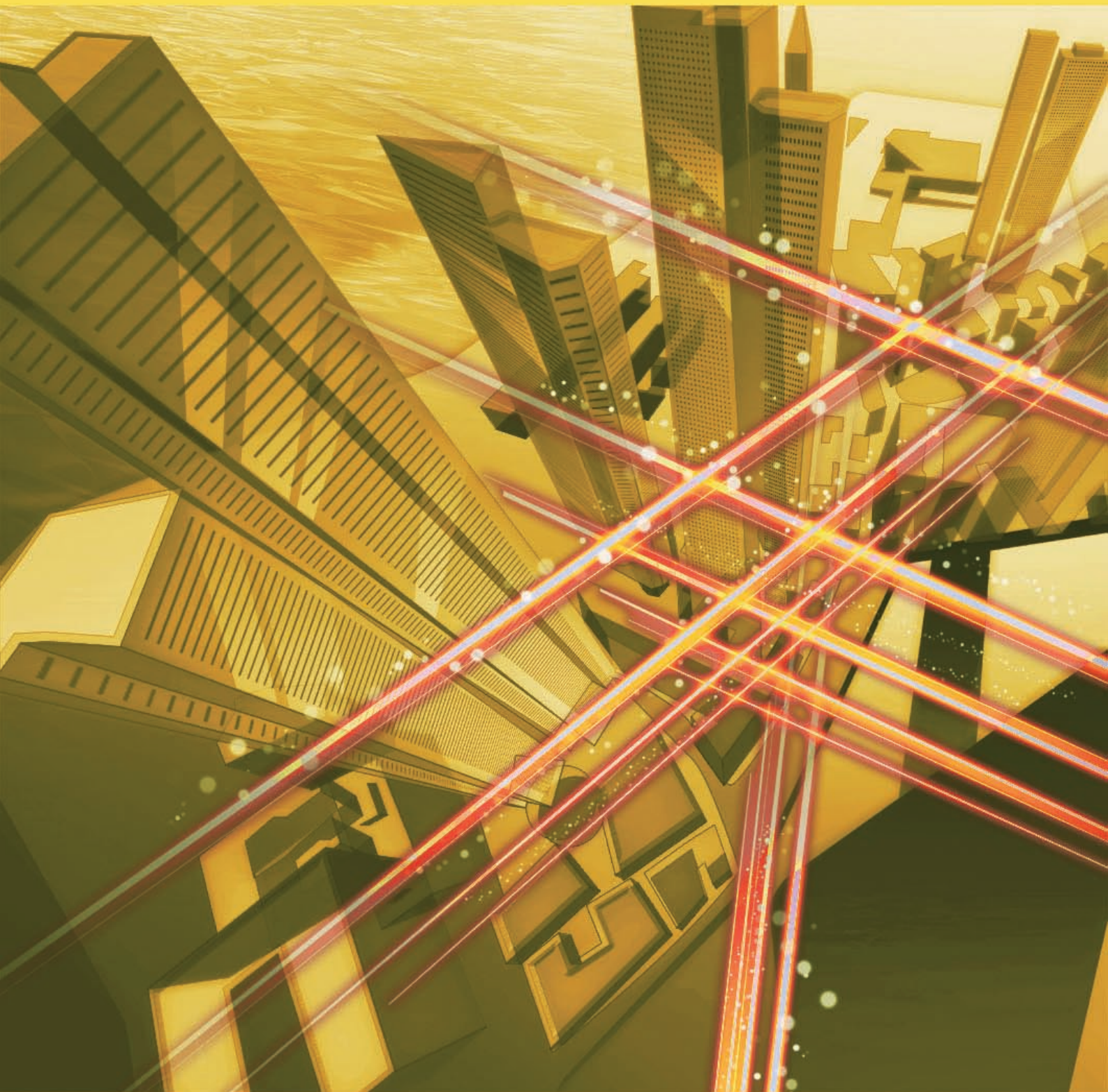


NTT Technical Review

10
2012



October 2012 Vol. 10 No. 10

NTT Technical Review

October 2012 Vol. 10 No. 10



View from the Top

Masayuki Yamamura, President of NTT EAST

Front-line Researchers

Koji Muraki
Senior Research Scientist (Distinguished Researcher),
NTT Basic Research Laboratories

Feature Articles: Evolving Threats and Cyber Security in Future

Emergence of New Cyber Attacks and
Future Directions in Security R&D

Detection, Analysis, and Countermeasure Technologies for
Cyber Attacks from Evolving Malware

