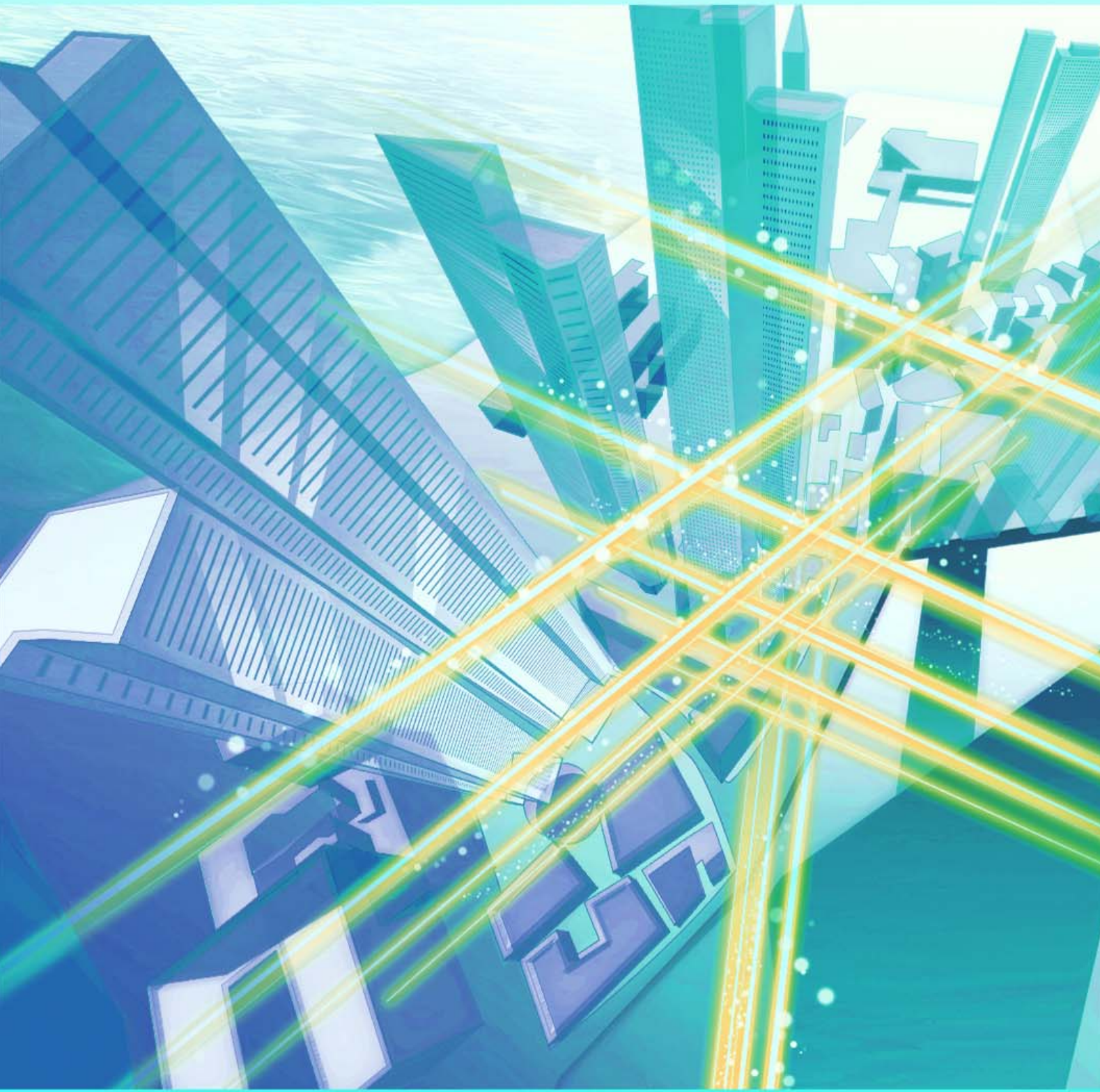
NTT Technical Review

5
2017



May 2017 Vol. 15 No. 5

NTT Technical Review

May 2017 Vol. 15 No. 5

Electronic Equipment Caused by Cosmic Rays

External Awards/Papers Published in Technical Journals and Conference Proceedings

- External Awards/Papers Published in Technical Journals and Conference Proceedings

Being Conscious of Contact Points between Accumulated Experience and External Stimuli

Kazuhide Nakajima
Senior Distinguished Researcher,
NTT Access Network Service Systems Laboratories

Overview

Data communications in Japan currently exceeds 2.5 Tbit/s, but it is predicted that demand will rise to 10 Pbit/s by the late 2020s. This forecast is creating concern that the transmission capacity of the existing optical fiber infrastructure could reach its limit. Kazuhide Nakajima is a Senior Distinguished Researcher at NTT Access Network Service Systems Laboratories, where researchers are working to solve this fast-approaching problem. We asked him about the latest research achievements in this field and his mindset as a researcher.

Keywords: optical fiber, multi-core fiber, space division multiplexing

Achieving the world's highest density optical fiber with deployable reliability

—Dr. Nakajima, please tell us about your current research activities.

I am researching the fabrication of multiple cores, that is, optical paths, within optical fiber with the aim of transmitting more information using just a single strand of optical fiber. In an optical fiber, light is confined within a core through the reflection of light generated by a difference in the refractive indices between the core and its outer periphery (cladding). This enables light to propagate within the core with an extremely small amount of attenuation in optical intensity. Here, light travels at an angle with respect to the interface between the core and cladding (including straight-line propagation with an angle of zero degrees). In this regard, there is single-mode fiber that allows the transmission of only one optical signal, and there is multi-mode fiber that allows the transmission of multiple optical signals. In addition, bending an optical fiber will cause a relative change in the angle of optical propagation, which in turn can prevent reflection, which causes light to leak from the core and reduces optical intensity (optical loss). Moreover, the simple fact that silica glass is used in most optical fiber can also give rise to breakage.

Recent years have seen an expansion of FTTH (fiber-to-the-home) services, and we can envision customers, who are not specialized technicians, being able to wire optical fibers themselves inside their homes in the future. In this case, however, the limits of optical fiber "bending" would become particularly

Free-bending optical cord achieves optical communications in a bent, bundled, folded, or knotted state.
Enables do-it-yourself optical wiring in a similar way to electrical wiring

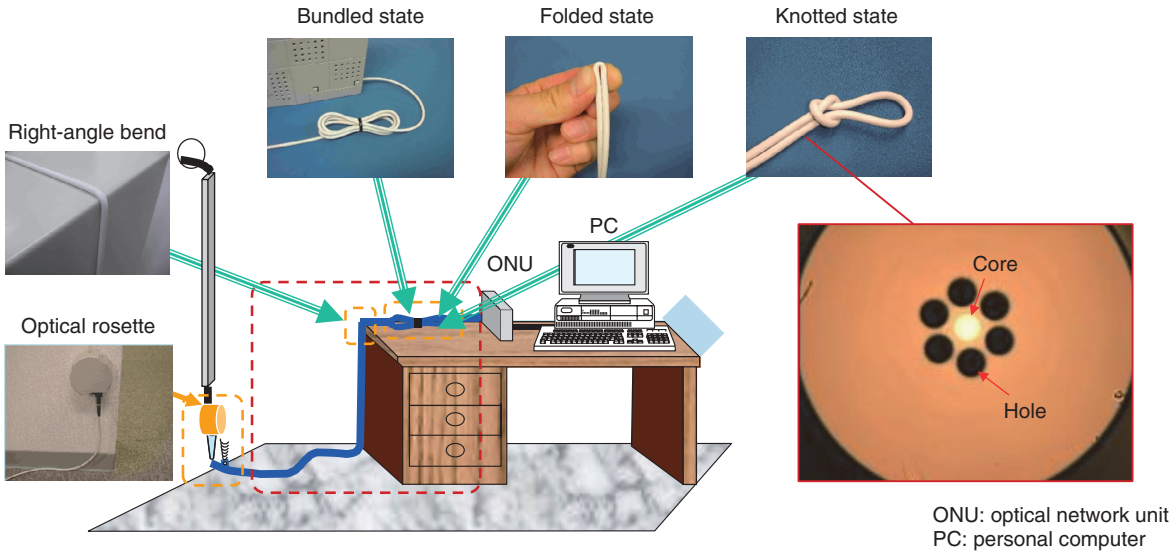


Fig. 1. Free-bending optical cord.

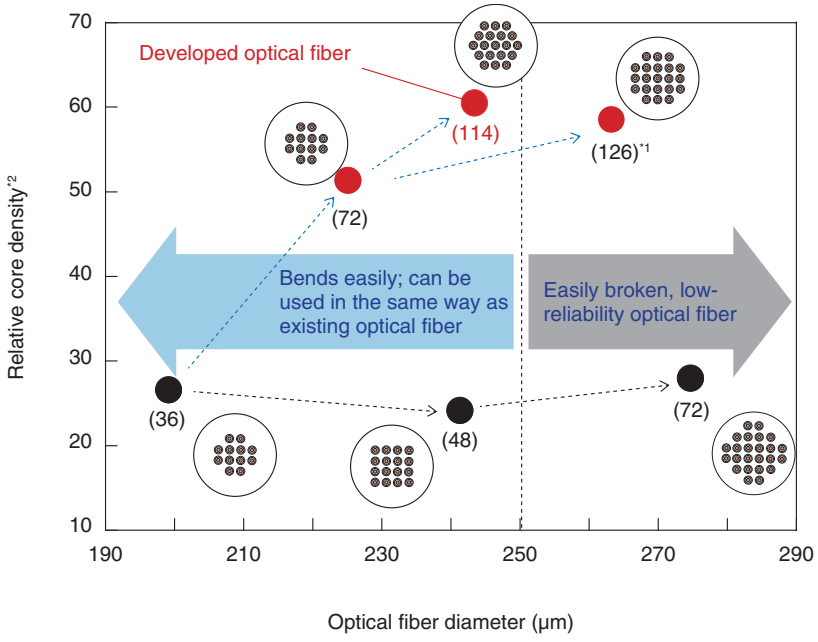
evident. At the same time, it is predicted that the demand for data communications will rise above 10 Pbit/s by the late 2020s, so we can also expect the existing optical fiber infrastructure to eventually reach its limit in transmission capacity.

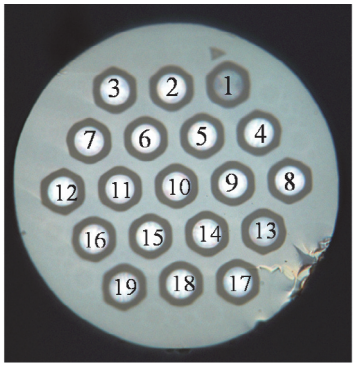
Against this background, my team has been working on (1) the development and deployment of bendable optical fiber that anyone can use (free-bending optical cord) and (2) the development of optical fiber that can increase transmission capacity without affecting existing facilities such as civil engineering works (optical fiber for space division multiplexing transmission).

We have found that light can be confined within the core even when bending the fiber by placing multiple holes in the cladding of the optical fiber (hole structure) and using the magnitude of the difference between the refractive indices of air and silica glass. Our free-bending optical cord has a structure that enables it to be bent, folded, and knotted (**Fig. 1**). This cord contains both a sheath section surrounding and protecting the optical fiber and a dust-proof connector. This technology has become an international standard in the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T).

One way of increasing transmission capacity in communications is to increase the number of optical fibers, but there is a limit as to how many optical fibers can be accommodated in an optical cable. Additionally, in the event that no space exists for accommodating more optical cables, it would be necessary to reconstruct underground and indoor optical wiring facilities. However, increasing the transmission capacity of optical fiber itself would not have any impact on existing facilities. This can be accomplished, for example, by using multi-mode fiber, which has a larger core than that of single-mode fiber and allows for multiple modes to propagate within a core, or by using multi-core fiber, which arranges multiple single-mode cores within a single optical fiber (space division multiplexing). With either of these configurations, however, it is difficult to achieve more than 50 channels (optical paths). This level of performance is not sufficient to meet the anticipated demand in transmission capacity.

For this reason, research and development (R&D) efforts on arranging multiple multi-mode cores in a single optical fiber (multi-mode multi-core fiber) to overcome existing transmission capacity limitations are progressing around the world. However, if the distance between cores becomes too short when increasing the number of cores, optical interference can arise between cores, and if the cladding surrounding





Cross section of fabricated optical fiber
6 modes × 19 cores = 114 channels

*1 Figures in parentheses indicate number of optical paths (no. of modes × no. of cores).
*2 Ratio of optical-signal propagation area to optical-fiber cross section (relative to existing optical fiber set to 1)

Fig. 2. World's highest density multi-core fiber.

a core is too thin, optical loss can be significant. In addition, optical fiber with a large diameter can easily break, making it unsuitable for deployment. To address these conditions, we teamed up with Fujikura Ltd. and Hokkaido University (Laboratory of Information Communication Photonics) to pursue R&D in this area and succeeded in achieving the world's highest density optical fiber.

We have known that an optical fiber with a diameter less than 250 μm could be used for more than 20 years in the field, so taking future transmission capacity levels into account, we set our objective to develop optical fiber with a transmission capacity of more than 100 channels while having a diameter of less than 250 μm. In the case of multi-mode fiber, the propagation distance differs depending on the optical reflection angle within the core, and as a result, the arrival time of light on the receiving side will likewise differ between modes. This difference makes signal processing on the receiving side complicated, a problem that has to be addressed. We minimized this time difference by adjusting and optimizing the core's refractive index profile. We also succeeded in suppressing optical interference and loss in optical fiber having a diameter of less than 250 μm by adjusting the core arrangement including the inter-core interval. The result was an optical fiber with 19 cores in a honeycomb-shaped arrangement, with each core supporting 6 modes for a multiplexing level of 114 transmission channels (= 6 modes × 19 cores) (**Fig. 2**). This is the world's highest density and is equivalent to more than 60 times that of existing single-mode and single-core optical fiber.

Taking back your remarks is OK—continue to ask yourself what you really want to do

—What kind of research activities were you involved in before obtaining world-leading research results?

I have been involved in the research of optical fiber itself since joining NTT in 1994. To give some background, I had done calculations on the characteristics of dual-core fiber during my university days, and thanks in part to that experience, I developed a desire to spread the use of optical communications throughout the world. With that in mind, I became engaged in this research. At that time, much attention was focused on wavelength division multiplexing (WDM) technology as a means of increasing transmission capacity by multiplexing optical signals of multiple wavelengths. The development of optical fiber applicable to WDM became my exclusive research theme.

Then, from 2000 on, I took up the research of optical

fiber having a hole structure. For some time, optical fiber was vulnerable to bending, and it was a request from another department to obtain optical fiber that could overcome this weakness and be used by anyone that got me started in this research. In 2005, we succeeded in developing and deploying for the first time in the world optical fiber with the new structure, which applies the effect of confining light by opening up holes in the cladding. These efforts led to the development of a strong optical fiber with no reduction in transmission performance, even it was accidently crushed by a chair. Since 2010, I have been researching the development of multi-core fiber as my main theme with the aim of increasing the transmission capacity of existing optical fiber.

—What difficulties did you face on your way to achieving such world-first technology?

Optical fiber confines optical signals by using materials with different refractive indices. Commonly used optical fiber creates a difference in the refractive index between the core and the cladding due to the addition of different types of dopants to silica glass. Naturally, the refractive indices of silica glass and air are different, and this property can be used to fabricate holes within the optical fiber and to fabricate a core without having to add any dopants to the silica glass. This is optical fiber with a hole structure. Such optical fiber requires that the holes be uniformly arranged, but doing so requires highly advanced technology. This technology had yet to be developed or reach the deployment stage.

Well, on receiving the request for bendable optical fiber, there were some discussions within my team as to whether to respond to this need as our next research theme or prioritize the development of fiber with a perfect hole structure. But during these discussions, it was discovered that light in optical fiber with a hole structure would not permeate the core boundary and would not leak even if the fiber was bent. We therefore wondered whether bendable optical fiber could be achieved by incorporating holes in fiber having ordinary cores, and we decided that this would be our research theme.

While proceeding with this research, information came to light that announcements on similar technology were being made by other institutions. Although our research had progressed to some extent, we had to bring it to a stage ready for presentation in only two weeks if we were not to be left behind. During this short period, our team made a unified effort not only to accelerate the research but also to prepare a presentation paper, complete procedures for acquiring patent rights, and other tasks. We had to battle time more than our competitors!

—What kind of researcher were you during this roll-out of world-leading technology?

A fascinating thing about research is that you can think freely about anything and about things that don't yet exist in the world and then go out and try to create them. It truly is a world of imagination and creation. That being said, I believe that I have been a very ordinary researcher up to this point. I have been immersed in my own world by probing deeply those things that interest me. For example, optical fiber must be uniform in composition, but when I deliberately tried to make it non-uniform, I was told by my superior to "research something useful," but I paid no attention. However, on hearing about the need for bendable optical fiber, I found that there is no value in just developing optical fiber itself. In other words, I realized that great research results are meaningless unless they can be put to practical use.

One more thing: my work in the standardization of optical fiber for use in telecommunications had a major influence on my research life. Since 2000, I have been participating in an ITU-T meeting that formulates international standards for optical fiber, and it was there that I learned that performance is not the top priority in creating a standard; a more essential requirement is that the standard be versatile and reasonable in use. This is certainly an opposing viewpoint or direction from research that places priority on cutting-edge technology and groundbreaking results (**Photo 1**).

These two experiences helped to make me conscious of the need for practical applications in the real world when researching advanced technology. That is, I came to realize the importance of finding contact points between the real world and the advanced technology of my research.

—Your viewpoint has drastically changed through your research activities. What do you take to heart in going forward?

I advance in a somewhat helter-skelter manner. Even in my present research on large-capacity transmission, I look back at my original objective at every opportunity. The research that we are now working on is of a long-term nature looking ahead 10 to 20

(From left) Kazuhide Nakajima (Question 5 Rapporteur, NTT),
Francesco Montalti (Study Group 15 Vice-Chairman, Tyco, Belgium),
Kazuyuki Shiraki (Question 8 Rapporteur, NTT),
Kunihiro Toge (Question 16 Rapporteur, NTT),
and Noriyuki Araki (Study Group 15 Vice-Chairman, NTT)

Photo 1. At ITU-T Study Group 15 meeting, September 2016.

years, so there will likely be few opportunities to receive concrete feedback. This is precisely why it is important that we closely analyze the results that we have so far obtained with the aim of creating something useful for society. This type of approach can lead to greater self-awareness of the value of our research. Stimuli from other people and from the outside are also important here. Let me give you two examples.

The first one relates to the time of our development of optical fiber that could actually be used inside the ordinary home. This turned out to be a major source of encouragement for me, but there was an incident that revealed that I had not been aware of the significance of that research. I was involved in the training of third-year employees as a lecturer, and one of the trainees asked a question, saying "Mr. Nakajima, why are you researching optical fiber?" I was actually lost for words. Looking back, I had been researching optical fiber since my university days, and although I had been interested in optical communications and optical fiber from the very start, it was not because I had a strong desire to enter this field. Rather, it was a result of chance events in which I seemed to encounter this field whenever I was at a crossroads on my career path. In addition, I considered that my interest in this thing called "optical fiber" and the dreams I had for it were what brought me to the present. After thinking about it for a while, I realized that the results of my ongoing research were now being used in the world and were of benefit to both NTT and society, and I noticed that that had boosted my confidence.

The other example concerns the ITU-T meeting that I have been participating in. This meeting is held every eight months in Geneva, Switzerland. At this meeting, participating countries and organizations make proposals while having heated discussions amid conflicting interests. These discussions are all conducted in English, which I am not totally comfortable with, and our task is to assemble these proposals into an international standard. Although this is a special overseas meeting for me, I would say that my evening meal was about the only thing I looked forward to. I would typically become so focused on the discussions that, without noticing it, I had turned my attention to the discussions themselves instead of searching for common ground to form a conclusion. So, during the weekend in the middle of the two-week session, I would refresh myself with some kind of activity such as mountain climbing. Such external stimuli would help me to clarify things in my head so that I could then bring all those discussions together

into an international standard.

Although it's important to set clear goals, no one knows what the future will bring. Research being what it is, you don't know what is right or wrong at first. Our group frequently discusses the direction we should be taking, while taking experimental data and real-world trends into account, and if necessary, we revise our research theme before moving forward. For this reason, I believe it's perfectly acceptable for a researcher to be anxious about his or her research and to retract an earlier statement. I understand there are times when a researcher may steadfastly refuse to back down after making a certain statement, but being bound by something you say may prevent you from advancing at all.

On top of this, I think it's important to listen carefully to what other people have to say. Flexibility is essential to get one's research out into society. Looking for contact points between a variety of matters and one's research results is an important factor in achieving deployable technologies. It's good to stick to one's work, but stubbornly refusing to change may prevent you from spotting those contact points.

Always give thought to what you want to accomplish

—What are your ambitions and outlook for the future?

I am not a theoretician. I have pursued research in a straightforward and persistent manner, continuing to reflect on the experimental data that I have collected until I'm satisfied. Going forward, I would like to improve my skills and abilities by continuing with this approach. My superior, who gave me much guidance from the time I entered the company, left me with these words when he left NTT: "It's too early to express thanks to me. Instead, work to create a path for those coming after you." I will always take these words to heart. Although I don't know when I, too, will leave NTT, at that time, I hope that I will have created such a path for future generations of researchers.

Of course, whether I stay at NTT or go elsewhere, optical fiber will always be part of my life. I want to continue thinking about new ways of using optical fiber. In addition, I want to be a researcher who talks about his dreams, and I want to move forward without abandoning thinking on my own.

A major objective of mine is to develop technology that can be used in future large-capacity transmission systems. The limit of optical fiber now in use is said to be 100 Tbit/s. Once implemented, optical fiber deployed in transmission paths will be used continuously for 20 to 30 years, and when that optical fiber is replaced, the aim is to achieve a transmission capacity about 100 times greater. We think there is the potential to achieve this because we have already achieved a density 60 times the existing level. However, there are still many issues that have to be addressed before actual deployment, so we continue our R&D efforts to achieve better results. Manufacturing technology is the key to deployment, so we plan to hold discussions with manufacturers and make best use of our mutual strengths. It is also important that we get multi-core fiber technology out into the world as soon as possible to plant the seeds of future large-capacity transmission systems.

—As an active researcher, what would you say to young researchers as to what is important to produce results?

Today's young researchers are highly motivated and highly skilled. However, at the risk of being misunderstood, they tend to be quiet and well behaved compared with my generation. In my time, there were even people who did not follow their superiors' directives, but today, such an attitude is not common. Perhaps the low number of entry-level employees has an effect here. It's not that I want to promote a rebellious attitude, but in order to find out why someone is not expressing an opinion, I will often ask: "What do you really want to do? What are you thinking about in your work?" If I ask this question enough times, I may get a brilliant, off-the-cuff reply. If you can form some kind of relationship, that person is apt to tell you exactly what is on his or her mind.

Nowadays, it feels that time is passing by faster than before. For this reason, I think we have less free time. To keep yourself from losing your way under such conditions, please have a dream. At the same time, dig deeply into your research but change your viewpoint if necessary. Please approach your work with this frame of mind.

In addition, don't hesitate to try something even if you feel it's not directly related to your own research. Doing so can broaden your horizons and reveal more of yourself in many ways. It can also help you uncover contact points for making your research results a reality. Last year, I assumed the position of a director in a small academic society. The objective of this society is to act as an intermediary between network

operators and vendors. Although my role is as an advisor, I thought when taking this role that it would be an experience that would be hard to come by otherwise, and I felt that it could help me form contact points that could make my research useful to society.

