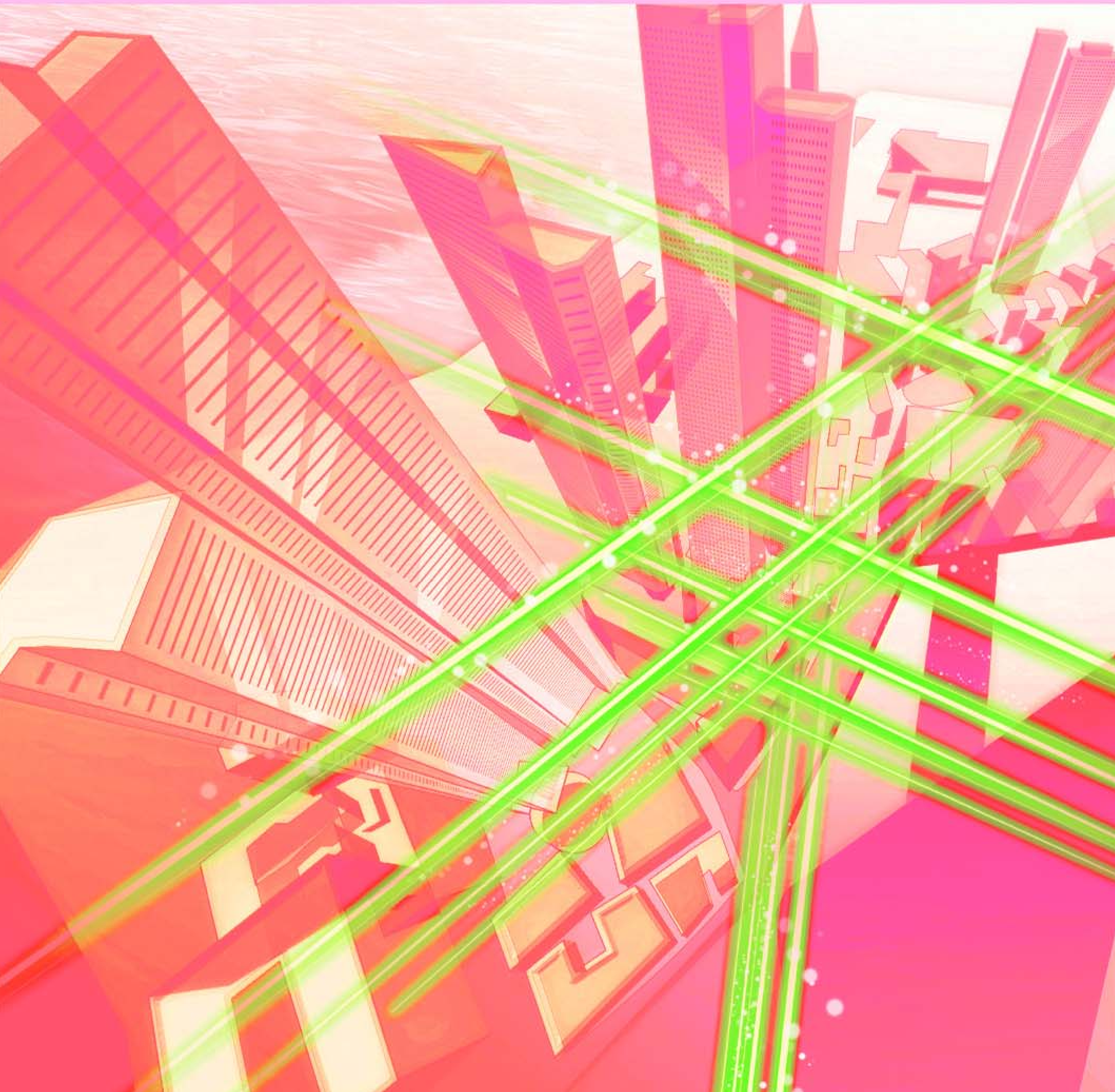
NTT Technical Review

3
2019



March 2019 Vol. 17 No. 3

NTT Technical Review

March 2019 Vol. 17 No. 3

View from the Top

Feature Articles: Front-line Cybersecurity Technology to Enable a Digital Society

Feature Articles: NTT R&D Forum 2018 Autumn Special Sessions

Regular Articles

Global Standardization Activities

External Awards/Papers Published in Technical Journals and Conference Proceedings

Building a Global Standard System to Win in Global Markets

Masaaki Moribayashi
Senior Executive Vice President,
NTT Communications

Overview

As the fourth industrial revolution takes hold around the world, Japan has much to achieve if it is going to maintain its international competitiveness in innovation. To this end, the Annual Report on the Japanese Economy and Public Finance 2018 issued by the Cabinet Office, Government of Japan, stated that Japan must establish a competitive edge in four areas of innovation: products, processes, marketing, and organization. We asked Masaaki Moribayashi, Senior Executive Vice President of NTT Communications, what will be necessary for NTT Communications to firmly establish itself as an international enterprise.

Keywords: global, reorganization, cloud solution

Changing the way we provide services by grasping the culture and lifestyle of local people

—It is said that your mission is to make NTT Communications into a company that can win in global markets.

I had always thought that I would like to make NTT Communications into a competitive company that can win in global markets, and I believe I have had the opportunity to do so. We are now in a period of reorganization with global business in mind, and I truly feel that we are taking concrete steps in this direction. I want to demonstrate our strengths to the fullest while pondering how best to complete this process of reorganization, and I want to focus on building the company into a robust enterprise in truly global markets. These are the dominant themes that occupy my mind at present.

Our business in global markets is growing year by year, but domestic sales still dominate. Outside Japan, people in our industry know about NTT Communications, but among the general public, few do, so our brand image has yet to penetrate society. There is therefore much room left for improvement in terms of increasing our name value and expanding our business in countries around the world.

In the 15 years I spent working in the United States, Hong Kong, and Europe, I was able to develop a good understanding of business characteristics in various regions of the world and to observe Japan from the outside. It is probably thought that keeping up with conditions in Japan can be difficult when you are overseas, but surprisingly, you can see Japan with an even sharper perspective when you are outside the country. In those 15 years, I came to understand well the strengths and weaknesses of both Japan and NTT.

Japan is unique in both a good sense and bad sense. In business, for example, the seniority system, lifetime employment, and hiring system of Japanese corporations are unique. While it is common in Japan to think that you cannot become a section chief until you reach a certain age, this is completely incomprehensible to people in other countries. In addition, no one is dismissed from a company in Japan other than for some extraordinary reason, and people for the most part do not negotiate their pay increases. In other countries, however, the norm is individual negotiation for pay and raises, so negotiations between an individual and the company that hires the individual are common, which is similar to the case of professional athletes negotiating for annual compensation.

However, if we are speaking about common practices, Japan is overwhelmingly better in the quality of service. For example, meals are delicious wherever you go, and parcels are delivered on time as promised. There is no other country with such attentive and efficient service. In England, I was generally unable to specify a time for delivery, and even if I could, it was not unusual for my parcel to arrive at a different time. In addition, it often took a long time to complete some kind of repair that I had requested. All in all, I could not receive the same kind of polite and reliable service that is taken for granted in Japan. We must be able to make this quality of service that is commonplace in Japan into one of our strengths in global markets. However, I think that it can be said that Japanese companies on the whole are not very proficient at making the best use of that strength.

—It seems that the way we apply the high quality of Japanese technology and service has to change.

Let me take railway operations in Japan and England as an example. Japan's railway network is so strictly controlled that even a train running one minute late prompts an apology. In England, there is no detailed timetable for subways (the Underground) or buses, just a notice on the station's electronic message board stating "The train will arrive X minutes later on platform X" just before that train arrives.

You might think it would be much appreciated if Japan's manner of accurate timetables and reliable operation were introduced in England, but it is not that simple. The fact is, there is no system that can implement Japan's railway mechanism, and there is no demand to run trains on such a strict schedule by spending money to construct such a system. In short, it seems to me that the approach to service in England is different. I believe that the principle "You will not sell anything unless you market things that fit the circumstances of that country" applies to all countries. And the same goes for the services provided by NTT Communications. Given Japan's reputation for superb quality, it would be easy to think that there are people who would be glad if Japanese services were to be sold in global markets. However, if the price is too high, the reply you get might be "We have no need for this" despite the attractive quality and functions.

Another good example from not so long ago concerns microwave ovens in the United States. First of all, Americans already had large, built-in ovens that were used for baking and roasting, and they had been around for decades. When microwave ovens were introduced in the U.S. to the general public in the 70s, they were simple devices with only a heating function, resulting in a fairly low-priced product. This is what appealed to them—fast heating of food. In contrast, the microwave ovens manufactured in Japan were high-function appliances that could change the manner of warming depending on the type of food that needed to be heated. This was useful and well-received because built-in ovens in Japan were not very common.

These differences were not a matter of a difference in technology but simply what the consumers looked for in a microwave oven. Americans, namely, wanted something they could pop food into and heat up quickly. For those consumers who had no need for functions other than pop-in and heat, such high-function microwave ovens could be thought of as expensive, over-engineered appliances that were essentially useless. Without a clear understanding of such a difference in social norms and required specifications, you cannot succeed in business.

Consequently, after obtaining a clear understanding of such cultural differences, our approach is to first market services of a global standard. Then, for customers who need more than standard services, we offer optional services that provide good value for the money. That is, I believe that our best course of action is to offer quality services appropriate to a global standard while also preparing an attractive lineup of options for customers wanting advanced services and products. In this way, all customers can choose what is best for them.

Making a big turn toward "solution provision" —trial and error through on-the-job training is the best shortcut

—So your strategy for winning in global markets is to begin by understanding other cultures and grasping the needs of customers.

That's right. The key point here is to achieve a thorough understanding of our customers' needs based on the concept of "design thinking" and to then determine how we can provide services that meet those needs as much as possible in an efficient manner. Another point discussed within the company is which of our strengths to bring to the forefront to compete effectively. For example, the cloud services provided by Amazon are of a magnitude greater in scale than ours due to bold upfront investment, so if we were to compare our services with theirs simply on the basis of a single function, we would be at a disadvantage. We are therefore steering the company in a direction in which we compete by providing solutions that customers need. To give a simple example, I am sure you would not go to a restaurant to eat ready-to-eat instant *ramen* (noodles). What does a customer desire in a restaurant? Well, in addition to the food itself, the customer wants to enjoy a meal and a dining experience that fits one's needs such as good service from the staff and maybe a nice interior and comfortable environment. Additionally, if one just wants to eat instant ramen, one can do so at home without having to take the trouble of going to a restaurant.

In terms of cloud services, we must change the way we work in providing such services. That is, instead of simply providing instant ramen (a single resource), we must adopt a method that determines what kind of meal (cloud solution) the customer would like to eat in what way and in what kind of environment and that identifies what is really needed by the customer. For this reason, we need many qualified people who can understand the customer's business and who possess extensive technical knowledge to make optimal proposals based on design thinking. Unfortunately, we still lack sufficient human resources in this regard. However, we have many people with great potential, and I would like these people to become experienced in the real business world as much as possible.

Although knowledge can be obtained to some extent through training and classes, you cannot learn everything in this way. It might be an old approach, but following a highly proficient senior around and observing that person's work in detail, and then making proposals on your own and failing any number of times, is the best shortcut to learning. When I took up my post in Europe, I witnessed the local practice in which new employees would *shadow*, or follow around, a talented senior employee to learn about work. These new employees might stumble in their job at first, but they learned and grew, and some even recorded top sales just two years later. On seeing results like these, I realized that this was the quickest way to get new people to learn.

—Have you previously been faced with a serious situation, such as pushing through reform or supervising a huge project?

I have had a variety of valuable experiences, but the one that stands out the most is my involvement in the datacenter business during my time in Hong Kong. Our company had a case in the past involving the purchase of datacenters. With the bursting of the bubble economy, however, those datacenters had become useless assets. Nevertheless, in the midst of opposing opinions, we acquired a company that owned datacenter buildings that were hardly being used and launched a genuine datacenter business. At that time, as head of NTT Com Asia in Hong Kong, I listened to what the people under me were saying and became convinced that we could succeed. With a positive frame of mind and believing in our ability to succeed, I made the decision without hesitation. On explaining my course of action to my seniors, I told them that my approach to work is to believe in my own eyes and ears and to make firm decisions without being swayed by dissenting voices around me, and they came to understand my position.

Additionally, after arriving in Europe in 2009, the experiences I had in integrating NTT Europe and NTT Europe Online were also very valuable, and they have become, in a sense, a dress rehearsal for the upcoming reorganization of the NTT Group's global business. Because of these experiences, I feel very positive and not overly worried about this reorganization. When I come across employees who are somewhat anxious about the whole thing, I tell them to have a positive attitude and not to worry.

When two separate companies are instructed to cooperate with each other, it is often the case that employees tend to focus on the company that they belong to. Even when the employees from each company come together to meet and brainstorm about some project, they tend to return with the proposal to their own workplace and discuss it again among themselves. However, if these two companies come to be integrated into one company, these employees return to one place instead of two and naturally come together. I had this experience when integrating those two companies in Europe. As long as you can control the flow, interactions will flow naturally. It can be difficult to direct that flow, so it is vitally important that top management repeatedly convey clear messages about strategy and direction to employees. The direction that everything must point to must be established. My mission in this reorganization of our global business, while a major challenge, makes for very enjoyable and worthwhile work. My basic philosophy is to think positive—don't worry too much and things will just keep moving in the right direction.

—It appears to be a time for creating new traditions in addition to the corporate DNA that the company has so far inherited.

Yes, it is essential that we add *partnering* to our DNA. NTT has historically been a company where many people have the mind frame of "I want to do all kinds of things on my own" and "I want to market what we create." Of course, it is vitally important that we differentiate ourselves through services incorporating our technologies and strengths. But at the same time, we will be left behind in the business markets if

we do not adopt a style that builds firm partnerships with other companies or people having excellent systems and services, creates ecosystems, and provides solutions instead of doing everything on our own. Even in the case of a company that we consider to be a competitor, the field in which we compete may actually be just a partial field, so there are times when it is better to join hands with that company. As reflected by the saying "The enemy of your enemy is your friend," it is important that we adopt a flexible approach so as to grow the business by tying up with a competing company when necessary.

When something good makes its appearance in the world, working on something similar in a copycat manner means you are already too late. Our resources and the money that we can invest are limited, so we cannot adopt a position of self-sufficiency in all things. At the risk of repeating myself, we will not survive in our business markets unless we decide on what direction to take and on what we have to do while offering services that utilize superb technologies and systems in the outside world.

This way of thinking has penetrated the company for the most part, but I would like to accelerate its application. However, I could steer the company in the wrong direction if I do not select what is good for us with a clear vision. These types of decisions constitute the mission of top management. I have said that partnering is important for us, but the flip side of this is thinking how to make positive use of our own technologies. It is not our purpose as a company to sell the technology of another company. If we ourselves do not have robust and impressive technologies, our strengths will not be apparent and partnering will be infeasible. Fortunately, we have technologies developed by the NTT laboratories. Going forward, we must provide solutions that include these technologies more than ever.

Keywords for growth: speed, agility, and a positive outlook

—Please tell us what you think the role of the NTT laboratories is and what types of technologies you look forward to.

In my previous work, I was also involved in cloud services, and in this regard, I have high expectations for security-related technologies under development at the NTT laboratories such as data concealment and secure computation. Our customers who use cloud services are very concerned about data security, so I would like to make these technologies into services as one of our strengths. The technologies of NTT are highly competitive in the world, and the laboratories are developing pioneering, breakthrough technologies. I would like to ask our researchers to create new technologies in rapid succession for use in society. These technologies do not have to be perfect—they can be in a form that can quickly make new ideas practical for commercial use. Seeking perfection takes time and can result in lost opportunities. Putting workable technology out into the world and receiving feedback provides a basis for the next step in research and development (R&D). In short, I would be most appreciative if our researchers could pursue R&D in such an agile manner.

—Mr. Moribayashi, could you leave a message for all NTT Communications employees?

I would be happy to. The NTT Group, including NTT Communications, has an exceptionally large number of highly professional employees. But at the company level, I think that these very capable people have yet to realize their full potential. I would like to establish a system and environment in which every employee can take on more challenging work with more responsibility, and I would like to ask everyone to take more initiative in their work. Some people may still have the seniority system or hierarchy in mind, but I would like to give anyone with ability and drive a chance, and I want to provide an environment in which everyone can demonstrate their abilities fully. If every employee can broaden his or her current range of activities and can take on work with more responsibility, I think an amazing amount of power will be generated within the company.

Finally, considering the many excellent employees of diverse nationalities that we have in our global operations, I would like to create a more stimulating environment in which they can flourish in their work.

Interviewee profile

■ Career highlights

Masaaki Moribayashi joined Nippon Telegraph and Telephone Public Corporation (now NTT) in 1984. He became President and Managing Director of NTT Europe Ltd. in 2009 and Senior Vice President and Head of Cloud Services of NTT Communications Corporation in 2016. He took up his present position in June 2018.

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

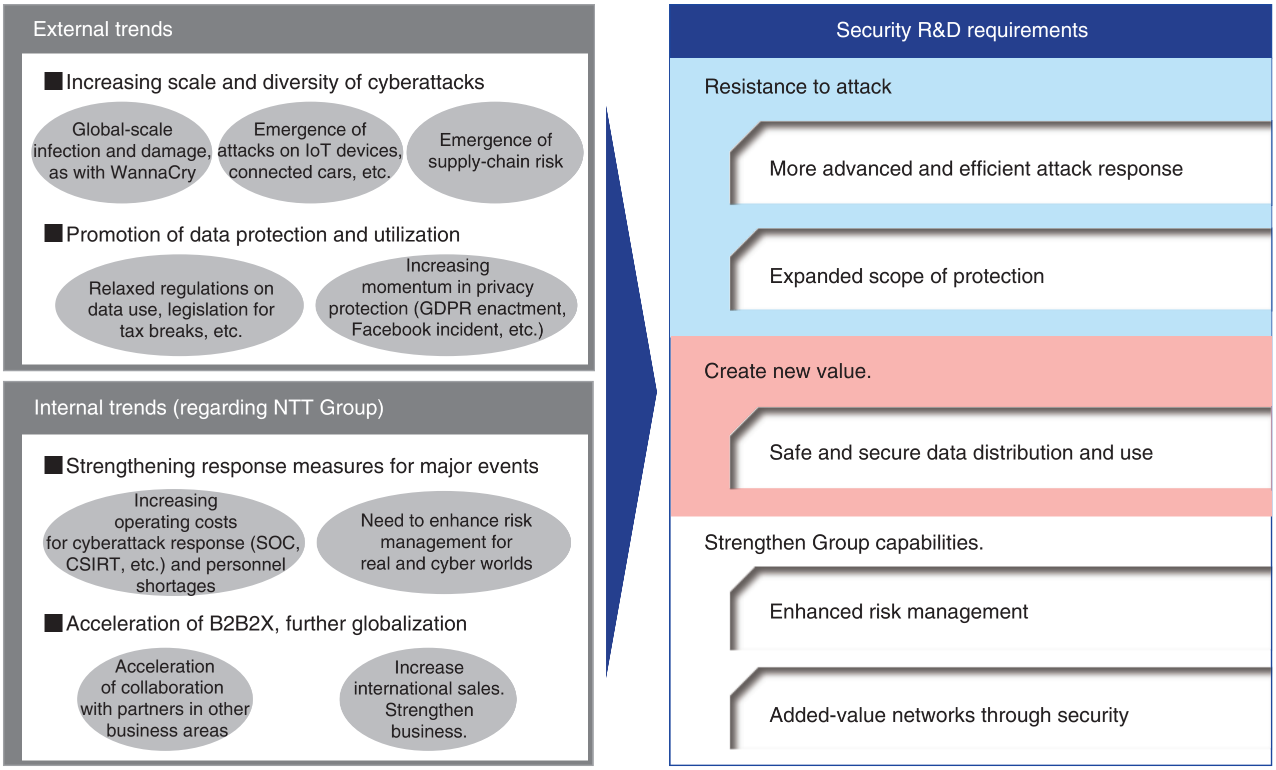
Society is going through major changes with the recent emergence of information and communication technology (ICT) and other innovative technologies. In what is being called *digital transformation*, advances in digital technology and data utilization are bringing high-level integration of cyberspace 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


External trends
■Increasing scale and diversity of cyberattacks
Global-scale infection and damage, as with WannaCry
Emergence of attacks on IoT devices, connected cars, etc.
Emergence of supply-chain risk
■Promotion of data protection and utilization
Relaxed regulations on data use, legislation for tax breaks, etc.
Increasing momentum in privacy protection (GDPR enactment, Facebook incident, etc.)
Internal trends (regarding NTT Group)
■Strengthening response measures for major events
Increasing operating costs for cyberattack response (SOC, CSIRT, etc.) and personnel shortages
Need to enhance risk management for real and cyber worlds
■Acceleration of B2B2X, further globalization
Acceleration of collaboration with partners in other business areas
Increase international sales. Strengthen business.
Security R&D requirements
Resistance to attack
More advanced and efficient attack response
Expanded scope of protection
Create new value.
Safe and secure data distribution and use
Strengthen Group capabilities.
Enhanced risk management
Added-value networks through security

B2B2X: business-to-business-to-X

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

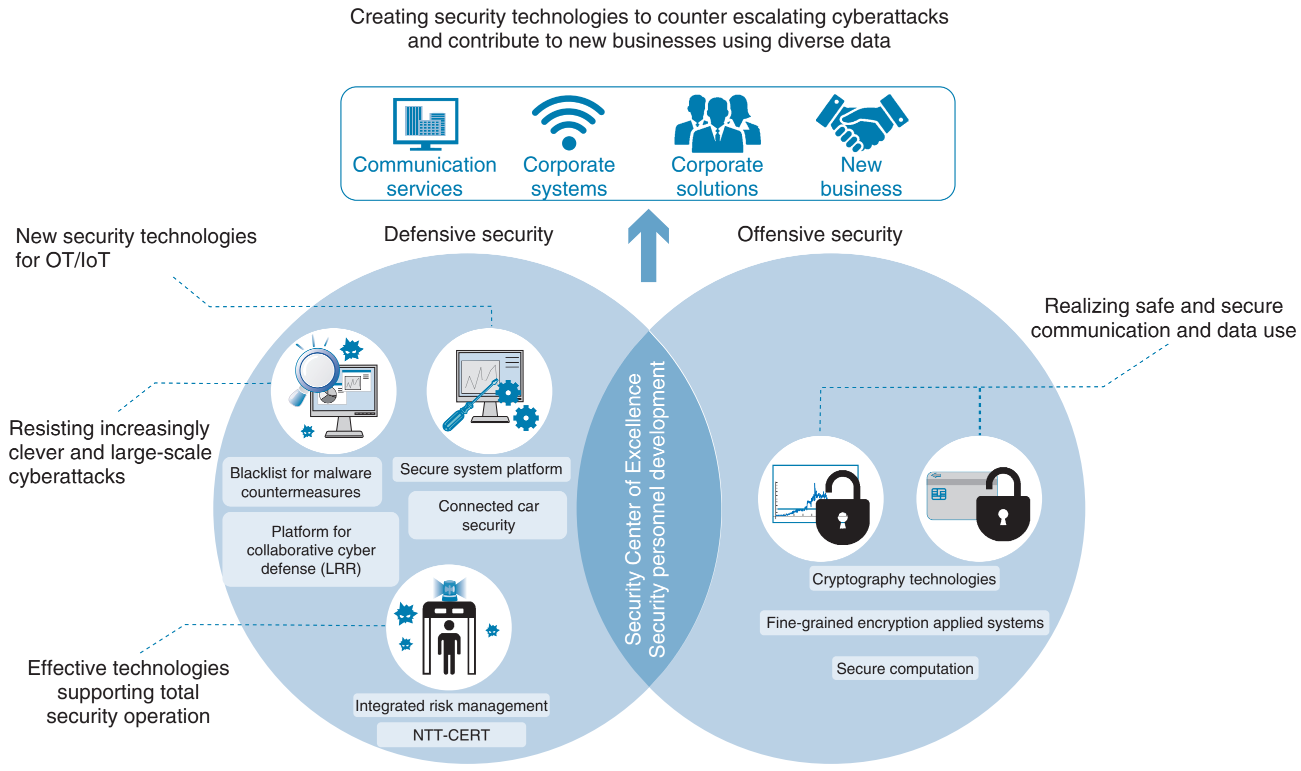
types of detailed data promises to yield new business opportunities such as accurately predicting events that could not previously be predicted, or refining targeting for marketing. Laws are also being revised to accommodate safe and secure businesses utilizing data, while closely examining developments 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


Creating security technologies to counter escalating cyberattacks
and contribute to new businesses using diverse data
Communication services
Corporate systems
Corporate solutions
New business
Defensive security
Offensive security
New security technologies for OT/IoT
Resisting increasingly clever and large-scale cyberattacks
Effective technologies supporting total security operation
Realizing safe and secure communication and data use
Blacklist for malware countermeasures
Secure system platform
Connected car security
Platform for collaborative cyber defense (LRR)
Integrated risk management
NTT-CERT
Security Center of Excellence
Security personnel development
Cryptography technologies
Fine-grained encryption applied systems
Secure computation

NTT-CERT: NTT Computer Security Incident Response and Readiness Coordination Team

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^{TM},” 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.