Cryptographic Techniques that Combine Data Protection and
Ease of Utilization in the Cloud Computing Era

Tighter Security Operations to Help Provide Brands
that are Safer and More Secure

Regular Articles

Unraveling an Exotic Electronic State for
Error-free Quantum Computation

Global Standardization Activities

Digital Signage Standardization

Practical Field Information about Telecommunication Technologies

Case Studies of Using the Gigabitcompatible Protocol Checker
as a Troubleshooting Tool for Home IP Systems

Papers Published in Technical Journals and Conference Proceedings

Papers Published in Technical Journals and
Conference Proceedings

Toward a Company that Inherits Workplace Skills and Connects the Community through Communications

Masayuki Yamamura
President of NTT EAST



Overview

The information and communications technology market is undergoing dramatic changes as smartphones and tablet computers become increasingly popular throughout society. The seamless convergence of wired and wireless communications is accelerating and even the management environment is changing by necessity. How is NTT EAST set up to face this changing world? We asked Masayuki Yamamura, who took up his new position as President of NTT EAST in June 2012, about his tactics, including his management philosophy and his approach to inspiring employees.

Facing a dramatically changing market from the customer's viewpoint

—Congratulations on your appointment to president. Looking again with a fresh eye, how do you view the management environment at NTT EAST?

Well, since I had already been working at NTT EAST before taking up this position, it's a bit difficult to look at things with a fresh eye. I think it's best if I continue to assess the situation as I've been doing up to now. That being said, my impression is that the management environment is changing at an accelerating pace. NTT EAST is in the business of fixed-line communications, and up until recently, our competitors were other fixed-line operators and cable television companies because mobile communications was essentially segregated from this business. Today, however, we have smartphones and tablets, and it has become commonplace to make high-speed Internet connections from mobile terminals. From the customer's viewpoint, it's the service that counts and not the facilities providing it, so we have entered into a competitive relationship with mobile communica-

tions too. In short, the competition is becoming increasingly diversified. At the same time, smartphones and tablets are penetrating society at an unprecedented speed, and it is difficult to foresee the trend from here on. The possibility that customers might abandon NTT EAST in droves cannot be denied. In this sense, the NTT EAST business environment is at an inflection point from which the future is hard to discern. This kind of change has occurred in the past, but today we are facing severe conditions—we must quicken the pace of our response with a sense of vigilance.

—Please tell us how NTT EAST intends to deal with this situation.

If we were to accommodate smartphones and tablets, I think that it would be to meet the diversified needs of our users. However, we must still respond to the diverse usage formats and needs of our customers with respect to fixed-line communications. Users of optical services include single persons and family members plus homeowners and renters. They also include people who work at home and people who

work at a company office or elsewhere. Meanwhile, in the case of family members, some may use optical services during the day and others during the evening. The usage format may also vary: optical services may be used to collect information, communicate with others, shop online, watch videos, or listen to music. To respond effectively to such user diversity, we must formulate measures for getting our customers to use our services over the long term and we must take up the challenge of expanding our business area to satisfy new needs.

Specifically, there are three measures that we must take, which I've talked about at various places since becoming president.

The first is to promote the use of optical services. Thanks to the efforts of NTT EAST employees, achieving 10 million subscribers for FLET'S HIKARI services is now within our reach. Up to now, however, we have been concentrating our energies on adding more subscribers by, for example, expanding the service area. But from here on, I would like to put more effort into achieving long-term use of our services. To this end, we have launched a new rate plan called Ninen-Wari that provides a monthly discount to users who subscribe to a two-year plan and we have also introduced a points service. We have also diversified the fee menu taking into account light users of services. Additionally, we now provide convenient services such as FLET'S Miruene that provides users with a means of visualizing the amount of energy used in a home. And on top of this, we have decided to promote the expansion of Wi-Fi environments through joint projects with local entities, such as the Yamanashi Free Wi-Fi Project that aims to install Wi-Fi spots at about a thousand locations within Yamanashi prefecture and the Jiyugaoka HIKARI Wi-Fi City Project in collaboration with the Jiyugaoka Shopping Arcade in Tokyo. I would like to expand these kinds of activities while listening closely to the opinions of each and every customer.

The second measure is to develop new sources of revenue. To this end, we are considering new network-based services that we would like our customers to use. For example, we could provide a service for managing a customer's facilities over the network or a service that would absolutely prevent the deletion of critical data in residents' files held by local governments by storing backup information at remote locations. Services like these can be provided in a cloud-based format thereby lowering initial costs and providing a user-friendly environment for customers. And to further diversify our business, I would like to



expand our offering of services for solving regional problems associated with disaster preparedness, the aging society, and other issues, that is, services that provide true benefits for our customers.