In this way, knowing that young researchers who may be worried or confused are traveling along the same path that I have traveled, I would like to make them reflect on their original objectives, help them set their sights firmly on their final goal, and support them to see other viewpoints. To repeat, I like the work of research and I enjoy thinking about and creating things that do not presently exist in the world. By all means, please come to like and even enjoy the fascinating work of research.

■ **Interviewee profile**
Kazuhide Nakajima

Senior Research Engineer, Supervisor (Senior Distinguished Researcher) and Group Leader of NTT Access Network Service Systems Laboratories.

He received an M.S. and Ph.D. in electrical engineering from Nihon University, Chiba, in 1994 and 2005. In 1994, he joined NTT Access Network Service Systems Laboratories, where he engaged in research on optical fiber design and related measurement techniques. He is also acting as the rapporteur of Question 5 in ITU-T Study Group 15. Dr. Nakajima is a member of the Institute of Electronics, Information and Communication Engineers, the Institute of Electrical and Electronics Engineers, and the Optical Society of America.

Research and Development of Security Concerns Relating to Growing Threats and Business Opportunities

Kazuhiko Okubo

Abstract

The Internet of Things era has resulted in many devices with security vulnerabilities being connected to networks, and this is resulting in a rapid increase in the number of security threats in new areas such as infrastructure facilities that have up to this point been regarded as safe. On the other hand, it is also creating new business opportunities with the utilization of diverse information. This article introduces the security research and development strategy of NTT laboratories from two perspectives: defeating new threats based on an understanding of environmental changes of this nature, and strengthening the competitiveness of our business.

Keywords: security, cyber-attack, R&D policy

1. Introduction

The Internet of Things (IoT) era is close at hand. It is said that by 2020 there will be 53 billion devices of many different types connected to the Internet. In some respects, this era has already arrived. For example, we are starting to see new businesses that store diverse types of information and share it between IoT systems and cloud services to deliver improved factory productivity, self-driving vehicles, personalized recommendation services, and smart cities that are more efficient and consume less electrical power.

IoT systems and cloud services accumulate vast amounts of diverse information, and it is expected that the ability to make effective use of this information will give rise to new business opportunities. Here, an important key to the expansion of business is the development of security technology that enables the safe use of information including sensitive data such as personal data and trade secrets.

However, the IoT era also brings various security challenges. The limited processing performance and lower manufacturing costs of IoT devices make it impossible for them to incorporate the conventional security measures used in personal computers (PCs) and the like, with the result that large numbers of IoT devices with poor security are being connected to the Internet. It is feared that IoT devices of this sort could easily be hijacked and controlled via botnets, enabling them to be applied in large-scale sophisticated cyber-attacks such as distributed denial of service (DDoS) attacks. For example, a widespread power outage in one place could conceivably be caused by a cyber-attack from hijacked IoT devices. Cases in which surveillance cameras and network television services were attacked in this way have been reported. In October 2016, a large number of websites (mostly in the US) went offline, and this was also attributed to a DDoS attack from malware called "Mirai" that had been used to hijack IoT devices [1].

To prevent this sort of cyber-attack, it is essential to implement measures such as disconnecting only abnormal devices from the network while maintaining the connections of normal IoT devices when IoT

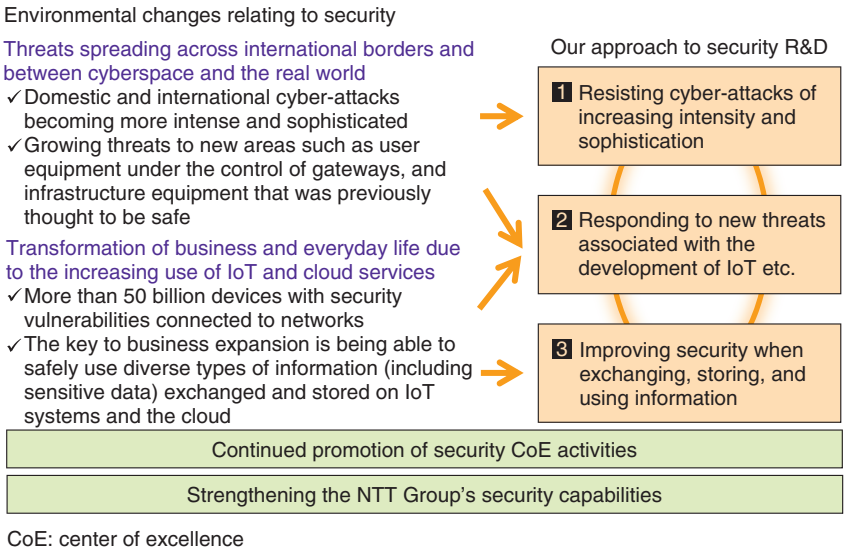


Fig. 1. Environmental changes and our approach to security R&D.

devices perform abnormal actions such as being turned into botnets.

2. Research and development (R&D) at NTT Secure Platform Laboratories

NTT Secure Platform Laboratories (hereinafter SC Labs) is conducting R&D aimed at enhancing the safety and security of cloud services and communication services provided by the NTT Group. Our mission is to create the world's most advanced security technology and to use secure technology to provide overall security improvements. To this end, our R&D is targeted at three main areas to adapt to recent changes in the security environment, as shown in **Fig. 1**. On the basis of this approach, we are carrying out a wide range of R&D from theory to the offering of product/technical know-how and operational support, with world-leading encryption technology and cyber-attack protection technology as our core competencies (**Fig. 2**).

Of the three security R&D approaches, the first two (resisting cyber-attacks of increasing intensity and sophistication, and responding to new threats associated with the development of IoT etc.) are referred to as *defense technologies* for countering cyber-attack threats, whereby we aim to contribute to improving the defenses of the NTT Group's network infrastructure and other key infrastructures. For the third approach (improving security when exchanging, storing, and using information), we are studying *offense technology* that increases the added value of NTT's products and materials used for corporate business such as cloud/network services that use IoT and services that use personal data.

2.1 Resisting cyber-attacks of increasing intensity and sophistication

At SC Labs, we are conducting R&D aimed at the creation of competitive proprietary technology and security intelligence in order to resist the growing severity and sophistication of domestic and international cyber-attacks. This is being done using our core competencies in areas such as world-leading cyber-attack detection, collection, and analysis technology while closely collaborating with group companies.

In the R&D of technology for collecting and blacklisting malicious website URLs (uniform resource locators) that cause malware infection and Internet protocol (IP) addresses that are used in attacks, we are working on information-gathering technology that emulates various web browser environments to counter malicious sites that change their behavior according to the client's web browsing environment, and information-gathering technology that deals with attacks on web application vulnerabilities, and we are operating honeypots that incorporate these results. Furthermore, we are working towards higher accuracy and broader coverage of security intelligence

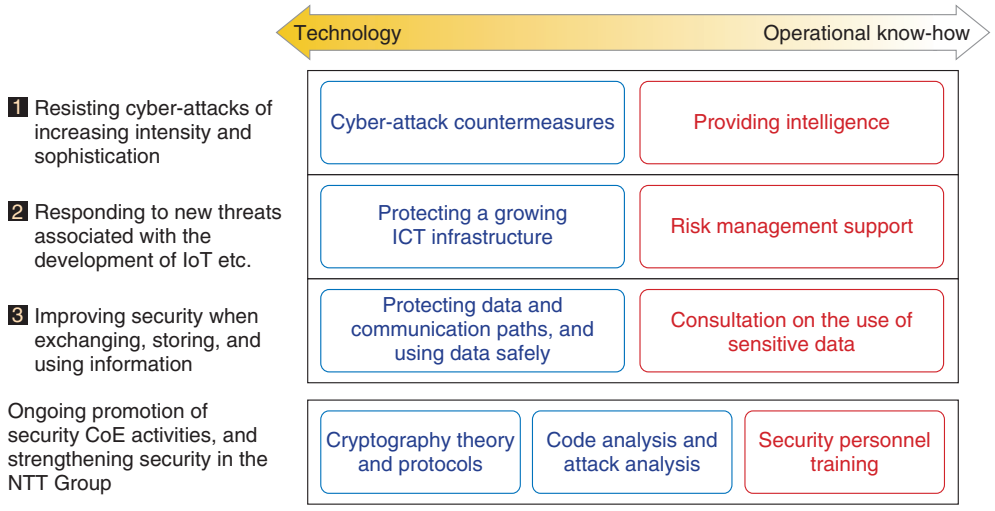


Fig. 2. Security R&D efforts.

based on advanced anti-malware technology. These technologies include dynamic malware analysis technology that analyzes the behavior of malware captured by honeypots and analyzes it by connecting to the Internet, technology for purposes such as detecting malicious HTTP (Hypertext Transfer Protocol) communication from user traffic, and technology for evaluating malicious domain names and IP addresses.

Also, in the R&D of security log analysis technology, to resist cyber-attacks that are becoming more sophisticated and harder to defend against every year, we are working on technologies including communication log correlation analysis and unknown malware detection technology that automatically extracts accurate analysis rules, and parameter profiling technology that can detect zero-day attacks with high precision.

These technologies contribute to the construction of a SIEM (security information and event management) platform aimed at strengthening the security operations of the entire NTT Group, and the development of a corporate MSS (managed security service) offered by the NTT Group.

In addition to these R&D efforts, we are also running NTT-CERT, which is a CSIRT (computer security incident response team) representing the entire NTT Group. Specifically, we are handling various types of incidents that have occurred in the NTT Group, conducting forensic studies to clarify the causes and analyze the effects of each incident, and coordinating inter-group cooperation to strengthen the group's ability to respond to cyber-attacks [2, 3].

2.2 Responding to new threats associated with the development of IoT etc.

In preparation for incidents such as the exploitation of device vulnerabilities by bots in a network environment assumed to comprise large numbers of diverse devices connected to a network, we are conducting R&D with the mission of establishing security technology related to the design, construction, and operation of secure systems that perform thorough risk assessment/management of resources that need to be protected at all stages of the life cycle.

Specifically, to improve cyber-attack defensive capabilities through integrated management of the control of systems and network equipment from a security point of view, we are working on: (1) the promotion of risk management and security through design at the system planning and design stages in order to reduce the number of incidents occurring after the system has been installed, (2) authenticity/integrity verification technology using encryption and security chips throughout the entire life cycle of connected equipment, (3) network soundness verification technology that monitors traffic and equipment status/operations of the entire network to eliminate or minimize damage, even in environments where new and old equipment are mixed together, (4) dishonest behavior detection technology that uses sensor information from a variety of IoT devices, and (5) security orchestration technology that implements

maintenance and prompt recovery of the necessary security level by performing appropriate control measures such as automatically detecting various attacks on the network.

Because devices that are connected to diverse networks in the IoT era will also be subject to diverse security threats in the same way as PCs and smartphones, it is also necessary to consider countermeasures. Although self-driving vehicle technology is in the spotlight as a symbol of the IoT era, its success depends on the implementation of cybersecurity measures in advanced vehicle control systems. In practice, cyber-attacks against vehicles, such as forcing them to operate incorrectly via a network, are starting to become a problem, and at SC Labs, we are considering applicable threats and countermeasures when vehicles are connected to networks.

These initiatives are introduced in detail in the articles "Secure Architecture for Critical Infrastructure" [4] and "Cyber-attack Countermeasures for Cars" [5] in the Feature Articles in this issue.

2.3 Improving security when exchanging, storing, and using information

To implement a safe and secure information distribution infrastructure, we are working on techniques for the secure use and operation of ciphers and techniques for the formation of encryption systems in order to keep data safe based on world-leading encryption technology and the cryptographic research on which it is based.

Interest in the use of personal data and trade secrets has grown rapidly following revisions to the Act on the Protection of Personal Information in September 2015 in Japan. However, due to difficulties in the case-by-case application of statutory requirements and the derivation of legal and useful data processing methods, advances in the utilization of sensitive data have not met expectations. At SC Labs, we are contributing to improving the added value in operating companies' security products by providing safe data utilization technology such as anonymization methods and secret computation methods, and consultation relating to the use of sensitive data in different applications and legal risk assessments of security and privacy issues.

Also, confidence in the reliability of service providers, certification authorities, and the like has been shaken due to occurrences such as frequent information leaks from businesses and interventions by state powers, and it is becoming apparent that there is a need for data protection and communication path protection measures that are less reliant on the security of servers or the morals of those that operate them. For such issues, we are working to develop technologies such as secure business chat applications that can maintain the security of communications even when information is leaked from the server, and authentication methods that can maintain security without the need for password management on the server [6].

Details of these efforts are introduced in the articles "A Secure Business Chat System that Prevents Leakage and Eavesdropping from the Server by Advanced Encryption Technology" [7] and "Key Points of the Amendments to the Act on the Protection of Personal Information, and Anonymization Methods for the Use of Personal Data" [8].

3. Future prospects

At SC Labs, with world-leading encryption technology and cyber-attack protection technology as our core competencies, we are conducting R&D that covers a wide range, from devising theories to offering product/technical know-how and operational support in order to contribute to the safety and security of cloud and communication services provided by the NTT Group.

References

[1] WIRED News on October 21, 2016. https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

[2] T. Hariu, K. Yokoyama, M. Hatada, T. Yada, T. Yagi, M. Akiyama, T. Ikuse, Y. Takata, D. Chiba, and Y. Tanaka, "Security Intelligence for Malware Countermeasures to Support NTT Group's Security Business," NTT Technical Review, Vol. 13, No. 12, 2015. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201512fa3.html

[3] F. Tanemo, I. Hayashi, M. Tanikawa, and T. Abe, "Tighter Security Operations to Help Provide Brands that are Safer and More Secure," NTT Technical Review, Vol. 10, No. 10, 2012. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa4.html

[4] M. Ueno, S. Kashima, Y. Igarashi, and M. Hori, "Secure Architecture for Critical Infrastructure," NTT Technical Review, Vol. 15, No. 5, 2017. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201705fa2.html

[5] M. Tanaka, J. Takahashi, and Y. Oshima, "Cyber-attack Countermeasures for Cars," NTT Technical Review, Vol. 15, No. 5, 2017. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201705fa3.html

[6] M. Matsui, H. Ohtsuka, T. Kobayashi, H. Okuyama, A. Nagai, and G. Yamamoto, "Milagro Multi-Factor Authentication," NTT Technical Review, Vol. 14, No. 12, 2016. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201612ra1.html

[7] R. Yoshida, Y. Okano, H. Okuyama, and T. Kobayashi, "A Secure Business Chat System that Prevents Leakage and Eavesdropping from

the Server by Advanced Encryption Technology," NTT Technical Review, Vol. 15, No. 5, 2017.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201705fa4.html
[8] K. Kameishi, K. Hirota, A. Fujimura, F. Magata, and Y. Ota, "Key Points of the Amendments to the Act on the Protection of Personal Information, and Anonymization Methods for the Use of Personal Data," NTT Technical Review, Vol. 15, No. 5, 2017.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201705fa5.html

Kazuhiko Okubo
Vice President and Head of NTT Secure Platform Laboratories.
He received a Master of Science in Management of Technology from the MIT Sloan School of Management, USA, in 2000. He joined NTT in 1989. He works at NTT Secure Platform Laboratories, where he divides his efforts between protecting the online activity of customers with security technology that can withstand even state-of-the-art cyber-attacks, and conducting research and development of technology that can strengthen our competitive edge by ensuring information can be used securely in businesses facing new threats.

Secure Architecture for Critical Infrastructure

Masami Ueno, Shingo Kashima, Yuminobu Igarashi, and Masahiro Hori

Abstract

Recent developments such as the Internet of Things mean that a wide variety of equipment is now being connected to networks. It is feared that this trend could lead to further increases in threats to cybersecurity. At NTT Secure Platform Laboratories, we are working on technology that can be used to protect critical infrastructure networks by investigating security incidents, automating the analysis and handling of incidents, and reducing latent security risks in devices and equipment.

Keywords: critical infrastructure, wide area networks, IoT

1. Introduction

As the Internet of Things (IoT) increases in scale, a growing number of devices are being connected to networks. This number has been predicted to reach 53 billion by 2020 [1]. The increasing quantity of equipment connected to networks poses an increased threat to cybersecurity. For example, there are already reports of online surveillance camera systems and video recorder equipment being infected with malware and incorporated into a botnet that was used to launch cyber-attacks including DDoS (distributed denial of service) attacks on other information technology (IT) services [2, 3]. IT is also being rapidly adopted in various key infrastructures including telecommunications, finance, aviation, rail transport, electricity, and gas with the aim of improving service quality and reducing costs, and several cases have been identified where this increased dependence on IT has adversely affected infrastructure services due to system failures [4–6].

Thus, even critical infrastructure networks are having to face increased threats due to the growing quantity of equipment connected to them, and countermeasures should be discussed urgently. This article discusses security countermeasures that can protect diverse kinds of key infrastructures from cyber-attacks, focusing in particular on the wide area networks[*1] that form part of the key infrastructure used by the communication industry.

2. Wide area network security

Traditionally, the security of a network is maintained by defining a secure zone where a security policy is enforced, and a non-secure zone where security may not be enforced, and by taking steps to protect the secure zone at the boundary between the two zones. Even in wide area networks, when seen from the viewpoint of the network provider, the facilities run by the network operator can be assumed to constitute a secure zone where security is adequately enforced, while the client-side facilities that lie beyond the customer premises equipment (CPE)[*2] such as home gateways (HGWs) and corporate routers are assumed to be a non-secure zone because they cannot be managed by the network operator, and their reliability cannot be assured. At the boundary between the CPE and network operator equipment, a

*1 Wide area network: General term for a network with a broader reach than a local area network (LAN), which would typically be used by a single organization. Specific examples include networks that use leased lines to interconnect geographically distant LANs, and virtual private networks built on the Internet.

*2 CPE: Equipment installed at the premises of an Internet service client in order to connect to the network.

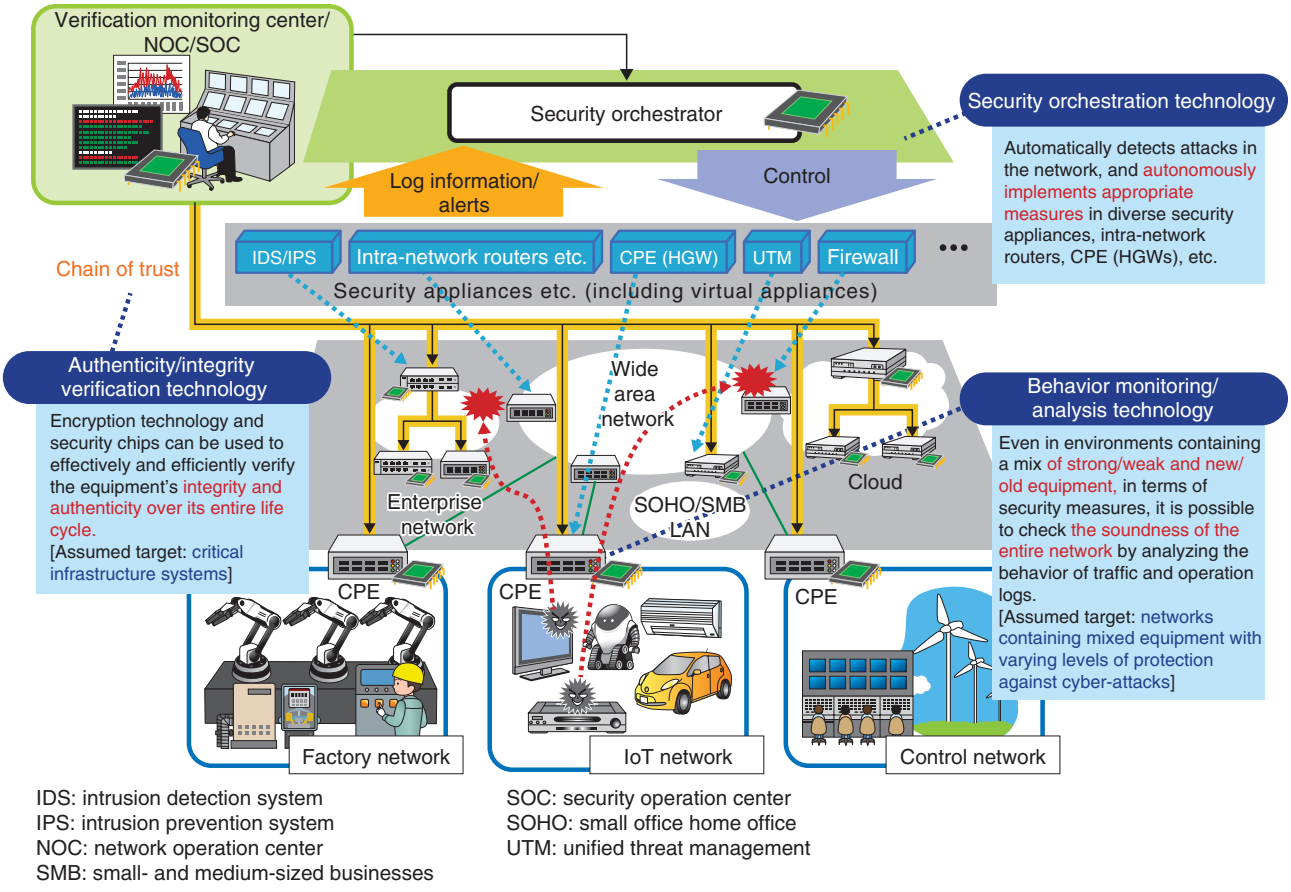


Fig. 1. Security technology research and development.

gateway device such as an edge router is installed so that the security of the network can be assured on a per-circuit basis.

In the future, however, since developments such as IoT will lead to further increases in the amount of equipment connected to client-side facilities, it is envisaged that traffic will need to be controlled by CPE devices situated closer to this equipment.

3. Mechanisms for protecting the security of a wide area network

To maintain the security of a wide area network and take prompt measures when any sort of incident such as an infection or attack has occurred, it is necessary to have mechanisms that can detect incidents, determine what countermeasures to apply to the detected incidents, and then implement these measures. Although the response mechanism for major security incidents is the same as the conventional approach, safeguarding the security of a wide area network in today's changing environment requires CPE devices that detect and deal with incidents in equipment in the non-secure zone while cooperating with mechanisms inside the secure zone. Since the CPE devices are situated at the boundary of the secure and non-secure zones, it is essential to take steps to mitigate their inherent risks (latent defects and misconfigurations, malware illegally embedded prior to shipment, etc.) and physical risks (illegal replacement of components, etc.).

In the following sections, we describe the technologies for behavior monitoring/analysis, security orchestration, and authenticity/integrity verification that are being researched and developed at NTT Secure Platform Laboratories to address these issues (**Fig. 1**).

4. Behavior monitoring/analysis technology

Intrusion detection systems (IDS) and intrusion prevention systems (IPS)[*3] are two examples of intrusion detection mechanisms for the protection of IT equipment. However, these systems are mainly targeted at personal computers and servers, and there are currently only a few products compatible with critical infrastructure systems or IoT equipment. In particular, IoT equipment and the control/monitoring equipment used in critical infrastructures and factories are typically deployed over a wide area and connected to the network in very large numbers, and they operate autonomously and unattended in a wide variety of environments. This differs significantly from the configuration of traditional IT equipment. Furthermore, since IoT equipment is often designed and produced for a specific application, it can be difficult for the equipment itself to implement security measures due to issues such as the equipment having limited functions or performance (equipment with security weaknesses), or being used continuously for long periods without regular security updates (old equipment).

To address this issue, we are researching behavior monitoring/analysis technology aimed at promptly ascertaining signs of security deterioration in the overall health of the system by detecting abnormal behavior in peripheral network equipment. More specifically, we are researching an anomaly detection technique whereby CPE devices such as HGWs placed at the perimeter of a non-secure zone are used to gather statistical information from the communication traffic and operating logs of old equipment or equipment with low security levels for which it is difficult to implement individual security measures. This information is used to construct an analysis model that represents the healthy state of a system containing the characteristics and usage patterns of the equipment, from which it is possible to discover behavior that departs from the normal (healthy) behavior exhibited.