Discovery of Silhouette—a New Threat to Privacy—and Our Efforts to Counter It

Takuya Watanabe

Abstract

To prevent damage due to threats that are unknown to users and businesses, it is important to understand potential security issues in systems before the attackers do and to take preventive measures before an attack occurs. This article describes the mechanism of a new privacy threat called Silhouette, discovered in the course of this sort of empirical research on threats, together with a method for handling the threat, and initiatives to reinforce services and browser security functions around the world.

Keywords: web security, social web services, privacy threats

1. About Silhouette

Social networking services, video sharing, and other social web services (SWSs), which create content through communication between people, have continued to evolve since they were first introduced and have now become an essential part of our lives. A survey [1] of Internet users revealed that the average person maintains five or more different SWS accounts. On the SWS sites, users' profiles and postings can be seen based on the account name, so personal information such as the name, photographs, and the activities of the person are linked to each account.

The Silhouette privacy vulnerability discovered by NTT Secure Platform Laboratories (NTT SC Labs) makes it possible for a third party to identify the SWS accounts held by a user when the user accesses a website of the third party. For example, when a malicious website unrelated to any SWS is accessed by means such as through a search engine, advertising on a public site, or a link in an email message, the malicious website can communicate with an SWS that the user may have an account with and collect information to identify the account name. This can be done in the background without the user's knowledge.

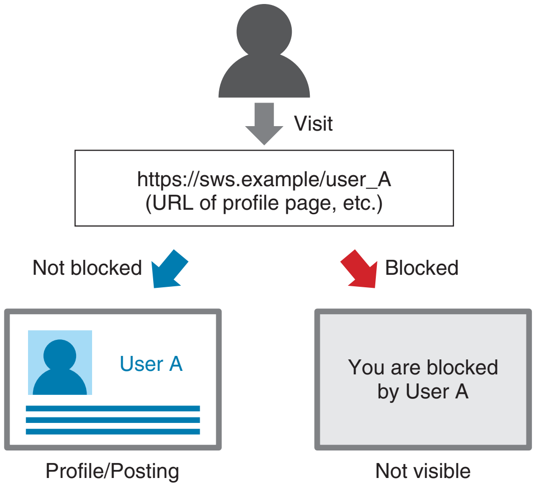
For this to work, the user needs to have left the web browser of their personal computer or mobile terminal logged-in to an SWS that is vulnerable to the threat and must visit the malicious website. Generally with SWSs, users automatically remain logged in until they logout explicitly and the cookies* are deleted. For this reason, users that have used a vulnerable SWS even once in the past may be identifiable by the malicious party.

2. Mechanism(s) resulting in the threat

This threat is carried out by maliciously exploiting the user-blocking function widely available on SWSs (**Fig. 1**). The user-blocking function is intended to enable ordinary users to control whether other users, who may be undesirable, can view their page, thus protecting themselves from behaviors such as harassment or spam. NTT SC Labs has identified a latent security issue in the user-blocking feature, which can control whether a page can be viewed by both malicious and legitimate users alike.

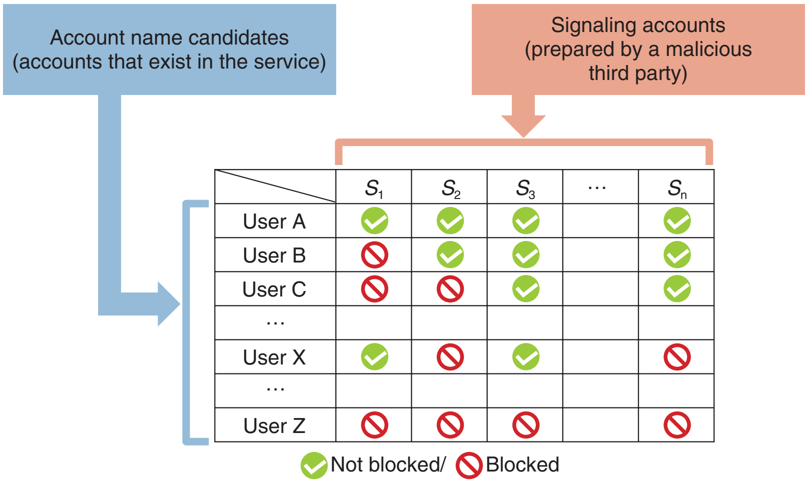
The malicious third party must first create multiple accounts on the SWS. These are known as *signaling accounts*. Then they systematically block certain

* Cookie: A feature enabling web services to store information in the browser of a visiting user so that it can manage sessions, user settings, login state, and other information.


Visit
https://sws.example/user_A
(URL of profile page, etc.)
Not blocked
Blocked
User A
You are blocked by User A
Profile/Posting
Not visible

URL: uniform resource locator

Fig. 1. User-blocking function.


Account name candidates
(accounts that exist in the service)
Signaling accounts
(prepared by a malicious third party)

	S_1	S_2	S_3	…	S_n
User A	✓	✓	✓		✓
User B	⊘	✓	✓		✓
User C	⊘	⊘	✓		✓
…					
User X	✓	⊘	✓		⊘
…					
User Z	⊘	⊘	⊘		⊘

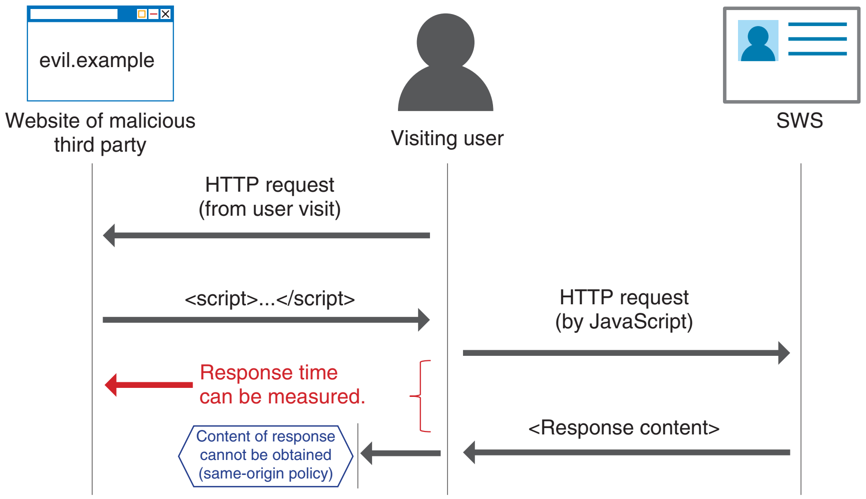
✓Not blocked/ ⊘Blocked

Fig. 2. Examples of patterns of blocked and non-blocked accounts.

users on the service to create combinations of blocked and non-blocked users. These patterns can then be used to uniquely identify user accounts (**Fig. 2**).

When a user visits the malicious website, the website contains a script for identifying the user account name, and the script makes requests for the pages of each of the signaling accounts. Browsers use the same-origin policy to protect sites, preventing data from leaking to other sites, so the third party is not able to obtain the content of the responses to this communication directly (**Fig. 3**). However, there is a statistical difference in response times for blocked and non-blocked requests. The malicious third party can use these differences to infer whether the visiting user is blocked from each of the signaling accounts. These results can then be used to identify the user's account name on the SWS by referring to the account blocking patterns prepared earlier.

Silhouette would be classified as a cross-site request forgery (CSRF) and side-channel attack. A CSRF is a type of web attack in which requests are sent to sites not intended by the user, to steal data or execute some malicious code. A side-channel attack is a generic name for attacks that use information


evil.example
Website of malicious third party
Visiting user
SWS
HTTP request (from user visit)
<script>...</script>
HTTP request (by JavaScript)
Response time can be measured.
<Response content>
Content of response cannot be obtained (same-origin policy)

HTTP: Hypertext Transfer Protocol

Fig. 3. Protecting response content using the same-origin policy.

from physical space, such as the response time or the power consumed, to infer sensitive information. This research has identified a security issue in how these services are designed, which enables threats to the privacy of legitimate users. This is done by making malicious use of the user-blocking function widely used by SWSs in an attack that combines a CSRF and a side-channel attack.

3. Countermeasures

In this section, countermeasures to this threat are described, which can be taken by both SWS operators and by users. Since the threat is a combination of CSRF and side-channel attacks, countermeasures can be implemented by preventing either of these attacks. Countermeasures for side-channel attacks require a specialized perspective on the characteristics of response timing, but there are well-known countermeasures for CSRF that only involve changes to the programming of the web service [2]. Below, countermeasures that focus on the CSRF component of the attack are introduced.

3.1 Assumptions

SWSs that are susceptible to this threat must have an account registration function and a user-blocking or similar function that enables a user to change whether another user is able to view the user's content pages (their profile etc.). Services without these functions are not vulnerable to this threat.

3.2 Countermeasures for the SWS

The first measure that an SWS can take is to use the cookie option called the SameSite attribute. A cookie with the SameSite attribute prevents requests from being sent to other sites by JavaScript or other means. As such, if this attribute is specified in the cookie used to manage the login state, a CSRF can be broadly prevented, including this threat. However, to use this feature, the user's browser must support SameSite, and the SWS must declare that it is using SameSite in the Hypertext Transfer Protocol (HTTP) header. As described below, the major browsers used around the world now support SameSite and can handle Silhouette thanks to the efforts of NTT SC Labs.

The second measure that can be taken is called request verification. In a CSRF, HTTP requests not intended by either the user or the service are generated. When this occurs, a well-known countermeasure [3] is to have the SWS or other service determine whether the request is legitimate by checking the referrer, which identifies the URL (uniform resource locator) of the website sending the request, or by checking a request parameter included as a CSRF countermeasure that contains a special code. Request verification is usually used for pages received using the POST method, such as posting to a web service, but it can also be used for pages received using the

GET method, such as a user profile. However, in this case, the verification fails when it is linked directly from a search engine or blog article, and such cases could be rejected as illegitimate requests.

To deal with this, the service can add a procedure in which it returns an intermediate page when the verification fails, and JavaScript on the intermediate page retrieves the content. This increases the number of requests needed to display the page, but it enables implementation of the countermeasure without obstructing access through direct links.

3.3 Countermeasures for users

One measure that can be taken by users is to use the private browsing mode in their browser. This mode has different names in different browsers, for example, Secret Mode, Private Window, or InPrivate, and when it is enabled, the browser does not use any prior cookie information and will delete any new cookie data stored when the session is ended. The threat of having the user's account name identified by visiting a third-party site can thus be prevented by enabling private browsing.

Another measure that users can take is to log out of the SWS. The threat can identify account names only if the user is logged in to the SWS. As such, the threat can be avoided by logging in to the service every time they use it and logging out as soon as they have finished using it.

4. Threat prevention efforts

NTT SC Labs has established a procedure to evaluate whether an SWS is vulnerable to Silhouette and has conducted a survey of all NTT Group SWSs and external SWSs that are well known around the world. As a result, we identified some well-known and influential international services that could result in account names being identified through this vulnerability. We have shared details of the vulnerability and countermeasures with these operators and collaborated in tests to verify the effectiveness of the countermeasures.

Through this effort, Twitter and other SWSs changed their specifications to improve security mechanisms and prevent the threat that makes it possible to identify account names. Major browsers including Microsoft Edge, Internet Explorer, and Mozilla Firefox also now support the SameSite cookie attribute using the method from this research or a similar method to prevent this vulnerability from being exploited.

Due to this contribution, the safety of most SWSs, used by more than 600 million users around the world, has greatly increased, and operators, including NTT, are able to use advanced functionality in designing secure web services. The results of this research have therefore led to a safer environment for using the Internet for users from short, medium, and long-term perspectives.

The paper [2] summarizing the discovery of this threat, its verification, and countermeasures, has also made an extremely great impact on improving web security. It was the first from Japan selected for the IEEE European Symposium on Security and Privacy, which is a prestigious academic conference, and was also selected for Black Hat Europe [4], a very influential international conference in the cybersecurity industry.

5. Future prospects

As part of research and development on cybersecurity at NTT SC Labs, we are developing methods for evaluating new threats, including the recently discovered Silhouette threat, and when an issue is discovered, we will work to implement countermeasures in collaboration with relevant organizations. By continuing to discover latent threats and develop countermeasures in the future, we will strive to be able to provide robust services, promote more secure web services and browsers, and facilitate safe and secure use of the Internet.

References

[1] Brandwatch, "121 Amazing Social Media Statistics and Facts." https://www.brandwatch.com/blog/amazing-social-media-statistics-and-facts/

[2] Information-technology Promotion Agency, Japan, "How to Secure Your Website," 5th Edition, 2011. https://www.ipa.go.jp/files/000017318.pdf

[3] T. Watanabe, E. Shioji, M. Akiyama, K. Sasaoka, T. Yagi, and T. Mori, "User Blocking Considered Harmful? An Attacker-controllable Side Channel to Identify Social Accounts," Proc. of 2018 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 323–337, London, UK, Apr. 2018.

[4] T. Watanabe, "I Block You Because I Love You: Social Account Identification Attack Against a Website Visitor," Black Hat Europe 2018, London, UK, Dec. 2018. https://www.blackhat.com/eu-18/briefings/schedule/index.html#i-block-you-because-i-love-you-social-account-identification-attack-against-a-website-visitor-12912

Trademark notes

All brand names, product names, and company/organization names that appear in this article are trademarks or registered trademarks of their respective owners.

Takuya Watanabe

Researcher, NTT Secure Platform Laboratories.

He received an M.E. in computer science and engineering from Waseda University, Tokyo, in 2016. He joined NTT in 2016 and has been engaged in research and development of the cybersecurity project.

Trial Service of Secure Computation System San-shi^{TM}

Hiroyuki Kitajo, Takuya Yamaguchi, Sanami Nishiyama, Gen Takahashi, Asami Miyajima, Keiichi Hirota, Shoko Nishida, and Junko Hashimoto

Abstract

To enable the safe and secure use of corporate secrets, personal data, and other types of data that must be kept confidential, NTT has developed Secure Computation System San-shi^{TM} that can perform tabulation and statistical processing securely and with practical performance without decrypting the data. As an initiative to stimulate the use of data, NTT is providing San-shi as a free trial service for a limited period so that many users can experience this secure computation technology. The advantage is that it enables integrated analysis without mutual disclosure of data among organizations while keeping the data encrypted. This article describes this initiative and introduces secure computation technology.

Keywords: secure computation technology, San-shi, cybersecurity

1. Background

Digital transformation is currently underway in a variety of fields, and this transformation is driving change toward a service economy, open systems, social networking, and smart systems. At the same time, the accumulation of cross-sector data and the skillful use of that data are expected to foster innovation and promote development and economic growth in a wide range of fields. However, the risk of incidents and the high social responsibility associated with data management and the need for data security measures to protect corporate strategy are factors that have hindered the expanded use of data.

To help eliminate these obstacles to data usage, NTT has taken a global lead in the research and development of secure computation technology that enables data processing while keeping the data encrypted. The advantage of secure computation technology is that data operations are invisible to everyone, except for the results of computation (**Fig. 1**), thereby enabling a new form of integrated analysis using data that up to now has been difficult for organizations to mutually disclose. Application examples of this technology have already been tested in several fields including multi-facility clinical research data analysis [1] and genome data analysis [2]. NTT has expanded the operations and functions of this technology, as well as enhanced the performance and made other improvements in developing Secure Computation System San-shi^{TM} (referred to below as San-shi) [3].

2. Overview of San-shi trial service

NTT's San-shi has been developed as a system having the advantage of secure computation technology that enables integrated analysis of data without mutual disclosure of data among organizations providing and/or using such data, while keeping the data encrypted. NTT has begun a free trial service of San-shi to enable many users in a variety of fields to experience this value. The trial period began on August 20, 2018, and runs through March 2019. At present, trial users can experiment with San-shi in various fields including healthcare, manufacturing, and system integration.

Using San-shi implemented on the cloud, users can

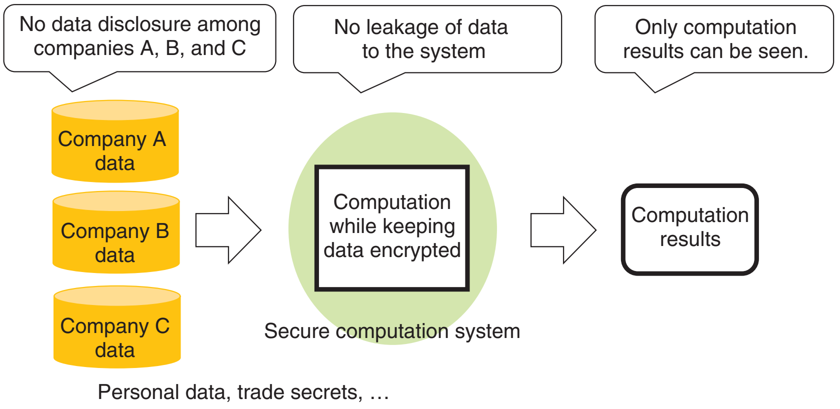

No data disclosure among companies A, B, and C
No leakage of data to the system
Only computation results can be seen.
Company A data
Company B data
Company C data
Computation while keeping data encrypted
Computation results
Secure computation system
Personal data, trade secrets, …

Fig. 1. Advantages of secure computation technology.

Table 1. Typical analysis scenarios provided in the trial service for customer use.

Feature	Scenario
Strengthen ties with other companies in the same industry.	Integrate and analyze the sales data of multiple companies in a region to enhance product assortment and avoid the loss of sales opportunities, thereby invigorating an entire regional trading zone.
Link data between different industries.	Combine and analyze purchase data of online sales companies and vital-signs data (BMI, pedometer data, etc.) held by companies providing health-support apps, and apply results to the marketing of health-related products and offering of product recommendations (expand advertising revenues).
Experience San-shi's operations and functions.	Discover what operations are possible against various types of data groups such as household attributes, household expenses, and food expenses.

BMI: body mass index

experience actual functions for tabulating and statistically processing data while keeping the data encrypted. Three types of scenarios and trial data that highlight the use of San-shi have been prepared to make it particularly easy for users to try out the system (**Table 1**).

The first scenario—strengthen ties with other companies in the same industry—increases the quantity of data (row data). The idea here is to invigorate an industry or solve problems in that industry without having to disclose information to a competitor. With a regional trading zone as an example, San-shi enables the user to securely register the sales data of multiple companies and store the data in a state that joins all of the data together. In this way, the user (data analyst) can check total sales figures for an entire trading zone, what merchandise had strong sales in different sales periods, and other details.

The second scenario—link data between different industries—increases the number of data items (column data). The ability to combine data belonging to different industries is expected to reveal new trends and generate new business value. To give an example, San-shi could be used to combine and securely register the purchase data of online sales companies and the vital-signs data of companies providing health-support apps, which would enable the user (data analyst) to determine the average number of steps taken by customers purchasing health food products by age group.

Finally, the third scenario—experience San-shi's operations and functions—gives users a free hand in trying out the operations and functions supported by San-shi. With San-shi, the user (data analyst) can securely register publically available statistical information (general-purpose micro data) and perform operations on that data associated with consumer expenditures, food expenses, insurance and medical expenses, and other details.

Additionally, for users who wish to experience San-shi beyond these typical scenarios, NTT supports the trial use of individual analysis scenarios based on data that users themselves possess.

3. Secure computation technology

Secure computation is the capability to perform computations on data while keeping the data encrypted. With most cyphers, data must first be decrypted to perform calculations with it, but this runs the risk of data leaks to data analysts, system operators, or elsewhere. Secure computation technology, however, enables computations to be performed while keeping the data encrypted, which prevents data analysts or system operators from seeing any data, including the results of computations in progress. This means that even confidential corporate information and trade secrets can be safely used for data computation.

The framework of secure computation technology was first established in the 1980s based on the theory of secure multi-party computation in the fields of computer science and cryptographic theory. However, the time required for computation was excessive (as the process was slow), presenting an obstacle to practical use. More recently, though, much research has been done to find ways to increase the computation speed and achieve practical implementations of secure multi-party computation. At NTT, we have developed a high-speed secure computation system based on secret sharing.

3.1 Encryption by secret sharing

NTT adopts secret sharing as the mechanism for encryption in its secure computation technology. Secret sharing is a scheme that enhances confidentiality by dispersing data into fragments called *shares*. In this scheme, information cannot be leaked from individual shares, and data can be recovered even if some shares are lost. This secret sharing scheme makes use of ISO/IEC 19592-2, a standard of the International Organization for Standardization (ISO). NTT members edited this standard and contributed to its formulation.

3.2 Multi-party computation based on secret sharing

NTT adopts multi-party computation based on secret sharing as the mechanism for computing while keeping the data encrypted. A multi-party computation system consists of multiple servers and a set procedure for exchanging data between those servers and performing operations on the data. Each server registers shares dispersed under the secret sharing scheme—data are always handled in this state of dispersed shares.

3.3 Safety of secure computation technology

There is no way that original data or computation results can be restored from individual shares on a server. However, given that shares are dispersed to and registered on multiple servers, it would be possible to restore the data if shares were to be obtained in an unauthorized manner from a certain number of servers. For this reason, appropriate management of each server is a precondition for safety.