Finally, the third measure is to improve productivity in the work that we do. There are various things that we need to do in this regard such as reducing costs and shortening working hours. In this way, I aim to achieve a turnaround in business results from ongoing drops in revenue to ongoing increases in revenues and profits while providing our customers with solutions to specific problems and opening up new sources of revenue.

Of course, these cannot be achieved unless all NTT EAST employees work together as one. My role is to talk frequently with the people who are implementing these measures to make sure that they are all moving together with a common sense of purpose. Since becoming president, I have been making the rounds of the branch offices and also talking with many employees in the head office.

Taking on challenges and using numerical results to get answers

—What kind of matters do you talk about in particular?

The topics differ from place to place, but what I tell everyone is that it is important that they try something, that they adopt the attitude of enjoying a challenge! No results will be forthcoming if nothing is attempted, so it is OK to fail. However, if a mistake is made, it is important to stop, make a course correction, and try something else. People tend to think that their measure or policy is correct, that a lack of results

is due to the current business environment, and that a little perseverance can eventually produce results. Numbers, however, are always honest, so a new course of action should be checked using figures. When implementing a particular measure, it should be possible to see some results in the figures in about half a year's time, so if such figures are practically unchanged after half a year, the measure should be deemed ineffective and gracefully withdrawn. In the past, the period for assessing the effectiveness of a measure was one year, but for present day needs, three months might be more appropriate.

—Isn't a three-month cycle quite a challenge?

I think it's essential to experiment with a variety of measures and absorb those that produce results if we are to respond to the diverse usage formats and needs of our customers. But to pursue such experimentation with sufficient speed, I think that a certain amount of delegation of responsibility is necessary. Trusting in the creative abilities of on-site personnel and transferring authority are important elements of this process as long as all efforts fit within an overall framework.

However, if we place too much emphasis on words like speed and three-month cycle, we run the risk of developing a bias toward short-term matters and immediate profits. For this reason, we must undertake our projects with a sense of urgency while keeping a medium-term outlook and keeping things in perspec-



tive. Conversation is also a key element in maintaining such a balance.

Management that appreciates employees' efforts

—What else do you hold important in your work?

Well, speaking of challenges, I have always thought that, at least one a year, I should try to do something that no one has been able to do before. For example, while general manager of the Tokyo branch of NTT EAST, I was able to get that branch to adopt on-site recruiting that it was said could not be adopted, and I was able to establish an urban development sales department when it was said that the organization of the branch could not be expanded. Furthermore, when I was at NTT Holding Company, everyone was shocked at my proposal of listing NTT Urban Development Co. on the Tokyo Stock Exchange, but I was able to push that through. As challenging as these problems were, I was somehow able to obtain the understanding of my superiors and get my proposals accepted.

On making the rounds of the branch offices, I sensed that a somewhat overly defensive approach was being taken. In the face of an increasing number of customers discontinuing their use of FLET'S HIKARI services, branches have had no recourse but to focus their efforts on measures that would in some way keep these customers. Nevertheless, I feel that a more aggressive stance should be adopted by making a simultaneous effort to explain the benefits of NTT EAST services and to persuade prospective customers to use those services.

And there is one more thing. At a certain point in the past, it dawned on me that it was part of my job to

recognize the difficulties that my subordinates went through as they accompanied and assisted me whenever I made an all-out effort to solve a problem at hand. I came to realize that, regardless of whether my superiors accepted a proposal on the basis of material painstakingly prepared by my subordinates, the process involved an exchange of ideas and opinions with those subordinates that was useful for the future. If my work style were to sing my own praises and just have the people around me prepare materials, I would only grow apart from them. Work should be an enjoyable endeavor, but if it involves only carrying out instructions, it can hardly be enjoyable and rewarding. An individual should be able to take some risk and accept responsibility for making judgments on his or her own and moving forward. I now see that results achieved together with my subordinates belong just as much to them as to me and that work can be even more enriching if credit is given where it is due.

Likewise, despite the hardships brought on by the Great East Japan Earthquake, employees in the affected areas did an absolutely outstanding job. The Miyagi area was without domestic gas for about a month, during which time people could not eat warm food despite the cold weather. Nevertheless, NTT EAST employees in the region put all their effort into restoring the infrastructure even though some of them had their homes ruined or their parents evacuated from Fukushima to safety elsewhere. Despite these severe conditions, these employees came to work and restored networks damaged by the disaster. Just hearing about their efforts and commitment is enough to bring tears to my eyes. The business of NTT EAST is built on the support of employees like these, and I've been thinking for some time that I should manage in a way that acknowledges the great efforts made by our employees.