5. Security orchestration technology

For the analysis and handling of detected incidents, most security product vendors provide products where the detection and control functions are linked by proprietary security appliances and the like, but these only work with the vendor's own products, or with the products of certain affiliated companies.

At NTT Secure Platform Laboratories, we are developing security orchestration technology as a vendor-agnostic framework for the automation and semi-automation of security operations that can link together the detection and analysis functions of diverse security equipment, and we are making it available to NTT Group companies. We have developed this as technology that cooperates with the operation of office security appliances and datacenters where there have been clear security vulnerabilities. As further developments in IoT are achieved in the future, we intend to expand the technology to orchestration including CPE devices such as HGWs. For example, by restricting the sources and destinations of traffic through the use of resources such as a pre-prepared whitelist for IoT devices that transmit data to few destinations, it is possible to implement traffic control on a per-equipment basis such as restricting or blocking the flow of traffic when an issue has arisen.

6. Authenticity/integrity verification technology

Security devices that perform detection and control functions are typically placed in the non-secure zone together with CPE devices. If the degree of confidence can be increased by reducing the latent risks and physical risks of these devices, then even if an incident does occur, it will be possible to deal with it more promptly.

At NTT Secure Platform Laboratories, we are working to increase the reliability of these devices and the equipment connected to them by researching a technique for reliably identifying the controlled equipment (authenticity verification) and a technique for confirming the correctness of software running in this equipment (integrity verification).

6.1 Authenticity verification

The purpose of our authenticity verification technique is to confirm that the control and communication equipment itself is operating correctly and is not being spoofed. This is done by designating a dedicated server node as the *root of trust*, and constructing a chain of relationships (trust links) from tamper-resistant components that extend this root of trust out to each item of equipment. Cryptography is used in this chain to authenticate the equipment, thereby confirming the authenticity of the system as a whole. The tamper-resistant components used here have

*3 IDS/IPS: The detection of fraudulent activity from outside the targeted IT system or network, or a defense system that performs such detection.

mechanisms that are very difficult to analyze externally or extract data from without authorization, and are therefore able to handle cryptographic keys safely.

6.2 Integrity verification

The purpose of integrity verification is to confirm that the software and data in control and communication equipment have not been tampered with. This is done by checking that the software in the equipment matches the correct values stored in tamper-resistant components based on the chain of trust established by the authenticity verification technology. Integrity verification has the advantage of ensuring scalability for the entire system and takes the entire software life cycle into account.

7. Future prospects

We have introduced countermeasures for wide area networks in order to protect the security of key infrastructures in situations where the amount of equipment connected to the network is expected to increase dramatically. Dealing promptly with the occurrence of any incident such as an infection or attack requires a mechanism for analyzing the incident and deciding what countermeasures to use, a mechanism for deploying these countermeasures, and a mechanism for reducing the inherent and physical risks of the equipment. At NTT Secure Platform Laboratories, we are working to address these needs with behavior monitoring/analysis technology, security orchestration technology, and authenticity/integrity verification technology. These technologies can be used not only in wide area networks but anywhere IT has been introduced to keep up with communication trends. In the future, we plan to make this technology applicable to many more areas including critical infrastructure systems.

References

[1] Ministry of Internal Affairs and Communications, “2015 White Paper on Information and Communications in Japan,” Chapter 5: ICT and the Future of Industry, Section 4, 2016. http://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2015/chapter-5.pdf#page=13

[2] B. Krebs, “DDoS on Dyn Impacts Twitter, Spotify, Reddit,” Krebs on Security, 2016. https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/

[3] T. Spring, “BASHLITE Family of Malware Infects 1 Million IoT Devices,” 2016. https://threatpost.com/bashlite-family-of-malware-infects-1-million-iot-devices/120230/

[4] Government of Japan, “The Basic Policy of Critical Information Infrastructure Protection (3rd Edition),” May 19, 2014, Information Security Policy Council; May 25, 2015 (Revised), Cybersecurity Strategic Headquarters. http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3_r1.pdf

[5] National Center of Incident Readiness and Strategy for Cybersecurity, “Report on IT Dependency Based on Change in Critical Information Infrastructure,” 2015 (in Japanese). http://www.nisc.go.jp/inquiry/pdf/itizon_gaiyou.pdf

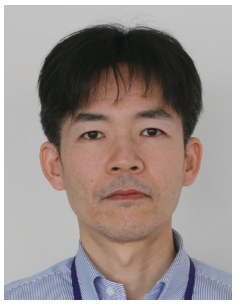
[6] InfoCom Research, Inc., “Report on IT Dependency Based on Change in Critical Information Infrastructure,” 2015 (in Japanese). http://www.nisc.go.jp/inquiry/pdf/it_izon_honbun.pdf

Masami Ueno
Senior Research Engineer, Secure Architecture Project, NTT Secure Platform Laboratories.

He received a B.E. and M.E. in computer science from Yamanashi University in 1991 and 1993. In 1993, he joined NTT Software Laboratories. He has been engaged in requirement engineering and development of a billing platform and digital rights management system. Since April 2012, he has been conducting research and development (R&D) on security orchestration technology. He is a member of the Information Processing Society of Japan.

Shingo Kashima
Senior Research Engineer, Secure Architecture Project, NTT Secure Platform Laboratories.

He received a B.S. and M.S. in computer science from Kyushu University, Fukuoka, in 2002 and 2004. Since joining NTT in 2004, he has been engaged in R&D of Ethernet virtual private networks, traffic monitoring techniques, and network security.



Yuminobu Igarashi
Senior Researcher, NTT Secure Platform Laboratories.

He received an M.S. in energy science from Tokyo Institute of Technology in 1994 and an M.S. in management of innovation and technology from University of Sussex, UK, in 2009. He joined NTT in 1994 and has been involved in the research and operation of virtual private networks. His current research interests are anomaly detection of IoT networks and devices. He is a member of the Institute of Electronics, Information and Communication Engineers.

Masahiro Hori
Senior Research Engineer, Secure Architecture Project, NTT Secure Platform Laboratories.

He received a B.E. in electrical engineering and an M.E. in information engineering from Kyushu University, Fukuoka, in 1986 and 1988. He joined NTT Software Laboratories in 1988 and studied object-oriented design methods, electronic money technology, and security for e-Government. He joined NTT Secure Platform Laboratories in 2012. He is currently studying a technique to confirm the correctness of software.

Cyber-attack Countermeasures for Cars

Masashi Tanaka, Junko Takahashi, and Yoshihito Oshima

Abstract

Cyber-attacks on cars have become a serious real-world issue following recent revelations in which it was verified that cars can be illegally operated via the Internet. Thus, there is an urgent need for security countermeasures to protect the safety and security of cars. This article introduces the current trends in car security and describes car security evaluation techniques and countermeasures that we are currently working on at NTT Secure Platform Laboratories.

Keywords: car security, connected cars, in-vehicle networks

1. Introduction

The proportion of electronic systems in vehicles has increased significantly in recent years. Nowadays, a wide variety of vehicle functions are controlled electronically by numerous vehicle control computers (electronic control units; ECUs) connected to in-vehicle networks. It is expected that a rich variety of automotive services such as connected cars and automated driving will be made possible by connecting these automotive systems to external networks.

However, the high speed at which automotive systems are being introduced and connected to external networks is raising important considerations regarding the cybersecurity aspects of vehicle design. Some cases relating to cyber-attacks on vehicles that have had real-world repercussions are introduced below.

1.1 Vehicle theft by duplicating key code

These days, most vehicles are equipped with immobilizer systems. These immobilizers use cryptography to authenticate the chip inside a key fob with a microcomputer in the vehicle, and only allow the engine to start if the authentication succeeds. This authentication is sometimes performed using the manufacturer's proprietary encryption algorithm, and there have been reports of attackers exploiting weaknesses in these algorithms to illegally obtain secret authentication keys.

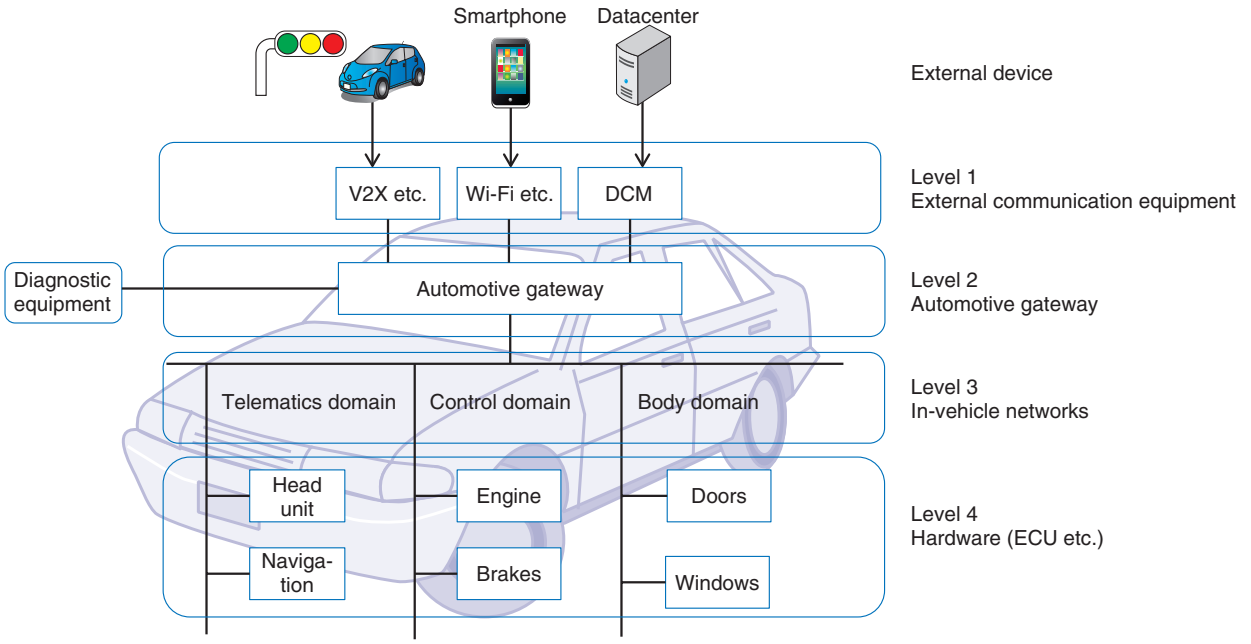
1.2 Using the OBD2 to hack a vehicle

The OBD2 (On-board Diagnostic, second generation) port is a standard diagnostic interface for vehicles. By connecting it to a data acquisition device and a personal computer (PC), it is possible to acquire and interpret messages that are exchanged via internal communication (e.g., controller area network (CAN) messages), and to infer the meaning of these messages in conjunction with the vehicle's behavior at that time [1]. It has been demonstrated that a PC can be used to exploit this information by injecting forged messages to perform actions such as tampering with the speedometer display or operating the steering and/or brakes contrary to the driver's intentions.

1.3 Unauthorized remote control of vehicles

In 2015, security researchers successfully hacked a Jeep Cherokee. They were able to take remote control of the vehicle's on-board computer and entertainment system, and remotely controlling the vehicle's brakes and steering over the Internet [2]. After that, Fiat Chrysler recalled 1.4 million vehicles. This remote hacking over the Internet had a great impact on the automotive industry.

As this example shows, cyber-attacks on vehicles



DCM: data communication module
V2X: vehicle-to-everything; a form of technology that allows vehicles to communicate with moving parts of the traffic system around them

Fig. 1. Automotive system architecture and hierarchical classification from a security viewpoint.

can have significant effects on modern society by infringing on people's property and personal safety. Efforts must therefore be made to implement security measures to prevent cyber-attacks on vehicles in order to achieve a safe and secure social infrastructure.

We introduce below some of the recent trends in countermeasures to vehicle cybersecurity threats, and the efforts that have been made so far at NTT Secure Platform Laboratories.

2. Vehicle security technology trends

The automotive system architecture that is becoming the norm in recent years is shown in **Fig. 1**, and a hierarchical classification of these systems is presented from a security viewpoint.

2.1 Automotive system architecture

(1) Level 1

Level 1 communicates with the outside world. It consists of on-board equipment for communicating with mobile networks, Wi-Fi* networks, and vehicle-to-vehicle/vehicle-to-infrastructure systems (e.g., V2X (vehicle-to-everything) communication).

(2) Level 2

Level 2 controls all the automotive systems in a vehicle. It consists of an automotive gateway that exchanges messages between internal ECUs and external devices communicated at Level 1 and exchanges messages between in-vehicle networks in the vehicle.

(3) Level 3

Level 3 is a network (in-vehicle network) that conveys messages between ECUs. It is partitioned into multiple in-vehicle networks according to the ECU applications and roles, such as a telematics domain for vehicle navigation and the like, a control domain for brakes and the like, and a body domain for door locks and the like. It uses in-vehicle communication protocols suited to each system such as a CAN or local interconnect network (LIN).

(4) Level 4

Level 4 controls each component of the vehicle such as the engine, brakes, and door lock functions. It consists of ECUs and other such components that perform a variety of functions.

2.2 Security of each level

(1) Security of Level 1 (external communication

* Wi-Fi is a registered trademark of Wi-Fi Alliance.

equipment)

This includes authentication and access control to confirm that the vehicle is communicating with trusted external systems or that the communication has been authorized, while blocking communication with other external systems. Communication channels established with external systems may need to be encrypted in order to prevent eavesdropping or the injection of unauthorized messages.

(2) Security of Level 2 (automotive gateway)

Level 2 tasks include i) filtering to ensure that only authorized messages can flow between external systems and in-vehicle networks, or between different in-vehicle networks, ii) key management to manage the keys used by the ECU for encryption and authentication, and iii) anomaly detection to detect security anomalies in messages flowing inside the vehicle.

(3) Security of Level 3 (in-vehicle networks)

This includes tamper detection by detecting when messages transmitted between ECUs have been rewritten, and performing encryption to prevent eavesdropping.

(4) Security of Level 4 (hardware (ECU etc.))

This includes the use of secure designing and programming methods to avoid the inclusion of vulnerabilities in programs running on the ECU and to secure booting to verify that the firmware and operating system have not been tampered with when starting up.

In the future, as connections to vehicle communication networks become more commonplace and a wide diversity of network-type services are made available, it is envisaged that cyber-attacks will also become more advanced and more sophisticated. Just as with the security countermeasures used in information technology systems, it is thought that it will be necessary to implement multi-stage, multi-layered defenses combining security technologies for each level of the vehicle hierarchy.

3. NTT research and development (R&D) activities in automotive security

R&D efforts focused on automotive security are underway at NTT. We describe those efforts in this section.

3.1 Overview

At NTT Secure Platform Laboratories, we are researching and developing security evaluation techniques that assess the resilience of vehicles to cyber-attacks, and countermeasures to attacks at each of the four security levels described above. As examples of security evaluation techniques and countermeasures, we introduce an attack at Level 3 that induces improper behavior in the LIN protocol and the countermeasures to this kind of attack. We also introduce some examples of our research into safety evaluation techniques and countermeasures for immobilizer authentication protocols related to Level 4 security.

3.2 Attacks that induce improper behavior in LIN and countermeasures against them

Many studies have recently been done on the security of in-vehicle networks, and most of them have been concerned with CAN, which is used to control vehicle parts such as the engine and brakes. In contrast, although significant threats would be presented if an attacker improperly gained control of LIN, which is used in controlling steering wheels, seats, and doors, it was not clear whether LIN is able to withstand attacks aimed at inducing improper behavior, or that any countermeasures are needed. In collaboration with other companies, we have therefore proposed an attack method to induce improper behavior in LIN, as well as countermeasures against this kind of attack [3].

LIN is based on a master-slave model. The master node transmits a header including the identifier (ID) that denotes the contents of the process, and the transmit/receive slave nodes corresponding to this ID start to transmit and receive data. Since the LIN specification does not define how to proceed after an error has been detected, LIN error handling mechanisms are application-dependent. For example, in some cases when the data transmitted by a node differ from the data on the bus, an error is detected, and the node handles the error simply by halting the data transmission and waiting for the next header. We have shown that the characteristics of this error handling mechanism can be used to make false data appear to be correct to the receiving slave node, thereby allowing incorrect behavior to be induced. Specifically, the attacker monitors the bus, and at the same instant that the correct data are transmitted following the reception of the header (**Fig. 2(a)**, **(b)**), the attacker injects false data to create a collision (**Fig. 2(c)**), whereby the transmission of the correct data is halted by the error handling mechanism. At the same time the transmission of the correct data is halted, the attacker injects false data, and this can be incorrectly recognized as correct data by the receiving slave node. This showed that it is possible to induce abnormal behavior contrary to the driver's intentions.

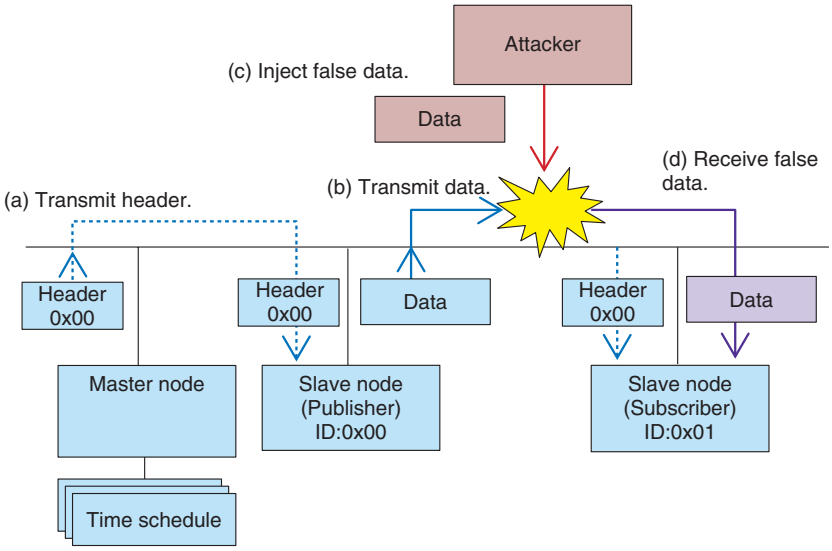


Fig. 2. Attack technique that induces abnormal behavior in LIN.

As countermeasures against this attack, we proposed a method to assign the significant bytes in data and a method to send an abnormal signal overwriting the false data when a communication error has occurred.

3.3 Evaluation techniques and countermeasures for immobilizer authentication protocols

In 2010, an authentication protocol that uses the standard cryptographic algorithm, the Advanced Encryption Standard (AES), was proposed for use in immobilizers instead of using proprietary cryptography for authentication. The authentication protocol has been subjected to previous theoretical analysis, and no vulnerabilities had yet been discovered. However, in our research, we found that the secret key stored in the key fob can be exposed by applying a fault analysis attack to the immobilizer system [4]. The fault analysis attack is a kind of implementation attack. In the protocol we targeted, the key fob contains three copies of the secret key; these copies are used in sequence in order to make it unlikely to fail even when used under harsh circumstances. By focusing on this characteristic of the key storage, we proposed an attack method that changes the value of the secret key stored in the key fob by a sequential fault injection (**Fig. 3(a)–(c)**) and reduces the key candidate space of the secret key ("Analyze" sections of Fig. 3).

There are two patterns for authentication protocols of this type: unilateral authentication, where the vehicle authenticates the key, and bilateral authentication, where the vehicle and key authenticate each other. We showed that it is possible to identify the secret key in a practical amount of time when using a unilateral authentication scheme, and that key extraction is also possible when using bilateral authentication, depending on factors such as the number of electronic key fobs that are available. We also proposed countermeasures to the proposed attack method such as performing a preliminary comparison of the encryption results calculated using each secret key in order to check for any changes in the key values.

4. Future prospects

It is expected that many more functions will be needed in order to implement the self-driving cars and connected cars of the future. In line with this trend, we can expect that the attack surfaces (attack paths) of vehicles will become broader, and that attack methods will become more advanced. At NTT Secure Platform Laboratories, we will continue with R&D relating to the security of in-vehicle networks and automotive systems, and we will provide cyber-attack countermeasures necessary to keep the next generation of vehicles safe and secure. We will also contribute to the realization of vehicle security services that work together with cloud services and a secure communication infrastructure that connects in-vehicle systems with external systems.

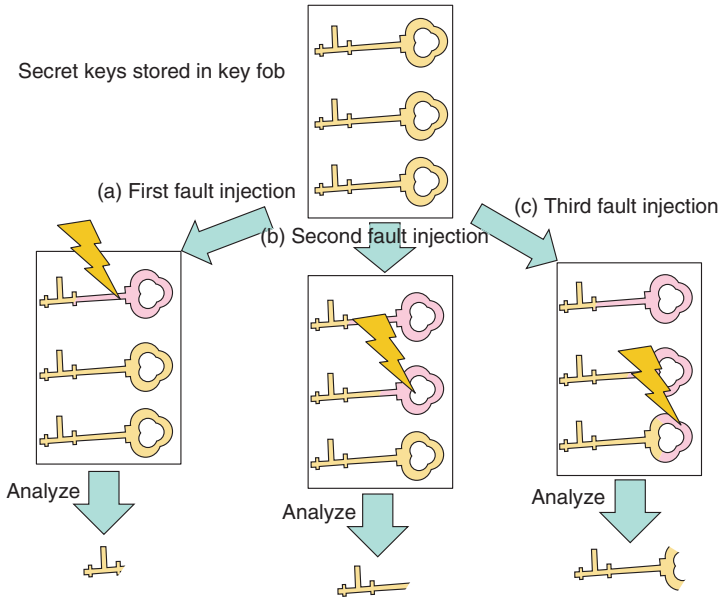


Fig. 3. Technique for evaluating immobilizer authentication protocols.

References

[1] C. Valasek and C. Miller, "Adventures in Automotive Networks and Control Units," DEF CON 21, Las Vegas, NV, USA, Aug. 2013.
[2] C. Valasek and C. Miller, "Remote Exploitation of an Unaltered Passenger Vehicle," Black Hat USA, Las Vegas, NV, USA, Aug. 2015.
[3] J. Takahashi, Y. Aragane, T. Miyazawa, H. Fuji, H. Yamashita, K. Hayakawa, S. Ukai, and H. Hayakawa, "Automotive Attacks and Countermeasures on LIN-Bus," J. Info. Process., Vol. 25, pp. 220–228, 2017.
[4] J. Takahashi and T. Fukunaga, "Fault Analysis and Countermeasures on an Immobilizer Protocol Stack," IEICE Trans. Fundamentals. (Japanese Edition), Vol. J99-A, No. 2, pp. 106–117, 2016.

Masashi Tanaka
Senior Research Engineer, Cyber Security Project, NTT Secure Platform Laboratories.
He received a B.S. and M.S. from Osaka Prefecture University in 1999 and 2001. He is presently researching cybersecurity of the Internet of Things (IoT).

Junko Takahashi
Researcher, Cyber Security Project, NTT Secure Platform Laboratories.
She received a B.S. and M.S. in physics from Waseda University, Tokyo, in 2004 and 2006, and a Ph.D. in engineering from the University of Electro-Communications, Tokyo, in 2012. She joined NTT Information Sharing Platform Laboratories in 2006. Her main research interest is the security of embedded systems such as side-channel analysis and automotive security. She was awarded the SCIS (Symposium on Cryptography and Information Security) 2008 paper prize. She is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and the Information Processing Society of Japan (IPSJ).