3.4 Principle of secure computation technology

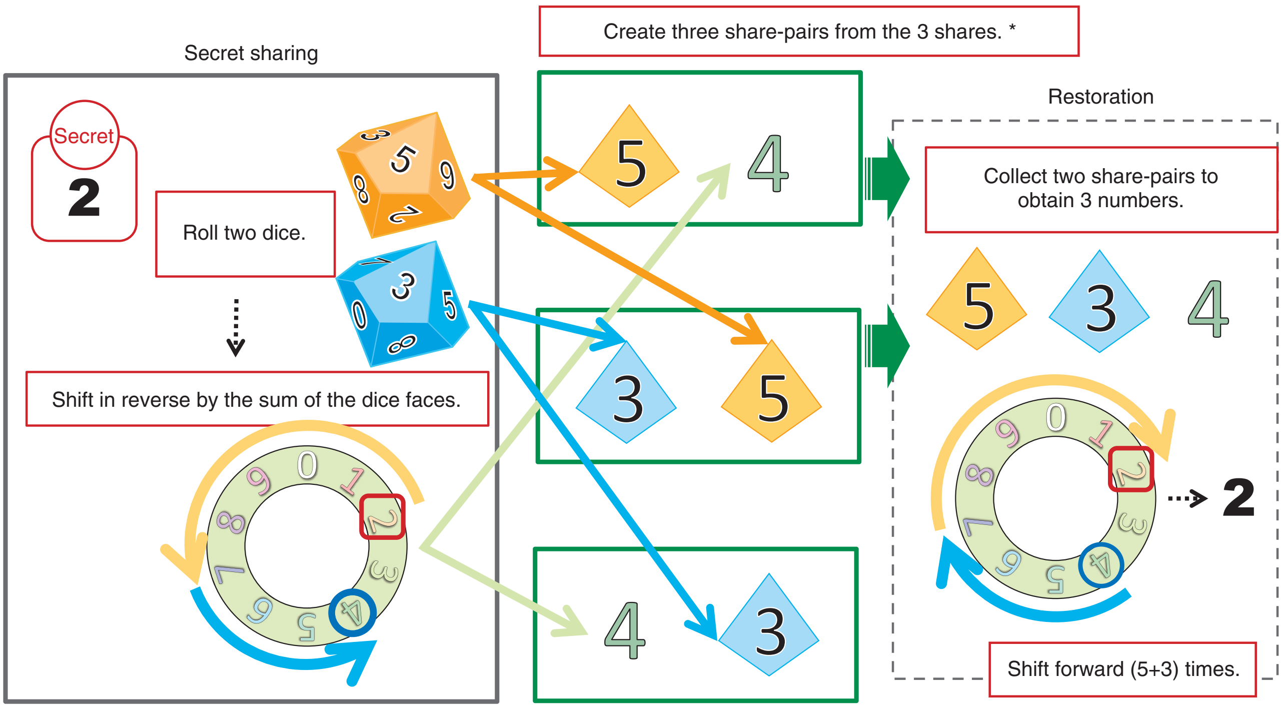
In secure computation technology, data are dispersed into multiple shares. Here, we introduce an example of dispersing “2” into three shares (**Fig. 2**). Generating shares in secret sharing is achieved by generating random numbers and performing computations based on those numbers. In this example, the share-generation process begins by generating two random numbers, each of which can take a value from 0 to 9. In the case where 5 and 3 are generated as random numbers, two of the three generated shares are taken to be 5 and 3. The process now computes the third share from these two shares by subtracting the sum of 5 and 3 (= 8) from original data 2 to obtain –6, which corresponds to 4 on the roulette wheel shown in the figure. The third share is therefore determined to be 4.

To restore the original data, the process collects the three shares 5, 3, and 4 and adds them up to get the value 12, which corresponds to 2 on the roulette wheel. The value of the original data is therefore determined to be 2.

Here, the process computes the shares generated in this way directly from each server. For example, a sum total, if desired, can be computed by simply summing the shares in the state in which they exist on each server. Finally, the result of the summation can be obtained by restoring the result of summing the values calculated on each server using the method described above.

4. San-shi features

NTT’s San-shi is a world-class secure computation


Create three share-pairs from the 3 shares. *
Secret sharing
Secret
2
Roll two dice.
Shift in reverse by the sum of the dice faces.
Restoration
Collect two share-pairs to obtain 3 numbers.
2
Shift forward (5+3) times.

* Three share-pairs: Created by combining two instances each of the 3 generated shares consisting of two dice faces and the shift result

Fig. 2. Principle of secure computation technology.

Table 2. Main operations of NTT's Secure Computation System San-shi^{TM}.

Data operation	Tabulation	Basic statistics		Tests
Table join	Frequency table (cross tabulation)	Total sum	Maximum	t-test
Filtering by conditions	Quantity table	Mean	Minimum	
		Variance	Median	Other
		Sum of products	Quantiles	Kaplan-Meier method

system that dramatically improves processing speed—a technical problem for many years in secure computation—while being capable of tabulating and statistically analyzing data on a scale of 100 attributes × 10,000,000 items within a realistic length of time. San-shi features an extensive set of tabulation functions and basic statistical operations, each of which can be executed at high speed.

4.1 Extensive operation variation

San-shi enables the user to execute the operations listed in **Table 2** on a graphical user interface (GUI) on a web browser or via an interface to "R" statistical analysis software without viewing the original data. The user can also create simple programs on "R" to perform regression analysis, principal component analysis, and other types of analyses according to the target application. The San-shi trial service provides the user with partial access to these interfaces.

In particular, San-shi's table-join function (a function that enables the data of multiple tables to be joined without leaking the join key) makes it possible to integrate the data of different companies and industries and obtain only the results of cross analysis without having to mutually disclose individually held data. This capability enables supply chains or customer

Table 3. Execution times of typical functions.

Function	Execution time (milliseconds)				
No. of data items	10^3	10^4	10^5	10^6	10^7
Addition	1	1	1	2	14
Multiplication	1	1	5	39	473
Sort	10	23	133	1274	12,255
Sum total	1	1	1	1	9
Sum of products	1	1	1	2	15
Quantity table creation	22	46	255	2252	22,676
Shuffle	1	1	8	60	731
Table join	19	65	518	4965	53,205
Data filter with prefix match	6	6	14	91	813
Data filter with numerical match	5	5	10	35	413

Measured with three personal computers (central processing unit: Intel Core i7 6900K, memory: 32 GB, solid state drive: 525 GB, operating system: CentOS 7.2) connected on a 10-Gbit/s network

data that overlap multiple companies to be analyzed, which can contribute to the creation of new value in the use of data that could not be achieved up to now within a single company or industry.

4.2 High-speed processing sufficient for practical use

In addition to adopting a secret sharing scheme [4], San-shi is able to provide both extensive operation variations as described above and faster processing through a proprietary speed-boosting algorithm and fast implementation method.

Secure computation technology based on secret sharing has two key advantages: the size of data basic to data processing is small, and the frequently used operations of addition and multiplication can both be executed at high speed. This means that San-shi can process a variety of operations at high speed compared with secure computation based on other types of encryption schemes such as homomorphic encryption.

In addition to the above, NTT has developed a basic algorithm for secure computation having extremely low computational and communication costs and has applied this algorithm using a fast implementation method. These measures have dramatically improved the processing speed, enabling NTT to achieve the world's highest speeds in executing operations of this type.

Execution times of typical functions are listed in **Table 3**. Sort processing of 10 million records can be performed in 12.2 seconds. This time can be compared with an execution time of about 1 second when sorting 10 million unencrypted records by a standard sorting algorithm. The difference in performance between secure computation technology and ordinary computer processing is therefore about one order of magnitude.

4.3 San-shi system

Secure computation technology enables multi-party computation over multiple servers operating in an integrated manner. The San-shi system consists of secure computation clients and three or four secure computation servers. The secure computation client that performs data registration divides data into shares under the secret sharing scheme and registers those shares on different servers. In addition, the secure computation client that performs data analysis issues requests to each server for computation (data analysis) and obtains only the results of computation. Here, data are registered in table format such as a relational database. The computation of mean or variance values, for example, can be requested by specifying the name of the table or column where the data are stored. Each server receiving such a computation request cooperates with the other servers to perform multi-party computation and returns computation results as shares to the secure computation client that performs the data analysis. This client then restores those shares to obtain the result.

5. Future development

Going forward, NTT aims to further promote the safe and secure use of confidential corporate and personal data through the San-shi trial service while endeavoring to develop and globally propagate data usage technology including secure computation technology.

References

[1] Press release issued by NTT on Feb. 14, 2012 (in Japanese). http://www.ntt.co.jp/news2012/1202/120214a.html

[2] Press release issued by NTT on July 12, 2016 (in Japanese). http://www.ntt.co.jp/news2016/1607/160712a.html

[3] Website of NTT on secure computation, http://www.ntt.co.jp/sc/project_e/data-security/secure_computation.html

[4] Press release issued by NTT on Oct. 23, 2017 (in Japanese). http://www.ntt.co.jp/news2017/1710/171023a.html

Hiroyuki Kitajo

Manager, R&D Produce Group, Research and Development Planning Department, NTT.

He received a Bachelor of Information Engineering from Tohoku University, Miyagi, in 2000. He joined NTT EAST in 2000. He has been in his current department since 2016, where he has been promoting information and communication technology (ICT) business and technologies for the medical and healthcare field.

Takuya Yamaguchi

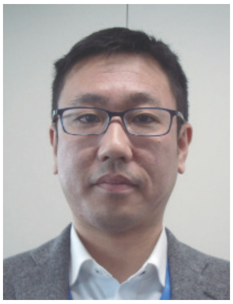
Manager, Produce Section (Security), Research and Development Planning Department, NTT.

He received a B.E. in physics from Sophia University, Tokyo, in 2000. He joined NTT EAST in 2000 and worked in corporate sales from 2000 to 2005. He was involved in developing security services at NTT EAST from 2006 to 2014. He has been in his current department since 2015, where he has been promoting security related business and technologies.

Sanami Nishiyama

Associate Manager, R&D Produce Group, Research and Development Planning Department, NTT.

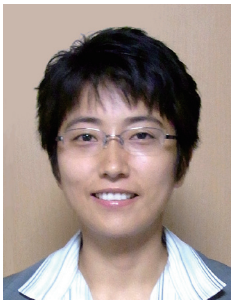
She received a Bachelor of Management Engineering from Nagoya Institute of Technology, Aichi, in 2000. She joined NTT WEST in 2000. She has been in her current department since 2018, where she has been promoting ICT business and technologies for the medical and healthcare field.



Gen Takahashi

Senior Research Engineer, NTT Secure Platform Laboratories.

He received a Master of Media and Governance from Keio University, Tokyo, in 2005. He joined NTT in 2006. His research interests include information security and cryptographic engineering. He received the SCIS Paper Award from the Institute of Electronics, Information and Communication Engineers (IEICE) in 2008.



Asami Miyajima

Senior Research Engineer, NTT Secure Platform Laboratories.

She received a Master of Science and Technology from Keio University, Tokyo, in 2000. She joined NTT in 2000. Her research interests include information security.

Keiichi Hirota

Senior Research Engineer, Data Security Project, NTT Secure Platform Laboratories.

He received a B.S. and M.S. from Mie University in 1995 and 1997, and a Ph.D. in informatics from the Graduate University of Advanced Study (SOKENDAI) in 2008. He joined NTT in 1997. His current research interests are security and privacy in information processing, information sharing, and data utilization. He is a member of the Information Processing Society of Japan.

Shoko Nishida

Research Engineer, NTT Secure Platform Laboratories.

She received an M.S. from Kyushu University, Fukuoka, in 2009. She joined NTT in 2009. Her research interests include information security.

Junko Hashimoto

Research Engineer, NTT Secure Platform Laboratories.

She received an M.S. from Kyushu University, Fukuoka, in 1999. She joined NTT in 1999. Her research interests include information security.

Research Trends in Post-quantum Cryptography

Keita Xagawa

Abstract

The growing recognition that quantum computers are soon to be a reality is driving research into post-quantum cryptography. This article introduces the Post-Quantum Cryptography Standardization project of the National Institute of Standards and Technology (NIST) in the United States, which is playing a core role in the research and development of post-quantum cryptography, and introduces NTT initiatives and independent research related to that project.

Keywords: cryptographic technology, post-quantum security, quantum computer

1. Post-quantum cryptographic technology

Today, a great deal of highly confidential information such as personal data and credit card numbers is being exchanged on the Internet. For this reason, cryptographic systems such as symmetric-key cryptography and public-key cryptography are being used to conceal the contents of such transmissions. In addition, authentication technologies such as digital signatures and message authentication codes (MACs) are being used to authenticate the other party and the content of the received message. Certain algorithms have found widespread use in public-key cryptography and digital signatures, namely cryptographic algorithms based on the difficulty of the factorization problem (RSA (Rivest-Shamir-Adleman) encryption, RSA signatures, etc.) and those based on the difficulty of the discrete logarithm problem (Diffie–Hellman key exchange, elliptic-curve Diffie–Hellman key exchange, Digital Signature Algorithm (DSA), etc.).

In 1994, Peter Shor, then of Bell Laboratories, proposed efficient algorithms using a quantum computer for solving these two problems. Consequently, if a quantum computer that can perform large-scale calculations in a stable manner can be built, cryptographic algorithms that are now in widespread use will no longer be secure. This is why the research, development, and standardization of cryptographic algorithms that a quantum computer cannot break or tamper with have become quite active as efforts continue to successfully develop a quantum computer. Within public-key cryptographic technology, cryptographic algorithms that have been designed based on problems for which quantum computers are considered to be weak in solving are referred to as post-quantum (public-key) cryptography.

2. Standardization trends in post-quantum cryptography

On the question of whether it is necessary to start a migration to post-quantum cryptographic algorithms, we refer to the formula proposed by Michele Mosca, co-founder and deputy director of the Institute for Quantum Computing, University of Waterloo, Ontario, Canada, as described below. Let us define x, y, and z as follows:

- x = number of years desired to maintain the security of generated information
- y = number of years needed to migrate to post-quantum cryptographic algorithms (research and development, standardization, and dissemination)
- z = number of years until a large-scale quantum computer is built

If $x + y > z$, ciphertext created after y years based on the thinking that “I want to keep this information secret for at least x years” may be cracked by a quantum

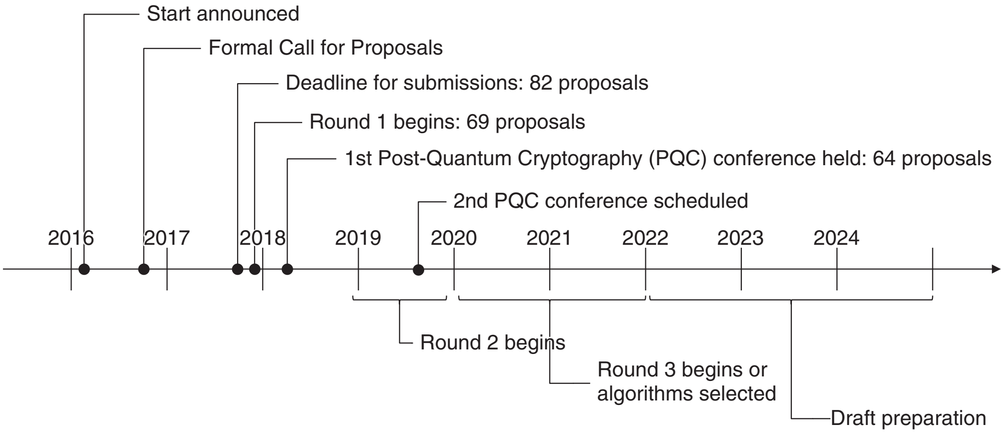

Start announced
Formal Call for Proposals
Deadline for submissions: 82 proposals
Round 1 begins: 69 proposals
1st Post-Quantum Cryptography (PQC) conference held: 64 proposals
2nd PQC conference scheduled
2016
2017
2018
2019
2020
2021
2022
2023
2024
Round 2 begins
Round 3 begins or
algorithms selected
Draft preparation

Fig. 1. Timeline of NIST project.

computer in less than x years. Accordingly, if it is thought that x + y > z is true at the present time, there is a need to study closely the standardization of and migration to post-quantum cryptographic technology.

Under the assumption that z number of years from today's state of quantum computer development is likely to be within a realistic range, organizations and standardization bodies in various countries are moving forward with migration studies, as outlined below.

- In Japan, the Cryptography Research and Evaluation Committees (CRYPTREC)* issued a report in 2014 on post-quantum cryptography titled "Survey on the Difficulty of Lattice Problems, etc."
- In the United States, the National Institute of Standards and Technology (NIST) began holding workshops in spring 2015 and announced in 2016 that it would commence standardization activities toward post-quantum public-key cryptographic techniques.
- Also in the United States, the National Security Agency (NSA) declared in August 2015 its intention to migrate its Suite B, the set of cryptographic algorithms for protecting classified information, to post-quantum cryptographic algorithms in the not too distant future.
- The European Telecommunications Standards Institute (ETSI) has been holding annual workshops on quantum cryptography and post-quantum cryptography since 2013.
- The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) have been holding study periods on post-quantum cryptography since 2015.
- The Internet Engineering Task Force (IETF) as well is overseeing a post-quantum signature project and is beginning to release results as request for comments (RFCs) (e.g., RFC 8391: XMSS: eXtended Merkle Signature Scheme).

Among these activities, we introduce here the NIST Post-Quantum Cryptography Standardization project, which is having a major impact on cryptographic technology standardization around the world.

3. NIST Post-Quantum Cryptography Standardization Project

The NIST Post-Quantum Cryptography Standardization Project began in earnest in 2016 with the aim of selecting and standardizing post-quantum cryptographic algorithms in the three categories of digital signature, public-key encryption, and key establishment.

The timeline for this project is summarized below (**Fig. 1**).

- February 2016: Announcement of the start of the Post-Quantum Cryptography Standardization Project
- August 2016: Release of NISTIR 8105, Report on Post-Quantum Cryptography
- August 2016: RFCs on Submission Requirements and Evaluation Criteria
- December 2016: Formal Call for Proposals

* CRYPTREC: A project established to evaluate and monitor the security of e-Government recommended ciphers and to survey and study appropriate implementation and operation methods of cryptographic techniques.

- November 2017: Deadline for submissions
- December 2017: Examination of documents and forms; Round 1 begins
- April 2018: First Post-Quantum Cryptography (PQC) Standardization Conference
- 2018/2019: Round 2 begins
- August 2019: Second PQC Standardization Conference (plan)
- 2020/2021: Round 3 begins or algorithms to be selected
- 2022/2024: Draft preparation to be completed

A total of 82 proposals were submitted by the deadline in November 2017; of these, 23 concerned digital signatures and 59 concerned encryption and key-encapsulation mechanisms. After an examination of documents and forms was conducted, Round 1 began in December 2017, at which time 69 proposals remained. However, 5 proposals were later withdrawn, resulting in a total of 64 proposals at present—19 for digital signatures and 45 for encryption and key-encapsulation mechanisms.

As mentioned above, the results of examining documents and forms left 69 candidate algorithms for Round 1. These candidates are not necessarily secure simply by reaching Round 1.

Immediately after the release of Round 1 candidates, lively discussions took place on the security of each method via the NIST pqc mailing list.

Among these candidates, many were shown to be breakable as summarized below.

- Guess Again (encryption, other)
- RaCoSS (signature, code)
- RVB (encryption, other) → withdrawn
- HK17 (encryption, other) → withdrawn
- CFPKM (encryption, multivariate polynomials)
- SRTPI (encryption, multivariate polynomials) → withdrawn
- Edon-K (encryption, code) → withdrawn
- Compact LWE (encryption, lattice)
- WalnutDSA (encryption, other)
- RankSign (signature, code) → withdrawn

It should be kept in mind that security evaluation techniques are expected to be improved going forward to Round 2.

4. NTT initiatives

NTT did not submit an original algorithm to these NIST Post-Quantum Cryptography Standardization activities. However, NTT is participating by making proposals for security enhancement techniques and security evaluation from a third-party standpoint and is working with other project members to ensure that suitable algorithms can be selected.

Furthermore, though the NIST Post-Quantum Cryptography Standardization Project is focused only on post-quantum public-key cryptographic algorithms, NTT is independently researching post-quantum symmetric-key cryptography as well.

4.1 Security enhancement technique

For secure communications to be carried out in the real world, public-key encryption algorithms must provide a level of security that is strong enough not only to conceal the message itself but also to prevent messages from being tampered with. Technically speaking, this is called chosen-ciphertext attack (CCA) security. At present, CCA security is considered to be an essential requirement for the realistic use of public-key encryption algorithms.

In this regard, techniques for converting a public-key encryption algorithm without CCA security to a public-key encryption algorithm with CCA security have been researched for some time, but it was not until 2010 that research began in order to determine whether such techniques were secure enough to counter attacks using a quantum computer. It was found that these techniques could indeed be effective against quantum computers but only with a drop in efficiency. However, no security enhancement technique that was effective against quantum computers without sacrificing efficiency was known to exist.

With this being the case, NTT developed a new technique that improves security by converting a post-quantum public-key encryption algorithm without CCA security to a post-quantum public-key encryption algorithm with CCA security [1].

This development makes it possible to configure a post-quantum public-key encryption algorithm according to the highest global standards with high efficiency. In addition, the technique has broad utility, enabling it to be applied to a variety of existing post-quantum public-key cryptographic schemes. It was found that it could be applied to at least seven of the candidate algorithms in the NIST Post-Quantum Cryptography Standardization Project.

The use of post-quantum public-key encryption algorithms based on this technology will enable cryptographic communications at about the same load as existing methods even in the post-quantum era.

4.2 Security evaluation from the outside

A cryptographic algorithm called Giophantus is one of the 69 candidate algorithms evaluated in the

NIST standardization project. This algorithm was originally presented in a paper under the name Indeterminate Equation Cryptosystem (IEC). The security of this scheme, while proven to be secure, is dependent on the difficulty of a certain problem. In this regard, large size parameters are required to ensure that the underlying problem is difficult. However, since IEC was designed so that the key size and ciphertext length would be short, the underlying problem with small size parameters was an issue.

Against this background, we proposed a new attack technique that could degrade security for small size parameters [2]. The results of an experiment using this attack technique revealed that practical cryptanalysis could be performed in 30–40 seconds on a desktop personal computer. As a result of this study, parameters for the Giophantus version of IEC submitted to NIST were significantly revised.

4.3 Post-quantum symmetric-key cryptographic technology

(1) Security evaluation techniques

A general-purpose quantum algorithm for attacking symmetric-key cryptography is presently unknown. Consequently, an attack that applies computer scientist L. K. Grover's algorithm for searching a database is currently known to be the most effective. For this reason, quantum attack techniques surpassing the Grover algorithm are being devised by analyzing in detail the inner workings of symmetric-key cryptography, and security evaluations using these techniques are being performed. At NTT, we have obtained results surpassing those of existing research by combining meet-in-the-middle attacks and quantum algorithms [3, 4].

It is also known that security can break down for some symmetric-key ciphers and MACs in cases where the attacker can access a cryptographic algorithm or MAC algorithm in a quantum manner. NTT has also been researching attacks of this kind and has shown that some symmetric-key ciphers can be broken by quantum related-key attacks [5].

(2) Security-proving technique

As described above, it is extremely important that the security of symmetric-key cryptography be assessed and proven considering the existence of attackers that instigate quantum-type accesses. NTT has developed a technique that proves the post-quantum security of hash functions even when attackers carry out quantum queries [6].

5. Future development

We plan to create a portfolio of security enhancement and security evaluation techniques and to continue studying the development and deployment of secure cryptographic communication technologies even after the successful development of quantum computers.

References

[1] T. Saito, K. Xagawa, and T. Yamakawa, "Tightly-secure Key-encapsulation Mechanism in the Quantum Random Oracle Model," Proc. of the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2018), Part III, Lecture Notes in Computer Science (LNCS), Vol. 10822, pp. 520–551, 2018.

[2] K. Xagawa, "Practical Cryptanalysis of a Public-key Encryption Scheme Based on Non-linear Indeterminate Equations at SAC 2017," Proc. of the 9th International Conference on Post-Quantum Cryptography (PQCrypto 2018), LNCS, Vol. 10786, pp. 142–161, 2018.

[3] A. Hosoyamada and Y. Sasaki, "Cryptanalysis against Symmetric-key Schemes with Online Classical Queries and Offline Quantum Computations," Proc. of CT-RSA (Cryptographers' Track at the RSA Conference) 2018, LNCS, Vol. 10808, pp. 198–218, 2018.