Solving Japan's problems through communications,
in close cooperation with customers

—Mr. Yamamura, what message do you have for NTT EAST employees?

I am convinced that communications is one means

of solving the diverse problems that currently surround Japan. Our intention at NTT EAST should be to solve each and every problem that is within our capabilities. Let's confront these problems together with our customers and create things that bring them satisfaction.

—Can the same be said for NTT researchers?

If we are talking about basic research performed over five- or ten-year cycles, I look at it as research in the pursuit of truth, so I would like to see those researchers do just that without distraction. Basic research is, of course, necessary, and I believe that the technologies born from such research are absolutely critical during a time of great changes in society. On the other hand, in developing practical applications with the aim of putting a technology on the market in a year or two, it is important to create value that will appeal to customers. Regardless of how advanced such technology may be in the field in question, it will be of little value if it is not accepted by customers. Even a product or service with great performance will fall by the wayside in an era that simply has no need for that level of performance. In any case, I think that a mindset that aims to create something that will satisfy the needs of customers is essential even for researchers.

Interviewee profile

■ Career highlights

Masayuki Yamamura received the B.E. degree in physical electronics and the M.E. degree in electronic engineering from Tokyo Institute of Technology in 1976 and 1978, respectively. He joined Nippon Telegraph and Telephone Public Corporation (now NTT) in 1978. He became a Member of the Board of NTT EAST and General Manager at the Tokyo branch in 2005, Executive Director in 2008, and General Manager of the Network Promoting Department in 2009. He was appointed President of NTT EAST in June 2012.

Basic Research is an Adventure! Pouring Intellectual, Physical, and Technological Power into Unexplored Worlds



Koji Muraki

Senior Research Scientist

(Distinguished Researcher)

NTT Basic Research Laboratories

The research of Senior Research Scientist Koji Muraki is revolutionary to the point of requiring physics textbooks to be rewritten. The paper written by Dr. Muraki and his colleagues on the $5/2$ state supporting the existence of non-Abelian quasiparticles, which are different from the fundamental particles in the natural world, was published in the magazine *Science* in 2012 to much acclaim. We asked Dr. Muraki to explain to us in layman's terms the results of this research and to tell us how he approaches the research process.

Making the most of past experience to manage an entire sequence of processes

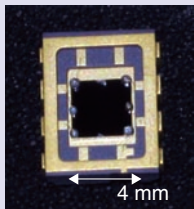
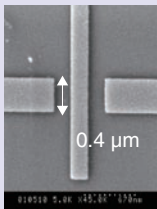
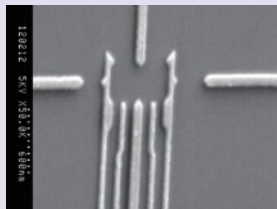



—Dr. Muraki, please tell us about your current research efforts.

In short, my colleagues and I are trying to combine heterostructures, which have artificially formed layers of different types of semiconductors, with finely processed nanostructures. Our goal is to obtain new properties not found in conventional semiconductors and new functions using those properties. To this end, it is important to exploit the quantum-mechanical features of electrons and make use of electron spin (rotational motion) in addition to electron charge (center-of-mass motion). We are paying particular attention to the effects that arise when many electrons

behave cooperatively—as they do in superconductors—in contrast to those obtained with non-interacting electrons moving independently. This kind of research requires high-purity semiconductor wafers having minimal effects from impurities, and to meet this need, we are researching ways of making ideal semiconductor wafers having absolutely no noise and no impurity effects.

—I can see that explaining cutting-edge technology is difficult. Could you give us a more concrete description?

We are fabricating semiconductors having structures and functions different from anything in the past. To fabricate a semiconductor device, one first needs materials, so our work begins with their

	Two dimensions	One dimension	Zero dimensions
Electrons	<p>Quantum well</p> 	<p>Quantum wire</p> 	<p>Quantum dot</p> 
People	<p>Field</p> 	<p>Hallway</p> 	<p>Elevator</p> 

Confining electrons in a small space results not only in the appearance of quantum-mechanical properties but also in remarkable mutual-interaction effects among the electrons that reflect the dimensionality. An analogy can be drawn with people. Although we all live in the same three-dimensional space, the distance we keep from others and the way that we communicate differs when we are playing sports on a field, passing each other in a hallway, or riding an elevator together.