Yoshihito Oshima
Senior Research Engineer, Supervisor, NTT Secure Platform Laboratories.
He received a B.E. and M.E. in electrical engineering from Hokkaido University in 1994 and 1996. He joined NTT in 1996 and is currently conducting R&D on IoT cybersecurity. He is a member of IPSJ.

A Secure Business Chat System that Prevents Leakage and Eavesdropping from the Server by Advanced Encryption Technology

Reo Yoshida, Yuki Okano, Hironobu Okuyama, and Tetsutaro Kobayashi

Abstract

In business-oriented chat applications, end-to-end encryption is needed to prevent governments and service providers from eavesdropping or leaking information. At NTT Secure Platform Laboratories, we are working on a prototype secure business chat system that not only prevents leakage from terminals by not leaving any data on the terminals, but also makes it possible to exchange and search messages without disclosing any secrets to the server. This article introduces the encryption technology used in this prototype system.

Keywords: multi-cast key distribution, proxy re-encryption, searchable symmetric encryption

1. Introduction

Prominent consumer-oriented messaging applications include LINE in Japan and Asia, and Facebook Messenger and WhatsApp in Europe and the US. Each application claims to have several million users. Following accusations of communication insecurities made by the former Central Intelligence Agency employee Edward Snowden [1] and by WikiLeaks [2], people have started to suspect that these chat room applications may be subject to eavesdropping and data theft by governments and messaging service providers. Furthermore, according to a safety assessment of typical messaging applications carried out by the Electronic Frontier Foundation [3], users are becoming much more interested in the specific security measures of each application and in how these measures are implemented. To address these growing concerns, LINE, Facebook Messenger, and WhatsApp are taking steps to improve the security of their chat applications by implementing measures such as end-to-end encryption, whereby messages are encrypted and decrypted in the user terminals so as to guarantee that service operators cannot eavesdrop on their messages.

Business-oriented chat applications include ChatWork and TopicRoom in Japan, and Skype for Business and Slack in Europe and the US. Unlike consumer-oriented applications, the chat data in these applications belong to the business, so most applications do not leave chat data on the terminals but instead keep this information on servers such as cloud services for each login. In this way, they can prevent leakage of data even if a terminal is lost or stolen.

2. Issues involving end-to-end confidentiality in business chat applications

In business chat applications, data are saved in a cloud service or some other form of server to prevent the chat data from being leaked when a device is lost or stolen. However, for business-oriented applications,

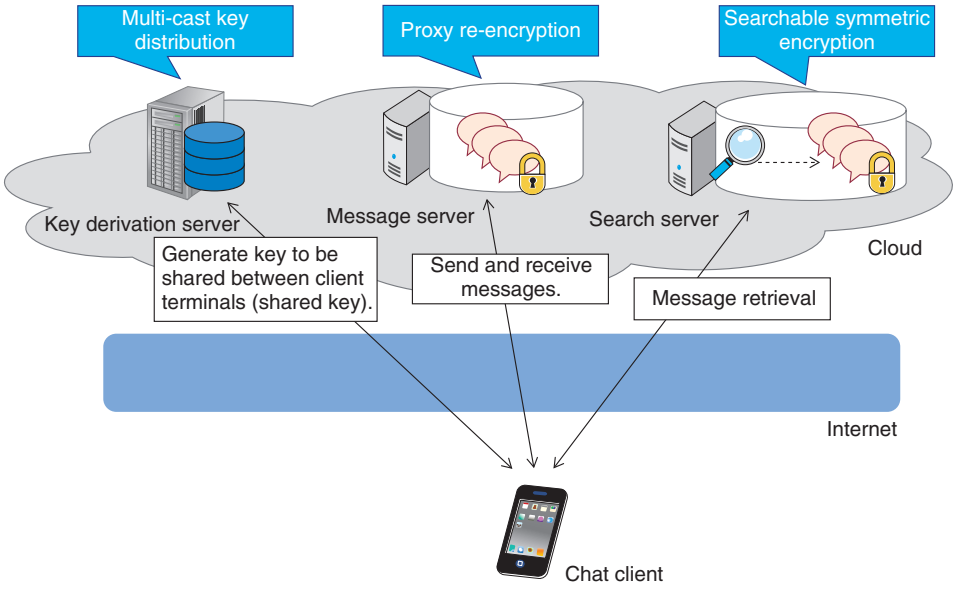


Fig. 1. System overview and technical features of encrypted business chat system.

it is assumed that there will be many users. Consequently, there will probably be frequent changes to the members of the chat rooms and messaging services as people move to new positions, new employees arrive, and older employees leave. With conventional encryption methods, it is therefore technically difficult to implement end-to-end encryption while preserving data on a server, and in fact, no applications have yet achieved this. Furthermore, although there are many server-side applications that can implement full-text searching of chat messages at higher processing speeds, it is technically difficult to search messages without disclosing information to the server, and this is another feature that is not yet supported by any applications.

In summary, there are three confidentiality issues that need to be addressed in business chat systems.

- Implementing multi-user chat functions with end-to-end encryption
- Storing encrypted chat data on a server and enabling the members authorized to view the data to be modified and updated as the chat room members are modified and updated
- Allowing full-text searching of chat messages on the server while maintaining the secrecy of chat information on the server

3. Approach of NTT Secure Platform Laboratories

At NTT Secure Platform Laboratories, we have been developing encryption technology for many years, and we are studying how it can be used to solve the abovementioned issues and implement a secure business chat system that prevents eavesdropping and leakage of chat contents from the server. As a result, we have developed the following three techniques:

- Multi-cast key distribution [4]
- Proxy re-encryption
- Searchable symmetric encryption

An overview of a business chat system to which these techniques have been applied is shown in **Fig. 1**.

4. Three techniques for implementing secure business chats

The three techniques developed to ensure that business chats remain secure are described in more detail in this section.

4.1 Multi-cast key distribution

A key sharing protocol is a protocol that allows keys used for the encryption and decryption of messages to be shared between clients by communicating over a non-secure communication path that may be subject to eavesdropping. These shared keys can then

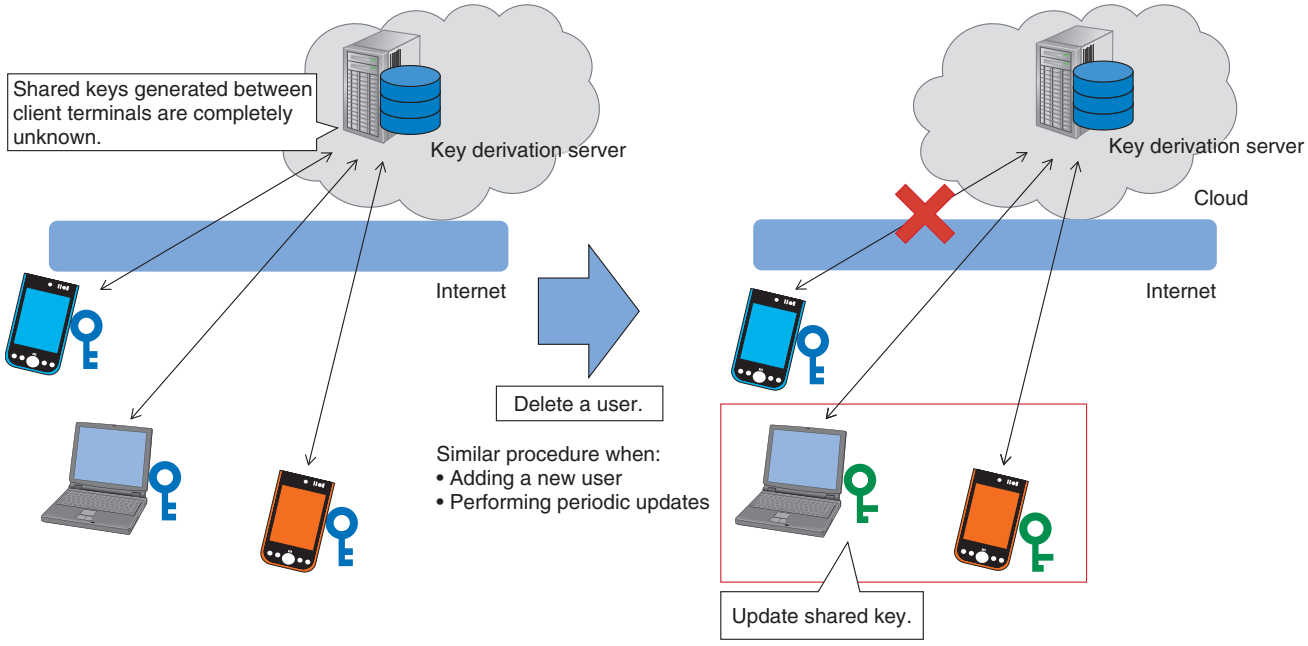


Fig. 2. Multi-cast key distribution.

be used to keep the communication secret. An example of a key sharing protocol that operates between two clients is the Diffie-Hellman key exchange, which is the protocol used by most existing business chat systems. However, when keys are shared among large numbers of clients, this two-user key sharing protocol must be performed repeatedly, which is inefficient. This can lead to technical issues when sharing keys among large numbers of users and may lead to capping the number of participants in a chat room.

With NTT's multi-cast key distribution technique, a key derivation server is placed in the center, and the keys are shared among multiple users via this server (**Fig. 2**). This is much more efficient than sharing keys among users directly. Since the shared key is generated by performing advanced calculations from secret information held by each user and the key derivation server, the shared key itself is not sent between the user and the key derivation server, and there is no way that the shared key can be known by the key derivation server. It is also possible to add new users and delete existing users, and the system includes a mechanism that updates the keys every time such an event occurs. This makes it possible to communicate information that is kept secret from the server and is only accessible to the users (however many) who are communicating at that time.

4.2 Proxy re-encryption

Proxy re-encryption is a technique whereby, instead of decrypting a ciphertext that can be decrypted with a key K1, a so-called re-encryption key RK is used to transform the ciphertext so that it can be decrypted with a different key K2. For example, a ciphertext addressed to user A on message server S could be transformed (re-encrypted) by server S using a re-encryption key so that it can be decrypted by user B. The plaintext of the original message is not made available to server S at any point.

In the business chat system introduced here, the shared key is updated by multi-cast key distribution when changes are made to the chat room members, for example, organization changes or changes of personnel. When this takes place, the data stored on the message server must be capable of being decrypted with the updated shared key. With NTT's proxy re-encryption technique, the data are re-encrypted and then decrypted using the updated shared key, without it being possible to decrypt any messages on the server (**Fig. 3**). Thus, even if a chat room member update occurs, the messages are never disclosed to the server and can only be decrypted by current chat room participants. With conventional proxy re-encryption techniques, the computer processing needed to re-encrypt all the encrypted chat data would be too slow to be of practical use for a business

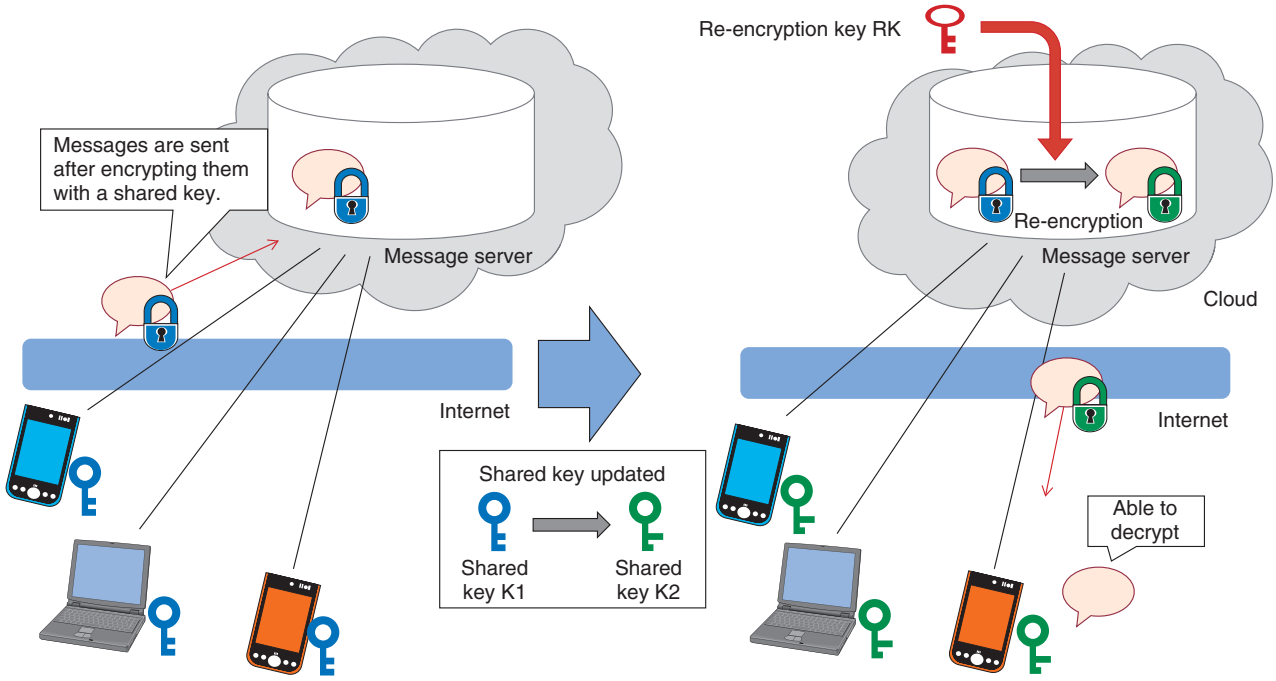


Fig. 3. Proxy re-encryption.

chat system. In NTT's proxy re-encryption technique, the processing is limited to only those parts of the data that need to be processed while keeping the data secure. In this way, we can perform re-encryption more efficiently than conventional proxy re-encryption techniques.

4.3 Searchable symmetric encryption

Searchable symmetric encryption is a technique that makes it possible to search for keywords in a set of data while the data and keywords remain encrypted. In a searchable symmetric encryption, the user generates a key (search key) and uses it to make a secret index to the data that are not disclosed to the search server. The server stores the user's secret index on the search server together with the encrypted data. The user uses the search key to send secret queries, and the server uses the secret queries and concealed index to search for the corresponding data without decrypting any of the data, and then sends the results back to the user (**Fig. 4**). In the keyword search function of a business chat system, it must be possible to retrieve the required information quickly from previous messages. NTT's searchable symmetric encryption technique can perform secret searches that are fast enough for business chat systems where real-time performance is needed. Even if new users are added, these users can also generate secret keywords and carry out searches using them.

5. Evaluation

We applied the above techniques to an existing business chat application in order to evaluate them. The client application's user interface was left unchanged, while the above encryption techniques were applied to add a new key derivation server and search server and to add re-encryption functions to the message server. We analyzed the operation of the client application and the data stored on the message server and search server, and we confirmed that the following functions were operating correctly (**Fig. 5**).

- Adding/removing users and updating shared keys (multi-cast key distribution)
- Re-encrypting messages when shared keys are updated (proxy re-encryption)
- Performing keyword searches using secret indexes and secret keywords (searchable symmetric encryption)

Table 1 compares the average processing times needed for logging in, exchanging messages, and performing keyword searches in a conventional chat system and in a chat system with the addition of the above three functions.

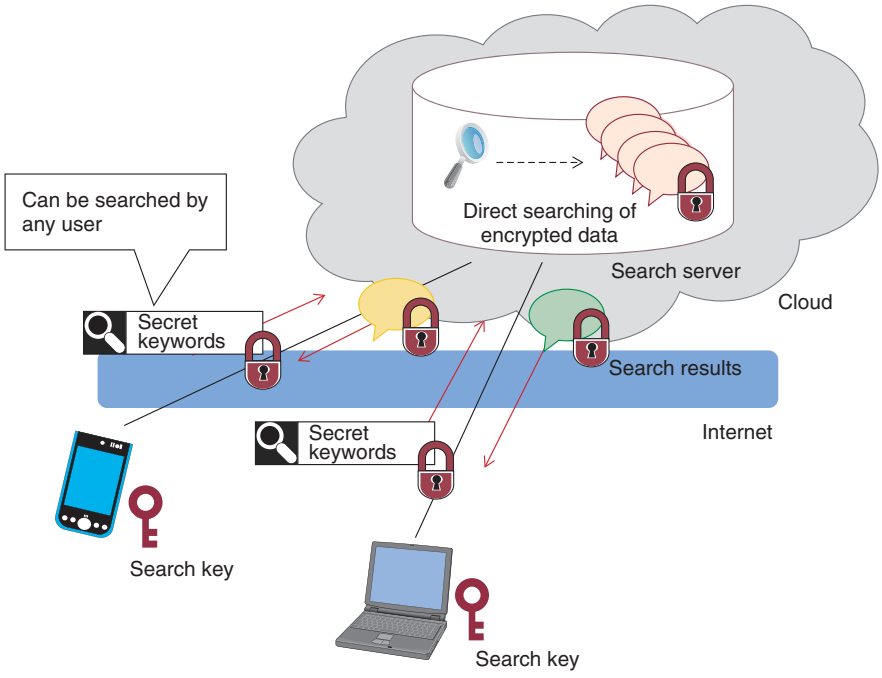


Fig. 4. Searchable symmetric encryption.

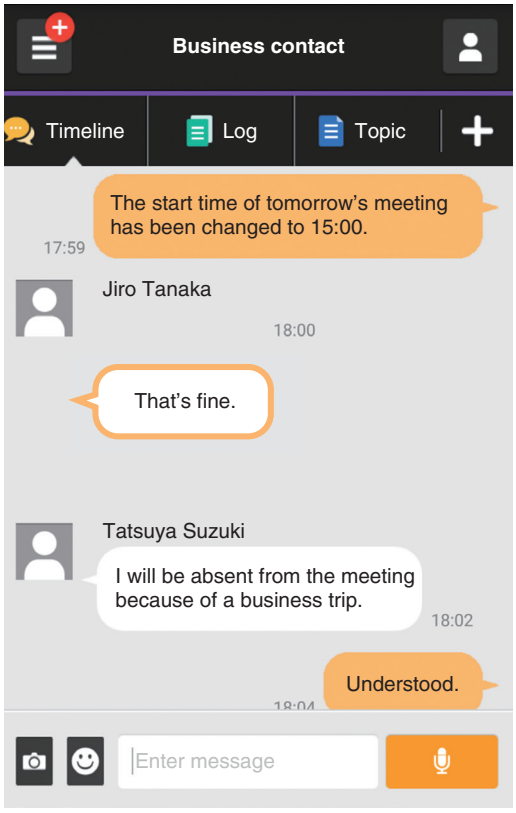


Fig. 5. Screen shot of an existing business chat application after applying the three functions.

Table 1. Comparison of average processing times in an existing business chat application.

Item	Ordinary processing time	Processing time with three additional functions
Enter chat room	3–4 seconds	3–4 seconds
Sending & receiving messages	≤1 second	1–2 seconds
Keyword search	≤1 second	≤1 second

6. Future prospects

We have devised encryption schemes for secure business chat systems that prevent eavesdropping and leakage of information from the server. We have also developed and tested a prototype business chat system that implements these encryption schemes and confirmed that its performance is sufficient to withstand practical use.

We plan to make this business chat system commercially available in the future. We will also publish the details of these encryption systems at conferences and in technical journals. We are also considering the possible application of this technology to other areas such as virtual private networks or email systems and are working to put it to practical use.

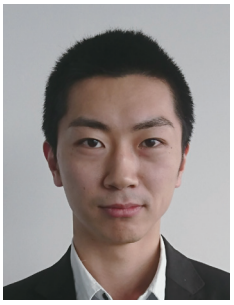
References

[1] G. Greenwald, "No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State," Picador USA (Reprint edition), 2015.
[2] WikiLeaks, https://wikileaks.org/nsa-japan/
[3] A Project of the Electronic Frontier Foundation, https://www.eff.org/secure-messaging-scorecard
[4] K. Yoneyama, R. Yoshida, Y. Kawahara, T. Kobayashi, H. Fuji, and T. Yamamoto, "Multi-cast Key Distribution: Scalable, Dynamic and Provably Secure Construction," Proc. of Prov. Sec. 2016, pp. 207–226, Nanjing, China, Nov. 2016.

Trademark notes

Reo Yoshida
Researcher, Data Security Project, NTT Secure Platform Laboratories.
He received a B.S. in mathematics from Nagoya University, Aichi, in 2007 and an M.I. in informatics from Kyoto University in 2009. He is presently researching cryptography and information security at NTT Secure Platform Laboratories.

Hironobu Okuyama
Senior Research Engineer, Data Security Project, NTT Secure Platform Laboratories.
He received a B.S. in mathematical sciences from Tohoku University, Miyagi, in 1990 and an M.S. in mathematical sciences from Chiba University in 1992. He is presently engaged in research on information security.



Yuki Okano
Researcher, Data Security Project, NTT Secure Platform Laboratories.
He received a B.S. and M.S. in mathematical sciences from Keio University, Kanagawa, in 2012 and 2014. He is presently researching information security.

Tetsutaro Kobayashi
Senior Research Engineer, Data Security Project, NTT Secure Platform Laboratories.
He received a B.Eng. and M.Eng. in electrical and electronic engineering from Tokyo Institute of Technology in 1993 and 1995, and a Ph.D. in information and communication engineering from the University of Tokyo in 2005. He is currently conducting research on information security. He was awarded the SCIS (Symposium on Cryptography and Information Security) 2000 paper prize.

Key Points of the Amendments to the Act on the Protection of Personal Information, and Anonymization Methods for the Use of Personal Data

Kumiko Kameishi, Keiichi Hirota, Akiko Fujimura, Fumihiko Magata, and Yukiyoshi Ota

Abstract

The Act on the Protection of Personal Information was amended in 2015 to promote further development of industry through the use of personal data while at the same time protecting people's privacy. In this article, we discuss the five amendments that were made to this act. We also describe an anonymously processed information system that could lead to the creation of new business for NTT, and we introduce NTT's proprietary Pk-anonymization technology that keeps information secure without harming its usefulness.

Keywords: Amended Act on the Protection of Personal Information, anonymization methods, personal data

1. Introduction

Amid calls for rules governing the use of big data and personal data that take legal issues and privacy into consideration, the Act on the Protection of Personal Information was amended in 2015 (referred to as the *amended law*[*1] [1] below), and government-led preparations are now being made prior to the full enforcement of this amendment on May 30, 2017. The structure of laws and ordinances relating to personal information is shown in **Fig. 1**. At the lowermost part of this structure, the Act on the Protection of Personal Information provides the basis for higher-level rules and guidelines, and the following items in the upper half of the structure should be seen by those trusted with personal information: Guidelines on Personal Information Protection Law [2], ministry guidelines, and Guidelines for Accredited Personal Information Protection Organizations.

Although the Guidelines for Accredited Personal Information Protection Organizations originally received a quiet reception, the new legal reforms are particularly important because they add items relating to the handling of *anonymously processed information* and make it obligatory for organizations to provide guidance and also include recommendations for compliance with the guidelines. The accredited personal information protection organizations[*2] that apply to the NTT Group include the Japan Data Communications Association (JADAC) and the Japan Institute for Promotion of Digital Economy and Community (JIPDEC).

*1 Amended law: The partial amendments on the Act on the Protection of Personal Information and the Act on the Use of Numbers to Identify Specific Individuals in the Administrative Procedure.

*2 Accredited personal information protection organization: A private organization that handles complaints and provides information for businesses for purposes such as ensuring the correct handling of personal information. There are currently 42 such organizations in diverse fields. Each organization formulates and publishes policies based on related ministry guidelines.

*Parts outlined with a dotted line have yet to be published (as of 19th April 2017).

Fig. 1. Structure of the Amended Act on the Protection of Personal Information.