[4] A. Hosoyamada and Y. Sasaki, "Quantum Demiric-Selçuk Meet-in-the-middle Attacks: Applications to 6-Round Generic Feistel Constructions," Proc. of the 11th Conference on Security and Cryptography for Networks (SCN 2018), LNCS, Vol. 11035, pp. 386–403, 2018.

[5] A. Hosoyamada and K. Aoki, "On Quantum Related-key Attacks on Iterated Even-Mansour Ciphers," Proc. of the 12th International Workshop on Security (IWSEC2017), LNCS, Vol. 10418, pp. 3–18, 2017.

[6] A. Hosoyamada and K. Yasuda, "Building Quantum-one-way Functions from Block Ciphers: Davies-Meyer and Merkle-Damgård Constructions," Proc. of the 24th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2018), Part I, LNCS, Vol. 11272, pp. 275–304, 2018.

Keita Xagawa

Scientist, Data Security Project, NTT Secure Platform Laboratories.

He received a B.S. from Kyoto University and an M.S. and D.S. from Tokyo Institute of Technology in 2005, 2007, and 2010. He joined NTT in 2010. His research work focuses on algebraic algorithms and provable security in cryptography. He is presently researching cryptography and information security at NTT Secure Platform Laboratories.

Co-innovating to Accelerate Transformation and Create New Value

Debra Bordignon
Chief Technology Officer,
Dimension Data Australia

Abstract

Dimension Data, an NTT Group company, recently opened its first Client Innovation Centre (CIC) in Sydney, Australia. This article introduces the CIC and presents examples of co-innovation generated at CIC between Dimension Data, their clients and partners, and the NTT research and development (R&D) laboratories. This article is based on a speech given by Debra Bordignon, Chief Technology Officer, Dimension Data Australia, at NTT R&D Forum 2018 Autumn on November 29, 2018.

Keywords: co-innovation, digital transformation, security, disruptive innovation, exponential technologies

1. Client Innovation Centre

On August 1, 2018, we opened the first Client Innovation Centre (CIC) in Sydney, Australia [1]. Our team created this center as a facility and as an engagement model for innovation with our clients, and we run this as One NTT. The purpose of CIC is to engage with our clients in co-innovation to accelerate their transformation in this digital era and to help them achieve new purpose and value. It has come about through the close relationships and collaborations we have with the NTT research and development laboratories (NTT R&D).

Our clients are curious and expectant around One NTT. Our clients are successful organizations, mostly with a rich analog heritage and assets. All of our clients are transforming their business to flourish in new times. Generally speaking, they are dealing with a legacy underbelly of brittle technologies, processes, and culture.

They are hoping for a deeper conversation with us about more strategic levels of innovation. They want us to step up to help them accelerate their journey towards digital transformation, as the integrator and manager of their digital estate. They are looking for opportunities to differentiate themselves in changing markets, through applied innovation with the ecosystems we can bring together, including the wonderful assets that we can bring from NTT R&D. In some cases, we are looking to co-create new value and jointly commercialize new solutions that can advance the digital economy and benefit society (**Fig. 1**).

It is a completely immersive experience that we have created with our CIC model, and we are not only bringing clients into this, but also creating complimentary industry forums to address some grand challenges together at a sector level.

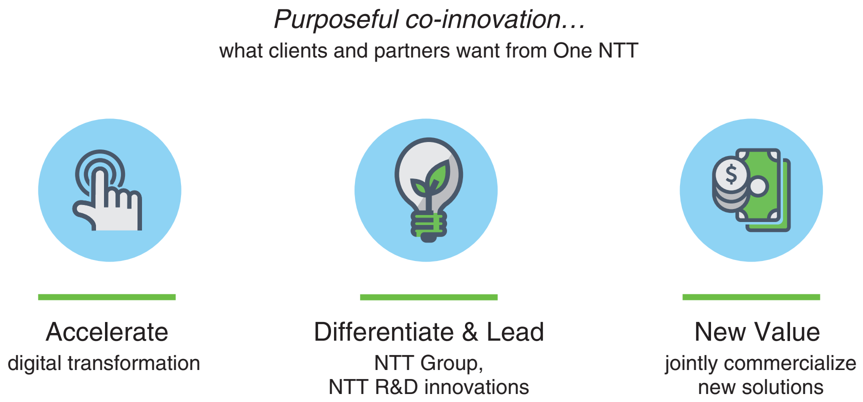


Fig. 1. Purposeful co-innovation through One NTT.

2. Vision of society

It has been four months since we opened the CIC, and we are already well engaged in purposeful innovation with numerous clients. The use cases that feature cutting-edge technologies from NTT R&D are provoking new thinking and intentions. Yet we are not merely bringing in R&D technologies from Japan; very importantly, our CIC is modeled on the ethos of Society 5.0 [2] and NTT's expression of that through the business-to-business-to-X (B2B2X) model for value creation. We feel that it is a really important time in the world today to bring a moral and ethical framework to the way that technology is used to shape future society and humanity, and Society 5.0 is something the whole world should be considering.

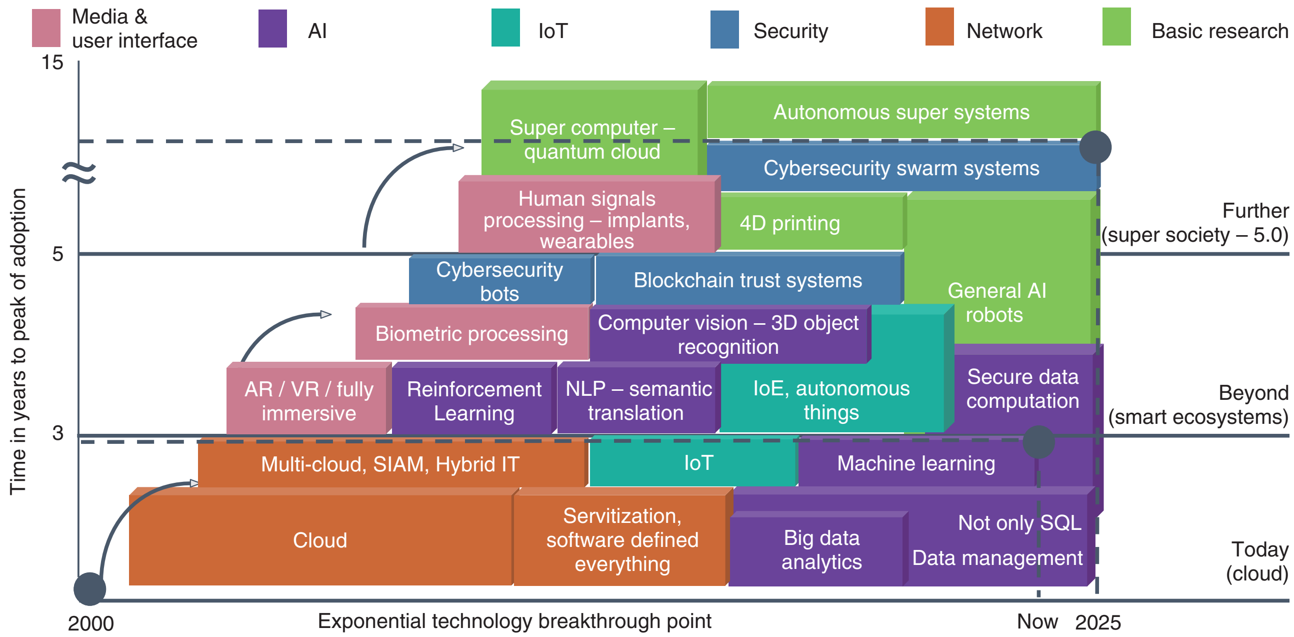
We need a vision for society because that provides the compass settings for what we are innovating towards. If we look at what's happening today, we see there is an explosion of applications and interfaces, mixed reality experiences, growing intelligence all around us, hyper-connected people and things. And data fuels the expansion of digital frontiers. All these changes are built upon the foundations of the Internet, mobility, social, cloud, and digital platforms.

However, what's coming in the next 15 years is very different. In 15 years' time, we will look back and recognize that today was really just the toy box of digital infancy. What will the world look like in 15 years? It will be a profound convergence between the physical and the cyber worlds where the interface will become *us*. Our gestures and our movements and thoughts are the data and application programming interfaces (APIs), and all the simplification of our experience will entail profound complexity under the covers. Dynamically driven from an intelligent edge and completely trustless, systems of record, systems of engagement, and systems of intelligence will follow architectural conventions that have not yet come about. Powering all of this will be, literally, a quantum change. This is the compass that we use for guiding innovation today, and when we take hops, steps or leaps forward with our clients, it's referencing scenarios from this future vision.

3. Transformation and innovation themes

At this NTT R&D Forum, we are experiencing a lot of amazing emerging technologies and the use case stories provided by the NTT R&D researchers suggest some practical applications. The Forum themes are media & user interface, artificial intelligence (AI), Internet of Things (IoT), security, network, and basic research, and each category provides numerous use cases to explore what NTT has to offer towards this future vision. We created a mapping that helps unpack what types of technologies are coming together and when and how they are maturing (**Fig. 2**). On the X-axis of this map is the actual point of a technology breakthrough where the linear improvements become exponential, and then it suddenly becomes possible to create commercially viable solutions from those maturing technologies. The Y-axis is the peak of the innovation adoption curve, which means the time when the adoption of solutions transitions from the early to the late majority.

Now, in our CIC, acting as One NTT, we are looking to work with technologies that can deliver value from now into the next five years. There are two types of innovation we conduct. One of them is working in


Media & user interface
AI
IoT
Security
Network
Basic research
15
5
3
Time in years to peak of adoption
Super computer – quantum cloud
Autonomous super systems
Cybersecurity swarm systems
Human signals processing – implants, wearables
4D printing
General AI robots
Cybersecurity bots
Blockchain trust systems
Biometric processing
Computer vision – 3D object recognition
AR / VR / fully immersive
Reinforcement Learning
NLP – semantic translation
IoE, autonomous things
Secure data computation
Multi-cloud, SIAM, Hybrid IT
IoT
Machine learning
Cloud
Servitization, software defined everything
Big data analytics
Not only SQL
Data management
Further (super society – 5.0)
Beyond (smart ecosystems)
Today (cloud)
2000
Exponential technology breakthrough point
Now
2025

AR: augmented reality
IoE: Internet of Everything
IT: information technology
NLP: natural language processing
SIAM: service integration and management
SQL: Structured Query Language
3D/4D: third/fourth dimension
VR: virtual reality

Fig. 2. Translating R&D into purposeful innovation.

this bottom line here of connecting the dots of all the technologies that are mature today but have not yet been joined together to create a simplicity and agility that help our clients to speed themselves up to be able to move to the next horizons. That's not always exciting as innovation, but it is very important.

The other area is to choose emerging technologies in this new category of *beyond* and to be able to accelerate the maturation and their early adoption into markets to create differentiation and a competitive advantage for our clients. That is our appetite of innovation through CIC.

Regarding digital transformation, every organization is intent on this, but I don't think it's universally agreed what it means. What does it really entail? Across our group, we have combined our research and collective experiences working with client organizations globally. We have identified six key business performance areas and within each of these, the capability investment intentions of businesses to achieve cohesive and sustainable success. All of this totals to a 3.9 trillion US dollar global investment in technology enabled transformation across 2020 (**Fig. 3**).

It is important to consider your overall business transformation and innovation goals against these performance areas and capabilities—do you have gaps, are you underinvested in some areas, where will you most benefit from acceleration or disruption? On this basis, what are the innovation priorities and how will we target and measure value?

Let me briefly explain what we mean by these capability investment vectors. The three in the bottom part of the figure are about establishing the digital foundations for an enterprise, the capabilities needed to participate in digital economics. The three in the upper part are about your transformative capabilities—what you do to achieve new purpose and create new value and prosperity for your organization.

In a little more detail, at the very bottom, we have cyber resilience, the ability to create a new DNA of cyber resilience, embedded in technologies, processes, practices, and culture. Digital fabric and the Internet of Everything is the shift in information technology (IT) to hybrid infrastructures matched to business performance needs, the marriage of IT and OT (operational technology) systems through IoT and the transformation of the IT organization from a cost

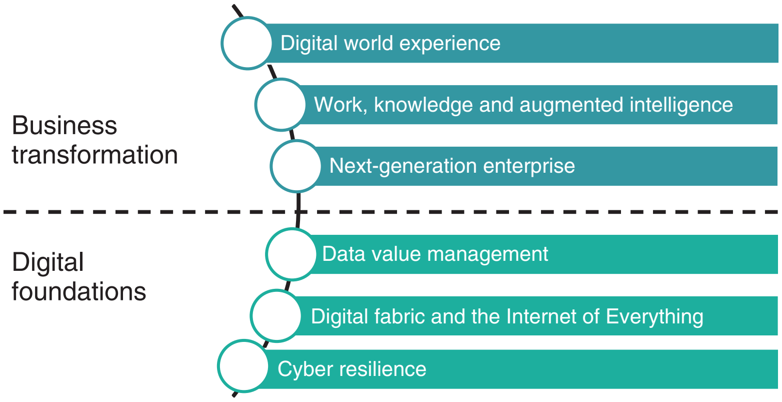

Business
transformation
Digital
foundations
Digital world experience
Work, knowledge and augmented intelligence
Next-generation enterprise
Data value management
Digital fabric and the Internet of Everything
Cyber resilience

Fig. 3. Demand themes for transformation and innovation.

center to business enabling services. Then, there is the area of data value management, which is essentially the digital heart transplant that most organizations truly need for data to become the lifeblood of the intelligent, digitally orchestrated enterprise and to become a valuable asset on the balance sheet.

In terms of business transformative capabilities, the first is the next generation enterprise. This entails the transition from relatively static and linear supply chain models to dynamic ecosystem business models. The technology re-platforming entails software defined and data driven APIs orchestrating these ecosystem flows. Work, knowledge, and augmented intelligence is about enabling knowledge workers to be their most effective selves, whether as creators, communicators, managers or decision makers, in the way they work with each other, visualize and use data, train their cognitive agents to support what they do. Finally, digital world experience is about the stakeholder and the changing nature of their expectations and their experience with your organization. The shift in focus from omni-channel to channel-less as digital becomes ambient within the atmosphere. And we are increasingly interacting with our stakeholders' AI agents and their personal data APIs. These six vectors map to the future society view.

Very often we find that our clients do not have such a cohesive approach to their transformation. Through the CIC model, we can help identify gaps, and direct innovation accordingly.

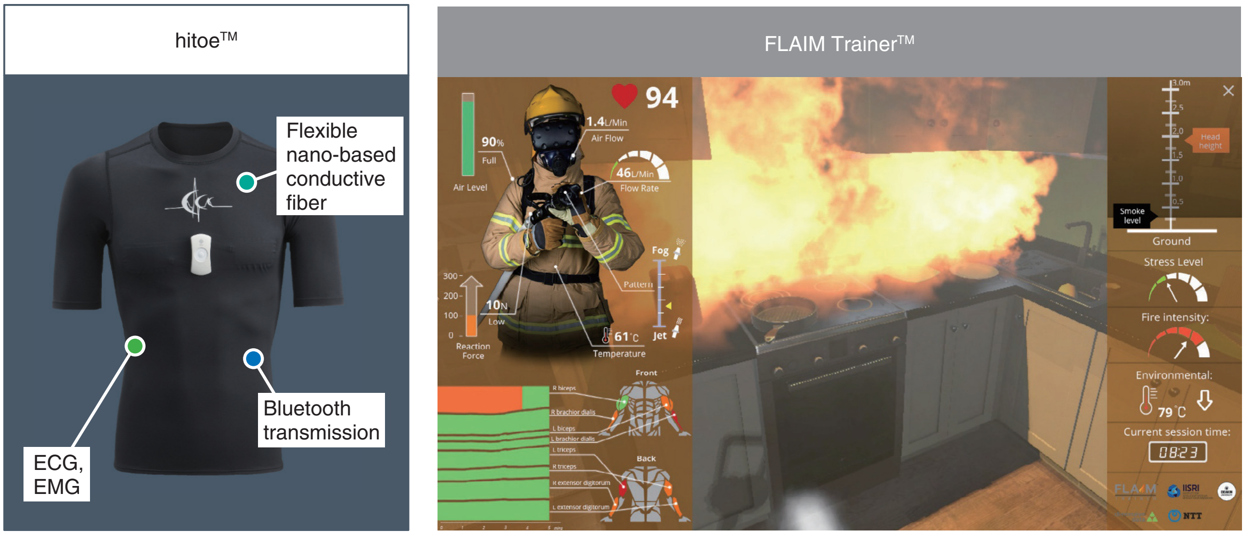
4. Benefiting from NTT R&D innovations

Now I would like to share with you two examples of what we have been able to create through our relationship with NTT R&D and our clients and partners. They illustrate the coming together of the right partnerships and interesting collective mixes of capabilities under the B2B2X model. We have the B2B of NTT R&D, ourselves and our university clients and partners, the NTT operating companies in the region, and of course the X, end user beneficiaries.

It is the one plus one equals many more than three phenomenon that is occurring here. Our collaborations and flows are becoming much more bi-directional with NTT R&D because we are bringing the use cases from industries and clients in markets that the NTT researchers find stimulating and that add to their thinking about their research projects. Indeed, we are also generating new intellectual property (IP), which we share back with NTT R&D. So it is a growing relationship of value co-creation.

4.1 FLAIM Trainer™

The first example is FLAIM Trainer™ [3] (**Figs. 4** and **5**). I would like to share with you the story about how this has come about because it's interesting to understand. Deakin University is an innovative university in Australia, they have a strong commercialization track record from their R&D. In the middle of 2017, they had created a solution called FLAIM Trainer, which is a virtual reality (VR) and haptics based firefighting solution with numerous simulator scenarios such as cars that are on fire, jets on fire, and other situations. Deakin University is also a close client/partner of Dimension Data Australia. In July 2017, we brought some members of Deakin University to the NTT R&D labs in Japan and explored a wide range of emerging technologies. Everything starts by focusing on something specific, and we felt



ECG: electrocardiogram
EMG: electromyography

Fig. 4. Train virtually, experience reality, measure performance.

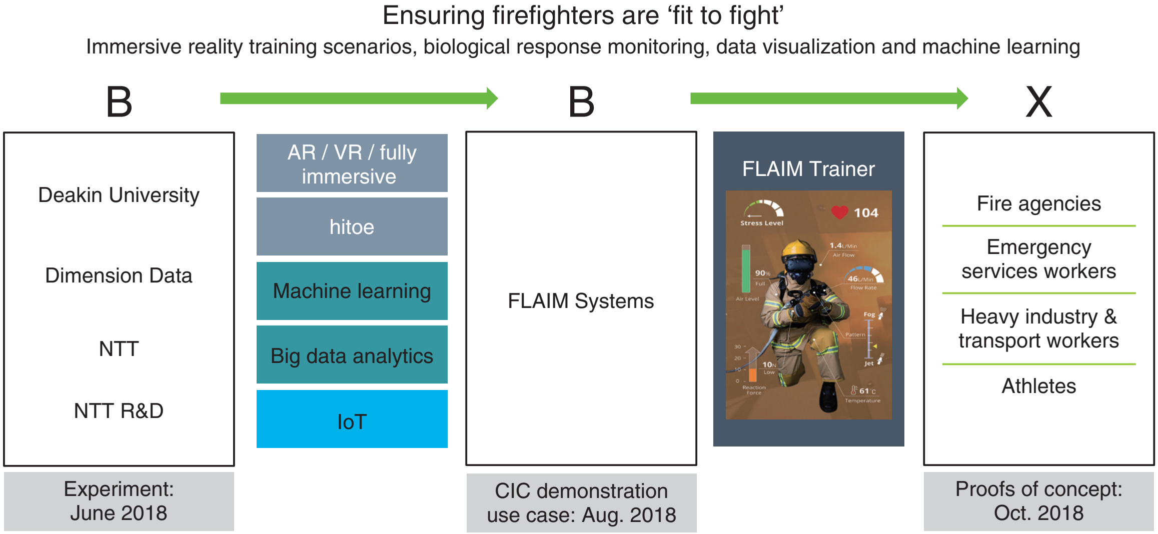

Ensuring firefighters are 'fit to fight'
Immersive reality training scenarios, biological response monitoring, data visualization and machine learning
B
B
X
Deakin University
Dimension Data
NTT
NTT R&D
AR / VR / fully immersive
hitoe
Machine learning
Big data analytics
IoT
FLAIM Systems
FLAIM Trainer
Fire agencies
Emergency services workers
Heavy industry & transport workers
Athletes
Experiment: June 2018
CIC demonstration use case: Aug. 2018
Proofs of concept: Oct. 2018

Fig. 5. B2B2X co-innovation for FLAIM Trainer™.

immediately that there was a great opportunity to enhance what they had created with FLAIM Trainer by adding the ability to biometrically monitor firefighters during their training.

So the idea of bringing FLAIM Trainer together with the NTT hitoe™ biosensing technology and our Dimension Data Australia data and analytics expertise was born. We started the prototype process, which Dimension Data managed, and very quickly we were able to create a solution which included electrocardiogram (ECG) sensing married with the VR experience, providing real-time visualization of the physiologic response alongside the environmental data about fog and temperature, and pressure flows from the hose. We brought this to the NTT R&D Forum held in February 2018. This created a lot of interest. FLAIM Systems Pty Ltd. (a start-up wholly owned by Deakin University), meanwhile, raised funds to commercialize its core offering.

We suggested to NTT R&D that this solution would indeed be greatly enhanced and would be unique in the market if we added in the ability to sense electromyography (EMG) muscular activity. NTT R&D agreed, and joint research has been undertaken by NTT R&D and Deakin researchers. We are now adding EMG capability into the hitoe sensing and the data platform solution. This will improve the 'fit to fight' insights and training approaches for fire departments and broaden applicability to other industries such as defense, ambulance, and heavy industries with safety issues for workers.

This use case has seen a relatively rapid translation to value, characterized by true collaboration and flow of IP in both directions. Most importantly, we have retained line of sight of B2B2X and the importance of taking a market focus.

4.2 Mass Data Observations and San-shi™

Now I'd like to share with you another example. This co-innovation has come about between NTT R&D, Western Sydney University, and Dimension Data Australia. This use case demonstrates two things: firstly, ways of bringing many forms and sources of data together to be able to use it for research purposes; but as well, with the addition of San-shi™, NTT's secure computation system, the potential to drive new standards in cloud data privacy and enable safe data sharing, which is demonstrably lacking at the moment in the world (**Figs. 6** and **7**).

Firstly, the journey of this co-innovation. Western Sydney University and Dimension Data have co-created a platform called Mass Data Observations. It is a large-scale data management platform that can accept all forms of data for exploration by researchers in projects that may be open and collaborative or discrete and privately conducted. In addition to this, the Mass Data Observations platform enables researchers to crowdsource research challenges and attract interest from people who may wish to collect data for them or become subjects in research projects. Both the researchers and the data contributors on this platform can be rewarded in RiByts, research incentive bitcoins. The idea is to drive a large-scale collaborative data-driven research ecosystem.

In July 2017 we brought some top researchers from Western Sydney University to NTT R&D labs in Tokyo, and just as with Deakin, we saw many things we would like to work with, but immediately we were struck by what we saw with San-shi, the prototype of a secure, multi-party data computation platform. In our view this was cutting-edge and potentially world-leading in the area of encrypted data analysis and secure multi-party data computation.

Given our enthusiasm and our access to test high value use cases with industry partners in Australia, NTT R&D agreed to accelerate the English version of San-shi. By January 2018, a cohort including experts from my team, Western Sydney University, as well as Deakin University, returned to Tokyo for knowledge transfer and we brought San-shi back to Australia, integrating it with Mass Data Observations, running on our cloud platform in Australia. We immediately started exploring and testing the capabilities and running use cases through it. The following use case is one of those examples.