Fig. 1. Number of spatial dimensions, which affects the mutual interaction of electrons.

preparation. The first step here is crystal growth in which we deposit atoms in an orderly fashion on top of a semiconductor substrate (wafer). Then, after processing this deposit into patterns for making a device, we apply current and measure the resulting voltage at temperatures near absolute zero. This sequence of processes is typical of the work we're involved in.

It is difficult to firmly say when research of this type began, but a number of people began to pursue this research in the 1970s, and some of that work led to Nobel prizes. Since then, many people have become involved, and within this research having such a long history, I would say that our group's work is, in a sense, very advanced.

The topic that we are currently focused on is mutual interaction between electrons (**Fig. 1**). It was Professor Leo Esaki, a Nobel Prize winner, who first proposed that quantum-mechanical properties appear when an electron is confined to a small space inside an artificially tailored semiconductor heterostructure. By quantum-mechanical properties, we mean that an electron can be likened to a wave. It was therefore thought that, if a single electron is behaving like a wave, it should be possible to obtain new properties and functions in a semiconductor. The focus of this

research has since expanded to mutual interaction among many electrons, which leads to physical phenomena that cannot occur with only one electron.

—*What exactly are non-Abelian quasiparticles?*

This might be difficult to explain, but to begin with, let's consider two electrons. Since one electron is identical to another, if these electrons exchange positions, the result is a state that is indistinguishable from the original one. On the other hand, in the case of non-Abelian quasiparticles discussed in the paper in Science [1], if two of these particles exchange positions, the result is a state that is different from the original one (**Fig. 2**). We wondered whether this property could be useful.

This is one example of the *many-body effects* that occur when many electrons are present. It does not appear in a crystal that is not of high purity. This is because two electrons interact with each other via the charge that each possesses. In terms of everyday phenomena, static electricity is an example of a buildup of charge, and two negatively charged objects repel each other. A semiconductor generally contains a high number of impurities, and since impurities also

Type	Particles		Quasiparticles	Statistics
	Fundamental particles	Composite particles		
Fermion	Electron	Proton, neutron	Hole	Abelian
Boson	Photon	Helium atom	Phonon	
Anyon (only in two dimensions)			1/3 quasiparticle	Non-Abelian
			(5/2 quasiparticle)	

Types of (quasi) particles and examples

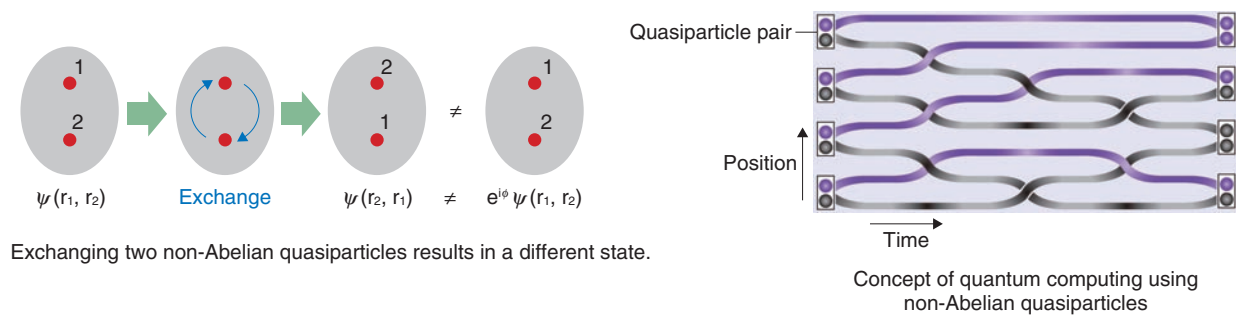


Fig. 2. Non-Abelian quasiparticles.

have charge, a mixture of such charges together with the electron charges that we are researching would prevent us from observing any mutual-interaction effects intrinsic to electrons.

To observe such effects, we must begin by removing impurities to raise the crystal’s purity. That is, we must create an environment in which electrons are completely unhindered by other matter. This kind of research requires a group of researchers having a variety of specialties who can work together toward a common goal. They include specialists at growing crystals, fabricating devices, making measurements, and theoretical analysis. With this approach, however, it may be difficult to appropriately connect the results obtained by each team of specialists. Since I have had experience with a variety of processes throughout my career, whenever a problem has arisen within a team, I have been able to interconnect the results of different processes and obtain an overall picture of the situation to solve the problem.

