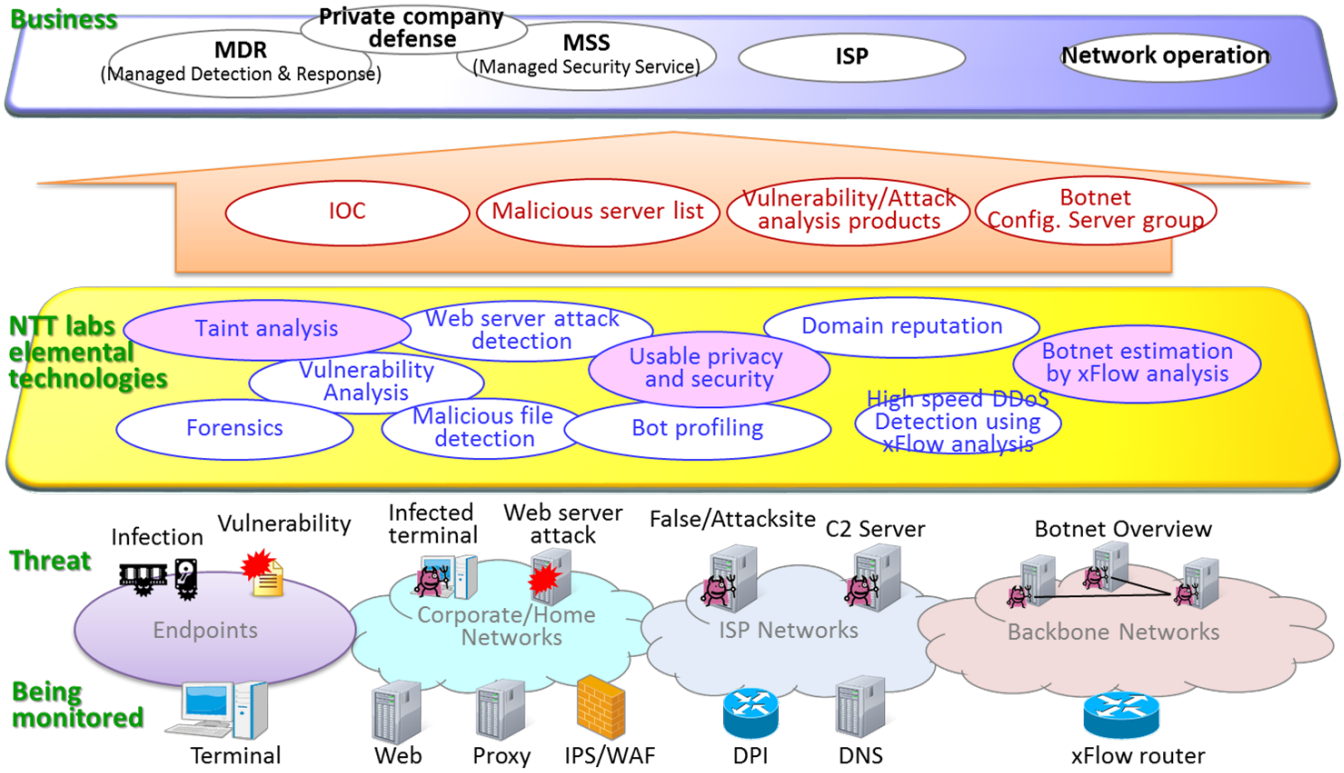

Figure 1: Cyberattack countermeasures in a game of cat-and-mouse.

are becoming not only more ingenious but also more increasing in scale by utilizing many devices infected with malware to conduct DDoS attacks.

Cyberattacks are getting smarter and increasing in scale in these ways, so the scope of monitoring needs to expand in order to oppose them. Conventionally, corporate, home and ISP networks were monitored, but this must expand to include both micro and macro perspectives, from endpoints to backbone networks (Fig. 1). Regarding endpoints, advanced Indicators of Compromise (IOC) are generated by using technologies such as taint analysis to precisely analyze malware behavior. Such IOC can be effectively used in Managed Detection and Response (MDR) and other products. On backbone networks, analysis of large volumes of flow data can reveal the overall structure (Herder, C2 server and bot terminals) of a botnet, and provide clues to appropriate countermeasures.

Although security technology developed in the past focused mainly on system and network security, a technical area called "Usable privacy & security" is recently increasingly getting attention in the world. It takes the perspective that it was the user that was ultimately deceived, and focuses on human-computer interaction. Specifically, it attempts to improve security by identifying causal gaps due to user unawareness or inappropriate action, and making system improvements accordingly. Such gaps in privacy and security are also leading to promising advances in honeypots that mimic user behavior and intelligent technologies for security experts.