Mass Data Observations is a powerful platform for bringing all sorts of data together to enable exploration of data. However, the challenge still remains, that when it comes to bringing sensitive data sets together from multiple parties, we have a serious issue with trust and quite rightly so, and this creates barriers to approval by ethics and governance committees, as anyone who does research knows. Therefore, the question is how to safely, securely, and economically make these data sets available for analysis. That's where we brought San-shi into the equation.

Data about fires in the state of New South Wales had never been brought together before to understand what the full social, economic, and health impacts of fires were, let alone trying to improve the outcomes. Ten million people live in the state of New South Wales. Before this research was conducted, data recorded that there were about five fires a day. In fact, there were 20. Deaths attributed to fires were about 500 over a 10-year period, but it was found that there were actually 9000 deaths. The emergency departments reported a couple of dozen injuries from fires a day, but in fact, there were over 213. So clearly, there were sources of information everywhere, and this information was never brought together to create a very clear picture of the impact of fires.

Researchers at Western Sydney University had researched this in the traditional way, spending three years and hundreds of thousands of dollars gaining ethics clearance and bringing together 11 different data sets, from the fire department, first responders, hospitals, register of deaths, primary care providers, insurers, and others.

We set out to show that the use of Mass Data Observations with San-shi created a 'trustless' technology

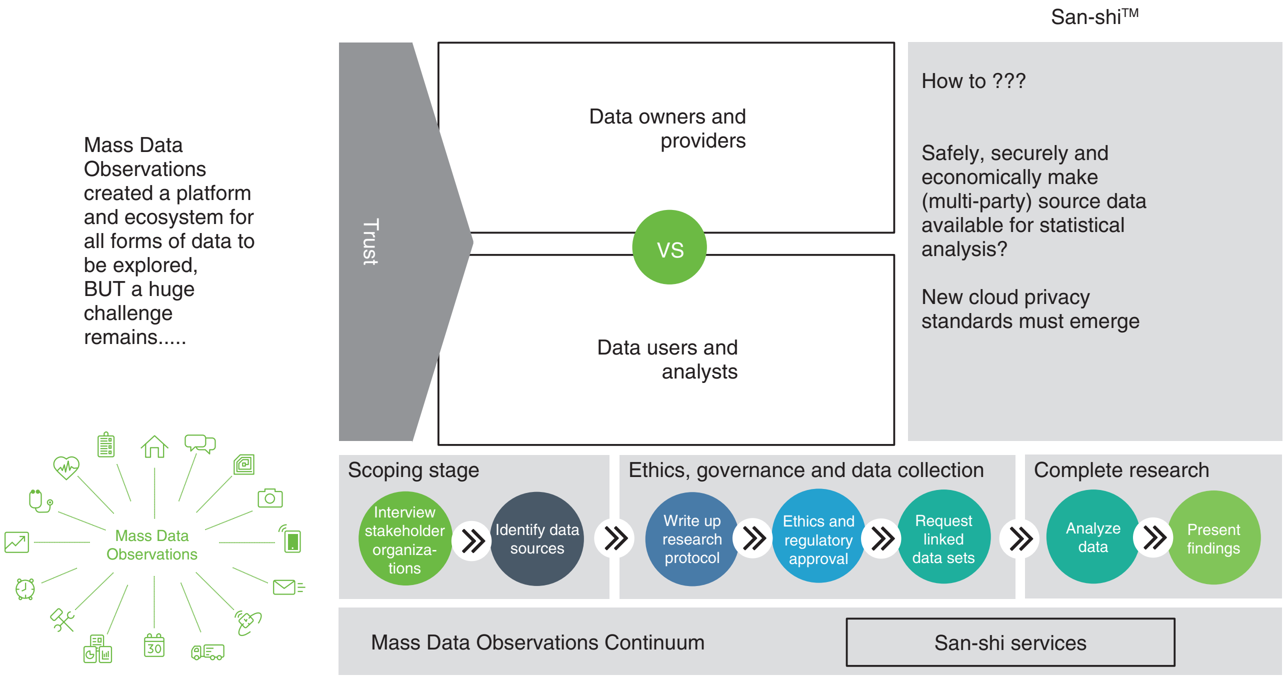

San-shi™
Mass Data Observations created a platform and ecosystem for all forms of data to be explored, BUT a huge challenge remains.....
Trust
Data owners and providers
VS
Data users and analysts
How to ???
Safely, securely and economically make (multi-party) source data available for statistical analysis?
New cloud privacy standards must emerge
Mass Data Observations
Scoping stage
Interview stakeholder organiza-tions
Identify data sources
Ethics, governance and data collection
Write up research protocol
Ethics and regulatory approval
Request linked data sets
Complete research
Analyze data
Present findings
Mass Data Observations Continuum
San-shi services

Fig. 6. Research innovation with San-shi™.

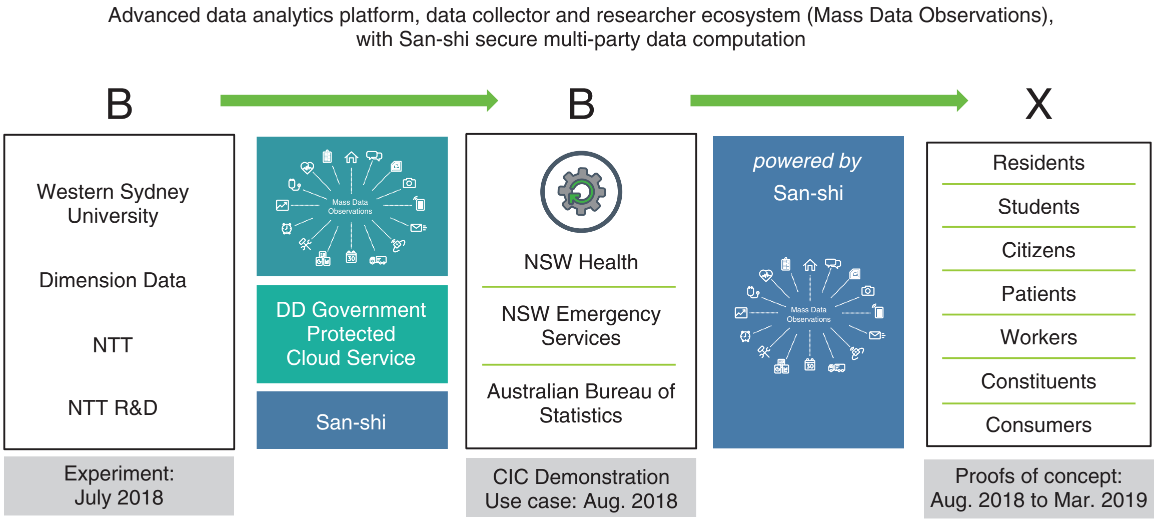

Advanced data analytics platform, data collector and researcher ecosystem (Mass Data Observations), with San-shi secure multi-party data computation
B
B
X
Western Sydney University
Dimension Data
NTT
NTT R&D
Experiment: July 2018
Mass Data Observations
DD Government Protected Cloud Service
San-shi
NSW Health
NSW Emergency Services
Australian Bureau of Statistics
CIC Demonstration Use case: Aug. 2018
powered by San-shi
Mass Data Observations
Residents
Students
Citizens
Patients
Workers
Constituents
Consumers
Proofs of concept: Aug. 2018 to Mar. 2019

Fig. 7. B2B2X co-innovation for ethically and securely exploring the data multiverse.

environment that could execute this challenge accurately and without the potential of breaches. This is important as in the future, this may reassure ethics and governance committees, expediting approval processes and affording significant time and cost-savings for sensitive multi-party data research use cases.

I will briefly explain how San-shi works. Eleven different sources of data were available; when they are ingested into San-shi, each data source is encrypted and split across multiple servers. It never exists inside the San-shi system in its original form. When a researcher wants to access that data to conduct statistical analysis, the data are brought together but never decrypted; they're analyzed in an encrypted state. The analyst never receives the source data; they only ever receive the output. The data sources are never held in their original state by San-shi, and the data are never actually touched by researchers—this is trustless secure multi-party computation [4].

Just think about what new value can be created from such a capability, unlocking research possibilities previously deemed not safe to conduct. In this use case about the impacts of fires, we can create new citizen services where people could check the safety records of buildings and certain appliances, and first responders would know much more about the spectrum of impacts from a fire and adopt the best choice of interventions. Indeed, firefighters could improve their training regime, and the government could enforce much better policies and public awareness around fire safety. Thus, this use case has been illustrative and powerful for us, and we are now exploring more use cases around San-shi, notably in healthcare policy and population-wide interventions.

5. Summation

These examples illustrate why we created the CIC and what outputs are being generated. We now have interest from other parts of the global NTT family, to use the CIC model as a template for engaging with NTT R&D, using B2B2X to drive strategic engagement in their markets and with their clients.

Returning to my opening remarks about what our clients and partners want from One NTT and an innovation relationship—to accelerate transformation, to differentiate and lead in their markets and/or to create new value through partnership—we are stepping up to this expectation, learning, and evolving with our clients.

If you are curious about these individual experiments but also the CIC model and the potential flows from research to innovation to commercialization, then please come and talk to us at our booths at this forum.

I leave you with a question. When you think about your organization's transformation and innovation needs, what would or could you want from a truly *One NTT?* Because when we bring this all together, what can be harnessed for you is truly amazing.

References

[1] Press release issued by Dimension Data, "Dimension Data Launches First Client Innovation Centre to Bring Cutting Edge Tech Down Under," Aug. 1, 2018.
https://www.dimensiondata.com/en/news/dimension-data-launches-first-client-innovation-centre-to-bring-cutting-edge-tech-down-under

[2] Government of Japan, "The 5th Science and Technology Basic Plan," Jan. 2016.
http://www8.cao.go.jp/cstp/english/basic/5thbasicplan.pdf

[3] T. Levin, S. Chessum, J. Mullins, N. Yoshihashi, and K. Hayashi, "Ensuring Greater Safety for Our Firefighters and Our Communities: Integrating FLAIM Trainer^{TM} and hitoe^{TM}," NTT Technical Review, Vol. 17, No. 2, pp. 24–31, 2019.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201902fa3.html

[4] 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^{TM}," NTT Technical Review, Vol. 17, No. 3, pp. 16–21, 2019.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201903fa3.html

Trademark notes

All brand names, product names, and company/organization names that appear in this article are trademarks or registered trademarks of their respective owners.

Debra Bordignon

Chief Technology Officer, Dimension Data Australia.

Debra sits on both the executive and the strategy and innovation committees at Dimension Data Australia. As CTO, she leads the portfolio strategy transforming the group in Australia to fulfil its vision to become the leading services integrator enabling digital enterprises and ecosystems.

She facilitates an exchange of global R&D and innovations between NTT, Dimension Data, and their partners and clients. She shapes co-innovation initiatives, strategic partnerships, and ventures, with a focus across the industries on higher education, the public sector, health, and financial services.

Debra holds a Bachelor of Applied Science, is a graduate of the Australian Institute of Company Directors, and has completed executive leadership education at Harvard Business School.

Leading in the Age of Digital Disruption

Marc Alba
Chief Disruption Officer, everis, and
Head of NTT DATA NextGen

Abstract

At everis, an NTT DATA Group company, a team consisting of 65 members is currently working to create solutions for existing companies by applying disruptive approaches. Half of the team is expert in technology such as artificial intelligence, machine learning, crowdsourcing, robotics, and blockchain, and the other half has expertise in business domains such as design, marketing, finance, and legal issues. This article describes the importance of digital disruption and the disruption initiatives by the NTT Group based on a speech given by Marc Alba, Chief Disruption Officer of everis, at NTT R&D Forum 2018 Autumn on November 30, 2018.

Keywords: disruption, digital, cloud

1. Evolving and maturing digital transformation

To start with, I will present a general context about the current momentum of digital transformation, where we are now, where we are coming from, and where we are going.

Around 2012, we had the first wave of digital transformation. It was really about social/mobile, and the "digital" became a part of our lives *in glass*. When I say "glass," I'm talking about screens. With mobile phones, tablets, and that kind of devices, we had "digital" through our screens. It was really about channels, connections, and interactions. The four letters S-M-A-C, representing social, mobile, analytics, and cloud, changed the world completely in less than 10 years, and that was connected to the third-generation of mobile communications (3G) and 4G. This wave also led to the significant growth of Google, Amazon, Facebook, Apple, and Samsung, referred to as GAFAS.

About one or two years ago, we had the second wave of digital transformation. Everybody agreed on calling that wave the AI (artificial intelligence)-first world. After being fundamentally based on the channels and the way we use them, the concept of "digital" suddenly came back to "silico" (to the hardware) such as graphics processing units (GPUs), field-programmable gate arrays (FPGAs), and application-specific integrated circuits. We needed to have hardware that makes AI fast enough for deep learning and machine learning, and a completely new generation of chips *in silico* were created. Companies like NVIDIA and Xilinx are now working a lot with GPUs and FPGAs. "Digital" moved to a new type of "silico" and microcomputers.

"Digital" is now moving to the relationship between humans and machines. I live in Boston in the Unites States. One of the hot topics there is social AI. It is about the relationship between humans and machines. Human-robotic iterations, digital empathy, digital trust, this is the new big thing. Our work around the relations between humans and machines, both hardware such as robots—social robots, personal robots, service robots—and purely digital chatbots and robo-advisors, is proving that humans can create very special relationships with these machines (in the wide sense of both phygital and digital ones).

We are currently working with young kids. They create a very special empathy with machines. We are also working with older people, and it is surprising to see how they also engage in a special relationship with machines. AI is moving from the cold AI, where it can seem fearsome, for example, humans against machines, to social AI. That is the second wave, and the enabling technologies are AI, robotics, machine learning, Internet of Things (IoT), and edge computing. We are also slightly shifting from 4G to 5G. In the first wave, four technologies changed the world. Now those five new technologies are adding to these four ones. Thus, nine technologies at the same time are changing all industries, all geographies, and all societies. It is the first time in human history to experience that number of disruptive technologies at the same time changing potentially any business and any industry.

Regarding the third wave of digital transformation, this is the foresight; it could be wrong, or it could be accurate. Our vision is that the next big shift of "digital" will involve "digital" entering three new domains.

The first domain is *digital in physio*. It means we are talking about 3D (three-dimensional) printing, additive manufacturing, and digital fabrication. The first time you create something in "digital." With "digital" you will be able to create tangible objects.

The second important domain is *digital in bio*, meaning living bodies. "Digital" becomes embodied in life. Part of the work we are doing is connected to digital biology, synthetic biology, and genomics. Now our human body can have the same rule of software. We can apply it more to the human body than to animals. That is a completely different shift. This is just emerging, but it should ramp up around 2020 or 2022.

The third domain is *digital in virtual*, which refers to virtual reality, augmented reality, mixed reality, and such. Our limited experience until now indicates that somehow there is still some hype around virtual reality, but by 2020/2022, virtual reality can probably overcome the complexity we have right now.

This third wave is what we call *phygital*, which combines *physical* and *digital*. What you have is "digital" penetrating into physical objects, human bodies, living bodies, and also the rise of synthetic reality.

The main problem we will have by 2020/2022, and at NTT we are busily working on, is what happens with more loads of data, because we are getting close to reaching the limits. So quantum computing and quantum communications will be very important, and we will need to find sufficient computing power. Obviously, 5G will be taking off in this third wave, and we will have amazing new capabilities through 5G.

These three waves are all about the same idea. "Digital" is like a virus. It's penetrating more and more facets of our daily lives. It can be humans, it can be a car, it can be a home, it can be a city, it can be a sport (**Fig. 1**). If you look at these different items of evolution in each of the phases of maturity of "digital," you see the same pattern. First of all, you have the single entity that becomes somehow connected and socialized and obtains more capability to embed analytics. After that, it can plug in intelligence, and it becomes more smart and autonomous. All of the items go through the same pattern.

All that vision I just presented about the third digital wave is really our best guess. We really do not know what will happen. Imagine that quantum computing is delayed for some reasons, and imagine any of the expected outcomes change. What is clear is that beyond the next two to three years we do not have the clarity to see what will happen. That is a big problem.

The fundamental question of this first block is how can we prepare ourselves for a world we cannot imagine? You in your work, you at home with your family, you as a human being. Six years ago, my wife and I had triplets as our first kids. The main question we had three years ago is which school should we send them to? Because most of the schools are conceived for a world that's no longer there. They are conceived for a world where you need to memorize things and develop calculation skills, which are less and less relevant. If we were to think about the skills we need, it would be the ability to continue to change, the ability to adapt, and the ability to judge what is relevant and what is not, what is trustworthy and what is not, among an almost infinite source of data and information. Conventional schools do not train for that. So, there are some fundamental questions behind all of the massive changes that are transforming our daily lives.

2. Digital disruption

What is crystal clear to us is that this discipline is called *disruption*. In fact, the idea of disruption goes back a long way. Joseph A. Schumpeter in 1911 wrote a book entitled "The Theory of Economic Development,"

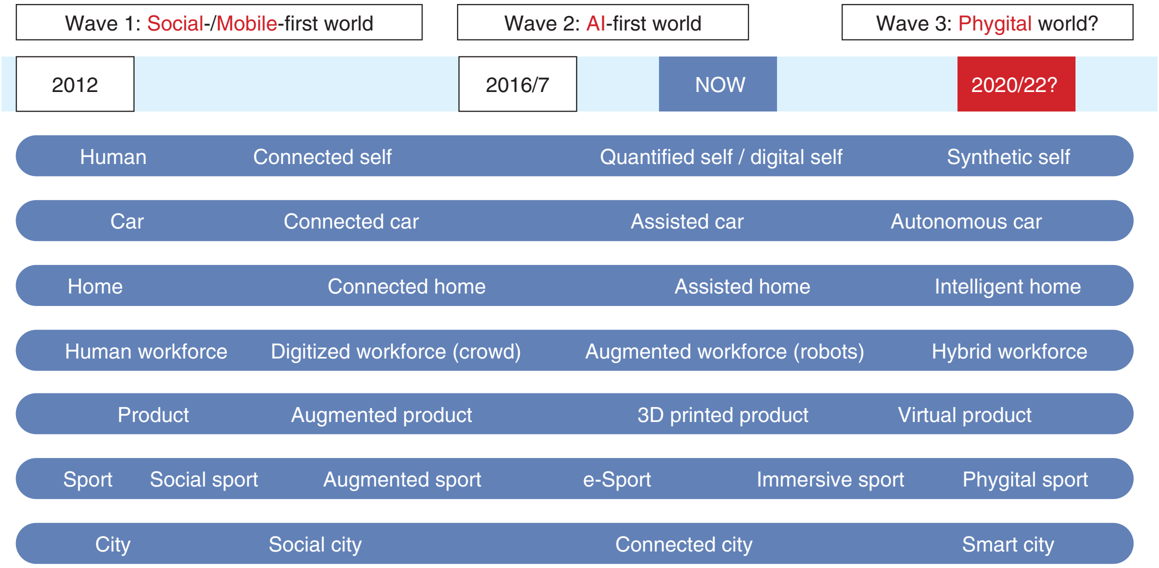


Fig. 1. Transforming our lives through “digital”: Internet of Everything.

where he talked about *creative destruction*. The idea behind creative destruction is that you have industries and new technologies that come and change everything. Destroying things to create something new becomes a dominant way of operating and doing business. Thus, destruction/disruption have been around for a long time. The concept itself goes back to 1995, when it was introduced by Clayton M. Christensen, who wrote “The Innovator’s Dilemma.” However, disruption combined with “digital” takes completely new dimensions. This is what I would like to elaborate on.

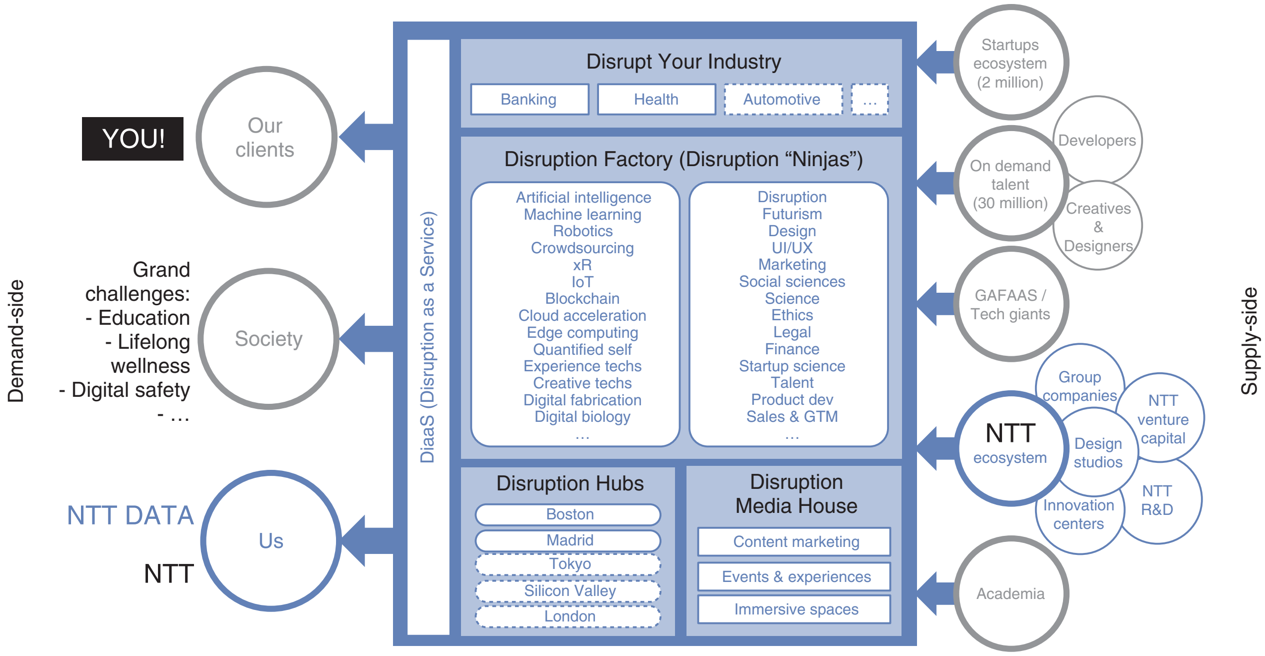
Some of these facts I will present now may seem very threatening, but the message I am trying to convey is completely opposite. The message behind these big threats is actually very positive. There are massive opportunities for those who know how to leverage them.

The lifespan of companies is declining. Being a big company was once a competitive advantage, but it’s losing the resilience it had before. In the five and a half years from January 2011 to July 2016, the number of *unicorns* substantially increased. Unicorns are companies that seemingly came from nowhere but had stock values that were over 1 billion US dollars individually. So all these companies are new entrants in the market and are reinventing the industry. In addition, if you look at three to five years before, many of the unicorns were concentrated in the United States. The world is becoming more and more flat. You can create a new disruptive company anywhere. With more players comes more democratization.

Another interesting factor to take into account is the concept of the Tech Oligopoly. It refers to Apple, Google, Microsoft, Amazon, and Facebook. These players have ecosystems to compete in many markets. In the beginning, they focused on their core competencies, but now they are entering the fields of retail, healthcare, and payments. These players combined with startups are shaking up all the domains and industries. Beyond the disruption in business ecosystems, what you have is also a general disruption in other domains like politics and social systems.

My statement here is that we should not see all these complexities only as threats. They are definitely threats, but behind big threats you also have huge opportunities. These threats are not like innovation but are more connected to disruption.