In the system that I described, when special electron states appear in an environment with no impurities at temperatures near absolute zero, we have been able to directly measure the rotational motion of an electron called *spin* and determine the state of each electron’s spin. In this way, we clarified that spin orientation was the same for all the electrons in ques-

tion.

The states that we are researching are related to a phenomenon called the *fractional quantum Hall effect* explained by Professor Robert Laughlin, who received the 1998 Nobel Prize in Physics for his work, but they are beyond the conventional understanding based on his theory, so our research results are attracting attention.

A researcher needs many options and skills at negotiating with other people.

—Looking back at the hardships you have so far encountered, which was the most difficult?

Perhaps this is the same with all research, but I was not able to obtain notable results as quickly as I would have liked, which means being largely ignored for a long time. I entered NTT in 1994 and it took two years before I was able to pursue the work that I truly wanted to do. And it wasn’t until 2001—my eighth year with the company—that I was able to present a noteworthy paper, which was published in Physical Review Letters [2]. Thinking that people throughout the world were perhaps reading my paper and approving of the findings that I presented gave me a great sense of accomplishment. At the same time, I

was keenly aware that obtaining the recognition that I sought for my work was not going to be easy.

Then, about five years later in 2006, I began to be asked to give invited talks. Now, with the publication of our paper in *Science*, I feel that my work has truly been recognized at long last. My journey to this point has been long indeed.

Following the publication of my 2001 paper, I entered a period in which I was worried about how I was going to move up to a higher level as a researcher. I was fortunate in being given the opportunity to do research in Germany at the Max Planck Institute for a relatively long period in the group headed by Professor Klaus von Klitzing (a recipient of the Nobel Prize in Physics), but even at that time, since I was like a stranger thrown into an unfamiliar environment, it was a struggle to persuade the people around me to help me pursue the work that I wanted to do.

But looking back at my first two years at NTT, though I was assigned to a post that I had wanted, I lacked the confidence to pursue even the work that I desired. This period in which I was not able to take the first step in my research journey was, in retrospect, the most difficult.

I now think, however, that my experiences during these difficult times have actually been beneficial to me. What I learned was that, as a researcher, I must have many options and must persevere in negotiating with other people to get them to agree with my plan of action. I also learned that I must never waver in facing the problems that lie in front of me—I must think seriously about what is the best direction to take.

NTT Basic Research Laboratories, where I am currently working, has established an environment in which researchers can pursue the work they desire with much peripheral support. This holds true for me too, but it's not the case that you can immediately pursue the research that you desire. If current conditions are such that you cannot pursue research exactly as you like, please keep in mind that there is always a chance of changing things, which means that you must never forget the need for patience.

Climbing to the top of a small mountain gives a far and wide view.

—So you treat adversity as an ally! Perhaps young researchers who are reading this article find themselves in the same environment. What advice would you give to them?

One of my hobbies during my time as a student was to play guitar in a band. As an amateur, I began by imitating the style of professional guitar players, and my aim was to play as much like them as possible. It is normal for a guitar player to pass through this stage and then start writing original songs. This is how professionals come to be. If we now substitute research for guitar playing, what comes to mind is that researchers would like to become professionals and write original songs with only minimal experience from an amateur period. This is because the world of research always demands something new and original. As in music, however, the truth is that it takes a really long time to become able to create an original piece of work as a professional, since basic techniques or technologies must be learned.

These days, however, the expansion of the Internet has greatly accelerated the speed at which information can be exchanged compared with that when I entered NTT. I believe that an environment that demands speed will include harried young researchers seeking originality in their research. It is better, however, to think of originality as something separate from speed. To me, originality is not simply something that one would like to express on one's own. Rather, originality is achieved as a result of pursuing for many years something that one is deeply interested in and then being recognized by others for such efforts with comments like "that person is an original researcher" or "that's research like his".

Simply speaking, isn't originality doing something different from others? When a person has a deep interest in something, won't that interest reflect that person's background? Even in the case of several researchers working on the same research theme, I believe that their individual viewpoints developed from their respective backgrounds can lead to new directions and discoveries.

Furthermore, among very successful researchers, is it not true that the research they pursued in school seldom became their life's work? I think that a research theme that becomes one's life's work is a matter of encounter. No researcher knows when the most important encounter in his or her career will occur. On the other hand, there is no guarantee that a cool theme that one is attracted to at present will continue to be exciting and maintain one's interest in the future. In fact, it is quite likely that it will not.

We can draw an analogy with climbing a mountain. If your dream or major goal is a high mountain, then the problem right in front of your eyes can be thought of as a small mountain. Now, making every effort to

reach the peak of that small mountain will give you a far and wide view of your situation while increasing the intellectual and physical power you need to climb the next higher mountain. By pursuing research in this way, I believe that a researcher improves his or her chance of an auspicious encounter.