3 SECURITY IN THE NON-IT FIELDS OF IOT/OT

The first time that Mirai, a prototypical malware infecting IoT devices, was used for a large-scale attack was a DDOS attack to the "KrebsOnSecurity" security blog in September 2016. It was the largest that had been seen at the time, at a reported 620 Gbps. The Mirai source code was then immediately released by someone called Anna-senpai, resulting in the creation of many variants, most of which were used in a stream of other large scale DDoS attacks. Figure 2 shows the Mirai attack mechanism that we clarified by downloading and analyzing its source code. According to this, we can find not only the attack mechanism is complicated but also each IoT device is extremely vulnerable. Specifically, high-speed telnet port scan and brute-force attack can be easily done. In these incidents, most of the owners were not aware that their IoT devices were being used in large-scale DDoS attacks. On the contrary, IoT device owners are being embarrassed by ransom-ware type variations. The ability to infect IoT devices with ransom-ware, rendering them inoperable if a ransom was not paid (by bitcoin for example), had already been verified in the laboratory. So, it is just a matter of time that this occurs as well.

In March 2018, as also reported in newspapers, it was discovered that the administrator screens of several hundred routers at a telecommunications operator were visible from the Internet. This is something generally true for IoT devices, but it is assumed that in all cases, the fundamental issue was

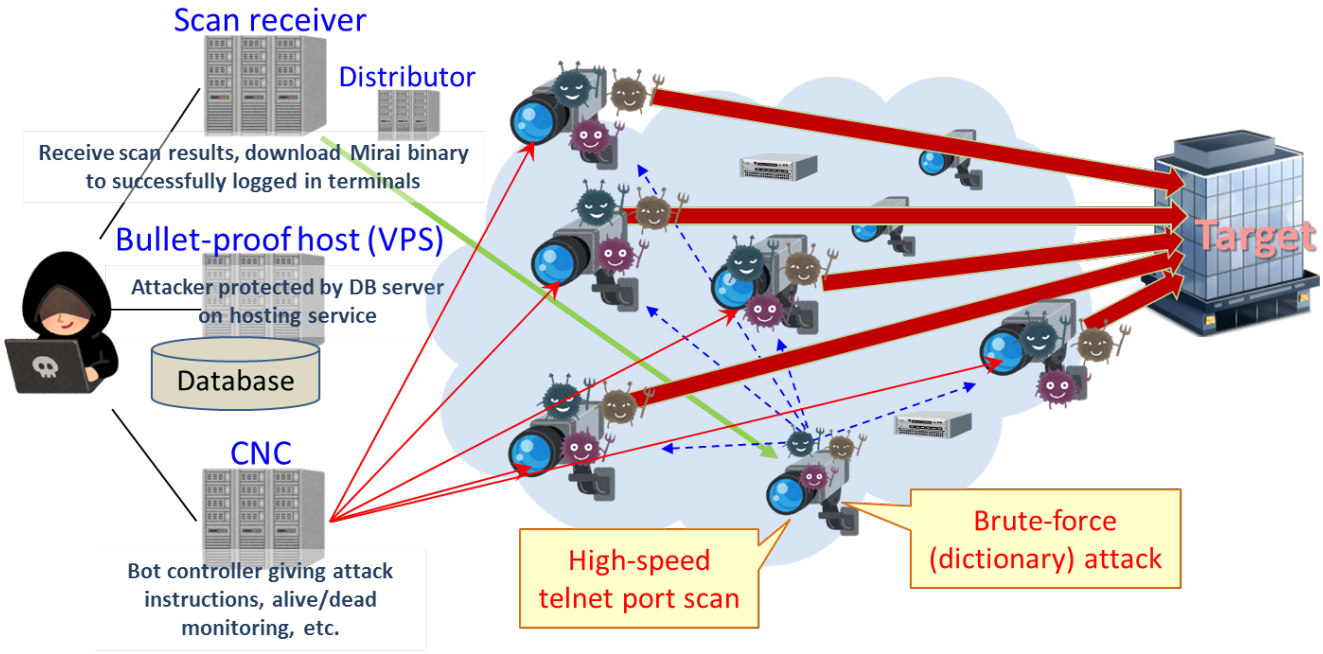

Figure 2: Mirai attack mechanism.

that the Web-UIs were open to external access for any of the following reasons.