I will try to explain the main difference between innovation and disruption. I will use the car as an example. In innovation, basically the rationale is “I want to improve on the car.” The starting point is a car. Your mindset is hooked to a car and it’s biased, so you will end up producing a better car. In disruption, you would not say “I want to improve on the car.” You would say “People and goods need to move around anyplace, anytime.” That would lead you to different approaches to create a novel Hyperloop, Waymo, Tesla, Waze, whatever. In innovation, the idea is to take existing solutions and make them better. In



GAFAAS: Google, Amazon, Facebook, Apple, Alibaba, and Samsung
GTM: go-to-market
R&D: research and development

UI: user interface
UX: user experience
xR: extended reality

Fig. 2. Disruption by NTT DATA/NTT.

disruption, the idea is to take problems and find different solutions. The main problem compared to not so many years ago is the speed of change. More and more technologies are being introduced, and we are attaining more and more capabilities; if innovation is combined with a lot of disruption to create new ways to solve problems, in a few years, you can have a dominant position in the market. Playing with two or three technologies that may look completely different could lead to major disruption. For example, IoT and AI and blockchain and the cloud.

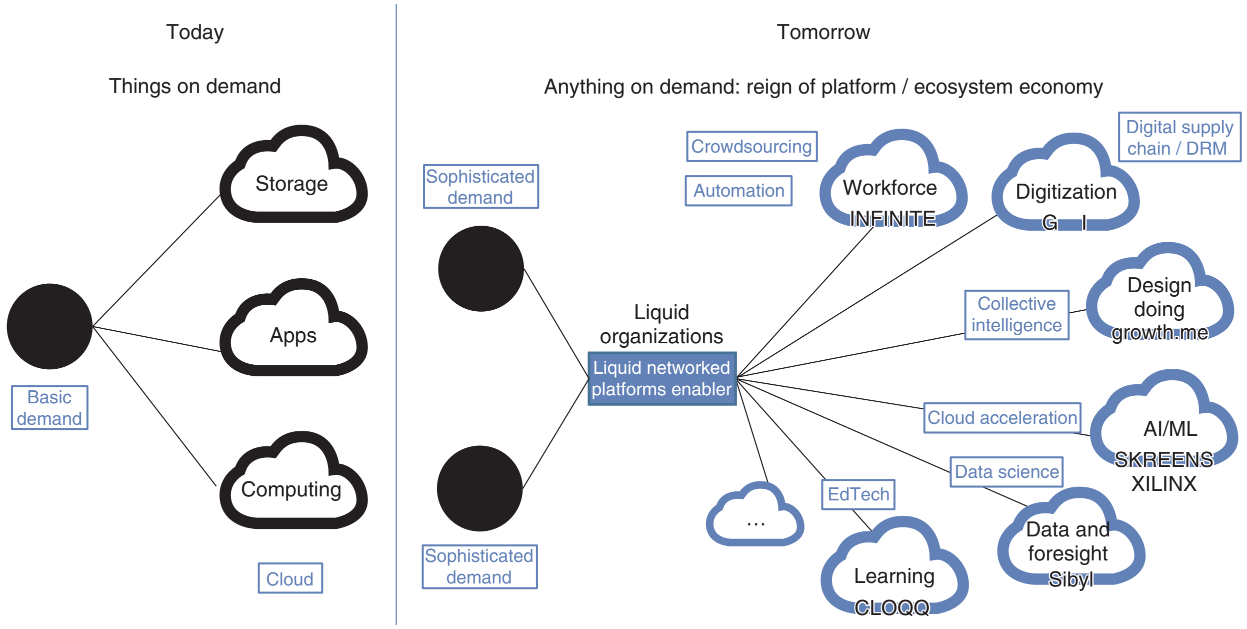
3. Disruption by NTT DATA/NTT

This is what we are selling and building as the NTT Group (**Fig. 2**). We are creating this platform so as to connect all the capacity we have as a Group itself—the NTT research and development laboratories, all our Group companies, networks, innovation centers, and design studios with ecosystems, with startups, crowdsourcing, and academia. What we are building is a factory to address the problem and apply a disruptive mindset and disruptive approaches to create completely different solutions.

We are now working on 20 disciplines. I have time to select a couple of them and show you the type of complex challenge we are trying to solve.

As shown in **Fig. 3**, all the on-premises services are moving to the cloud; this can be storage, apps, or computing. Now what we are observing is a new massive trend, which is that anything a company might need can be moved to an on-demand system. This is what is called *liquid organization*. You can create a whole company without having anything, not even employees. All these names you have here are products we have built. This solution basically involves getting all employees without hiring any of them through crowdsourcing. This platform can create any digital content without hiring any creative agencies or any marketing agencies. It is really moving into the concept of *cloudification*. All those assets that a company might need from knowledge, data, AI as a Service, are really pushed to the cloud. This is the concept we are working on.

Another domain we are working on, which is extremely strategic and extremely interesting, is shown in **Fig. 4**. The left side of the figure is the current model of all our interactions as consumers with tech giants. We are producing a lot of data such as consumer data, producer data, financial data, social



DRM: digital rights manaegment
ML: machine learning

Fig. 3. From things on demand to anything on demand.

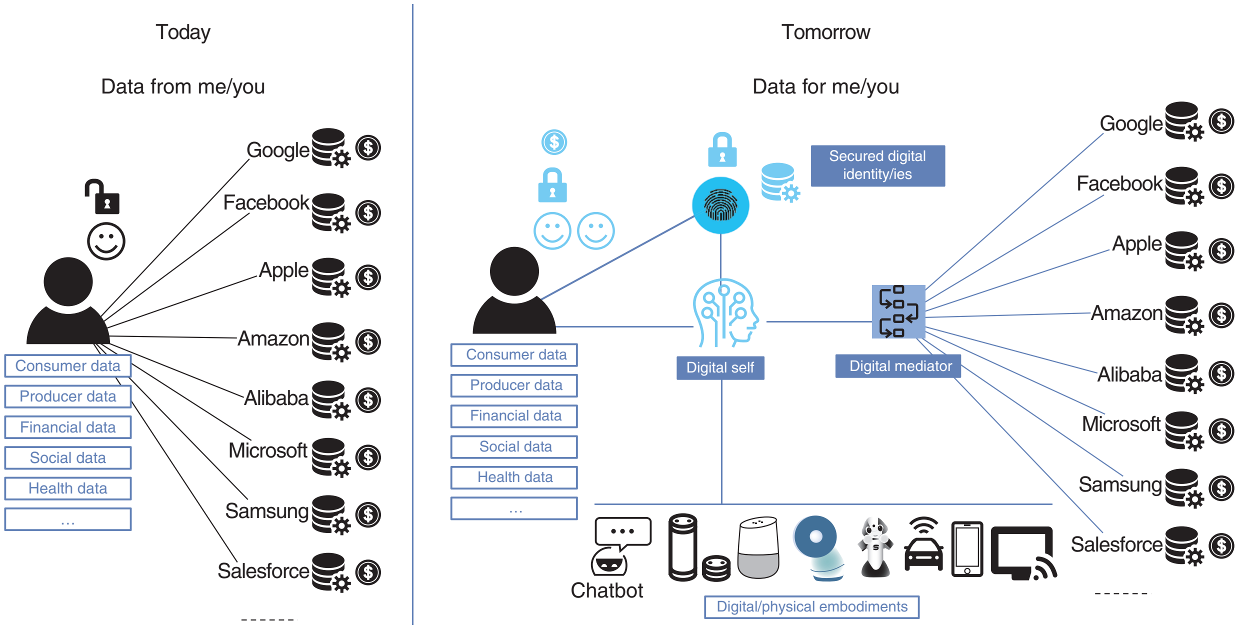


Fig. 4. From data from me/you to data for me/you.

data, and health data. All of these players are somehow operating through them as they capture data. We feel we are happy because we have good services, but the underlying model is completely asymmetric. We own the data, we produce the data, but we play into the hands of these service providers or platformers.

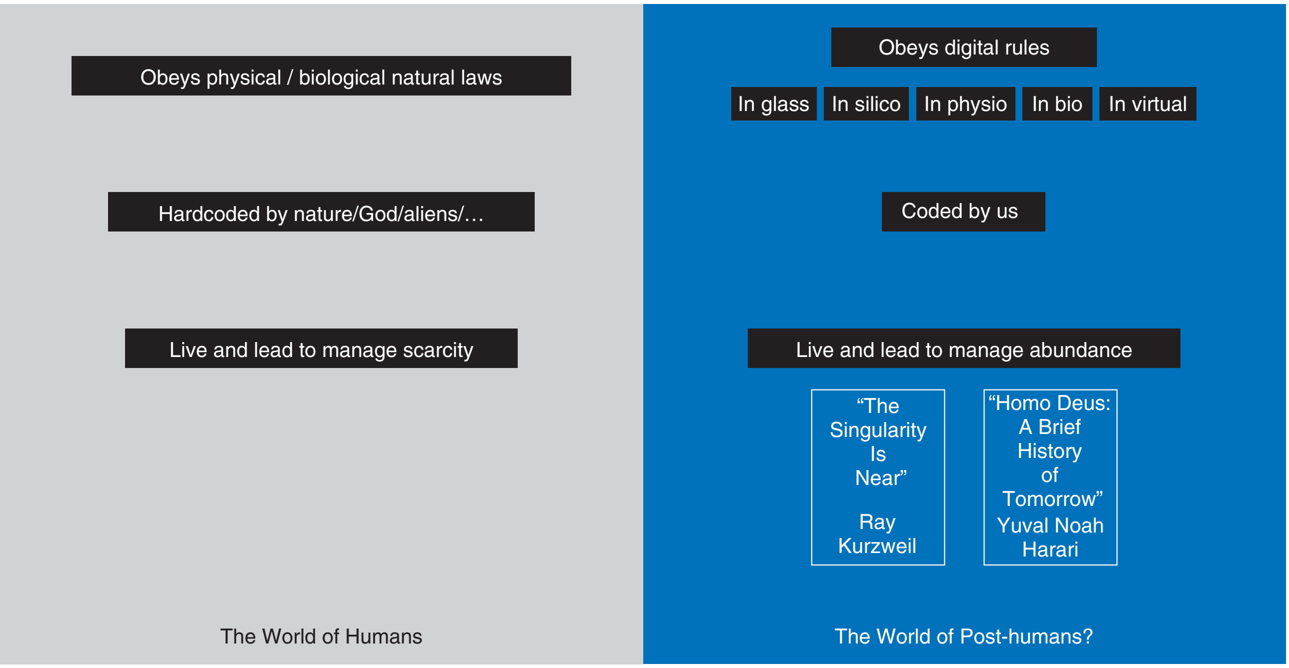

Obeys physical / biological natural laws
Hardcoded by nature/God/aliens/…
Live and lead to manage scarcity
The World of Humans
Obeys digital rules
In glass
In silico
In physio
In bio
In virtual
Coded by us
Live and lead to manage abundance
"The Singularity Is Near" Ray Kurzweil
"Homo Deus: A Brief History of Tomorrow" Yuval Noah Harari
The World of Post-humans?

Fig. 5. From scarcity to abundance.

What we are trying to build is a completely new model, which is "I should own the data," "I should govern the data," "I should monetize the data," me as a consumer. This is leading us to create all these series of new agents (center in the figure). The first one is creating the concept of *secured digital identities* where I put my data automatically. We then created the approach of a *digital self*; it becomes like your digital twin. It's not a chatbot, it's far beyond chatbot; it becomes your interactions, your intelligence, to operate the data. The model we are trying to shift is moving from the model in which each user interacts with each player to the model where we have a digital mediator that interacts with these players and eventually creates a new business model for you to realize a return on your investment of your data.

4. From scarcity to abundance

So, what's next? I don't think anybody has any idea. This is my best guess: We are moving in the long run from scarcity to abundance (**Fig. 5**). Once you plug in all the digital rules, all the physical objects in everything, suddenly you are not limited, you do not have hardcoded items for the people, you are able to code anything on the planet earth. I strongly advise you to read "The Singularity Is Near: When Humans Transcend Biology" by Ray Kurzweil. That is a very good reference. In 2045 singularity will start, and many things will change. That is a must to understand the concept behind all of that, which is probably about evolution, from you as a human to a post-human. That is the long run.

The good news is for these longer visions, disruption will be more and more important because the frenzy of changes will be more and more massive and much faster.

This idea is very significant and ambidextrous (**Fig. 6**). Play with these three dimensions in any of your companies, or any of your businesses and organizations. Running the business is extremely important; otherwise you die. Evolving the business is also important because it gives you more defensive strategies. However, to reinvent, kill your business to create the new business. Hacking the business is about disruption, and disruptive innovation is also extremely important.

Being in a big company having a lot of success is no longer a big advantage. You need to un-learn to relearn. Socrates said, "I only know one thing, and that is I know nothing." You need to have a lot of humbleness. Look at the world with the eyes of children. That's what is behind the quotes.

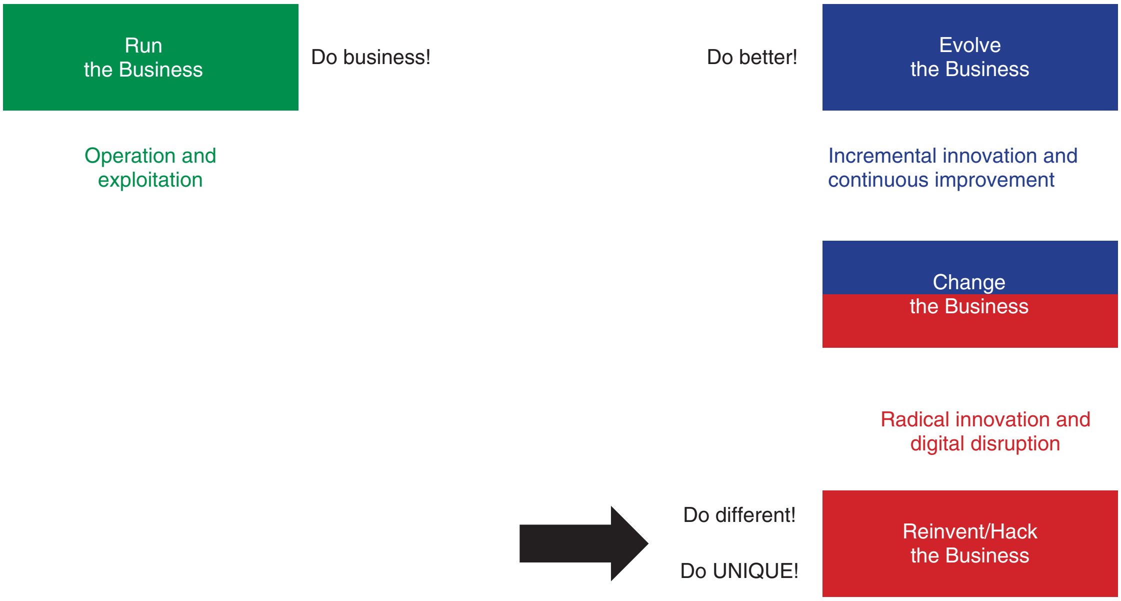


Fig. 6. Ambidextrous leadership.

Trademark notes

All brand names, product names, and company/organization names that appear in this article are trademarks or registered trademarks of their respective owners.

Marc Alba

Chief Disruption Officer, everis, and Head of NTT DATA NextGen.

Marc Alba is a leading expert in disruptive innovation, entrepreneurship, exponential technologies, digital transformation, regional development, and socioeconomic transformation. Throughout the past 20 years, he has served in diverse positions (researcher, entrepreneur, chief innovation officer, transformation director, founder of non-profit movements, and advisor of a large and varied set of both private and public organizations) that in combination provide him with a holistic perspective of the key socioeconomic challenges that businesses and societies are facing worldwide. He has carried out his activities in multiple sectors, including automotive, telecom, industry, banking, insurance, government, energy, and non-government/non-profit organizations.

Marc is the (co-)author of 5 books and has written more than 100 publications and articles. His latest books are i-Leaders (Innovation Leaders): From the Business of Innovation to the Innovation of Business and The Key to Spain's Transformation: Civil Society Takes the Floor. He is also the co-founder of the civil society initiatives TransformaEspaña and TransformaTalento (TransformTalent), and the originator of the innovation management methodology COTIM (Cash-Oriented Total Innovation Management).

Currently, Marc works as a Managing Partner of the everis Group. He sits on the company's Steering Committee as the Chief Disruption Officer. He is the founder and head of everis NextGen and the NTT DATA Disruption Hub. He is also a Fellow of the everis Foundation and President of the TransformaEspaña Association. He is actively involved in various boards and think tanks related to innovation, entrepreneurship, regional development, and education.

He was born in Africa (Kinshasa, Congo). His collaborators define him as a citizen of the world, humanist, and work lover. He is 45 years old, married, and the father of seven-year-old triplets, Maria, Miguel, and Marc.

Intent-based Service Management to Improve Resource Design Efficiency for Cloud Services

Chao Wu, Shingo Horiuchi, and Kenichi Tayama

Abstract

As cloud services have expanded, an increasing number of service providers are implementing various kinds of services and functions such as web services and machine learning in the cloud environment. To provide the cloud service promptly and improve customer satisfaction, a cloud service provider needs to efficiently design the resources in accordance with the service requirements. This article presents an intent-based service management framework that enables the needed cloud resources to be derived in accordance with the service provider's service requirements, cloud environmental conditions, and operation policies.

Keywords: intent-based service management, cloud, virtual machine

1. Current practices of cloud resource design

The cloud has become a popular choice for service providers (SPs) to allocate new service workloads or migrate existing ones. The SP, when requesting new cloud services or asking to scale existing ones, is concerned about the service requirements such as the functionality of the service, the levels of security and availability, and the ability to handle workloads. In contrast, the cloud service provider (CSP) needs to know the composition of resources and the amount of resources to be allocated to fulfill the service requirements from the SP (**Fig. 1**). Therefore, the CSP needs to analyze the service requirements from the SP, and on the basis of the results needs to design cloud resources. Current practices of designing the cloud resources include:

(1) Cloud-consultant approach

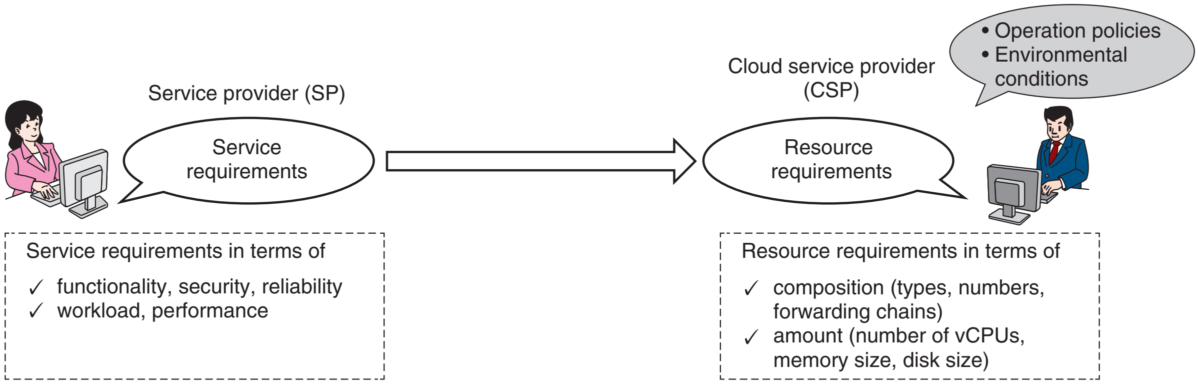
The SP is assisted by cloud consultants from the CSP who collect the SP's service requirements and determine resource details accordingly. This approach results in a high operating expenditure for the CSP and takes them a relatively long time to deliver services.

(2) Self-service approach

The SP is provided with a management interface to manage cloud resources and service needs in order to determine their resource requirements. This approach requires the SP to have IT (information technology) expertise and may be a barrier to SPs wishing to enter the market.

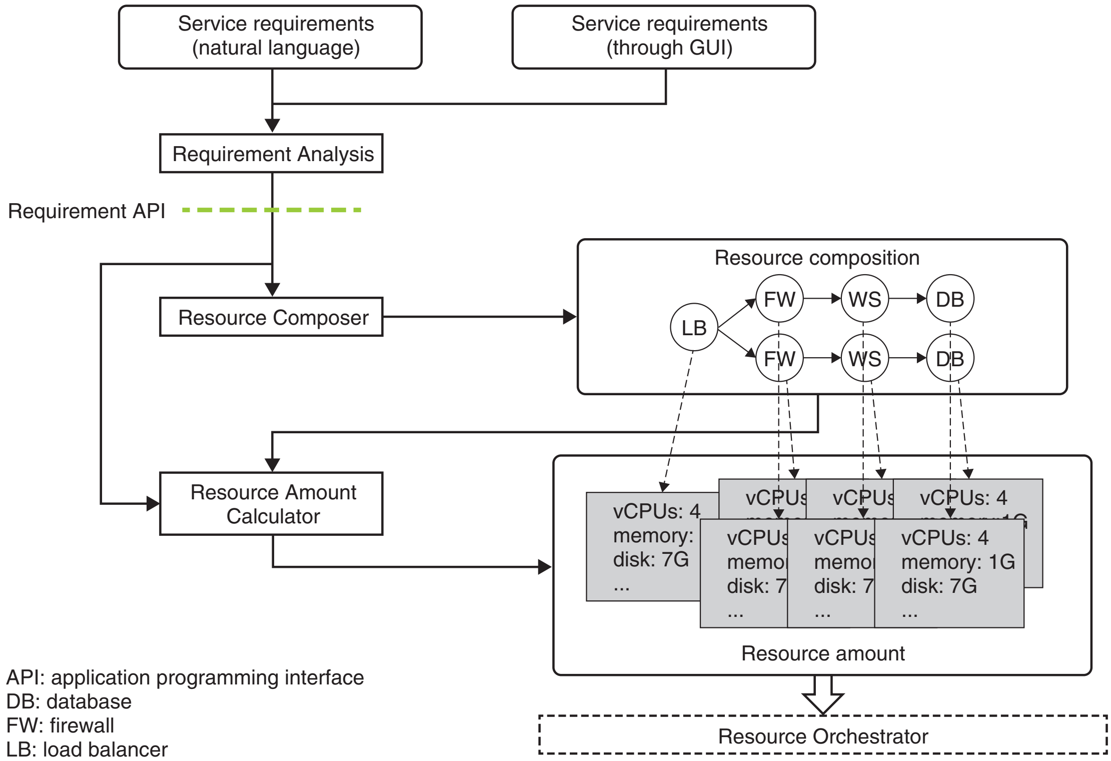
In both approaches, the transfer from service requirements to resource requirements relies heavily on an individual human's decision-making process.

In response to these issues, to more efficiently design and operate cloud resources, we have been researching an intent-based service management (IBSM) framework that analyzes the service requirements expressed through various channels (e.g., natural language (i.e., a *human* language such as Japanese or English, rather than a computer command language), graphical user interface (GUI), etc.) and determines the composition and amount of resources accordingly. Meanwhile, the output of IBSM can be used as the input of a cloud resources orchestrator, for example, OpenStack Heat, thus enabling the automation of the process from receiving a service request to service delivery and operation.


Service provider (SP)
Service requirements
Cloud service provider (CSP)
• Operation policies
• Environmental conditions
Resource requirements
Service requirements in terms of
✓ functionality, security, reliability
✓ workload, performance
Resource requirements in terms of
✓ composition (types, numbers, forwarding chains)
✓ amount (number of vCPUs, memory size, disk size)

vCPU: virtual central processing unit

Fig. 1. Cloud resources are designed in accordance with service requirements.



API: application programming interface
DB: database
FW: firewall
LB: load balancer
WS: web server

Fig. 2. IBSM framework.