2. Key amendments to the Act on the Protection of Personal Information

We will refer to **Fig. 2**, which was prepared based on government materials relating to the key amendments to the Act on the Protection of Personal Information, to describe five points that appear to have a particularly large impact on business, based on the contents of the promulgated enforcement rules and regulations.

2.1 Clarification of the definition of personal information: introduction of individual identification codes (amended law, Article 2, Paragraph 2)

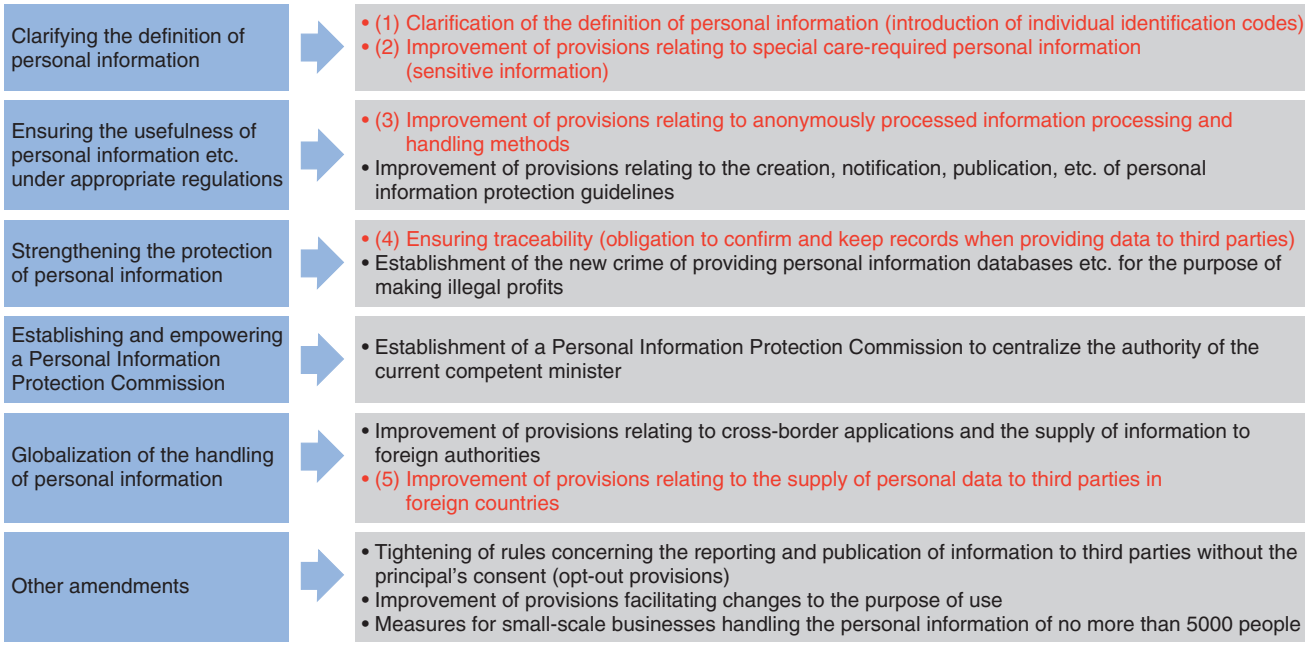
The concept of individual identification codes was introduced as a way of identifying specific individuals in a set of information so that personal information could be referenced without using a person's name or other details. Specifically, it includes biometric information such as fingerprint/face authentication data and vein pattern data, *My Numbers* (social security/tax numbers), passport numbers, driving license numbers, and pension account numbers. For example, an individual set of fingerprint data for authentication stored inside a smartphone or USB (universal serial bus) memory stick with a fingerprint authentication function constitutes personal information, thus making it necessary to check the provisions regarding how this information is handled by businesses.

2.2 Personal information requiring special care (amended law, Article 2, Paragraph 3)

Personal information that must be handled carefully typically comprises information that would be liable to cause discrimination and/or prejudice if mishandled. This includes sensitive information such as the principal's race, creed, social status, and medical history. Since the introduction of this amendment, personal information that must be handled carefully can no longer be handled without consent, so it is necessary to obtain in advance a principal's consent even for simple workplace health questionnaires and the like.

2.3 Anonymously processed information (amended law, Articles 36–39)

The amended law defines anonymously processed information as information that has been processed to make personal information impossible to identify a specific individual, and from which it is impossible to restore this person's personal information, and a system where this information can be distributed subject to certain regulations. When supplying personal information to a third party, it is necessary to obtain the principal's consent, but anonymously processed information has the advantage that the principal's consent does not have to be obtained.



Source: Website of Cabinet Secretariat, bills to the 189th ordinary Diet session, Mar. 2016 (in Japanese).
http://www.cas.go.jp/jp/houan/150310/siryou1.pdf

Fig. 2. Key amendments to the Act on the Protection of Personal Information.

2.4 Ensuring traceability (obligation to confirm and keep records when providing data to third parties) (amended law, Articles 25 and 26)

A service provider that receives personal data from another party is subject to various obligations including confirming the background of what was transferred, and keeping records including the items of information that were transferred, and when the transfer took place. This is intended to ensure that personal information obtained and divulged by illegal means is prevented from circulating endlessly. This requires checking whether an existing contract has been commissioned or has third-party provisions, and if necessary adding log acquisition functions.

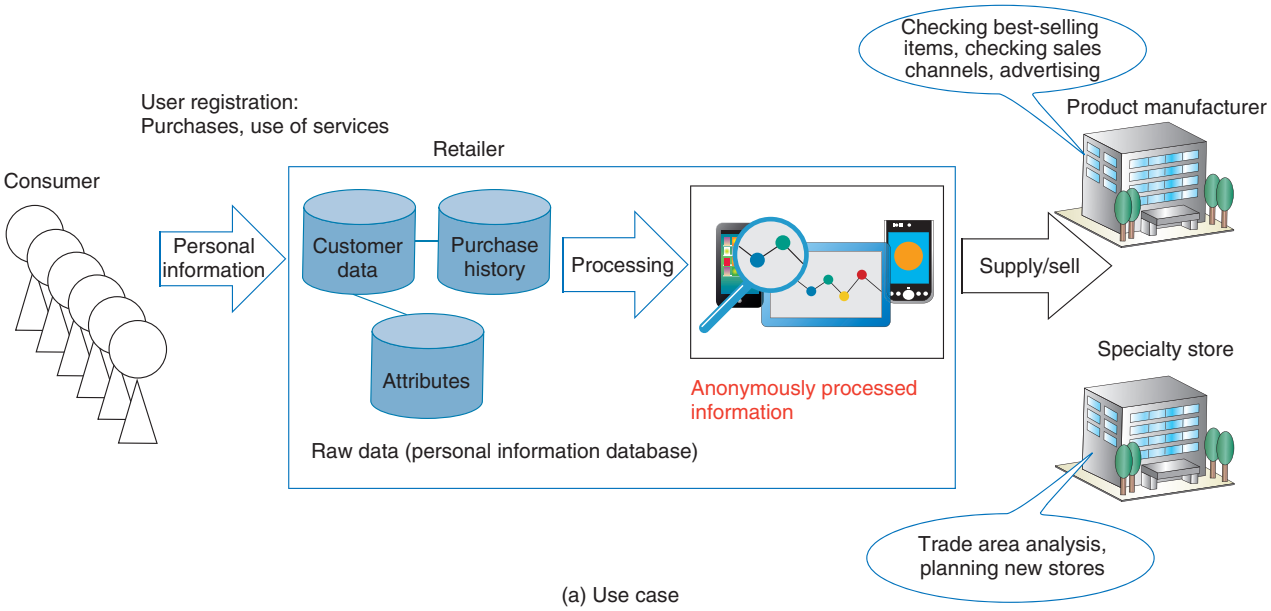
2.5 Provision of personal data to third parties in foreign countries (amended law, Article 24)

A third party in a foreign country is defined as a person or persons (including corporate bodies) located in a foreign country (but not a company's foreign branch offices or the like). When personal data are provided to a third party in a foreign country, it is in principle not possible to do so without the principal's consent. This consent must be obtained even when entrusting employee information to a cloud service provided by a foreign entity. Exceptions to this rule include businesses in countries designated by the Personal Information Protection Commission, and businesses that have been certified based on the APEC Cross Border Privacy Rules (CBPR) system, for which consent is not required [3].

3. Creation of new business through the use of anonymously processed information

Anonymously processed information is information related to an individual that has been processed to protect people's identities from being disclosed. It has the advantage that the principal's consent is not required when the information is provided to a third party, and it is therefore expected that new business will be created to take advantage of this feature.

Some use cases of anonymously processed information are illustrated in **Fig. 3**. When a consumer registers with a retailer in order to access services or purchase goods, the retailer stores raw data such as the consumer's customer data and purchase history. The retailer might choose to process these raw data and supply or distribute the processed data so that other people can use them to identify best-selling items, analyze sales channels, or plan the opening of



(a) Use case

(i) Raw data (personal information)

Customer ID	Registration date (YYYYMM DD)	Name	Address (full address including postal code)	Date of birth (YYYYMM DD)	Gender (male/ female)	Purchase history (date, purchase details)	Where purchased (1: In store, 2: Online)	Payment method (1: Cash, 2: Credit card)	Attribute 1 (home delivery requested)	Attribute ...

Processing

- Delete or replace items that could identify individual customers (names, etc.).
- Round off numerical values, etc.

(ii) Anonymously processed data

Provisional ID	Address (partial address, specifying city and district only)	Age bracket (in 10-year increments)	Gender (male/ female)	Purchase history (year and month, category)	Where purchased (1: In store, 2: Online)	Attribute 1 (home delivery requested)	Attribute ...

(iii) Statistical information

Product category	Purchase amount by age bracket (e.g., monthly sales trends)							
	10s	20s	30s	40s	50s	60s	70 and over	Total amount
Food								
Commodity								

(b) Processing the data set

Fig. 3. Conceptual illustration of anonymously processed information usage.

Table 1. Examples of anonymously processed information methods.

Method	Overview
Deleting items/records/cells	Delete descriptions of personal information included in personal information databases and the like before they are processed.
Generalization	Descriptions included in the information to be processed can be replaced with higher-order concepts or numerical values, and numbers can be rounded to the nearest whole value. For example, *cucumbers* could be replaced with *vegetables* in purchase history data.
Top (bottom) coding	This is the process of especially large values and especially small values in the numerical values being summarized and integrated into a personal information database requiring anonymization. For example, in age-related data, the numerical data for people aged 80 and over should be summarized as "≥80 years" data.
Micro-aggregation	After personal information consisting of a personal information database or the like is grouped together in preparation for anonymization processing, it should be replaced by a representative description of the group.
Data exchange (swap)	The process of anonymizing a personal information database or the like by (randomly) swapping the descriptions and other information included in the personal information constituting the database
Addition of noise (errors)	The addition of random numbers with a certain distribution so numbers can be replaced with other arbitrary values
Pseudo-data generation	The creation of artificially synthesized data and including the data in a personal information database during anonymization processing

new stores. It is possible to use data anonymization for this subject.

Possible ways of processing these data are shown in Fig. 3(b). In table (i), the retail operator manages users according to their customer identifications (IDs) and records each customer's registration date, name, address, date of birth, and gender. Furthermore, each customer ID is associated with information including a purchase history (date, purchase details, amount paid), where purchased (in store, online), payment method (cash, credit card), and whether or not a home delivery service was used. Under the current law, this information might have been provided to product manufacturers in the form of statistical information as shown in table (iii), but one might consider processing these data in such a way that they contain slightly more detail without revealing any personal information.

As in table (ii) above, the information is processed so that it can be used to find out how many products in a particular category were purchased during a particular period, and whether they were purchased in store or online. To avoid identifying individuals, the number of purchases is rounded, and any information that could be used to identify someone (such as their name or address) is deleted. The processed data are expected to be used for marketing purposes such as allowing product manufacturers to check the performance of strong sellers, or finding out if a product category of interest has been accepted into the envisaged customer layer, or whether or not home deliveries are popular.

4. Anonymization methods we have developed

In anonymization processes according to the amended law, personal information is required to be processed so as to make it impossible to identify specific individuals. Since it is very difficult to prove that a specific individual cannot be identified, the guidelines [4] state that in practice, rather than requiring the elimination of all technical possibilities of identifying a person by any means whatsoever, it should at least be impossible for a personal-information-handling business operator or an anonymously processed information-handling business operator to identify a specific individual using ordinary business skills and methods.

Specific methods and standards for anonymization processing are to be determined separately for each industry according to the abovementioned detailed regulations and guidelines. For example, in the anonymously processed information guidelines [4] and the Anonymously Processed Information Creation Manual [5], methods such as top (bottom) coding and noise addition are presented (**Table 1**). In practice, when these methods are used for anonymization processing, it is necessary to study what sort of processing methods should be applied by clarifying the use cases of personal data, and identifying the risks of outcomes such as the identification of individuals by partitioning the data items according to identifiers, attributes, and history.

To use these data for actual business, in addition to ensuring that they are anonymized and do not allow

the identification of individuals, there is also a greater need to process the data so that they can be used effectively. At NTT Secure Platform Laboratories, we have developed an anonymization method based on NTT's own evaluation measure called Pk-anonymity where the evaluation measure of k-anonymity is replaced with a probabilistic measure [6]. This is the first ever method that introduces randomness by stochastic rewriting of item values, which has been mathematically proven to have a level of security equivalent to that of k-anonymity. In anonymization based on Pk-anonymity, the values are stochastically rewritten and are thus different from the original data, but can be processed into data that are statistically close to the original data by using a probability-based method called Bayesian inference. A processing method called generalization is often used in k-anonymization. For example, the word *cucumbers* might be changed to *vegetables* in order to change the level of detail in the data. However, in Pk-anonymization, the data are rewritten without changing the level of detail. For example, *cucumbers* might be changed to *tomatoes*. It is thought that this method could be useful for the analysis of marketing data or the like where people want to see detailed data distributions.

At NTT Secure Platform Laboratories, we are preparing to provide services to tie in with the enforcement of the amended law by continuing to research and develop anonymization methods such as these, by participating in joint research initiatives and verification trials together with businesses that actually use this sort of data, and by taking part in national contests related to anonymization methods in order to gather technical know-how related to the anonymization of diverse types of data.

5. Future prospects

As progress is made with the related guidelines of the amended law and revisions to the Guidelines for Accredited Personal Information Protection Organizations, we also plan to review the provisions related to the protection of personal information by businesses, and to investigate business models that make effective use of anonymized data. In line with current trends in legal systems, we will continue to support the NTT Group in both legal and technical aspects and continue to take part in external activities including academic activities.

References

[1] T. Hioki and Y. Itakura, "Mechanism of the 2015 Amendment to the Act on the Protection of Personal Information," Shojihomu, 2015 (in Japanese).
[2] Personal Information Protection Commission JAPAN, http://www.ppc.go.jp/en/
[3] Personal Information Protection Commission, "Guidelines on Personal Information Protection Law (Provision to a Third Party in a Foreign Country)," 2016 (in Japanese).
[4] Personal Information Protection Commission, "Guidelines on Personal Information Protection Law (Anonymously Processed Information)," 2016 (in Japanese).
[5] Ministry of Economy, Trade and Industry, "Reference Material for Use by Service Providers when Considering Methods for the Creation of Anonymously Processed Information (Anonymously Processed Information Creation Manual) Ver. 1.0," 2016.
[6] "Focus on the News: Development of a New Personal Data Anonymization System for the Big Data Era—Providing Advanced Privacy Protection While Retaining the Data's High Utility Value," NTT Technical Journal, Vol. 26, No. 5, pp. 51–52, 2014 (in Japanese).

Kumiko Kameishi
Senior Research Engineer, Secure Architecture Project, NTT Secure Platform Laboratories.
She received a B.S. and a Master of Environmental Science from University of Tsukuba in 1989 and 1991. She jointed NTT Telecommunication Networks Laboratory in 1991. She is studying information security and privacy issues of personal data services. She is a member of the Information Processing Society of Japan (IPSJ).

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 for Advanced Studies (SOKENDAI), Kanagawa, in 2008. He joined NTT in 1997. His current research interests include security and privacy in information processing, information sharing, and data utilization. He is a member of IPSJ.

Akiko Fujimura
Research Engineer, NTT Secure Platform Laboratories.
She received an LL.B. and a Master of Media and Governance from Keio University, Kanagawa, in 1997 and 1999, and a J.D. from Chuo University, Tokyo, in 2008. She joined NTT Information Sharing Platform Laboratories in 1999 and has been engaged in research on technological and legal issues of information security, personal information protection, and privacy protection.

Fumihiko Magata
Senior Research Engineer, Secure Architecture Project, NTT Secure Platform Laboratories.
He received an LL.B. from Chuo University, Tokyo, in 1992. He jointed NTT in 1992. He is currently studying information security in the interdisciplinary field of social science and information engineering. He is a member of the Japan Society of Security Management and the Information Network Law Association. He is a Professional Engineer (Information Engineering).

Yukiyoshi Ota
Senior Research Engineer, Secure Architecture Project, NTT Secure Platform Laboratories.
He received an M.E. in electrical engineering from Osaka University in 1992 and jointed NTT the same year. He is currently researching information security. He is a member of the Institute of Electronics, Information and Communication Engineers.

Discovery of a Stable Molecular State Consisting of Photons and an Artificial Atom

Shiro Saito, Kosuke Kakuyanagi, Sahel Ashhab, Fumiki Yoshihara, Tomoko Fuse, and Kouichi Semba

Abstract

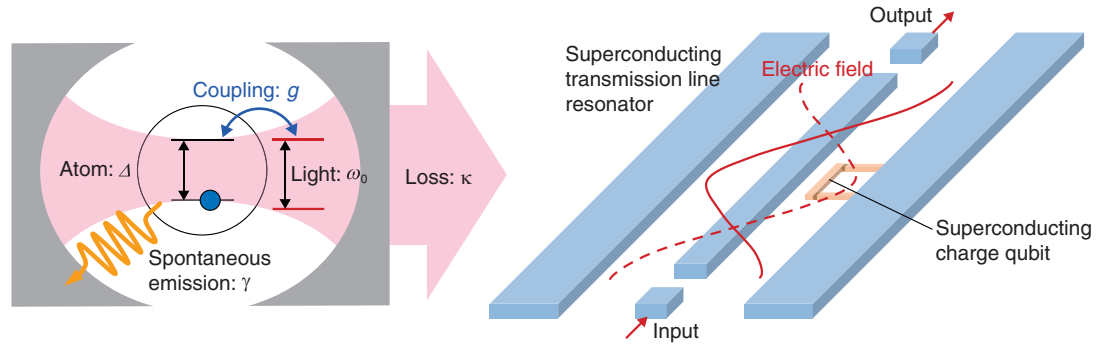
In a joint study with the National Institute of Information and Communications Technology and the Qatar Environment and Energy Research Institute, we have conducted experiments to alter the strength of interactions between a superconducting artificial atom and microwave photons. We have confirmed the existence of a qualitatively new lowest energy ground state where an artificial atom is dressed with virtual photons to form a novel type of molecule. Our research makes it possible to control the interactions between matter and light over a range of energies orders of magnitude higher than has hitherto been possible. This is expected to have applications in quantum technologies including quantum communication, quantum computing, and next-generation ultraprecise atomic clocks.

Keywords: superconducting artificial atom, circuit QED, deep strong coupling regime

1. Introduction

The interaction between atoms and light described by quantum electrodynamics (QED) was first formulated in the early 20th century. By treating light as particles (photons), QED can accurately describe phenomena such as the absorption, emission, and scattering of photons by atoms. At that time, QED treated light in free space, where the light fields are naturally modeled using infinitely extended plane waves. Because the energy of a photon in such a plane wave is spread over a very large volume, the interaction (coupling) strength between atoms and light is extremely small. Researchers are therefore looking at ways of increasing the strength of these interactions by confining light in the space between two opposing mirrors (i.e., a cavity). This will strengthen the coupling of light to an atom situated inside this cavity. This field—which is called cavity QED—has been attracting attention because it allows optical responses to be controlled at a single atom level, which is a fundamental requirement for the implementation of quantum information technologies.

The superconducting quantum bits (qubits) that have been studied with the aim of implementing quantum information technologies in the microwave regime have energy levels resembling those of atoms. For this reason they are called *artificial atoms*. Their greatest advantage is the design flexibility of superconducting circuits, enabling the design of systems where superconducting qubits interact with superconducting resonators. This system, which is called a circuit QED system, can achieve coupling of unprecedented strength between superconducting qubits and microwave photons confined inside a superconducting resonator circuit. Using a circuit QED system, we have successfully demonstrated strong coupling several orders of magnitude stronger than in the optical cavity QED regime. This article introduces the new physical phenomena that we have observed as a result.



(a) Cavity QED

(b) Circuit QED

Weak coupling, Jaynes-Cummings model

$$H_{JC} = \frac{1}{2}\hbar\Delta\hat{\sigma}_z + \hbar\omega_0\hat{a}^\dagger\hat{a} + \hbar g\,(\hat{\sigma}_+\hat{a} + \hat{\sigma}_-\hat{a}^\dagger)$$

Atom Light Coupling

Strong coupling, Rabi model

$$H_{JC} = \frac{1}{2}\hbar\Delta\hat{\sigma}_z + \hbar\omega_0\hat{a}^\dagger\hat{a} + \hbar g\hat{\sigma}_x(\hat{a} + \hat{a}^\dagger)$$

Atom Light Coupling

(c) Hamiltonian

Fig. 1. Quantum electrodynamics and model Hamiltonians.

2. Cavity QED

The simplest model of interactions between atoms and light in QED consists of single-mode (single-wavelength) light interacting with a simple two-level atom. Such a system is thought, however, to be difficult to implement, as it is impossible to confine light to a single mode in free space (space of infinite extent). This led to the idea that if light is confined to a resonator comparable in size to its wavelength, then the wavelength will change from continuum of modes to discrete modes, one of which will be able to interact with the atom. This led to the emergence of cavity QED. These systems are generally classified according to three key parameters: (1) the coupling strength (g) between the atom and light, (2) spontaneous emission rate (γ) from the atom, and (3) loss rate (κ) of light from the resonator (**Fig. 1(a)**). The strong coupling regime is achieved when the coupling strength is greater than the other two parameters ($g > \gamma, \kappa$), while the system is said to be in the weak coupling regime when the converse holds ($g < \gamma, \kappa$). Even in the weak coupling regime, phenomena such as enhanced spontaneous emission from the atom due to coupling with the resonator (Purcell effect) are observed.

In general, interactions between the atom and light are weak, and it is not easy to achieve strong coupling even when using a resonator. A group led by Serge Haroche at the École Normale Supérieure in Paris prepared Rydberg atoms with electrons excited to very large orbitals with principal quantum numbers of n = 50 and 51. Because of the large size of the electron orbitals, the Rydberg atoms had dipole moments some 1250 times greater than that of a single atom, and they were able to couple strongly to the electric field of light. The researchers also reduced the spontaneous emission rate γ from the atoms by using circular electron orbitals with good symmetry and suppressed the loss rate of light κ from the resonator by creating a Fabry-Perot cavity with spherical mirrors made of superconducting niobium with low dissipation. As a result, they entered the strong coupling regime, where photons spontaneously emitted from an atom remain in the cavity and are once again absorbed by the atom. This repeated emission and absorption resulted in a phenomenon called vacuum Rabi oscillation [1]. This showed that it is possible for quantum information in the atoms to be transferred to photons, and vice versa. This property attracted attention as a fundamental technology of quantum information processing. Haroche received the 2012 Nobel Prize in physics in recognition of this achievement and his other contributions in the field.