- Default ID/PWDs were extremely simple
- Operation possible without changing default ID/PWD
- The same default ID/PWD is used for all units of a given product or all products from a given vendor
- Online manuals giving default ID/PWD can be seen online by anyone

To address the issue, the Ministry of Internal Affairs and Communications in Japan has revised regulations governing communications operators to begin implementing necessary measures within 2018 [2]. As part of this, National Institute of Information and Communications Technology (NICT) Act is working to be revised. Specifically, it will augment NICT's duties with details such as adding a five-year limited survey of IoT devices with inadequate password settings. The revision and enactment of laws are scheduled to complete in fiscal year 2018.

From a technical development point of view, because IoT devices are limited in computing resources of CPU, memory, disk space, battery and the like, existing IT security functions such as anti-virus software cannot be used. Thus, a new range of security technologies for IoT devices covering authentication/authorization, configuration management, and detection and response must be established from scratch. Such necessary technologies can also be classified into functional elements of the USA National Institute of Standards and Technology (NIST) Cybersecurity Framework [3]. The Framework enables organizations regardless of size, degree of cybersecurity risk, or cybersecurity sophistication to apply the principles and best practices of risk management to improve security and resilience. The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today.

For authentication/authorization, an example would be a next-generation authentication technology not requiring password management at the server (Fi. 3). Such a technology would provide some secret information to the device from an initial registration server when the client is first initialized. It would be used together with a simple, device-specific ID, like the PIN number used with a cash card, to implement authentication. This would allow operation without managing passwords of individual IoT devices, and cost reduction of issuing and using certificates needed for authentication.

Regarding configuration management, detection and response, when various IoT devices are connected under a gateway, devices can be identified or estimated accurately. Then, the configuration must be discovered even in LAN environments with severe operating conditions. This can be done by analyzing the output characteristics of commonly used ARP frames and using noise cancelation. IoT device specific information can then be used to discover devices with vulnerabilities. Graph theory and other techniques can also be used to detect traffic anomalies excluded from a white list of usual communication counterparts. This enables to classify abnormal communication as a part of an attack or otherwise, and handle it with a communication control alert, quarantine, or other means.