—*Dr. Muraki, what does research mean to you?*

I think of basic research as the work of making a map. This is a map not of an area that is already known but rather of unexplored terrain. Making a map means entering an unknown place, and in this sense, it is truly an adventure. To reach that place requires tools and technology, but having an eye for selecting the right tools and developing the skills for using them correctly are also necessary. Those already known to researchers are like the maps available at bookshops. Having an original map unknown to others is crucial to the success of the adventure. A researcher needs not only knowledge but also technical skills and physical stamina, and of greatest importance, the researcher must have a strong will that is unaffected by daily outcomes. My aim is to pursue work that redraws maps, that opens up paths to previously unknown places.

References

- [1] L. Tiemann, G. Gamez, N. Kumada, and K. Muraki, “Unraveling the Spin Polarization of the $\nu = 5/2$ Fractional Quantum Hall State,” *Science*, Vol. 335, No. 6070, pp. 828–831, 2012.
- [2] K. Muraki, T. Saku, and Y. Hirayama, “Charge Excitations in Easy-Axis and Easy-Plane Quantum Hall Ferromagnets,” *Phys. Rev. Lett.*, Vol. 87, No. 19, 196801, 2001.

Koji Muraki

Senior Research Scientist (Distinguished Researcher) and Group Leader of the Quantum Solid State Physics Research Group, NTT Basic Research Laboratories.

He received the B.E., M.E., and Ph.D. degrees in applied physics from the University of Tokyo in 1989, 1991, and 1994, respectively. He joined NTT Basic Research Laboratories in 1994. From 2001 to 2002, he was a visiting researcher at the Max Planck Institute for Solid State Research, Stuttgart, Germany. His research interests are focused on many-body effects in low-dimensional semiconductor structures. He is a member of the Physical Society of Japan and the Japan Society of Applied Physics.

Emergence of New Cyber Attacks and Future Directions in Security R&D

Tohru Matsuno, Toru Kawamura, Kazuhiko Ohkubo, Hidetsugu Kobayashi, Katsumi Takahashi, and Shigeru Kayaguchi

Abstract

From the viewpoint of a telecommunications operator, NTT is researching and developing new technologies for dealing with cyber attacks that are immune to existing ones. Cyber attacks have been evolving into large-scale, multifaceted attacks and their targets have grown to include clouds, smartphones, and industrial systems, raising concerns about their impact on society as a whole.

1. Introduction

1.1 ICT market trends

Corporate activities are undergoing major changes typified by keywords such as global and convergence. The information and communications technology (ICT) market is also changing as trends such as social networking, cloud computing, and multi-device lifestyles gain momentum. As the ICT market changes, so does the environment surrounding security issues (**Fig. 1**). The objectives of cyber attacks are changing and attacking techniques are becoming increasingly large-scale and multifaceted. In addition, new types of malware are continually being created, making it difficult for countermeasures to keep up with them. At the same time, cryptographic technology used for protecting data must be convenient to use from the viewpoint of users and security operations must provide a unified, advanced response both before and after the fact for various envisioned situations.

This article surveys the changes taking place in the environment surrounding security and introduces the direction of security-related research and development (R&D) in NTT to deal with these changes.

1.2 Evolution of cyber attacks

In the early days of cyber attacks, the perpetrators were mainly individuals who were simply intent on being mischievous or showing off their technical

proWess. In short, their objectives were individual in nature. Recently, however, attackers and their objectives have expanded. Groups of individuals on the Internet who share the same ideology and convictions and other types of groups that may even include national institutions have become attackers. These new types of attackers also have new objectives: in addition to financial gain, they may seek to disrupt the activities of entities (companies, public institutions, etc.) having different ideas and principles from themselves or steal confidential information. This means that their objectives have become ones that can have a major impact on society and the business world.

The techniques for mounting attacks are also changing. To achieve the above objectives, a type of attack called an advanced persistent threat (APT) has emerged. It carefully prepares and executes scenarios that combine multiple approaches and methods. Corporations and organizations that have already suffered APT attacks include major search engine sites, energy-related industries, and public offices. The APT attack aims to access confidential information and corrupt systems in a way that could have a major impact on society as a whole.