3. Circuit QED

The basic element of a superconducting quantum

circuit is an LC resonator consisting of an inductor of inductance L and a capacitor of capacitance C. The resonator has equally spaced energy levels, and if its temperature is sufficiently low compared with the level spacing, it is able to exhibit quantized level effects. Since the levels are equally spaced, though, it is not possible to form qubits or artificial atoms using two specific levels. However, by introducing a Josephson junction into the circuit (where it acts as a nonlinear inductance), we can produce a superconducting artificial atom. A Josephson junction has both an inductance component and a capacitance component, and the properties of the artificial atom vary according to the relationship between these components.

Magnetic flux is a good quantum number in a junction with greater inductive energy and produces an artificial atom that is more sensitive to magnetic fields, whereas electric charge is a good quantum number in a junction with greater capacitive energy and produces an artificial atom that is more sensitive to electric fields. The level spacing of superconducting artificial atoms produced in this way covers the microwave band from a few gigahertz to several tens of gigahertz. To enter the strong coupling regime between microwaves and superconducting artificial atoms, the microwaves must be confined inside a superconducting resonator with a strong field (magnetic or electric).

To develop a resonator that works well with superconducting artificial atoms arranged on a two-dimensional chip, we can choose from two types of resonators. One is a superconducting LC resonator consisting of lumped circuit elements, and the other is a distributed superconducting resonator consisting of a half-wave transmission line coplanar waveguide. We should design the superconducting artificial atom to an inductive or a capacitive regime to match the fields produced by each resonator (**Fig. 1(b)**). The most important feature of this system (circuit QED system) is that it is possible to artificially design both the atoms and the resonator, enabling the formation of an ultrastrong coupling regime that has not been possible to achieve in cavity QED.

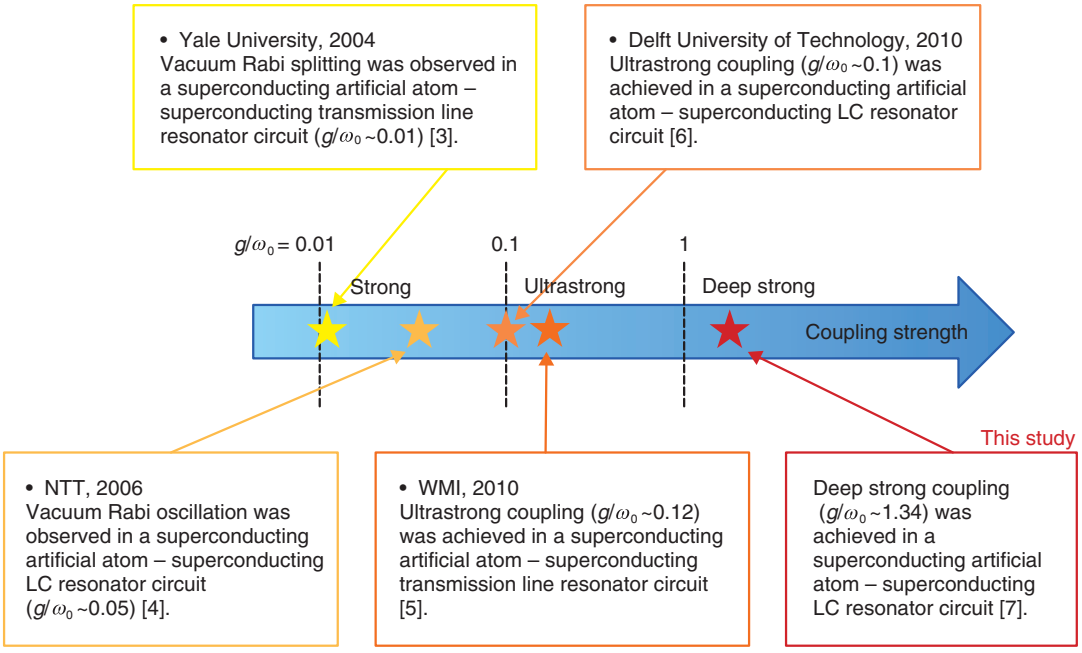
Experiments that paved the way to modern circuit QED were performed independently and almost simultaneously in 2004 at Delft University of Technology and Yale University [2, 3]. The team at Yale University used a charge-type superconducting artificial atom with a coplanar superconducting transmission line resonator to realize strong coupling via an electric field. They observed vacuum Rabi splitting in the resonator's transmission spectrum. At NTT, we observed in 2006 vacuum Rabi oscillations using a magnetic flux type artificial atom coupled to a superconducting LC resonator [4].

These experiments in the strong coupling regime were reproduced well by the Jaynes-Cummings model (**Fig. 1(c)**), but two experiments in the ultrastrong coupling regime that did not satisfy this approximation were reported in 2010 [5, 6]. The spectra could not be reproduced by the Jaynes-Cummings model in the region where the coupling strength g of an artificial atom satisfies the condition $g > 0.1\Delta, 0.1\omega_0$ (where Δ is the atom's transition frequency and ω_0 is its light frequency). In our research, we have further intensified the coupling strength to produce the deep strong coupling regime ($g > \Delta, \omega_0$), and we confirmed the appearance of a new lowest energy ground state [7]. The coupling strengths that have so far been observed in circuit QED are compared in **Fig. 2**.

4. Flux qubits and LC resonators

The sample used in this research is shown in **Fig. 3**. The superconducting artificial atom we used was a flux-type device in which the superconducting current I_P flows anticlockwise |L> or clockwise |R>, while the superconducting resonator was a lumped element LC resonator. Under a suitable magnetic field, a superposition state between |L> and |R> is realized in the superconducting artificial atom, and it behaves as a quantum two-level system. In the superconducting resonator, the amount of stored energy is determined by the magnitude of the alternating current flowing in the loop, and the addition of each individual microwave photon excites the resonator in its equally spaced energy levels given by the resonant frequency. The alternating current in the resonator when there are zero microwave photons (vacuum state) is called the zero-point fluctuation current (I_{ZPF}). The artificial atom and the superconducting resonator are coupled via a magnetic field with coupling strength g. The coupling strength is expressed as the product of the coupling inductance L_C, I_P, and I_{ZPF}.

Unlike a charge-type artificial atom that couples to a resonator via electric fields, a flux-type atom can share the coupling inductance between the artificial atom and resonator, which makes it possible to take full advantage of L_C. When a Josephson junction is used as the coupling inductance, it is possible to achieve a much larger coupling inductance than with



WMI: Walther-Meißner-Institute for Low Temperature Research

Fig. 2. History of coupling strength in circuit QED.

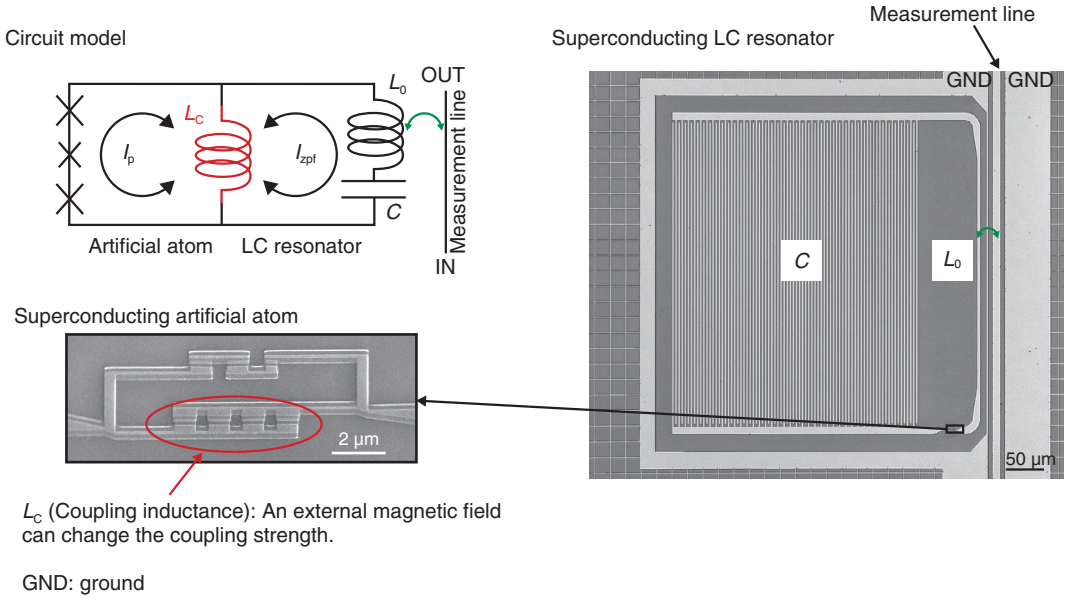


Fig. 3. Superconducting artificial atom – LC resonator coupled system.

a conventional linear circuit. On the other hand, when the resonator is designed with a small L_0 and large C (Fig. 3), it is possible to increase I_{ZPF} while keeping the resonant frequency constant. In this way, by making use of the flexibility in circuit design (a major feature of superconducting circuits), we produced a

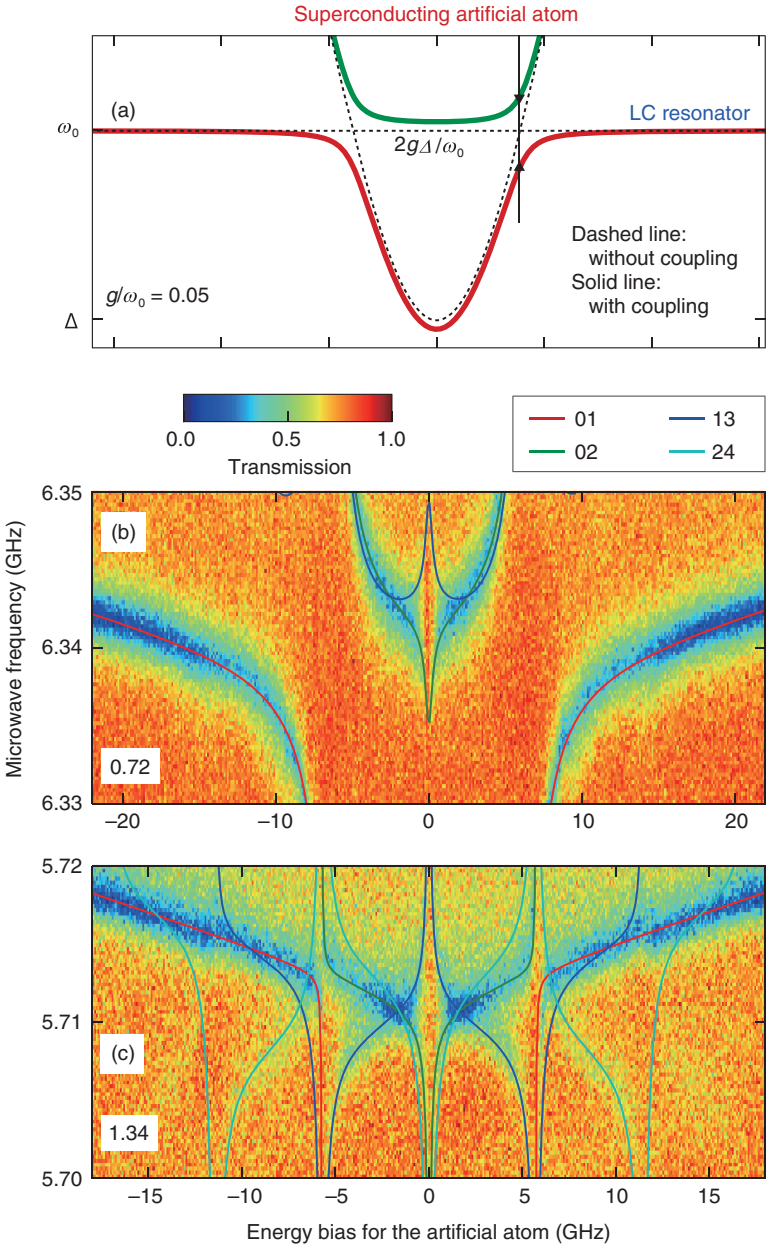
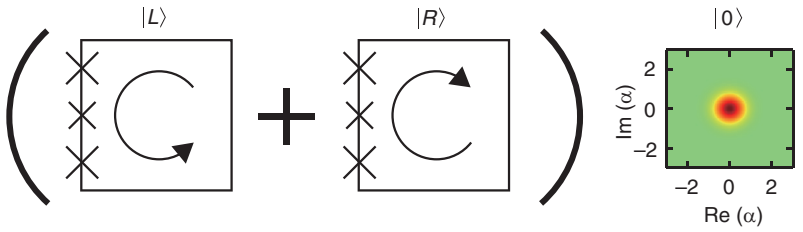


Fig. 4. Transmission spectra for the coupled system.

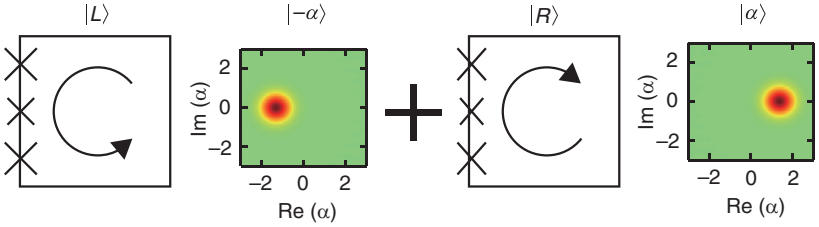
sample operating in the deep strong coupling regime.

5. Confirmation of deep strong coupling regime

In a system where a superconducting artificial atom and LC resonator are strongly coupled, anti-crossings of the energy levels (vacuum Rabi splitting) are observed at points where the transition energies of the two are equal (**Fig. 4(a)**). The size of these anti-crossings $2g\Delta/\omega_0$ represents the effective coupling strength. To measure the energy levels in this study, we measured the transmission characteristics of a microwave waveguide inductively coupled to the LC resonator (**Figs. 4(b)(c)**). At frequencies corresponding to the spacing between any two energy levels, absorption takes place and the microwave transmission intensity decreases. In Fig. 4(b), the vacuum Rabi splitting was observed and the signal disappeared at zero energy bias. In contrast, in Fig. 4(c), complex energy levels were observed including a



(a) Typical lowest energy state (ground state)



(b) New ground state: atom and light are entangled

Fig. 5. Energy ground state of the coupled system.

reduction of the vacuum Rabi splitting. These energy levels are well reproduced by simulations based on a model that does not use a rotating wave approximation (Fig. 1(c)). From the theoretical fits, the values of g/ω_0 are obtained respectively to be 0.72 and 1.34 for Figs. 4(b) and (c), indicating that the circuits are in the deep strong coupling regime.

At the point where the artificial atom has zero energy bias, the ground state of the uncoupled circuit is expressed as the product $(|L\rangle + |R\rangle)|0\rangle$ of the artificial atom's ground state $|L\rangle + |R\rangle$ and the resonator's vacuum state |0>. However, the ground state in the deep strong coupling regime is expected to be an entangled state (**Fig. 5**) of $|L\rangle|-\alpha\rangle + |R\rangle|\alpha\rangle$ (where $|\alpha\rangle$ and $|-\alpha\rangle$ are the microwave photon coherent states). Our numerical simulations reproduced these complex energy level structures very well, suggesting the existence of entanglement between the artificial atom and microwave photons. By measuring the artificial atom in a suitable way, we should be able to create a macroscopic microwave photonic superposition state (Schrödinger's cat state; $|-\alpha\rangle + |\alpha\rangle$) from this entangled state. This state has the degrees of freedom of multiple photons and is expected to have applications including noise-resilient quantum computing and precise frequency measurements.

6. Future prospects

In this research, we achieved an entangled state between a single superconducting artificial atom and microwave photons in the deep strong coupling regime. According to some theoretical studies, a similar ground state may not occur in the deep strong coupling regime for multiple artificial atoms and photons. Hence in the future, we plan to verify this theory by increasing the number of artificial atoms. Also, to improve the quantum state control techniques for quantum communication node technology and to achieve better control of ground states in multi-body systems, we plan to continue with research aimed at improving the techniques for manipulating these entangled states and clarifying the dynamics of light absorption and emission.

References

[1] M. Brune, F. Schmidt-Kaler, A. Maali, J. Dreyer, E. Hagley, J. M. Raimond, and S. Haroche, "Quantum Rabi Oscillation: A Direct Test of Field Quantization in a Cavity," Phys. Rev. Lett., Vol. 76, No. 11, pp. 1800–1803, 1996.

[2] I. Chiorescu, P. Bertet, K. Semba, Y. Nakamura, C. J. P. M. Harmans, and J. E. Mooij, "Coherent Dynamics of a Flux Qubit Coupled to a Harmonic Oscillator," Nature, Vol. 431, pp. 159–162, 2004.

[3] A. Wallraff, D. I. Schuster, A. Blais, L. Frunzio, R.-S. Huang, J. Majer, S. Kumar, S. M. Girvin, and R. J. Schoelkopf, "Strong Coupling of a Single Photon to a Superconducting Qubit Using Circuit Quantum Electrodynamics," Nature, Vol. 431, pp. 162–167, 2004.

[4] K. Semba, "Entanglement Control of Superconducting Qubit Single

Photon System," NTT Technical Review, Vol. 6, No. 1, 2008.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200801sp6.html
[5] T. Niemczyk, F. Deppe, H. Huebl, E. P. Menzel, F. Hocke, M. J. Schwarz, J. J. Garcia-Ripoll, D. Zueco, T. Hümmer, E. Solano, A. Marx, and R. Gross, "Circuit Quantum Electrodynamics in the Ultrastrong-coupling Regime," Nat. Phys., Vol. 6, pp. 772–776, 2010.
[6] P. Forn-Díaz, J. Lisenfeld, D. Marcos, J. J. García-Ripoll, E. Solano, C. J. P. M. Harmans, and J. E. Mooij, "Observation of the Bloch-Siegert Shift in a Qubit-oscillator System in the Ultrastrong Coupling Regime," Phys. Rev. Lett., Vol. 105, No. 23, pp. 237001-1–4, 2010.
[7] F. Yoshihara, T. Fuse, S. Ashhab, K. Kakuyanagi, S. Saito, and K. Semba, "Superconducting Qubit-oscillator Circuit beyond the Ultrastrong-coupling Regime," Nat. Phys., Vol. 13, pp. 44–47, 2017.

Shiro Saito
Distinguished Researcher/Senior Research Scientist, Supervisor, Hybrid Nanostructure Physics Research Group, Physical Science Laboratory, NTT Basic Research Laboratories.
He received his B.S., M.S., and Dr.Eng. in applied physics from the University of Tokyo in 1995, 1997, and 2000. In 2000, he joined NTT Basic Research Laboratories, where he has been engaged in quantum information processing using superconducting circuits. He was a guest researcher at Delft University of Technology in the Netherlands from 2005–2006. He has been a guest associate professor at Tokyo University of Science since 2012. He was appointed a Distinguished Researcher of NTT in 2012. He received the Young Scientist Award from the Japan Society of Applied Physics (JSAP) at the Spring Meeting in 2004. He is a member of the Physical Society of Japan (JPS) and JSAP.

Kosuke Kakuyanagi
Senior Research Scientist, Hybrid Nanostructure Physics Research Group, Physical Science Laboratory, NTT Basic Research Laboratories.
He received his B.S., M.S., and Ph.D. in science from Hokkaido University in 2000, 2002, and 2005. He joined NTT Basic Research Laboratories in 2005 and has been studying superconducting qubits. He is currently engaged in an experimental study of a Josephson bifurcation readout method. He is a member of JPS and JSAP.

Sahel Ashhab
Senior Scientist, Theory, Modeling and Simulation Group, Qatar Environment and Energy Research Institute (QEERI), Hamad Bin Khalifa University, Qatar Foundation.
He received a B.S. in physics from the University of Jordan in 1996 and an M.S. and Ph.D. in theoretical condensed-matter physics from the University of Illinois at Urbana-Champaign, USA, in 1998 and 2002. From 2002 until 2004, he was a postdoctoral researcher at the Ohio State University, USA. From 2004 until 2013 he was a research scientist at RIKEN, Saitama, Japan. He moved to QEERI in 2013. He researched Bose-Einstein condensation in cold atomic gases during his Ph.D. and postdoctoral work and is currently conducting theoretical studies on quantum phenomena in various types of electric circuits.

Fumiki Yoshihara
Senior Researcher, Advanced ICT Research Institute, National Institute of Information and Communications Technology (NICT).
He received his B.S., M.S., and Ph.D. in engineering from Kyoto University in 1998, 2000, and 2003. He was a research scientist at RIKEN from 2003 until 2014. He moved to NICT in 2014. His research interests include superconducting artificial atoms and superconducting circuit quantum electrodynamics.

Tomoko Fuse
Senior Research Scientist, Advanced ICT Research Institute, National Institute of Information and Communications Technology (NICT).
She received her B.S., M.S., and Ph.D. in science from Kyoto University in 2002, 2004, and 2007. She was a research scientist at Delft University of Technology from 2007 until 2010 and at RIKEN from 2010 to 2014. She joined NICT in 2014. Her past work includes doing research on quantum dots in carbon nanotubes and semiconducting nanowires. She is currently studying superconducting qubits in circuit quantum electrodynamics.

Kouichi Semba
Executive Researcher, Advanced ICT Research Institute, Frontier Research Laboratory, National Institute of Information and Communications Technology (NICT).
He received a B.S. and M.S in science, and a Dr.Eng. in applied physics from the University of Tokyo in 1983, 1985, and 2002. In 1985, he joined NTT Electrical Communication Laboratories in Ibaraki, Japan. In 1987, he moved to NTT Basic Research Laboratories. During 2002–2003 he was a visiting researcher at the Quantum Transport Laboratory at Delft University of Technology in the Netherlands. Upon returning to NTT and until 2012 he was the leader of the superconducting quantum physics research group. He has also been a lecturer at Waseda University (2005), a Guest Professor at Tokyo University of Science (2008–2012), at the National Institute of Informatics (2010–2012), and at Osaka University (since 2017). In 2013, he joined NICT as an Executive Researcher. He is a member of JPS, JSAP, and the American Physical Society.

Creating a New Ecosystem for NFV/SDN Technical and Business Development: the Challenge of NTT Laboratories and Dimension Data APAC

Akeo Masuda

Abstract

Network functions virtualization and software-defined networking are changing the process of turning technology into commercial services, including the process of standardization. With this development, collaboration with other service providers in commercializing new technologies and the role of integrators are both growing in importance, especially as the granularity of functional components becomes ever smaller. This article introduces the NTT Information Network Laboratory Group's activities in promoting global deployment of NTT research results through collaboration with Dimension Data, one of the NTT Group integrators.

Keywords: network functions virtualization, software-defined networking, network architecture

1. Standardization activities in the process of network system development

For decades, the NTT laboratories have borne responsibility for research and development (R&D) of network systems that provide the infrastructure for various services such as voice, video, Internet access, and enterprise services.

In addition to creating new technologies, the laboratories had been engaged for many years in international standardization, a critical process to ensure successful commercialization of developed technologies. The importance of standardization includes ensuring interconnectivity between different networks, promoting implementation of new technologies by vendors, and enabling service providers to procure equipment and software products stably and at low cost. Even if NTT has developed remarkable technologies, the implementation of those technologies will be very expensive if they are used only at NTT. Unless the technology concerned is key to the carrier's service differentiation, it is beneficial to standardize the technology because this will lead to many service providers adopting common methods and specifications. This will in turn increase the demand for the product and reduce the product cost thanks to economies of scale, enabling service providers to lower their service charges or to make their operations more profitable.

Defining the functional structure of a system and standardizing the functionality of each functional component and the interconnections between them (modularization) enable vendors to develop products with highly specific functionality. This facilitates entry of vendors skilled in a particular field into the market, thereby expanding the alternatives of vendors available to service providers. A wider range of alternatives not only promotes competition, which results in a drop in prices, but also reduces carriers' dependence on specific vendors, making stable procurement

possible.