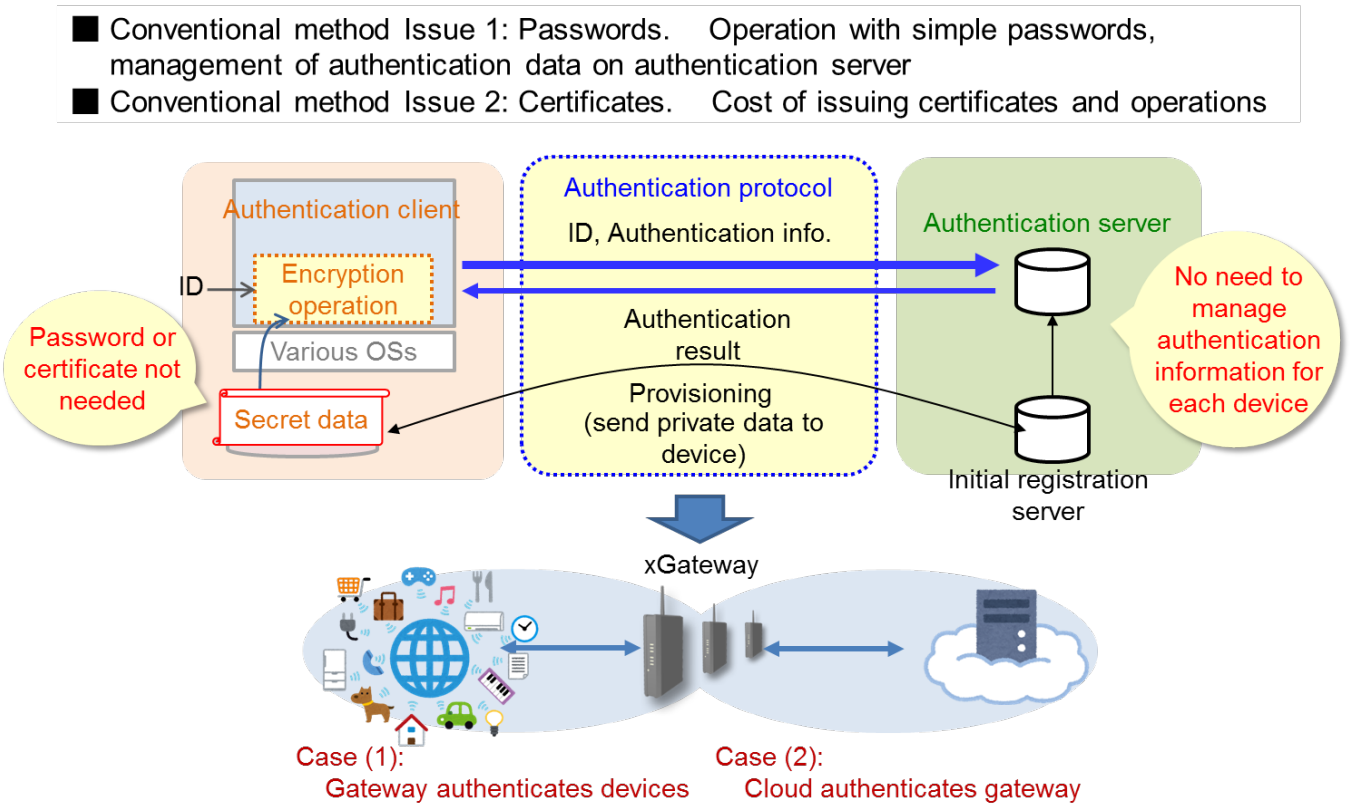

Figure 3: Next generation authentication technology for IoT.

Similarly, security technology for OT must also be re-established from the start, and unique aspects particular to this domain, such as industrial protocols, must also be handled. InteRSePT® is composed of "Real-time detection/handling" and "Security integration management" through a joint development between MHI, Mitsubishi Heavy Industry, and NTT [4]. Sensor and other data on the network is comprehensively monitored by InteRSePT to detect malicious cyberattacks using control commands that were difficult to deal with using earlier technology. Security rules can be changed in real time for each operational state of the devices, to detect anomalies quickly, handle unknown cyberattacks and maintain system availability.

4 SECURITY ASPECTS OF PROTECTING CRITICAL INFRASTRUCTURE

From 2009 into 2010, a malware called Stuxnet infiltrated nuclear facilities in Iran causing real damage and becoming the first known cyberattack on critical infrastructure. The fact that industrial control systems not connected to the Internet could be infected through USB memory was a major shock at the time.

When considering the increasing cyber-risks for critical infrastructure, important points include the followings.

(1) Characteristics of being large-scale and involving complex linked systems
(2) Changes in the environment toward application of general purpose, open, and new technologies

Regarding the former (1), it is not unusual for infrastructure facilities to have thousands of server devices, and tens to hundreds of thousands of control devices. If a cyberattack is successful on even one of these locations, the effects could be widespread. Thus, technology is needed to continually check that components are authentic and have not been illicitly infiltrated or modified, to prevent abnormal operation as shown in Fig. 4. Authenticity checking technology builds a chain of trust (trust reference points) and enables to reliably detect any system falsification occurring on a large-scale system, system-wide and from startup through operation.

The authenticity checking resembles a technique used in an IC (Integrated Circuit) passport. In other words, an IC passport has a plastic card with a contactless IC chip built into the center of the passport booklet. It stores basic passport information including the passport holder's name, nationality, birth date, and passport number, as well as a facial image (exactly digest data of facial image) read from the photo in the PDF of the passport application. At passport control, it is very easy for an officer to discover foreigners that substituted the facial image by comparing the digest data such as "hash value." It is just a concept to introduce