2. IBSM framework

IBSM [1] consists of three main function blocks: Requirement Analysis, Resource Composer, and Resource Amount Calculator (**Fig. 2**). Below, we introduce each function and the approaches [2] to achieve them.

2.1 Requirement Analysis

SPs describe the service requirements through various channels such as natural language and GUIs. The Requirement Analysis block is responsible for

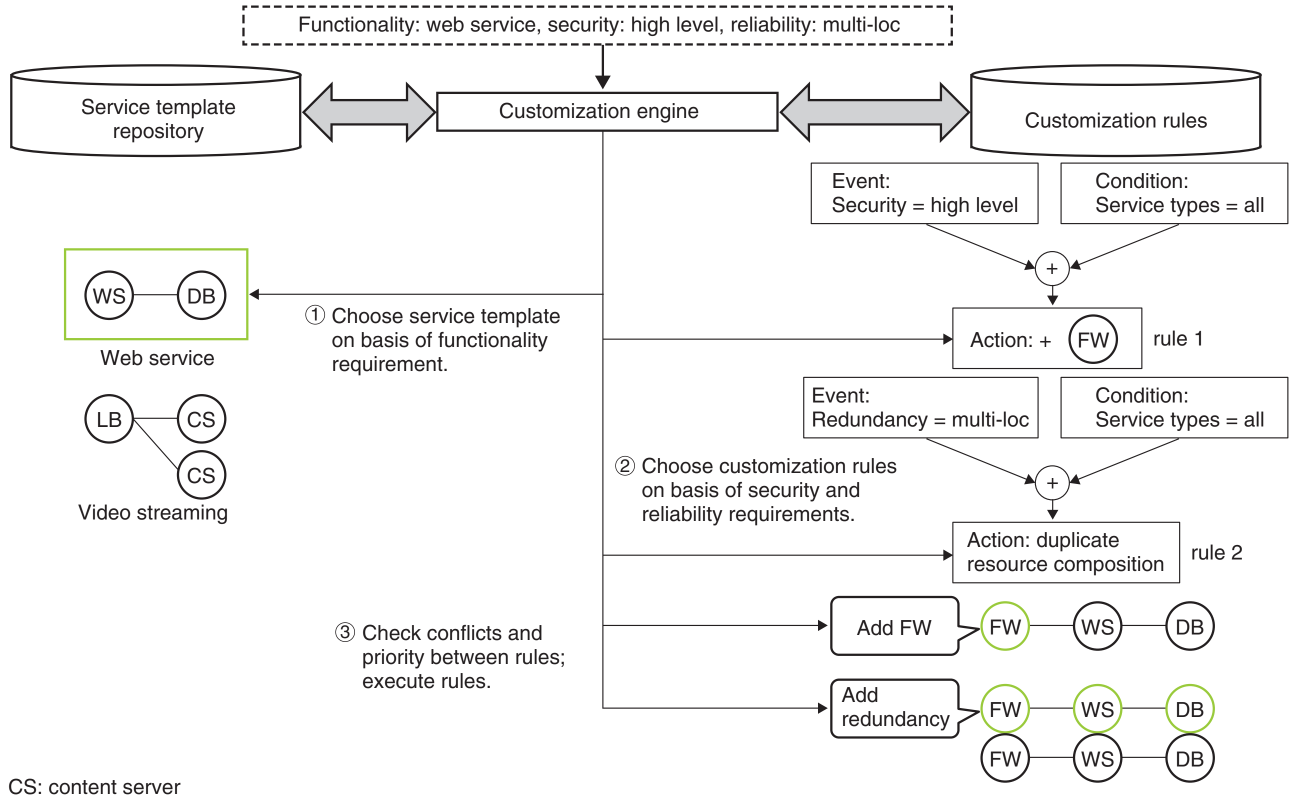

Functionality: web service, security: high level, reliability: multi-loc
Service template repository
Customization engine
Customization rules
Event: Security = high level
Condition: Service types = all
+
Action: + FW
rule 1
Event: Redundancy = multi-loc
Condition: Service types = all
+
Action: duplicate resource composition
rule 2
WS
DB
Web service
LB
CS
CS
Video streaming
① Choose service template on basis of functionality requirement.
② Choose customization rules on basis of security and reliability requirements.
③ Check conflicts and priority between rules; execute rules.
Add FW
FW
WS
DB
Add redundancy
FW
WS
DB
FW
WS
DB
CS: content server

Fig. 3. Resource Composer.

parsing these service requirements and categorizing the requirements into atom requirements including the requirements of functionality, security, reliability, workload, and performance.

2.2 Resource Composer

The Resource Composer block takes the output of the Requirement Analysis block and enables the resource composition to be automatically determined in accordance with the service requirements, especially the requirements of functionality, security, and reliability. There is an existing approach to determine the resource composition in accordance with predefined service templates, but this approach leads to the problem of a dramatic increase in the number of service templates as the service variations increase. To solve this problem, as shown in **Fig. 3**, a Resource Composer is based on a small number of basic service templates that can be customized on the basis of service requirements.

2.3 Resource Amount Calculator

The resource Amount Calculator's roles and functionalities include:

- Upon delivery of a cloud service, it determines the amount of resources needed to satisfy the performance requirements. Besides the workload and performance requirements, environmental conditions and operation policies need to be considered to determine the amount of computation resources allocated to virtual machines (VMs).
- After the delivery of the cloud service, if there are changes in workload, environmental conditions, and operation policies, it adjusts the amount of computation resources allocated to VMs to ensure continuous satisfaction of the performance requirements.

In the following, we explain why the workload, performance requirements, environmental conditions, and operation policies need to be taken into consideration to determine the amount of resources.

(1) Workload and performance requirements

The SP processes the service workload in the cloud environment, and in most cases, requires the performance requirements to be met. In this article, *workload*

Table 1. Examples of workload and performance requirements.

	Workload			Performance requirements	
	Type	Features	Amount	Processing time restriction	Processing percentage restriction
(a)	Web server requests (get)	Web page size: 30 KB, etc.	10,000 requests per second	Keep average process time of requests under 1 second	Successfully process over 95% of requests
(b)	Neural network (training)	Layers, nodes of each layer, activation function, etc.	Training set: 32 x 32 pixels 256 color x 10,000	Train 1 epoch in less than 10 min	...

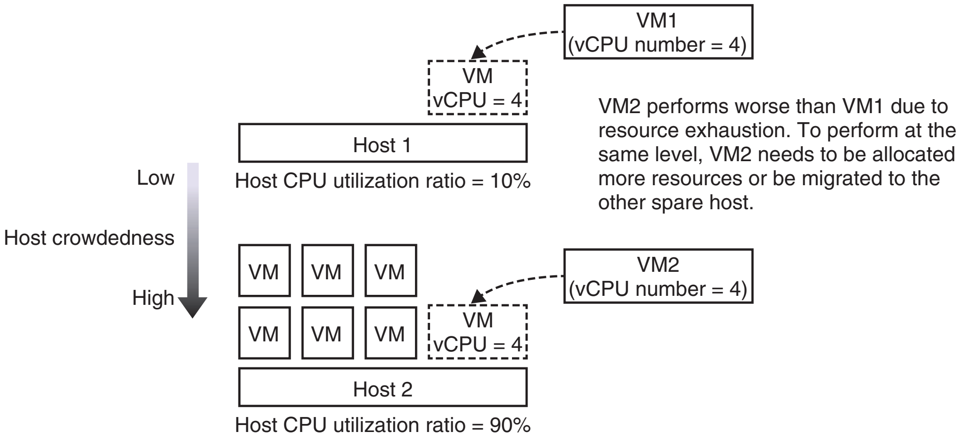

VM1
(vCPU number = 4)
VM
vCPU = 4
Host 1
Host CPU utilization ratio = 10%
VM2 performs worse than VM1 due to resource exhaustion. To perform at the same level, VM2 needs to be allocated more resources or be migrated to the other spare host.
Low
Host crowdedness
High
VM
VM
VM
VM
VM
VM
VM2
(vCPU number = 4)
VM
vCPU = 4
Host 2
Host CPU utilization ratio = 90%

Fig. 4. Example of how environmental conditions affect VM's performance.

refers to the type, features, and amount of processing. The performance requirements can be divided into two main categories: the processing time restriction and the processing percentage restriction. Two examples of workload and the corresponding performance requirements are given in **Table 1**. For a certain workload, the computation resources allocated to the VMs directly affect the processing time and percentage achieved. Thus, workload and performance requirements must be considered when deciding the amount of resources allocated to VMs.

(2) Environmental conditions

Environmental conditions in this work are the conditions of the physical host to which the VM is allocated. Static environmental conditions include the central processing unit (CPU) clocks and memory architecture of the host; dynamic conditions include the resource utilization ratio of the host, also referred to as host crowdedness in this work. Given the consideration that the static environmental conditions are of relatively low variation and are not subject to change for a relatively long time span for a given CSP, we focus on dynamic environmental conditions in this work. An example of changes in environmental conditions affecting the performance of VMs is shown in **Fig. 4**. To satisfy the performance requirements, environmental conditions clearly need to be considered when determining the resource amount.

(3) Operation policies

Operation policies that need to be followed while providing a cloud service can be decided by the SP or CSP. The policies restrict the resource usage within a desired range. For instance, putting restrictions on the resource utilization ratio inside the VM, for example, 50–80%, prevents resources from being overused or underused, thus improving the resource efficiency and enhancing the satisfaction of service requirements. Furthermore, for a service composed of multiple VMs, setting the utilization ratio restrictions in the same range prevents bottlenecks in the service chain from occurring. The amount of resources allocated to VMs is a crucial factor in meeting the

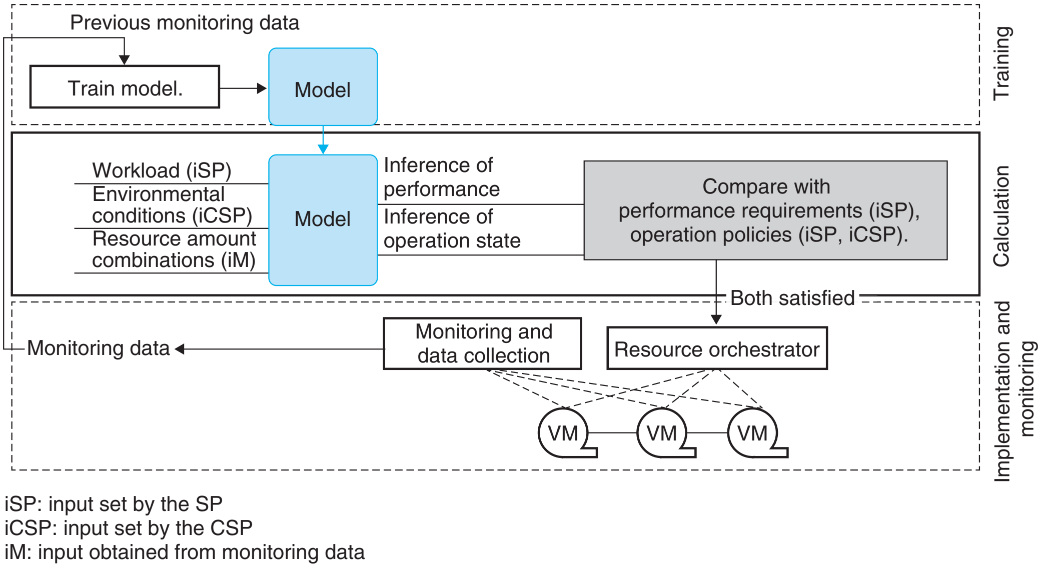

Previous monitoring data
Train model.
Model
Training
Workload (iSP)
Environmental conditions (iCSP)
Resource amount combinations (iM)
Model
Inference of performance
Inference of operation state
Compare with performance requirements (iSP), operation policies (iSP, iCSP).
Calculation
Both satisfied
Monitoring data
Monitoring and data collection
Resource orchestrator
VM
VM
VM
Implementation and monitoring
iSP: input set by the SP
iCSP: input set by the CSP
iM: input obtained from monitoring data

Fig. 5. Resource Amount Calculator.

restrictions of the utilization ratio inside the VM.

The structure of the Resource Amount Calculator is shown in **Fig. 5**. The Resource Amount Calculator uses a model between the workload, environmental conditions, and resource amount and the performance and resource utilization ratio inside the VM, as shown in the figure. The model is trained based on the log data collected during the previous service provision period. In the calculation phase, given the workload requirement, the current environment conditions, and the combinations of the number of vCPUs (virtual CPUs) and memory size, the performance and operation state are inferred by using the trained model. The input parameters can be set by the SP or the CSP or obtained from the monitoring data as shown in the figure. Next, if the inferred performance and operation state satisfy the performance requirements and the operation policies, the corresponding combination of resource amounts is output as the feasible solution for the Resource Amount Calculator.

3. Application scenarios of IBSM

IBSM can be used to assist in the consultation, design, and operation phases in cloud service delivery. For example, in the consultation phase for an SP that plans to migrate services implemented in an on-premises environment into a cloud environment, IBSM is used to show the performance that can be achieved after the migration and the needed cloud resources and cost. In the design phase, IBSM enables the automatic design of resources. Thus, service design time and human labor can be expected to be reduced. In the operation phase, IBSM is able to adjust the resource composition and amount in accordance with the changes, thus ensuring the continuous satisfaction of service requirements, which contributes to higher customer satisfaction.

4. Future plans

This article introduced an automatic service design technology for a cloud service under development at NTT Access Network Service Systems Laboratories. Our plans in the near future are to verify the effectiveness of the technology for representative workloads in the cloud service, identify the specific functions needed for different phases of cloud service delivery, and conduct trial experiments to enhance commercial use of the technology.

References

[1] C. Wu and S. Horiuchi, “Intent-Based Service Management -- To Decrease Complexity of Virtualized Network Management,” IEICE Tech. Rep., Vol. 117, No. 305, ICM2017-28, pp. 41–46, Nov. 2017.

[2] C. Wu and S. Horiuchi, “Intent-based Service Management,” Proc. of the 21st Conference on Innovation in Clouds, Internet and Networks (ICIN 2018), Paris, France, Feb. 2018.

Chao Wu

Research Engineer, Access Network Operation Project, NTT Access Network Service Systems Laboratories.

She received a B.E. in engineering from Zhejiang University, People's Republic of China, in 2009 and an M.E. in engineering from Waseda University, Tokyo, in 2013. In 2014, she joined NTT Access Network Service Systems Laboratories, where she has been researching and developing management mechanisms for telecommunications. She is also involved in standardization efforts of the next-generation operations support system in the European Telecommunications Standards Institute Experimental Networked Intelligence (ETSI ENI) and TM Forum.

Shingo Horiuchi

Senior Research Engineer, Access Network Operation Project, NTT Access Network Service Systems Laboratories.

He received a B.E. and M.E. in engineering from the University of Tokyo in 1999 and 2001. In 2001, he joined NTT Access Network Service Systems Laboratories, where he has been researching and developing access network operation systems. He has also been involved in standardization efforts for operations support systems in TM Forum as a member of the Open Digital Architecture (ODA) Project since 2014. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

Kenichi Tayama

Senior Research Engineer, Supervisor, Access Network Operation Project, NTT Access Network Service Systems Laboratories.

He received a B.E. and M.E. in electrical engineering from the University of Electro-Communications, Tokyo, in 1993 and 1995. He joined NTT Optical Network Systems Laboratories in 1995. He also worked at NTT EAST's IT Innovation Department and NTT-ME's Network Operation Center, where he researched and developed network operations support systems. He is a member of IEICE.

International Standards Adopted by ITU-T to Address Soft Errors Affecting Telecommunication Equipment

Hidenori Iwashita

Abstract

ITU-T (International Telecommunication Union - Telecommunication Standardization Sector), a specialized agency of the United Nations, approved standards relating to soft errors that affect telecommunication equipment on November 13, 2018. These standards stipulate design, testing, and quality estimation methods, as well as reliability requirements concerning measures designed to mitigate malfunctions (soft errors) in telecommunication equipment on the ground chiefly caused by cosmic rays. The adopted standards will help in establishing more reliable networks.

Keywords: soft error, irradiation test, neutron

1. Introduction

In recent years, the number of soft errors[*1] caused by cosmic radiation neutrons has been increasing gradually even in telecommunication equipment located on the ground (**Fig. 1**). The soft error disappears as soon as the semiconductor device concerned is restarted or the affected data are overwritten. A soft error in data can cause a malfunction or system outage, but it is difficult to reproduce such a transient error and identify its cause. Soft errors can have a serious impact on users, so such errors are a major problem for system operators. Telecommunication equipment is designed so that such malfunctions do not affect network services. However, because soft errors are difficult to reproduce, they have not been sufficiently verified at the development stage.

Recently, however, it has become possible to measure the effects of soft errors on telecommunication equipment by using a compact accelerator-driven neutron source[*2]. This makes it possible to determine the effects of soft errors and take preventive measures in advance before vendors sell products and telecommunication carriers introduce telecommunication equipment into operating networks [1]. Nevertheless, while it has become possible for carriers to improve network quality dramatically by mitigating soft errors at the stages of equipment development and introduction, there is a need for requirements that serve as the benchmark for countermeasure methods and evaluation.

2. ITU-T Recommendations concerning soft errors

Against this background, at the October 2015 meeting of the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T)

[*1] Soft error: Unlike a hard error, which is a fault that causes permanent malfunctioning of a semiconductor device, a soft error is a temporary error that disappears as soon as the semiconductor device concerned is restarted or the data concerned are overwritten.

[*2] Accelerator-driven neutron source: A facility for producing neutrons through a nuclear reaction caused by irradiating the target with protons or electrons that are sped up by an accelerator.

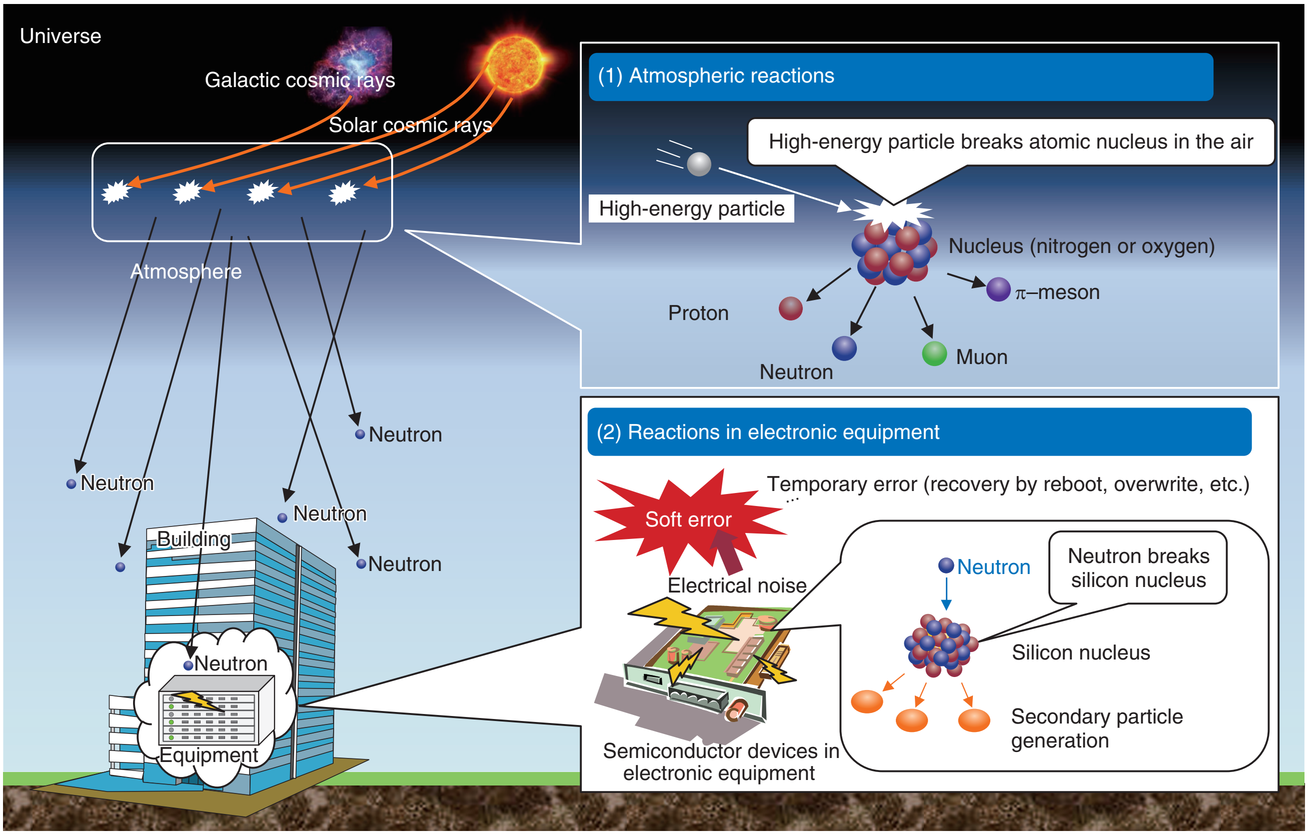

Universe
Galactic cosmic rays
Solar cosmic rays
Atmosphere
Neutron
Neutron
Neutron
Neutron
Building
Neutron
Equipment
(1) Atmospheric reactions
High-energy particle breaks atomic nucleus in the air
High-energy particle
Nucleus (nitrogen or oxygen)
π–meson
Proton
Neutron
Muon
(2) Reactions in electronic equipment
Temporary error (recovery by reboot, overwrite, etc.)
Soft error
Electrical noise
Neutron
Neutron breaks silicon nucleus
Silicon nucleus
Secondary particle generation
Semiconductor devices in electronic equipment

Fig. 1. Mechanism of soft error occurrence.

Study Group 5 (SG5)*3, commencement of a study on soft errors in telecommunication equipment was approved with the intention of defining requirements on measures to mitigate soft errors, ranging from design techniques to evaluation methods. The Ad Hoc Committee on Soft Error Testing (SOET Adhoc) member companies worked together and developed draft Recommendations [2]. The ITU-T has now approved these Recommendations.

The Recommendations stipulate the design, testing, and quality estimation methods and reliability requirements concerning soft errors. They include benchmarks that vendors and carriers can use to select measures against soft errors that are appropriate for the required reliability level.

The soft-error-related standards approved by ITU-T consist of five Recommendations and a supplement. An overview of the Recommendations is shown in **Fig. 2**, and the list of Recommendations is given in **Table 1**. A timeline of the standardization of Recommendations and measures to mitigate soft errors is given in **Table 2**.