For a long time now, standards bodies such as the ITU (International Telecommunication Union), IEEE (Institute of Electrical and Electronics Engineers), and 3GPP (3rd Generation Partnership Project) have developed standards that have served as the foundation for various telecommunication services. Of course, they continue to play an important role, but the role each organization plays in each technical field and the standardization process each adopts have been changing. From the late 1990s to the 2000s, the Internet protocol (IP) became mainstream. It has been widely adopted as a common technology for linking the service layer with the transmission layer. Most of the technologies for IP were standardized by the IETF (Internet Engineering Task Force) through the leadership of US vendors. The result was that the functions for IP networks are concentrated in big boxes called routers and that the router market is dominated by a small number of major vendors. Service providers around the world have had no other choice but to depend on products from these vendors (vendor lock-in).

2. Standardization in the age of network functions virtualization and software-defined networking

The late 2000s saw web technology and cloud computing gain a strong foothold, raising demand for datacenter networks. Cloud providers such as Google and Facebook began to question the conventional ways of procuring and operating network devices. As the 2010s dawned, there was a giant shift in technology to software-defined networking (SDN) and network functions virtualization (NFV). In a word, they represent attempts to re-examine the way network functions are structured, and to open up and standardize the interfaces between functions. The aim is to split the dedicated devices such as large routers into smaller functional units. When this is achieved, software functions for routing, for example, do not necessarily have to run on a large router but can run on a far less expensive general-purpose server. As the functional requirements for each device become smaller, barriers to market entry become lower. Even hardware functions such as packet transfer will eventually become commoditized.

Standardization is still important for realizing NFV/SDN. It is necessary to determine how each functional entity should be split into functional units (architecture) and how these functional units should be interconnected. Standardization of these has been driven by the ONF (Open Networking Foundation) and ETSI (European Telecommunications Standards Institute). Alongside these activities, a different approach has risen. So-called *open communities*, in which service providers and vendors cooperate in developing products up to the stage of implementation and make the result open to the public, have gained more importance. When the granularity of functions is low, a wide variety of functional combinations becomes feasible. This poses a danger, as it could lead to greater complexity for users, making it difficult for them to choose a solution.

To avoid this, it has become important to implement and operate functions for trial purposes. In the last two years, several open communities have been founded to address technologies for carriers. These communities include the OPNFV (Open Platform for NFV), OSM (Open Source Management and Orchestration), CORD (Central Office Re-architected as a Datacenter), OCP (Open Compute Project) Telecom Project, and the Telecom Infra Project. One of the characteristics of these organizations is that their operation is mainly led by service providers in the US and Europe such as AT&T, Deutsche Telekom, and Telefonica. The lowering of the entry barrier will encourage many vendors to enter the market. This will in turn raise the relative influence of the purchasers, that is, service providers.

Because each service provider has a different history, capability, and market according to their regional characteristics, sometimes their directions and the requirements for the demanded technologies become diverse. If one desires to let their direction become the mainstream and to encourage many vendors to implement it, it needs to work with other service providers to develop a mutually agreed upon idea, thereby increasing the demand for products that implement it. This means that it has become more important than ever for service providers to cooperate in the phase of creating the vision and developing the technologies.

3. Role of R&D in expanding global business

In recent years, the NTT Group has been pressing forward with efforts to expand global business. As the domestic market matures and the population of the country gradually declines, it seems only natural that NTT has been seeking to grow by changing its business models in Japan, for example, the previously announced Hikari Collaboration Model, and by

expanding its global business. This change means that the direction NTT's R&D should take has had to be re-examined. The commonly accepted marketing strategy recommends that R&D investment be focused on an emerging market where participants compete to gain an initial share rather than to a mature market where each competitor's market share is more or less stable. R&D in the networking area does not necessarily need to adhere to this principle because this R&D function has the continuous mission to support the operation of efficient and stable infrastructure.

However, if network-related R&D is to assert its raison d'être in the midst of extensive use of general-purpose technologies and the ever-growing trend of outsourcing telecom infrastructure operation, it must look at new activities in new fields. A question that arises from this new approach is how network R&D can contribute to the expansion of NTT's global business. A clue lies in the future direction chosen by system integrators.

As NFV/SDN accelerates modularization of devices, the role of integrators in selecting appropriate components and assembling them in such a way that they operate correctly will grow in importance. Dimension Data (DD), one of the NTT Group integrators, ensures that information technology (IT) business strategy evolves in four stages [1]. It envisages that IT business will shift from the first stage: great technology (product delivery), to the second stage: technology attached services (deploy and support), then the third stage: consulting and managed services, and finally to the fourth stage: platform services, where everything is provided, including the software/hardware resources, as a service based on a volume charging model. This can also apply to business for telecom service providers. Many service providers have already begun to outsource the operation of their networks, and new service providers have emerged who wish to run their business without the ownership of equipment as their asset.

Amid this market trend, network R&D can seek its value proposition in leading to establish the right NFV/SDN architecture, defining the common specifications that fit into this architecture, and transferring these technologies to NTT Group integrators. A commonly employed architecture can lead to many service providers choosing products that support common specifications. When this happens, an integrator with high technical expertise in this field can seize many business opportunities in consulting, delivery, and support of network systems at a large number of clients. Furthermore, because the technologies are common, such an integrator can offer the outsourced operation of multiple telecom infrastructures within the region. Operating multiple networks leads to improved efficiency, and it will make it much easier to provide various functions as a platform. A key to achieving this is to establish the right architecture and have it used by many service providers. It should be noted that only R&D organizations are able to, and are expected to, take on these tasks.

4. NetroSphere concept

In 2015, the NTT Information Network Laboratory Group announced the NetroSphere concept [2] in order to push the development of NFV and SDN and to advocate the future direction beyond them. In the long term, this concept is aimed at modularization at much higher granularity compared to what current NFV/SDN looks for. In the short term, we are developing an overall architecture that will enable carrier networks to use general-purpose products, and technologies that will ensure reliability and scalability—the two properties still lacking today—in order to make what NFV/SDN is intended to achieve a reality [3].

In the development of technologies based on this concept, it is important to actively participate in open communities such as those mentioned above, collaborate with service providers throughout the world to create greater demand for the technologies, and enlist the participation of integrators, who assemble components. To do this, since the announcement of the concept, the Information Network Laboratory Group has had discussions with service providers, vendors, and integrators in Europe, the US, and Asia. In order to execute these initiatives effectively, we have started a new type of engagement with Dimension Data Asia Pacific (DDAP) since 2016.

5. Collaboration with DDAP

DD is a global enterprise that became a member of the NTT Group in 2010. They have five business regions: Europe, North America, Asia and the Pacific (APAC), the Middle East and Africa, and Australia.

There are several reasons why we have selected the Asia region (Southeast Asia, India, and New Zealand) for collaboration with other service providers and for future business engagement and why we have begun to cooperate with DDAP. First, this is one of the markets where the greatest growth is expected. The

demand for renewal of the infrastructure is expected to rise. Moreover, many service providers have just begun to formulate an overall architecture for such updates, and we will be able to find partners that are keen to explore the new technologies there. Second, this region is simply close to Japan. Although many forms of communication are available today, the fact that travel distance is short and time differences are small makes it easy to cooperate. Lastly, people in this region have a certain level of respect for Japanese culture and technologies. It helps to establish communication by developing a relationship based on mutual trust with people in this region who actually tune in to what we are doing, hoping to learn from Japan.

Our collaboration with DDAP targets two areas: development of inter-service provider partnerships and new business opportunities.

(1) Activities to find service provider partners in APAC region

We meet with our service provider clients together in order to introduce the NetroSphere concept, exchange opinions, and propose collaboration. DDAP's client base includes many service providers with which the NTT laboratories have had no contact in the past. Furthermore, this engagement enables us to meet people involved in decision making on technical direction and procurement that the laboratories usually do not have any contact with. In addition, the involvement of local sales teams facilitates the communication with our partners.

In general, one of the challenges in conducting business overseas is determining how to overcome barriers in language, culture, and business practices. A look at existing global business successfully conducted by telecom service providers reveals that they target regions to which they are closely related culturally and linguistically. For example, German service providers typically aim at East Europe, French service providers target Africa, and Spanish service providers focus on South America. These are the regions where these countries were formerly colonial powers; hence historic, cultural, and linguistic links already exist.

I have heard stories that the NTT Group has also tried many times to explore business based on R&D achievements targeting Southeast Asia but encountered difficulty in communicating directly with customers there, so had little success. We hope to overcome such barriers through support provided by DDAP's local sales experts in communicating and establishing effective connections with the clients.

(2) Technical collaboration for developing new businesses

To promote widespread use of our technologies and turn them into business opportunities, it is necessary to have service providers understand the applicability and the benefits of these technologies. For this, we need to transfer the technologies to DDAP so that they themselves can propose, deliver, and support our technologies. It is also important for NTT laboratories to understand the management strategy and requirements of those service providers and enhance the applicability of the technologies that we are planning to propose. For this purpose, we have established a Network CoE (center of excellence) where we can conduct proof of concept (PoC)* demonstrations in collaboration with client service providers using DDAP's facilities. Through these efforts to verify promising technologies and vendor products together with clients, DDAP aims to strengthen the relationship with its clients, expand its ability to propose new technologies, and develop new businesses based on NTT laboratories' technologies. The NTT laboratories, for their part, hope to strengthen their presence in the world by taking the results achieved in this region and transferring them to the rest of the world as field-verified technologies from Asia.

6. Future prospects

As DDAP responds to rapid progress in technology and implements reforms of its business model, it has high expectations for collaboration with NTT laboratories in their sales activities targeting service providers. The NTT laboratories, for their part, take this as a good opportunity to explore a new approach to conducting R&D in collaboration with integrators within the NTT Group and to study ways of commercializing R&D results. As part of this effort, the author has been stationed at the DDAP Head Office in Singapore since August of 2016 and has been engaged in the above-mentioned activities that involve making proposals to service providers and establishing the Network CoE. We will intensify collaboration between the two organizations and move steadily forward in the hope of contributing to the development of the NTT Group in both R&D and business.

* PoC: Here, PoC means a field trial or verification that service providers generally conduct when they seek to employ new technologies.

References

[1] J. Goodall, “Dimension Data—The Transformational Journey,” Oct. 2015.
www.ntt.co.jp/ir/library_e/presentation/2015/151002_2.pdf

[2] Press release issued by NTT on February 19, 2015.
http://www.ntt.co.jp/news2015/1502e/150219a.html

[3] Feature Articles: Initiatives for the Widespread Adoption of Netro-Sphere,” NTT Technical Review, Vol. 14, No. 10, 2016.
https://www.ntt-review.jp/archive/2016/201610.html

Akeo Masuda
Senior Manager, NTT Network Service Systems Laboratories / Dimension Data APAC.

He received a B.S. from the University of Tokyo in 1997, and an M.S. and Ph.D. from Waseda University, Tokyo, in 2006 and 2009. He joined NTT Network Service Systems Laboratories in 1997 and is currently engaged in planning and developing strategies for global collaborative development of NFV & SDN related technologies. His role at Dimension Data APAC is to create a new ecosystem among service providers, system integrators, and vendors in order to bring emerging technologies to reality. In his 20-year career in the telecommunications industry, he has achieved both academic results and system development concerning software engineering, content delivery networks, IP quality of service, IP-optical networking, network virtualization, SDN, inter-domain routing, and wireless access protocols.

Event Report: NTT R&D Forum 2017

Yojiro Nishiyama, Hiroto Ishii, Yuji Uekusa, Haruhisa Nozue, Kazushi Maruya, and Ryuji Yamamoto

Abstract

NTT held NTT R&D Forum 2017, an annual event, at NTT Musashino Research and Development Center from February 13 to 17, 2017 (with February 13 and 14 reserved for press tours and NTT Group company employees) under the theme "Open the Way—Towards 2020 and Beyond." This article reports on this five-day event.

Keywords: R&D Forum, information transmission, innovation

1. Overview of the forum

The NTT Group is making an all-out effort to become a *value partner* that will continue to be preferentially selected by customers. At NTT R&D Forum 2017, lectures and exhibits were presented on the latest research and development (R&D) results that support this effort. Specifically, the forum introduced in an easy-to-understand manner technologies related to artificial intelligence (AI), the Internet of Things (IoT), security, cloud computing, and networks, as well as other technologies that will shape the world in 2020. The forum was attended by both domestic and overseas customers of the NTT Group, staff members of partner companies, IR (investor relation) stakeholders, and people from government agencies and universities.

2. Lectures and workshops

In his keynote address entitled "Generating New Value with xICT—Advancing B2B2X Business—" on February 15, Hiroo Unoura, NTT President and CEO, talked about advances in the business-to-business-to-X (B2B2X) business model, and the NTT Group's activities related to IoT and the use of big data.

He remarked on the imminent arrival of the age of IoT and big data, in which hitherto impossible data analysis would be made feasible by applying advanced machines and AI to the gigantic volume of data generated by IoT. He pointed to one of the directions this age could take, where municipalities would act as a hub of the initiatives to create data collection mechanisms and to formulate rules that ensure the safe and secure use of data so that the whole of society would be able to share and use this wealth of information. As specific examples of activities undertaken by the NTT Group and municipalities, President Unoura introduced collaborations with Fukuoka City and Sapporo City, and R&D on security and information processing technologies. In addition, he stated that the time is ripe for NTT to "contribute to the creation of a safe, secure, and prosperous society through communications that serve people, communities, and the global environment," which is a mission statement in the NTT Group CSR Charter formulated in 2006. He also said that the NTT Group will be dedicated to transforming itself into a next-generation business (**Photo 1**).

President Unoura's keynote address was followed by another keynote address from Hiromichi Shinohara, NTT Senior Executive Vice President and Head of the R&D Strategy Department, under the title of "NTT R&D—Leading the Way to B2B2X." He said that NTT is aiming for AI that augments and draws forth latent human abilities. Specifically, NTT is working on four types of AI: Agent-AI, Heart-Touching-AI,

Photo 1. Keynote address by Hiroo Unoura, President and CEO, NTT.

Photo 2. Keynote address by Hiromichi Shinohara, Senior Executive Vice President and Head of R&D Strategy Department, NTT.

Ambient-AI, and Network-AI. With regard to IoT, NTT will use technologies represented by such keywords as *natural*, *reassuring*, and *real-time* to develop what NTT calls Sentient-IoT, which signifies IoT with sensing capabilities. NTT's effort to provide hospitality-related services geared for 2020 has evolved from concept testing in the laboratory to field trials. He noted that NTT is actively collaborating with partners to create new value through the use of ICT (information and communication technology) (**Photo 2**).

On the following day, February 16, two workshops were held. Kazuhiko Okubo, Vice President and Head of NTT Security Platform Laboratories, gave a lecture entitled "Innovative Technology to Stay One Step Ahead of Cyber Menaces that will Spread in the IoT Era When Conventional Measures Are No Longer Effective." He reviewed cybersecurity issues in the conventional information technology (IT) fields, described new threats in the nascent fields of operational technology and IoT, and introduced NTT's R&D activities to counter these threats. Hiroyuki Kazama, Head of Research and Development Headquarters, and Head of NTT DATA's Evolutional IT Center, gave a lecture entitled "Accelerating Innovation with NTT DATA R&D." He presented the three main foci of his company's R&D activities, which can be represented by the words *foresight*, *co-creation*, and *incubation*. These activities are aimed at achieving continuous innovation in collaboration with customers through the use of IT. He gave specific examples to illustrate these activities.

In the workshop held on February 17, Shingo Tsukada, Senior Distinguished Researcher, NTT Basic Research Laboratories, delivered a lecture entitled "Challenges of Using "hitoe" Sensing Fabric as a Wearable Vital Signs Sensor in Medical, Worker Safety, and Sports Applications." Dr. Tsukada explained the wearable sensing fabric "hitoe," beginning with its development history and going on to its technical features and fields of application, citing some specific examples. He also discussed the prospects for future research activities.

On the same day, Hiroshi Ishiguro, Professor, Department of Systems Innovation, Graduate School of Engineering Science, Osaka University, and Visiting Director of ATR Hiroshi Ishiguro Laboratories, gave a special lecture entitled "Fundamental Issues of Interactive Androids." Anticipating the coming robot society, he discussed the requirements for and the basic issues of androids that interact with humans, from two perspectives: "What is the sense of presence?" and "What is a dialogue?" He gave a number of illustrative examples (**Photo 3**).

Those attending the lectures seemed to be favorably impressed by the R&D activities introduced by these speakers.

3. Exhibition of research results and topical sessions

Also presented at the forum were demonstrations and panel exhibits of R&D results on 97 different topics, including four exhibits from NTT DOCOMO,

Photo 3. Special lecture by Hiroshi Ishiguro, a professor at Osaka University and Visiting Director of ATR Hiroshi Ishiguro Laboratories.

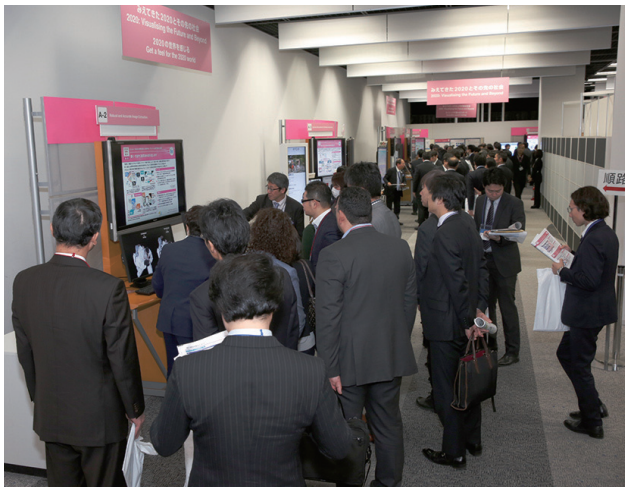


Photo 4. 2020: Visualizing the future and beyond.

four from NTT DATA, and three from NTT i^3.

NTT seeks to create innovation based on new concepts and to bring about the transformation of society by collaborating with a wide range of partners. To enable visitors to the forum to experience "Open the Way," our concept of exploring a new world through the above efforts, the exhibition was classified into five areas: "2020: Visualizing the future and beyond," "corevo®—Evolving the generation of new values," "IoT and security for the next-generation business," "Networks for the coming 2020 and beyond," and "Basic research exploring the future." We also tried out a new form of exhibit in an outdoor venue to provide the "Interactive technology experience."

3.1 2020: Visualizing the future and beyond

The forum exhibited prototypes to enable visitors to get hands-on experience with how various technologies can be applied in 2020 and beyond. Related technologies were also introduced (**Photo 4**).

(1) Get a feel for the 2020 world

There were exhibits of technologies, in particular the immersive telepresence technology "Kirari!®," that can reproduce events taking place at remote sites with a high sense of reality. These technologies transmit video footage of a sports event or a live entertainment event to a remote site in such a way that people watching the video can feel a sense of unity with the spectators or the audience at the actual event site and share their excitement in real time, thereby transcending the barriers of geography.

(2) Japanese hospitality in the future

At the forum, we offered an official smartphone app that provides a number of services: a navigation service that enables users to create a personal time-effective route plan and obtain a walking route based on their interests and the computed degree of congestion at the forum site; a point-and-search guidance service that combines multiple recognition technologies that are tailored for the characteristics of the search target object; and a bot concierge service that generates answers to questions about specific exhibits. At the center of the forum site, which has a vaulted ceiling, there were directional signs to guide streams of people based on the degree of congestion. On the second floor, the Sky Compass provided navigation from above using a drone. Additionally, the "corevo for Reception" service recommended exhibits to visitors by speaking to them. Thus, the visitors were able to experience various technologies that can be used at public facilities such as airports, railway stations, and stadiums, as well as on the street and at entertainment events.

(3) Innovative sports training

We are working to elucidate the unconscious (implicit) brain functions that enable athletes to gain skills, and the state of mind needed for winning in sports, and to improve these in order to enhance athletic performance. We are integrating multiple sports research approaches such as measuring sports behavior and precisely evaluating brain functions. The forum introduced the sports brain science project, which embraces these activities and provides feedback to athletes.

Photo 5. corevo®—Evolving the generation of new values.

Photo 6. IoT and security for the next-generation business.

3.2 "corevo®"—Evolving the generation of new values

In recent years, AI has been attracting attention in a wide range of fields. The NTT Group's AI technology "corevo®," which can become an engine for accelerating the creation of new value, was presented in the forum (**Photo 5**).

(1) AI making life more comfortable

"corevo for Drivers" was a conceptual demonstration of how interactions with various AI technologies can assist a person in concentrating on driving safely and comfortably. Heart-Touching-AI provides a service that cares for a person's physical and psychological well-being. Ambient-AI provides navigation that combines a variety of information. Agent-AI makes it possible for a system to conduct a natural dialogue with the user by understating his/her intention.

(2) AI supporting people

We are aiming at a world in which people can share and use a variety of devices connected to a network. This will be achieved by tacit computing, a concept in which Network-AI understands the value of all sorts of devices owned by individuals and organizations and finds devices useful for the user at present and connects them to him/her.

3.3 IoT and security for the next-generation business

We exhibited cutting-edge IoT technologies that are at the forefront of IoT evolution and security technologies, both of which enable us to support the businesses of our customers as their value partner (**Photo 6**).

(1) IoT: Sense and digitize

The wearable vital sensing fabric "hitoe" can be used to measure biological information such as the heart rate and myoelectrical responses of an athlete during exercise. The obtained biological data can be integrated with information acquired by video and other sensors and then sent to the user, which enables the user to experience the same tension, uplifting feeling, and fatigue felt by the athlete, thereby enhancing the user's excitement in watching a sports event or enhancing an athlete's training.

(2) IoT: Data and software logistics

Two technologies that contribute to improving productivity and efficiency in manufacturing were exhibited. IoT data sharing platform technology uses edge computing to collect a large amount of data with low latency. It makes it possible to manage data sent from various machines in a factory in a consistent manner. Application delivery technology sends industry apps to edge servers so that these apps can continue to evolve.

(3) IoT: Analytics and prediction

At the forum, we showcased technologies for improving the productivity of farm work and for detecting faults in agricultural machinery, thereby reducing farming costs. These technologies analyze a large volume of data collected from farms and machinery using NTT's big data analysis methods such as Non-negative Multiple Tensor Factorization (NMTF) and online machine learning. Technology for creating new value using big data from the water management and environmental infrastructures was also exhibited.

(4) Security: Managed security and IoT security

Photo 7. Networks for the coming 2020 and beyond.

Photo 8. Basic research exploring the future.

In anticipation of a time when IoT devices will cooperate with each other, we have developed a mechanism by which a system can easily grant or cancel the authorization to operate an individual IoT device in order to shut out malicious devices. In the exhibit, this mechanism was demonstrated using cargo exchanges between IoT devices as an example. Only authorized IoT devices exchanged cargo. This was done autonomously without human intervention.

(5) Security: Security and privacy for business

The amendment of the Act on the Protection of Personal Information, which will come into force on May 30, 2017, permits unidentifiable personal information to be used without the consent of the individuals concerned. Use of such information is attracting much attention. The forum introduced NTT's technologies to create, or support the creation of, useful anonymized information that satisfies the standards defined by the revised law. These technologies have built on NTT's know-how on the use of various anonymization technologies and evaluation experiments using real data in different fields.

3.4 Networks for the coming 2020 and beyond

We are aiming to co-create a better future with our partners. The forum gave a glimpse of the future network through cloud computing technologies and a wide array of network technologies characterized by flexibility and readiness based on the NetroSphere concept (**Photo 7**).