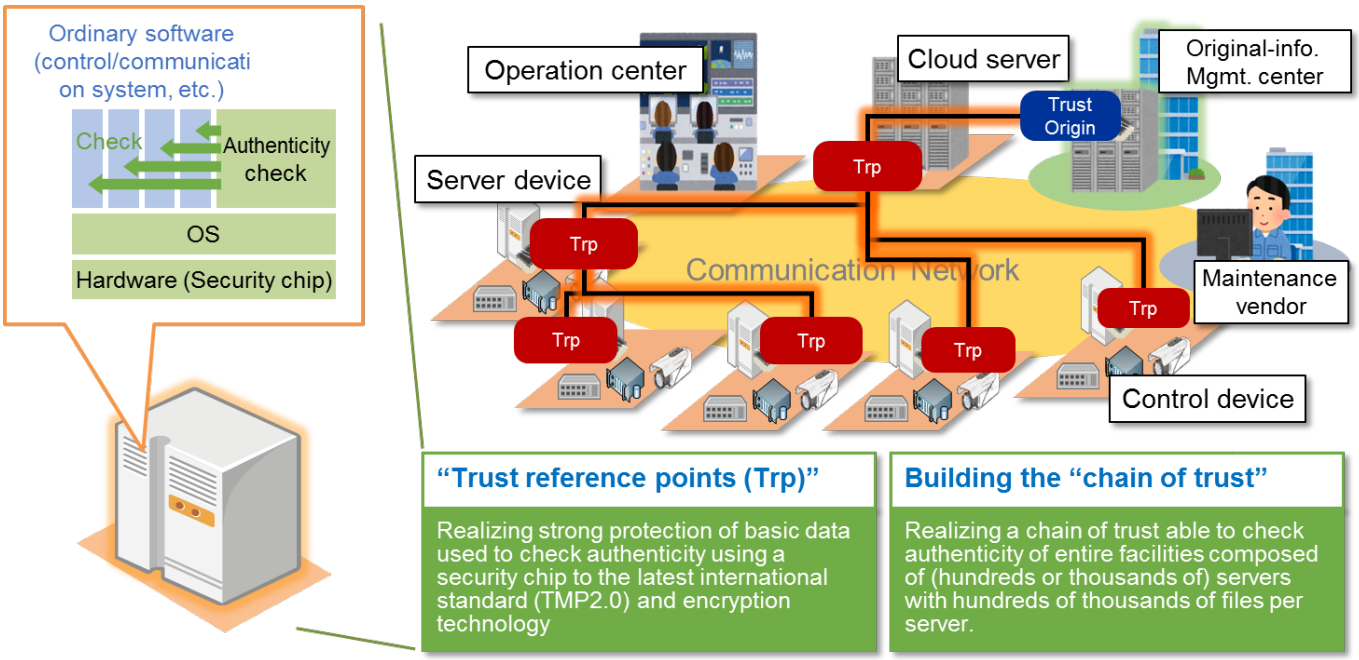

Figure 4: Detecting system falsification with authenticity checking technology.

such a mechanism into individual devices that are components of a critical infrastructure facility.

Regarding the latter (2), Internet technologies and open source software such as Linux continue to be adopted, making it easier to obtain vulnerability and other information needed for attacks. As such, a major assumption is that, for devices and networks where the authenticity checking technology cannot be built-in, there is a need for bolt-on technology able to monitor and analyze system behavior for anomalies.

Behavior monitoring and analysis technology can adapt automatically to diversifying devices and handle unknown attacks by using AI technology (unsupervised deep learning). Also, it can handle particularities of control communication, with signals from multiple devices having unique packets overlapping within several milliseconds.

Parts of both the authenticity checking technology and behavior monitoring and analysis technology are currently under development by the New Energy and Industrial Technology Development Organization (NEDO). It is done under the Council for Science, Technology and Innovation Strategic Innovation creation Program (SIP) called "Cyber-security for Critical Infrastructure". Please see the related Web site for details [5] [6].

New 5G technologies are also under development for implementation and commercialization in 2019. So, work to identify risks brought by the spread of these new technologies and to study security measures to deal with them will become increasingly important in the future. Specifically, increased risk could come from more powerful attacks utilizing characteristics of 5G networks, including higher bandwidth, ultra-low latency, and more simultaneous connections. New types of cyberattack may also come from diversification in the use and forms of IoT devices, increasing dependence of infrastructure, and even from attacks on networking devices including devices at telecommunications providers. As such, conventional network security architectures focusing on protecting voice and data must be supplanted. Therefore, a new security architecture for 5G should be studied urgently, emphasizing the following vital perspectives.

1. Network, service, and hybrid user authentication
2. Virtual network slice security management
3. Network countermeasures for large-scale DDoS attacks
4. Traffic monitoring and anomaly detection, including on wireless segments
5. Protection of private information (ID, location data, personal content, etc.)

5 DATA UTILIZATION IN SOCIETY

According to revisions made to the personal information protection law and enacted in May 2017, personal data processed to create "anonymized data" can be provided to third parties without agreement from the people involved as shown in Fig. 5. Anonymized data is defined as information regarding individuals that has been processed such that particular individuals cannot be identified from the processed data. In creating such data, all regulations 1 to 5 stipulated in Article 19 of the enforcement regulations [7] must be met [8]. Rules No. 1 to 4 are very easy to be done because of data deletion regarding name, biometric data, ID, very expensive purchase, etc. On the other hand, rule No. 5 is very difficult to be done in spite of such an exemplification as "If there is data regarding elementary