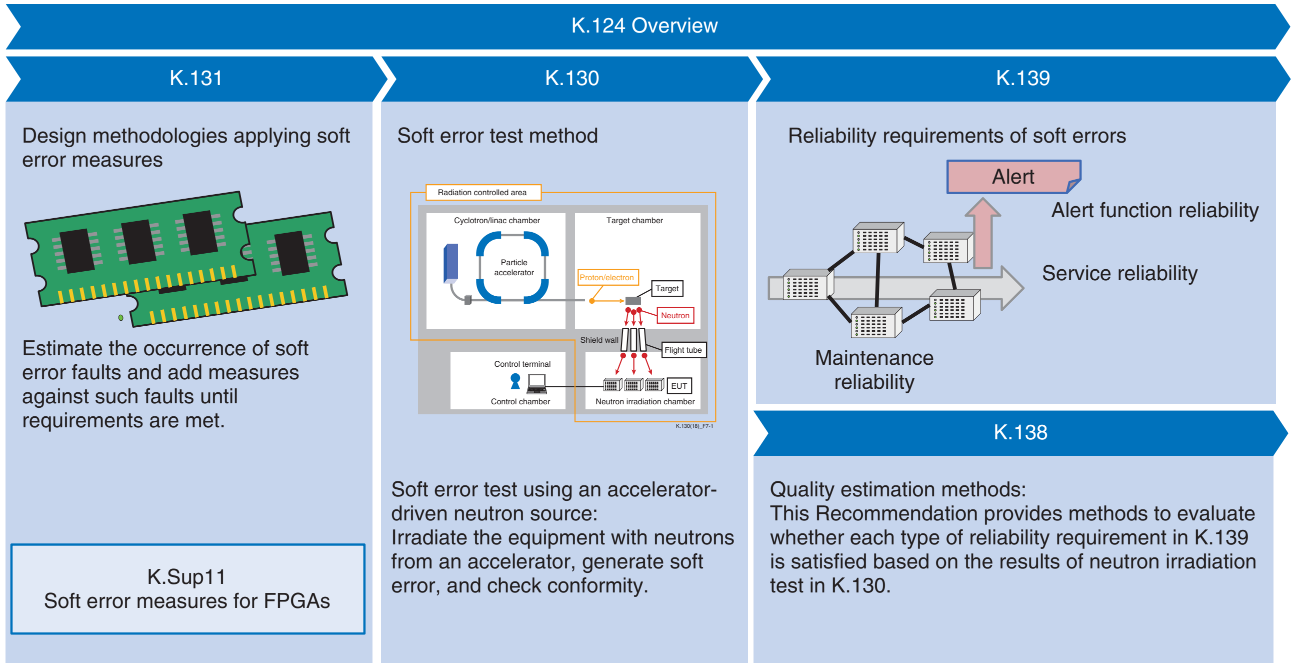
The Recommendations and supplement define the following items.

2.1 K.124 (Overview): Overview of particle radiation effects*4 on telecommunication systems [3]

This Recommendation describes the mechanism by which particle radiation causes soft errors, the impact of soft errors generated in telecommunication equipment, mitigation methods, and the need for further Recommendations to address soft errors. Soft errors are mainly caused by particle radiation of neutrons and alpha particles. Neutrons are generated by cosmic rays, and alpha particles are generated by minute

*3 ITU-T SG5: ITU-T is an ITU organization that issues Recommendations with a view to standardizing telecommunications. SG5 investigates issues related to the environment and climate change.

*4 Particle radiation effects: The impact of particle radiation (emitted energy in the form of neutrons, alpha particles, etc.) on semiconductors. In recent years, the number of soft errors caused by neutrons generated in the atmosphere by cosmic rays has been increasing in semiconductors used in ground-level equipment.



Design methodologies applying soft error measures

Estimate the occurrence of soft error faults and add measures against such faults until requirements are met.

K.Sup11
Soft error measures for FPGAs

Soft error test method

Soft error test using an accelerator-driven neutron source:
Irradiate the equipment with neutrons from an accelerator, generate soft error, and check conformity.

Reliability requirements of soft errors

Quality estimation methods:
This Recommendation provides methods to evaluate whether each type of reliability requirement in K.139 is satisfied based on the results of neutron irradiation test in K.130.

EUT: equipment under test
FPGA: field-programmable gate array

Fig. 2. Overview of soft error Recommendations.

Table 1. List of soft error Recommendations.

Recommendation	Subject	Title
K.124	Overview	Overview of particle radiation effects on telecommunication systems [3]
K.130	Test	Neutron irradiation test methods for telecommunication equipment [4]
K.131	Design	Design methodologies for telecommunication systems applying soft error measures [5]
K.Sup11	Supplement	Supplement to K.131 - Soft error measures for FPGAs [6]
K.139	Requirements	Reliability requirements for telecommunication systems affected by particle radiation [7]
K.138	Quality estimation	Quality estimation methods and application guidelines for mitigation measures based on particle radiation tests [8]

Table 2. Timeline of standardization of measures against soft errors.

2015	2016	2017	2018
▲August TTC SOET Adhoc was opened.	▲December K.124 (Approval)		▲January K.130, K.131 (Approval)
▲October New work item proposal was approved in ITU-T SG5 meeting.			▲November K.138, K.139 (Approval)

TTC: The Telecommunication Technology Committee quantities of radioisotopes contained in materials used in semiconductor devices.

The occurrence of soft errors caused by alpha particles can be reduced by using high purity materials such as low-alpha-particle plastics.

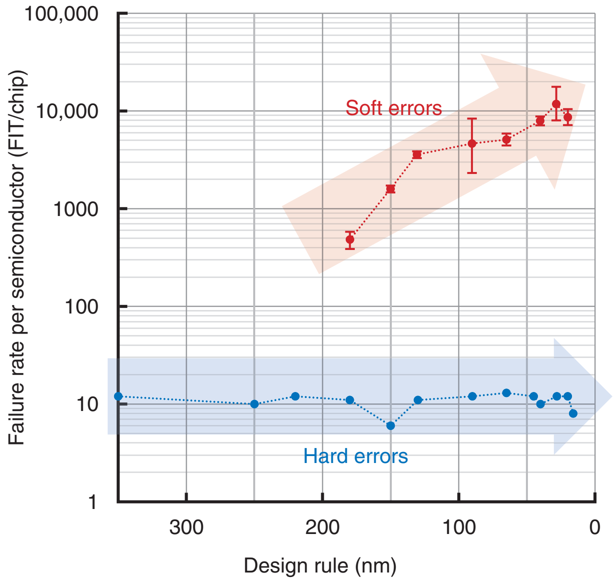
Soft errors caused by cosmic rays are caused by the following factors. In space, high-energy particles, mainly protons, are dispersed as a result of sun and supernova explosions. When these high-energy particles enter the Earth's atmosphere, they collide with nitrogen and oxygen nuclei in the atmosphere, causing a nuclear reaction. At this time, neutrons inside the nucleus are scattered. Although most of the neutrons generated in the atmosphere normally penetrate semiconductor devices and have no effect, on rare occasions they undergo nuclear reactions with the silicon nuclei that make up semiconductor devices, and these reactions generate various charged particles. This creates electrical noise and causes a temporary soft error.

2.2 K.130 (Test): Neutron irradiation test methods for telecommunication equipment [4]

This Recommendation describes methods and test procedures for generating soft errors in telecommunication equipment using accelerator neutron sources. When proton/electron particles accelerated by an accelerator are irradiated to a target (lead, tungsten, beryllium, lithium, etc.), a nuclear reaction occurs, and neutrons are generated. When telecommunication equipment is irradiated with these neutrons, it is possible to irradiate 1 million to several hundred million times more neutrons than in the natural world and to reproduce soft errors in a short time.

2.3 K.131 (Design): Design methodologies for telecommunication systems applying soft error measures [5]

This Recommendation describes a method of designing telecommunication devices constituting a carrier communication network to prevent or reduce soft errors. First, the basic configuration of the telecommunication devices to be covered is described as it relates to mitigating soft errors. A definition and method of regulating reliability of equipment in the event of soft errors are explained, and a procedure for developing equipment to prevent soft errors in order to comply with the reliability regulation is described. Countermeasures to soft errors are particularly important with field-programmable gate arrays (FPGAs), so details on the soft error occurrence rate in FPGAs are also described in this article, and K. Sup11, supplementary material to K.131, is introduced as a measure to alleviate the effects of soft errors in FPGAs [6].



FIT: failure in time

Fig. 3. Failure rates of hard errors and soft errors of LSIs (large-scale integrated circuits).

2.4 K.139 (Requirements): Reliability requirements for telecommunication systems affected by particle radiation [7]

This Recommendation describes the reliability requirements for equipment needed to ensure reliable networks in the event of soft errors.

As semiconductor devices become highly integrated, the number of soft errors compared to hard errors is increasing rapidly (**Fig. 3**). However, unlike hard errors, soft errors can be greatly reduced by introducing appropriate countermeasures. Therefore, using the rate of conventional hard errors as a guide, we set a range within which the number of failures caused by soft errors and the occurrence rate of the main signal interruption fell within a statistical error range (**Fig. 4**). However, in rare cases, a silent failure may occur due to a soft error. All silent faults must be prevented in the operation of network services. Therefore, we established a reliability standard such that no silent faults would occur even after approximately 10,000 years of neutron irradiation.

As a result, we defined three reliability standards designed to reduce the failure exchange rate, reduce the main signal interruption rate, and prevent silent

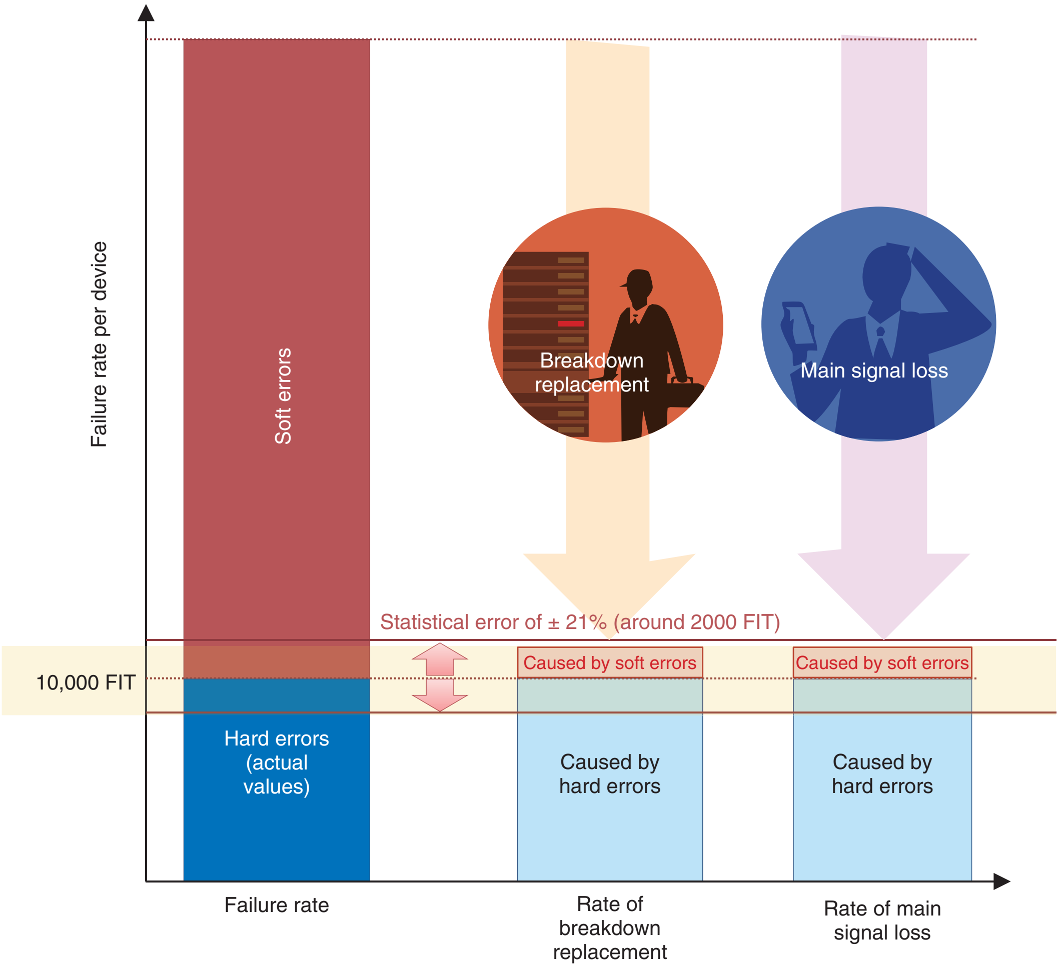


Fig. 4. Approach to setting reliability requirements.

failures. The reliability of large networks can be ensured by meeting these criteria.

2.5 K.138 (Quality estimation): Quality estimation methods and application guidelines for mitigation measures based on particle radiation tests [8]

This Recommendation describes how to evaluate whether the reliability requirements for soft errors of telecommunication devices defined in K.138 (quality estimation) are satisfied based on the results of neutron irradiation tests described in K.130 (test). The test described in K.130 indicates that soft errors can be reproduced in a short time by irradiating neutrons with an intensity of 1 million to several hundred million times that of natural fields. An example of the evaluation is shown in **Fig. 5**. First, a neutron beam is irradiated to generate a soft error. The main signal condition is confirmed with the measuring instrument, and the alarm generation condition is confirmed by the alarm monitoring terminal.

The generated event is classified into three reliability criteria. For example, in the first soft error in the figure, a device alarm occurred, and the main signal was cut off. In this case, it is counted as an event corresponding to MR (maintenance reliability) because maintenance is assumed to be necessary. Also, the main signal has been cut off, so it is counted as an event corresponding to SR (service reliability). The second soft error was automatically corrected; thus, there was no device alarm and no effect on the main signal. In this case, it is not counted in any confidence level.

The effect of the main signal and the equipment alarm condition are continuously checked during the test. For example, with the eighth soft error, the main

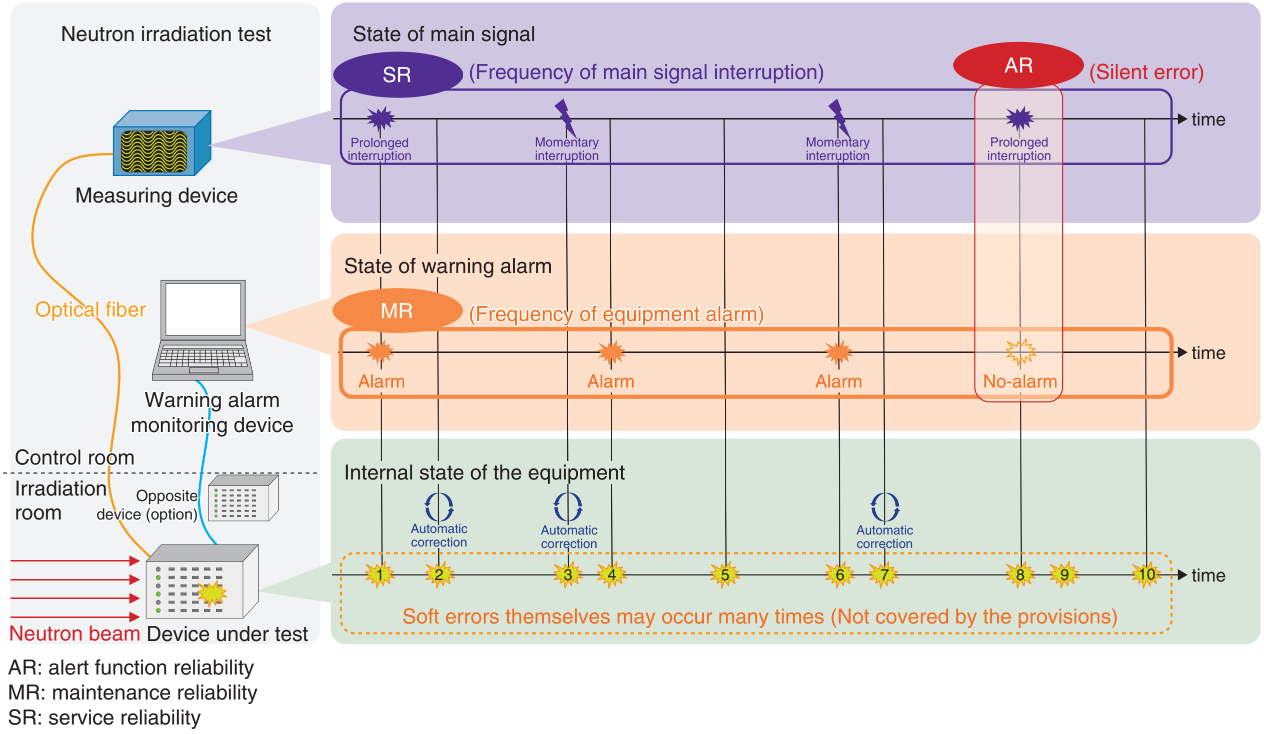


Fig. 5. Example of quality estimation methods.

signal is disconnected, but there is no device alarm. This corresponds to a silent failure and can be counted as one AR (alert function reliability). In this way, events corresponding to each reliability criterion are counted. In addition, the natural operating time and frequency converted from the irradiation time can be used to determine whether the standard value is satisfied.

3. Future outlook

It is expected that widespread deployment of telecommunication equipment that satisfies the requirements defined in these Recommendations will improve the reliability of telecommunication services.

References

[1] Xilinx, “Device Reliability Report,” UG116 (v10.9), Sept. 2018. https://www.xilinx.com/support/documentation/user_guides/ug116.pdf

[2] Website of The Telecommunication Technology Committee, SOET Adhoc (in Japanese), http://www.ttc.or.jp/j/info/bosyu/20150804/

[3] Recommendation ITU-T K.124, https://www.itu.int/rec/T-REC-K.124-201612-I

[4] Recommendation ITU-T K.130, https://www.itu.int/rec/T-REC-K.130-201801-I/en

[5] Recommendation ITU-T K.131, https://www.itu.int/rec/T-REC-K.131-201801-I/en

[6] Supplement 11 to ITU-T K-series Recommendations, https://www.itu.int/rec/T-REC-K.Sup11-201809-I/en

[7] Recommendation ITU-T K.139, https://www.itu.int/rec/T-REC-K.139-201811-I/en

[8] Recommendation ITU-T K.138, https://www.itu.int/rec/T-REC-K.138-201811-I/en

Hidenori Iwashita

Research Engineer, Transport Network Innovation Project, NTT Network Service Systems Laboratories.

He received a B.S. and M.S. in nuclear engineering from Hokkaido University in 2006 and 2008. He joined NTT Network Service Systems Laboratories as a researcher in 2008. He is involved in researching and developing a packet transport multiplexer (PTM), PTM cross-connect (PTM-XC), PTM adapter for dedicated services, and an Ethernet private line system. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

External Awards

FIT2018 Best Paper Award

Winner: Masamichi Hosoda, NTT Service Evolution Laboratories; Hiroshi Sakamoto, Tomoki Murakami, NTT Access Network Service Systems Laboratories; Yasushi Hanakago, NTT Service Evolution Laboratories; Makoto Umeuchi, NTT Access Network Service Systems Laboratories; Tadashi Mouri, NTT Service Evolution Laboratories; Tomoaki Ogawa, NTT Access Network Service Systems Laboratories; Masaru Miyamoto, NTT Service Evolution Laboratories
Date: December 5, 2018
Organization: The 17th Forum on Information Technology (FIT2018)

For "Wireless LAN Station Position Estimation Method by Access Point Using Distributed Antenna System."
Published as: M. Hosoda, H. Sakamoto, T. Murakami, Y. Hanakago, M. Umeuchi, T. Mouri, T. Ogawa, and M. Miyamoto, "Wireless LAN Station Position Estimation Method by Access Point Using Distributed Antenna System," Proc. of FIT2018, CA-007, pp. 59–64, Fukuoka, Japan, Sept. 2018 (in Japanese).

Papers Published in Technical Journals and Conference Proceedings

Self-foldable Graphene Polymer Bilayer Films

T. F. Teshima, C. S. Henderson, M. Takamura, Y. Ogawa, S. Wang, S. Sasaki, Y. Kashimura, H. Nakashima, and Y. Ueno

Biointerfaces International 2018, p. 93, Zurich, Switzerland, August 2018.

Microscopic three-dimensional (3D) assembly of graphene is of interest in the development of nano-devices, flexible electronics, and biointerfaces with cells or tissues. Self-foldable or manually buckled flexible polymer films have been hitherto utilized to load graphene and induce wrinkling or folding. However, the external force applied from these templates causes mechanical fracture or electrical disconnection of graphene. Therefore, it is technically difficult to construct micro-scale 3D graphene without delamination or slipping of pristine graphene. In this study, we show that the graphene itself transforms into 3D shapes, by using π-π stacking interaction with parylene thin film.

Electrical Spectrum Synthesis Technique Using Digital Pre-processing and Ultra-broadband Electrical Bandwidth Doubler for High-speed Optical Transmitter

F. Hamaoka, M. Nakamura, M. Nagatani, H. Wakita, H. Yamazaki, T. Kobayashi, H. Nosaka, and Y. Miyamoto

Electronics Letters, Vol. 54, No. 24, pp. 1390–1391, November 2018.

Proposed is an electrical spectrum synthesis technique that converts low-speed signals to a high-speed signal using transmitter-side digital signal processing (DSP) and an ultra-broadband electrical bandwidth doubler. The transmitter-side DSP converts a high-speed signal to low-speed upper and lower sideband signals, down- and up-converts the low-speed signals into baseband signals, and adds and subtracts the in-phase and the quadrature components of the baseband signals. The digital pre-processed low-speed signals output from digital-to-analogue converters are multiplexed to the high-speed signal by the bandwidth doubler, which consists of analogue multiplexers designed and fabricated using in-house indium phosphide heterojunction bipolar transistor technologies. A 120 GBaud quadrature phase shift keying signal has been successfully generated by using the proposed technique as a demonstration of a high-speed optical transmitter.

Self-folded Three-dimensional Graphene with Tunable Shape and Conductivity

T. Teshima, C. S. Henderson, M. Takamura, Y. Ogawa, S. Wang, Y. Kashimura, S. Sasaki, T. Goto, H. Nakashima, and Y. Ueno

Nano Letters, Vol. 19, No. 1, pp. 461–470, January 2019.

In this study, we demonstrate the facile formation of predetermined 3D polymeric microstructures simply by transferring monolayer graphene. The graphene adheres to the surface of polymeric films via noncovalent π-π stacking bonding and induces a sloped internal strain, leading to the self-rolling of 3D microscale architectures. Micropatterns and varied thicknesses of the 2D films prior to the self-rolling allows for control over the resulting 3D geometries. The strain then present on the hexagonal unit cell of the graphene produces a nonlinear electrical conductivity across the device. The driving force behind the self-folding process arises from the reconfiguration of the molecules within the crystalline materials. We believe that this effective and versatile way of realizing a 3D graphene structure is potentially applicable to alternative 2D layered materials as well as other flexible polymeric templates.

Power of Uninitialized Qubits in Shallow Quantum Circuits

Y. Takahashi and S. Tani

The 22nd Annual Conference on Quantum Information Processing (QIP 2019), Boulder, CO, USA, January 2019.

We study the computational power of shallow quantum circuits with $O(\log n)$ initialized and $n^{O(1)}$ uninitialized ancillary qubits, where n is the input length, and the initial state of the uninitialized ancillary qubits is arbitrary. First, we show that such a circuit can compute any symmetric function on n bits that is computable by a uniform family of polynomial-size classical circuits. Then, we regard such a circuit as an oracle and show that a polynomial-time classical algorithm with the oracle can estimate the elements of any unitary matrix corresponding to a constant-depth quantum circuit on n qubits. Since it seems unlikely that these tasks can be done with only $O(\log n)$ initialized ancillary qubits, our results give evidence that adding uninitialized ancillary qubits increases the computational power of shallow quantum circuits with only $O(\log n)$ initialized ancillary qubits. Lastly, to understand the limitations of uninitialized ancillary qubits, we focus on sub-logarithmic-depth quantum circuits with them and show the impossibility of computing the parity function on n bits.

120-GBaud 32QAM Signal Generation Using Ultra-broadband Electrical Bandwidth Doubler

F. Hamaoka, M. Nakamura, M. Nagatani, T. Kobayashi, A. Matsushita, H. Wakita, H. Yamazaki, H. Nosaka, and Y. Miyamoto

The Optical Networking and Communication Conference & Exhibition, San Diego, CA, USA, March 2019.

We propose an electrical spectrum synthesis technique using digital pre-processing with an interband crosstalk compensation and newly developed ultra-broadband electrical bandwidth doublers. A 120-GBaud PDM-32QAM (polarization-division-multiplexed 32-level quadrature amplitude modulation) signal (net rate: 954.2 Gb/s) has been successfully generated.