(1) Network for co-created services

Service providers are required to respond to changes in their business environments such as growing diversity in user terminals and progress in IoT technology. NTT seeks to co-create innovative and competitive services with service providers using network virtualization technology. New networks conceived by NTT research were introduced and illustrated with some demonstrations.

(2) Technologies to enhance networks

There were exhibits on various cutting-edge technologies that will drive the evolution, or facilitate the efficient development and operation, of networks and information systems that support society. These included system architecture for building a flexible network, and cloud and data technologies.

3.5 Basic research exploring the future

A goal of NTT's basic research is to bring about a transformation of society by discovering new underlying principles, extending the performance limits of materials, and developing technologies that are friendly to the earth and its inhabitants. A specific example is a quantum neural network, which is a computer based on a novel principle using quantum electronics technology. It uses networked optical parametric oscillators to solve combinatorial optimization problems at high speed. It finds solutions to maximum cut problems of a 2000-node complete graph with a computation time of less than a ten-thousandth of a second. The quantum neural network will find applications in various fields where optimization of a large amount of data is required (**Photo 8**).

3.6 Interactive technology experience

Technologies that provide novel visual or emotional experiences when watching an event were also demonstrated. Henshin Kabuki was an interactive

Photo 9. Interactive technology experience.

exhibition that combined kabuki and the advanced technologies of the NTT laboratories. A highly realistic experience of a sports event in a virtual space was made possible by using mixed reality technology. It combines high-reality video technology, haptic technology, and technology for measuring and analyzing biological information with the wearable sensing fabric "hitoe" that picks up vital signs. Providing the biological information of racers to viewers enables them to share in the excitement of a race (**Photo 9**).

NTT R&D Channel, a "niconico" live broadcast of the forum, was broadcast twice (February 13 and 16). It featured the latest quantum neural network technology and introduced the main exhibits in an easily understandable manner. It enabled people who were unable to come to the forum to get a glimpse of NTT's latest technologies. We received favorable comments from many viewers.

4. Conclusion

The forum was attended by more than 12,500 people, which far exceeded last year's attendance. We believe that the ever-increasing number of visitors reflects growing expectations for NTT R&D, as indicated by comments from visitors such as "My expectations for the strategy for growth through R&D have heightened," and "I expect that advances in R&D will strengthen our international competitiveness." There were also many comments from those interested in business applications, for example, "I want to see the specific business value of these technologies," and "I want to see more technologies that have already been commercialized."

We will endeavor to develop new services and technologies so that we can meet the strong expectations expressed by visitors for NTT R&D.

Authors (from left): Yojiro Nishiyama, Associate Manager, R&D Vision Group, NTT Research and Development Planning Department; Kazushi Maruya, Manager, Research Planning Department, NTT Science and Core Technology Laboratory Group; Haruhisa Nozue, Manager, Planning Department, NTT Information Network Laboratory Group; Hiroto Ishii, Manager, R&D Planning, NTT Research and Development Planning Department; Ryuji Yamamoto, Manager, R&D Management, Planning Department, NTT Service Innovation Laboratory Group; Yuji Uekusa, Manager, Planning Department, NTT Information Network Laboratory Group

Soft Error Test Service Commences to Reproduce Soft Errors—Abnormal Operation of Electronic Equipment Caused by Cosmic Rays

1. Introduction

NTT, in partnership with Nagoya University and S.H.I. Examination & Inspection, Ltd. (SHIEI hereinafter), has verified the applicability of a compact accelerator-driven neutron source[*1] available to general companies for reproducing faults of electronic equipment caused by cosmic rays (soft errors)[*2] and has also established a test method to reproduce soft errors.

In addition, NTT Advanced Technology Corporation (NTT-AT hereinafter) started a soft error test service using a compact accelerator-driven neutron source in December 2016.

As telecommunications equipment becomes more compact and energy-efficient with higher functionality and performance, this service promises to improve equipment reliability by enabling the prediction of abnormalities caused by soft errors in the development and testing stage, as well as confirmation of error detection and remediation systems designed to cope with soft errors. There are also plans to expand the scope of this application to other types of electronic equipment requiring high levels of reliability.

2. Background

In recent years, there has been strong demand for compact electronic equipment that conserves energy and has high functionality and high performance, meaning that semiconductor devices used in the equipment require high levels of integration. As semiconductor devices become more integrated and miniaturized, the electric charges required to determine bits in devices have become smaller and smaller.

Meanwhile, the earth is constantly being showered with neutrons that occur as a result of cosmic rays colliding with the atmosphere. Consequently, the semiconductor devices are easily affected by tiny charges of the secondary particles in neutrons resulting from the cosmic rays. This means that the rate of soft errors is on the rise compared to that of older electronic equipment.

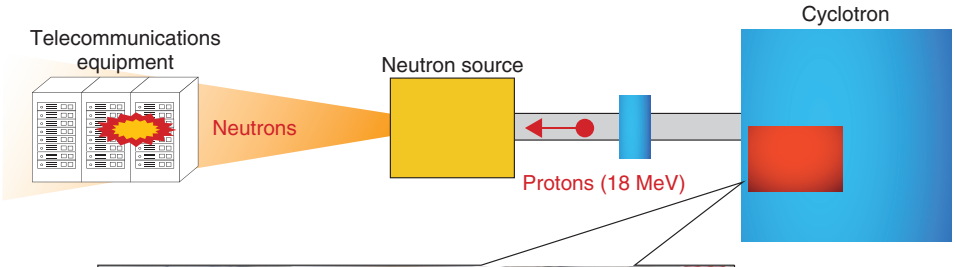
NTT speculated that soft errors could be triggered intentionally using a compact accelerator-driven neutron source. Hence, soft error testing technology was jointly established at Hokkaido University's compact accelerator-driven neutron source.

As soft errors in telecommunications equipment gain an increasing amount of attention around the world, NTT Network Service Systems Laboratories has led standardization activities in the International Telecommunication Union, Telecommunication Standardization Sector (ITU-T). In fact, ITU-T K.124 "Overview of particle radiation effects on telecommunications systems" was approved as a Recommendation in December 2016.

From these beginnings, NTT has continued joint research with SHIEI and Nagoya University in order to confirm that soft error testing is possible with a compact accelerator-driven neutron source owned by a general company, with the objective of commercializing a soft error testing service. The results of the research have enabled NTT-AT to begin providing a soft error testing service.

*1 Compact accelerator-driven neutron source: A comparatively small accelerated neutron source several meters in size.

*2 Soft errors: Temporary errors that are resolved by restarting devices and overwriting data, as opposed to *hard errors* that cause devices to malfunction permanently.



Manufacturer/Model	Sumitomo Heavy Industries/CYPRIS370
Accelerated particles	protons
Acceleration energy	18 MeV
Accelerator size	2.4 × 1.8 × 2.0 m

*Photo provided by SHIEI

Fig. 1. Soft error testing system with the SHIEI-owned compact accelerator-driven neutron source.

3. Joint experiment results

The SHIEI-owned compact accelerator-driven neutron source was used to conduct joint experiments in order to (1) reproduce soft errors, (2) greatly reduce the time to reproduce soft errors, and (3) build a system to control the area irradiated with neutrons (**Fig. 1**). In this experimental system, neutrons were produced by irradiating a beryllium target in a cyclotron with protons accelerated to 18 MeV.

Prior to the experiment, a particle transport simulation was performed to determine the spatial distribution of the neutrons.

(1) Soft error reproduction

We confirmed that soft errors could be reproduced using the SHIEI-owned compact accelerator-driven neutron source.

(2) Significant reduction in soft error reproduction time

Testing was done in the vicinity of the neutron generation source in this accelerator, and we verified that the time taken to reproduce soft errors was reduced to 1/100 that of the older method. This is equivalent to about 100 million times faster than that of the natural world. We also confirmed that this ratio can be freely adjusted.

(3) Controlling the neutron irradiation area

In this experiment, we confirmed that the irradiation area can be controlled to handle irradiation of particular LSI (large-scale integrated circuit) devices within a system, or irradiation of entire systems. Specifically, we confirmed that testing is possible with irradiation of only a specific area of a few square centimeters or a wide area of about 50 × 50 cm.

For Inquiries
Planning Department, Public Relations Section,
NTT Information Network Laboratory Group
http://www.ntt.co.jp/news2016/1612e/161219a.html

External Awards

Achievement Award
Winner: Masayuki Abe, NTT Secure Platform Laboratories
Date: June 2, 2016
Organization: The Institute of Electronics, Information and Communication Engineers (IEICE)

For his pioneering research on cryptographic protocol and its elemental technology.

Specially Selected Paper
Winner: Junko Takahashi and Yosuke Aragane, NTT Secure Platform Laboratories; Toshiyuki Miyazawa, NTT Technology Planning Department; Hitoshi Fuji, NTT Secure Platform Laboratories; Hirofumi Yamashita, Keita Hayakawa, Shintarou Ukai, and Hiroshi Hayakawa, Denso Corporation
Date: February 15, 2017
Organization: Information Processing Society of Japan (IPSJ)

For "Automotive Attacks and Countermeasures on LIN-Bus."
Published as: J. Takahashi, Y. Aragane, T. Miyazawa, H. Fuji, H. Yamashita, K. Hayakawa, S. Ukai, and H. Hayakawa, "Automotive Attacks and Countermeasures on LIN-Bus," Symposium on Cryptography and Information Security, 4F2-5, Kumamoto, Japan, Jan. 2016.

ICM Research Award
Winner: Akio Watanabe, Yoichi Matsuo, Keishiro Watanabe, Keisuke Ishibashi, and Ryoichi Kawahara, NTT Network Technology Laboratories
Date: March 9, 2017
Organization: IEICE Technical Committee on Information and Communication Management (ICM)

For "Multiple Isolating Actions Extraction from Action Logs for Clarifying Trouble-shooting Process."
Published as: A. Watanabe, Y. Matsuo, K. Watanabe, K. Ishibashi, and R. Kawahara, "Multiple Isolating Actions Extraction from Action Logs for Clarifying Trouble-shooting Process," IEICE Tech. Rep., Vol. 116, No. 124, ICM2016-13, pp. 27–32, July 2016.

EMCJ Young Engineer Award
Winner: Mahmood Farhan, NTT Network Technology Laboratories
Date: March 10, 2017
Organization: IEICE Technical Committee on Electromagnetic Compatibility (EMCJ)

For "Artificial Mains Network for Conducted Disturbance from 2 kHz" and "Voltage Feedback Amplifier with Ferrite-cores for Common-mode Noise Suppression."
Published as: M. Farhan, K. Okamoto, H. Tatemichi, and K. Takaya, "Artificial Mains Network for Conducted Disturbance from 2 kHz," IEICE Tech. Rep., Vol. 115, No. 427, EMCJ2015-121, pp. 99–104, Jan. 2016. M. Farhan, S. Yoshikawa, K. Okamoto, K. Takaya, and A. Nishikata, "Voltage Feedback Amplifier with Ferrite-cores for Common-mode Noise Suppression," IEICE Tech. Rep., Vol. 115, No. 509, EMCJ2015-130, pp. 33–37, Mar. 2016.

Best Paper Award
Winner: Fumihiko Ishiyama, Yuichiro Okugawa, and Kazuhiro Takaya, NTT Network Technology Laboratories
Date: March 12, 2017
Organization: 13th IEEE International Colloquium on Signal Processing & Its Applications (CSPA 2017)

For "Linear Predictive Coding without Yule-Walker Approximation for Transient Signal Analysis - Application to Switching Noise."
Published as: F. Ishiyama, Y. Okugawa, and K. Takaya, "Linear Predictive Coding without Yule-Walker Approximation for Transient Signal Analysis - Application to Switching Noise," Proc. of CSPA 2017, pp. 46–50, Penang, Malaysia, Mar. 2017.

IEICE Fellow in 2016
Winner: Akira Takahashi, NTT Network Technology Laboratories
Date: March 24, 2017
Organization: IEICE Communications Society

For his research and development of QoE (quality of experience) evaluation, design, and management for speech and video communication services and his contribution to international standardization.

Young Researcher's Award
Winner: Yuki Minami, NTT Network Innovation Laboratories
Date: March 24, 2017
Organization: IEICE

For "An Infrastructure for Application Customization based on SDN/NFV."
Published as: Y. Minami, Y. Mochida, and J. Ichikawa, "An Infrastructure for Application Customization based on SDN/NFV," Proc. of the IEICE General Conference, B-6-72, Fukuoka, Japan, Mar. 2016.

Young Researcher's Award
Winner: Masaki Wada, NTT Access Network Service Systems Laboratories
Date: March 24, 2017
Organization: IEICE

For "Characteristic Evaluation of Spectral-hole Burning of 2-LP Mode Erbium Doped Fiber."
Published as: M. Wada, T. Sakamoto, S. Aozasa, T. Mori, T. Yamamoto, and K. Nakajima, "Characteristic Evaluation of Spectral-hole Burning of 2-LP Mode Erbium Doped Fiber," Proc. of the IEICE General Conference, B-13-19, Fukuoka, Japan, Mar. 2016.

Young Researcher's Award
Winner: Rie Tagyo, NTT Network Technology Laboratories
Date: March 24, 2017
Organization: IEICE

For "Communication Quality Estimation with Degradation for Specific Attribute Combination."
Published as: R. Tagyo, D. Ikegami, G. Kawaguchi, and A. Takahashi, "Communication Quality Estimation with Degradation for Specific Attribute Combination," Proc. of the IEICE General Conference, B-11-8, Fukuoka, Japan, Mar. 2016.

Young Researcher's Award
Winner: Haruka Suzuki, NTT Secure Platform Laboratories
Date: March 24, 2017
Organization: IEICE

For "A Study of Attribute Assurance of Data Generated by Individuals."
Published as: H. Suzuki, G. Takahashi, K.Fujimura, T. Nakamura, and K. Hayakawa, "A Study of Attribute Assurance of Data Generated by Individuals," Proc. of the IEICE General Conference, D-9-18, Fukuoka, Japan, Mar. 2016.

Achievement Award
Winner: Tatsuaki Okamoto, NTT Secure Platform Laboratories
Date: June 30, 2017 (award ceremony date)
Organization: The Japan Society for Industrial and Applied Mathematics

For his research on basic theory and applied technology of public key cryptography.

Papers Published in Technical Journals and Conference Proceedings

Anomaly Detection in a Telephone System by Using Traffic Balance Analysis
T. Moriya, N. Tanji, and S. Seto
IEICE Transactions on Communications (JPN edition), Vol. J99–B, No. 9, pp. 799–805, September 2016.
This paper proposes an anomaly detection method for telephone systems by monitoring the change of vector of nodes' traffic. To improve the detection performance in a telephone system's traffic, a function that reduces fluctuation of the vector was applied and evaluated in an actual telephone system.

Design of Homogeneous Trench-assisted Multi-core Fibers Based on Analytical Model
F. Ye, J. Tu, K. Saitoh, K. Takenaga, S. Matsuo, H. Takara, and T. Morioka
Journal of Lightwave Technology, Vol. 34, No. 18, pp. 4406–4416, September 2016.
We present a design method of homogeneous trench-assisted multicore fibers (TA-MCFs) based on an analytical model utilizing an analytical expression for the mode coupling coefficient between two adjacent cores. The analytical model can also be used for crosstalk (XT) properties analysis, such as XT reduction amount versus trench width, trench depth, and other fiber structural parameters as compared with normal step-index MCFs. Furthermore, the model can be used to search for core positions for further XT reduction in non-close-packed structures. For instance, we show that a dual-ring structure is the quasi-optimum core layout starting from a one-ring structured 12-core fiber. Based on the analytical model, a square-lattice structured 24-core fiber and a 32-core fiber are designed both for propagation-direction interleaving (PDI) and non-PDI transmission schemes. The proposed model provides a powerful tool for designing high-count homogeneous TA-MCFs.

Speech Sound Naturalness Alters Compensation in Response to Transformed Auditory Feedback
S. Hiroya and T. Mochida
5th Joint Meeting of the Acoustical Society of America and Acoustical Society of Japan, 3pSC84, Honolulu, HI, USA, November/December 2016.
Articulatory compensations in response to real-time formant perturbation have revealed that auditory feedback plays an important role in speech production. However, these compensatory responses were at most 40% for formant shifts and varied depending on vowel type and subjects. Although previous formant perturbation studies have been done using linear predictive coding (LPC), it is known that the estimation accuracy for low vowels and female speech would be degraded due to a glottal source-vocal tract interaction. To improve the accuracy, we have developed a real-time robust formant tracking system using the phase equalization-based autoregressive exogenous (PEAR) model which utilizes the glottal source signals measured by electroglottography. In this study, we compared compensatory responses to real-time formant perturbation using PEAR and LPC. Eleven Japanese subjects (seven females) read Japanese mora (/hi/ or /he/) with headphones. The first two formant frequencies were altered. Results showed that compensatory responses using PEAR were significantly larger than those using LPC. Moreover, the naturalness of altered speech sounds was improved by PEAR. This indicates that improving speech sound naturalness by PEAR led to larger compensatory responses. Therefore, our system would be useful to understand the auditory feedback mechanisms in more detail.

A Study on Reduction of Violation Behavior of Security Rules
Y. Okano and H. Okuyama
IPSJ Journal, Vol. 58, No. 1, pp. 258–268, January 2017.
Information leakage incidents in organizations are often caused by insiders. In particular, it is a common issue that employees violate security rules such as giving priority to work. In this study, we focus on behaviors involving the taking of business related information out

of the workspace without permission, which is often seen in violation behaviors. We consider situations of takeout behaviors and the psychology of the concerned parties, and we find factors of those behaviors and consider deterrents. We carried out hearings with people in charge of security management and group interviews with people who have taken information out illegally. We also hypothesized factors and deterrents and implemented a questionnaire to verify the hypotheses. We found that pressure from outside is the underlying cause of takeout behaviors. We show that it may not be possible to prevent those behaviors through employee training alone and consider that it is also necessary for the employees to recognize the information leakage risk the organization faces and also the risk they face, and we facilitate the employees' execution of normal procedures when they take information outside or work overtime. Additionally, a help desk regarding takeout of business related information is established.

Visualizing Video Sounds with Sound Word Animation to Enrich User Experience

F. Wang, H. Nagano, K. Kashino, and T. Igarashi

IEEE Transactions on Multimedia, Vol. 19, No. 2, pp. 418–429, February 2017.

Sound information in videos plays an important role in shaping the user experience. When sound is not accessible in videos, text captions can provide sound information. However, conventional text captions are not very expressive for nonverbal sounds because they are designed to visualize speech sounds. Here, we present a framework to automatically transform nonverbal video sounds into animated sound words and position them near the sound source objects in the video for visualization. This provides natural visual representation of nonverbal sounds with rich information about the sound category and dynamics. To evaluate how the animated sound words generated by our framework affect the user experience, we implemented an experimental system and conducted a user study involving over 300 participants from an online crowdsourcing service. The results of the user study show that the animated sound words can effectively and naturally visualize the dynamics of sound while clarifying the position of the sound source as well as contribute to making video-watching more enjoyable and increasing the visual impact of videos.

High-capacity Dense Space Division Multiplexing Transmission

T. Mizuno and Y. Miyamoto

Optical Fiber Technology, Vol. 35, pp. 108–117, February 2017.

In this paper, we review space division multiplexing (SDM) transmission experimental demonstrations and associated technologies. In past years, SDM achieved high capacity transmission through increased spatial multiplicity, and long-haul transmission through improved transmission performance. More recently, dense SDM (DSDM) with a large spatial multiplicity exceeding 30 was demonstrated with multicore technology. Various types of multicore and multimode SDM fibers, amplification, and spatial multi/demultiplexers have helped achieve high-capacity DSDM transmission.

Embodiment Bridging over Cyber Spaces and Physical Spaces: Comments on Kitazaki's Article

T. Amemiya

Japanese Psychological Review, Vol. 59, No. 3, pp. 324–329, March 2017.

The possibility of implementing 'we-mode' among users in cyber spaces, which is proposed by Kitazaki, is discussed by reviewing the studies on body ownership and the sense of agency, both of which are strongly involved in self-body perception and recognition. The movement of a body in cyber space should strongly correlate with that in the physical space, but not necessary be rendered as realistic. Furthermore, the interaction and relationship between the spaces from the point of view of both a sense of realistic self-body in a cyber space and behavior changes after an experience in a cyber space are discussed to consider the possibility of creating 'we-mode' bridging of the physical and cyber spaces.

Chaotic Laser Based Physical Random Bit Streaming System with a Computer Application Interface

S. Shinohara, K. Arai, P. Davis, S. Sunada, and T. Harayama

Optics Express, Vol. 25, No. 6, pp. 324–329, March 2017.

We demonstrate a random bit streaming system that uses a chaotic laser as its physical entropy source. By performing real-time bit manipulation for bias reduction, we were able to provide the memory of a personal computer with a constant supply of ready-to-use physical random bits at a throughput of up to 4 Gbps. We pay special attention to the end-to-end entropy source model describing how the entropy from physical sources is converted into bit entropy. We confirmed the statistical quality of the generated random bits by revealing the pass rate of the NIST SP800-22 test suite to be 65% to 75%, which is commonly considered acceptable for a reliable random bit generator. We also confirmed the stable operation of our random bit steaming system with long-term bias monitoring.

Modular Representation of Layered Neural Networks

C. Watanabe, K. Hiramatsu, and K. Kashino

arXiv:1703.00168 [stat.ML], March 2017.

Deep neural networks have greatly improved the performance of various applications including image processing, speech recognition, natural language processing, and bioinformatics. However, it is still difficult to discover or interpret knowledge from the inference provided by a deep neural network, since its internal representation has many nonlinear and complex parameters embedded in hierarchical layers. Therefore, it becomes important to establish a new methodology by which deep neural networks can be understood.

In this paper, we propose a new method for extracting a global and simplified structure from a layered neural network. Based on network analysis, the proposed method detects communities or clusters of units with similar connection patterns. We show its effectiveness by applying it to three use cases. (1) Network decomposition: it can decompose a trained neural network into multiple small independent networks, thus dividing the problem and reducing the computation time. (2) Training assessment: the appropriateness of a trained result with a given hyperparameter or randomly chosen initial parameters can be evaluated by using a modularity index. And (3) data analysis: in practical data it reveals the community structure in the input, hidden, and output layers, which serves as a clue for discovering knowledge from a trained neural network.

Fractal and Spinodal-decomposed Turbidities of Nanoporous Glass: Fluctuation Picture in Turbid and Transparent Vycor

S. Ogawa and J. Nakamura

Journal of the Optical Society of America A, Vol. 34, No. 4, pp. 449–463, April 2017.

The light propagation and scattering in monolithic transparent nanoporous materials such as Vycor glasses exhibit two optical turbidities, both of which are slightly deviated from the λ^{-4} Rayleigh wavelength dependence in the visible region: one is a transient white turbidity τ_f, characterized by the convex-upward dependence on the inverse fourth power of wavelength, and the other is turbidity τ_{sp} inherent to the structural inhomogeneity, characterized by the convex-downward dependence. The former is attributed to a fractal-like percolation network of imbibed or drained pores as a consequence of transient imbibition or drainage of wetting fluid into or from the pore space. The latter is attributed to the structural inhomogeneities inherent to the original dry porous glass, which are produced by spinodal decomposition. In this paper, we develop a general scheme to estimate the transmittance spectra of Vycor through the turbidities τ_f and τ_{sp} in the visible region on the basis of the theory of dielectric constant fluctuations. We show the applicability and its limitation of the turbidity analysis of the photospectroscopically measured data as a method to study the correlation functions that characterize the pore space and the structural features of isotropic transparent nanoporous media, on the presupposition that there exists no light attenuation other than the scattering.