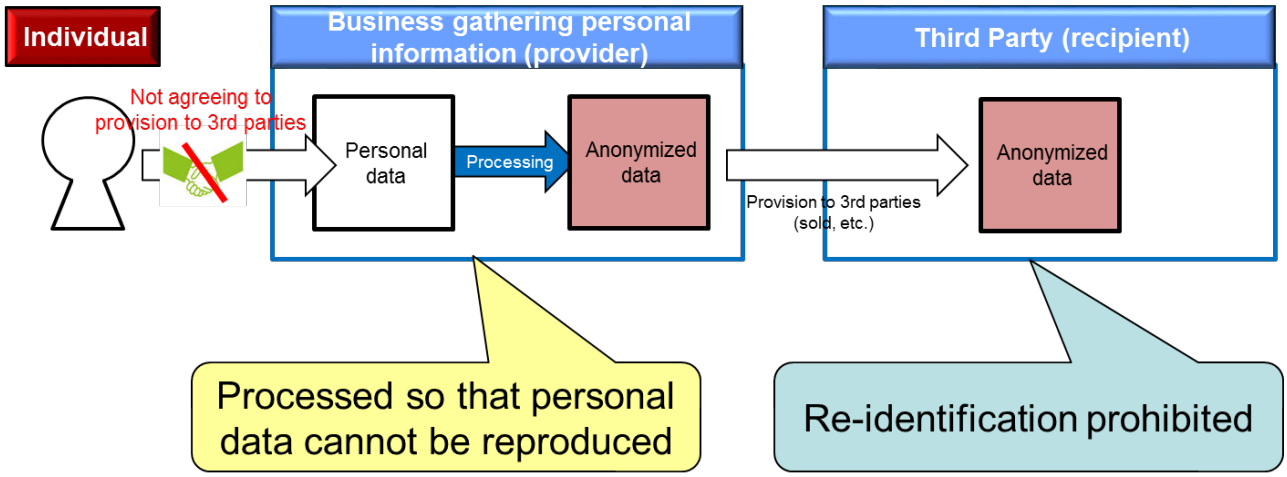

Figure 5: Outline of the revised Personal Information Protection Act.

school students over 170 cm tall, replace it with “150 cm or taller".

1. Delete descriptions which can identify a specific Individual
2. Delete personal identification codes
3. Delete linkage codes which link personal information and obtained information
4. Delete idiosyncratic descriptions
5. Take appropriate action considering the properties and differences between descriptions in personal information

With k-anonymization, which is a typical advanced anonymization technique, k-anonymity, which is an index of safety, is achieved through data generalization; data is processed such that it cannot be narrowed down to k or fewer persons with the same information. However, in doing so it is difficult to maintain both safety and usefulness of the data. In contrast, Pk-anonymization [9] is considered relatively more effective, because it can achieve safety equivalent to k-anonymization while preserving usefulness. As shown in Fig. 6, the method executes data randomization, in other words, addresses are replaced keeping city level and ages are also replaced keeping at 1 position different from data generalization by k-anonymization.

There is also a need around the world to use data without releasing it externally, even in anonymized form. “Secure Computation” involves processing data in its encrypted form and can be useful for such cases. There are many schemes for secure computation. However, schemes based on secret sharing [10] [11], which is an ISO standard, are the most practical from the perspectives of the definition of safety,

Name	Address	Sex	Age	Occupation
Sato	Shinjuku, Tokyo	M	45	Company Employee
Suzuki	Mitaka, Tokyo	M	41	Company Employee
Abe	Shinjuku, Tokyo	F	37	Homemaker
Nagasawa	Shinagawa, Tokyo	F	35	Homemaker
Yamamoto	Funabashi, Chiba	M	51	Self-employed
Kobayashi	Chiba City, Chiba	M	57	Self-employed
Uchida	Kashiwashi, Chiba	M	59	Self-employed

Random-ization

Name	Address	Sex	Age	Occupation
	Shinjuku, Tokyo	M	57	Company Employee
	Mitaka, Tokyo	M	41	Self-employed
	Funabashi, Chiba	F	37	Homemaker
	Shinagawa, Tokyo	M	35	Homemaker
	Shinjuku, Tokyo	M	51	Company Employee
	Chiba City, Chiba	M	45	Self-employed
	Kashiwashi, Chiba	F	59	Self-employed

Maintains safety equivalent to k-anonymization and preserves data usability

Figure 6: Pk-anonymization.

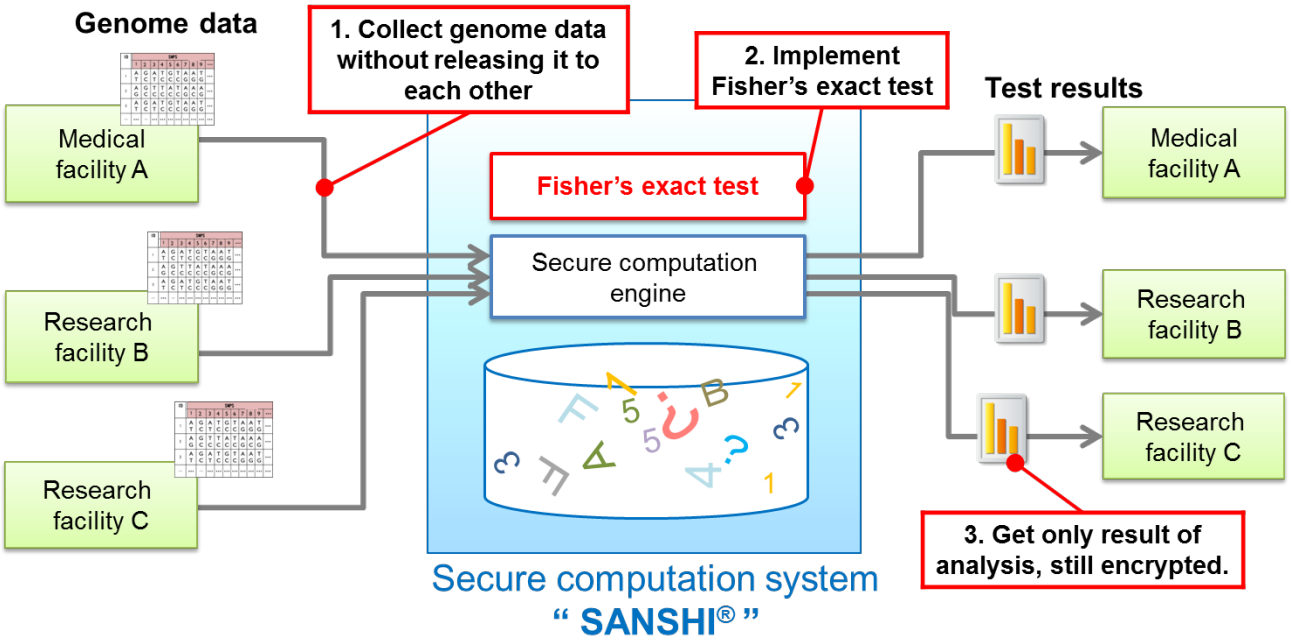

Figure 7: Secure computation system: "SANSHI". (算師®)

general purpose computations, sensible performance and international standardization. We hope use of this technology will spread in the future. Incidentally, NTT together with Tohoku Medical Megabank Organization (ToMMo) have used secure computation to implemented Fisher's exact test, to analyze the relationships between human DNA variations and diseases [12]. This is the first such implementation in the industry (Fig. 7).

6 SECURITY FOR THE SINGULARITY (2045 PROBLEM)

Singularity, also called Kurzweil's law of accelerating change, suggests that by 2045 as follows; a $1,000 computer will have performance of approximately 10 peta FLOPs, which is ten billion times that of the human brain and a sufficient base for AI to reach a technical singularity. Automated cyberattacks using AI are already appearing, advanced hacking using AI is likely to become mainstream. As well, it will become necessary to use automated technologies with AI on the defensive side. Actually at the world's largest hacking contest in DEFCON 2016, 7 computers automatically hacked each other's computer. So, it is no exaggeration to say that AI hacking has already begun. In doing so, attacks to machine learning have also been identified as an issue. Examples of attacks are to create input that induces false recognition, to contaminate classifier training data, and to steal the classifier itself by submitting queries to the classifier [13].

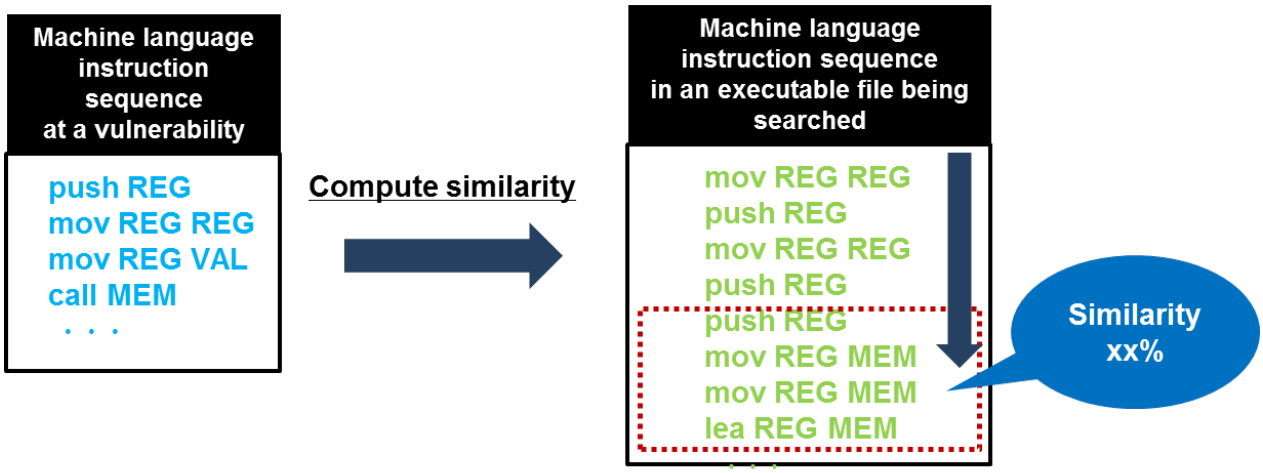

Figure 8: AI hacking-related technology to identify vulnerable points.

To deal with these, there is an urgent need to establish technologies able to detect vulnerabilities in executable binaries and to detect conditions that trigger an attack using symbolic execution. Regarding vulnerability detection, for instance, comparing an existing vulnerable binary code and a target binary code enables to identify vulnerable points by computing similarity as shown in Fig. 8.

Technical development of AI will bring great change and diversification in human thought/behavior and assumptions regarding societal structures. Therefore, research on legal systems, which function as societal standards, is also becoming crucial. The following steps need to be taken for a smooth transition from AI development to societal implementation.

1. Assuming application of AI, anticipate potential effects on people, society, and industry, and real relationships among them
2. Check current laws with knowledge of AI and analyze individual concerns
3. Propose a new legal system for the AI era, for future legislation and policy

Related activity is appearing in Japan [14], and related joint research is being actively developed at the RIKEN Center for Advanced Intelligence Project (AIP) and NTT Laboratories.

7 CONCLUSION

This article has given a comprehensive outline of security technologies essential in future technical development, mainly to eliminate threats and security issues anticipated with the arrival of digital transformation era. It has discussed, from a technological point of view, both offensive and defensive security perspectives. Then, it has given consideration to individual functional elements of the USA National Institute of Standards and Technology (NIST) Cyber Security Framework: Identify, Protect, Detect, and Respond. Moreover, it stated that perspectives of not only technology but also legal system are necessary for efficient security-risk management and effective countermeasures implementation.

REFERENCES

[1] Digital Transformation https://en.wikipedia.org/wiki/Digital_transformation
[2] Partial revision of NICT Regulations http://www.soumu.go.jp/main_content/000536856.pdf
[3] Framework for improving critical infrastructure cybersecurity http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
[4] InteRSePT®: A Cybersecurity technology realizing safe and secure operation of control systems enters the market http://www.ntt.co.jp/news2018/1804e/180425b.html
[5] What is the Cross-ministerial Strategic Innovation Promotion Program?http://www8.cao.go.jp/cstp/panhu/sip_english/5-8.pdf
[6] Secure Architecture for Critical Infrastructure https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201705fa2.html
[7] Enforcement Rules for the Act on the Protection of Personal Information (Tentative translation) https://www.ppc.go.jp/files/pdf/PPC_rules.pdf
[8] R, Osumi, K. Takahashi: “Personal Data Anonymization and Use,” Seibunsha (Japanese).
[9] Dai Ikarashi, Ryo Kikuchi, Koji Chida, Katsumi Takahashi: "k-Anonymous Microdata Release via Post Randomisation Method," International Workshop on Security (IWSEC), 2015
[10] NTT Secret Sharing technology Selected as First International Standard for Secret Sharing Technology (Japanese) http://www.ntt.co.jp/news2017/1710/171023a.html
[11] ISO/IEC 19592-2 Information technology -- Security techniques -- Secret sharing -- Part 2: Fundamental mechanisms
[12] Koki Hamada, Satoshi Hasegawa, Kazuharu Misawa, Koji Chida, Soichi Ogishima, and Masao Nagasaki: "Privacy-Preserving Fisher's Exact Test for Genome-Wide Association Study," International Workshop on Genome Privacy and Security (GenoPri), 2017.
[13] David Wagner on Adversarial Machine Learning at ACM CCS’17 https://syncedreview.com/2017/11/07/david-wagner-on-adversarial-machine-learning-at-acm-ccs17/
[14] Ministry of Internal Affairs and Communications, “AI Network Society Promotion Council,” http://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/

(Received October 8, 2018)

Kazuhiko Ohkubo is a vice president and the head of NTT Secure Platform Laboratories. He received his B.S. in information engineering from the University of Tsukuba in 1987 and M.S. in electrical engineering from the University of Tokyo in 1989. He also earned his M.S. degree in management of technology from the MIT Sloan School of Management, USA in 2000. He is a member of IEICE and IEEE.