1.3 Expansion of countermeasures through technical innovation

In the past, the targets of cyber attacks were mainly

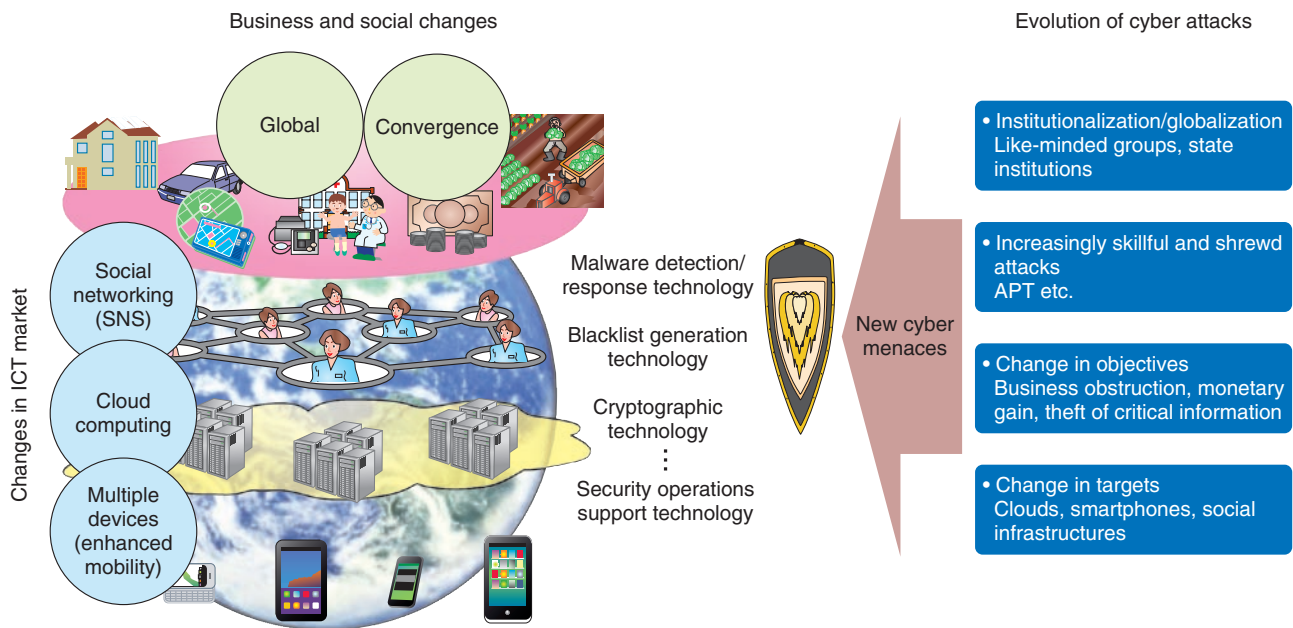


Fig. 1. Changes in ICT market trends and security environment.

the servers of computer systems and the personal computers of individual users. Nowadays, however, a wide variety of terminals including smartphones and tablets are connected to the network while operating systems and other operation platforms are becoming increasingly generalized and information distribution is becoming more open in nature. For example, mobile phones in Japan traditionally operated on separate operation platforms specified by different makers. Smartphones, however, are being provided on globally standardized operation platforms such as Android as a shift takes place from closed content distribution unique to each carrier to content distribution on an open market. These developments are creating an environment similar to the past situation with personal computers that makes it easy for attackers to devise attack methods and to increase the number of targets susceptible to an attack.

The number of cases of smartphones affected by malware is on the increase, suggesting that serious problems like the leakage of personal information will only intensify as smartphone users increase in number.

New issues are now coming to the fore as the cloud service operators make changes to the technologies that they use. Cloud computing is a technology that has significant benefits such as prompt system development and significant cost reductions because users

have no need to actually own the facilities they need. The use of clouds, though, can generate concern about security because users must entrust their confidential information to cloud service operators.

Up to now, each company has owned and managed its own corporate systems, but advances in cloud computing are prompting the shift of some management processes—such as the checking of operating conditions and the operation history of systems owned and managed by companies (customers)—to cloud service operators. However, as the cloud resources provided by cloud service operators can change dynamically, it is becoming increasingly difficult for companies (customers) to fully grasp the configuration of the systems they own and manage. To carry out security audits in a manner similar to that of conventional corporate systems, cloud operators need to provide a trail that can sustain an audit (**Fig. 2**).

In addition, even control systems for public and corporate infrastructures that have traditionally been closed using proprietary technology are introducing general-purpose technology because of its cost benefits, thereby creating new targets of attacks. For example, the malware called Stuxnet can penetrate certain industrial control systems even in environments segregated from the Internet. Its use to mount a cyber attack on a nuclear complex has made the

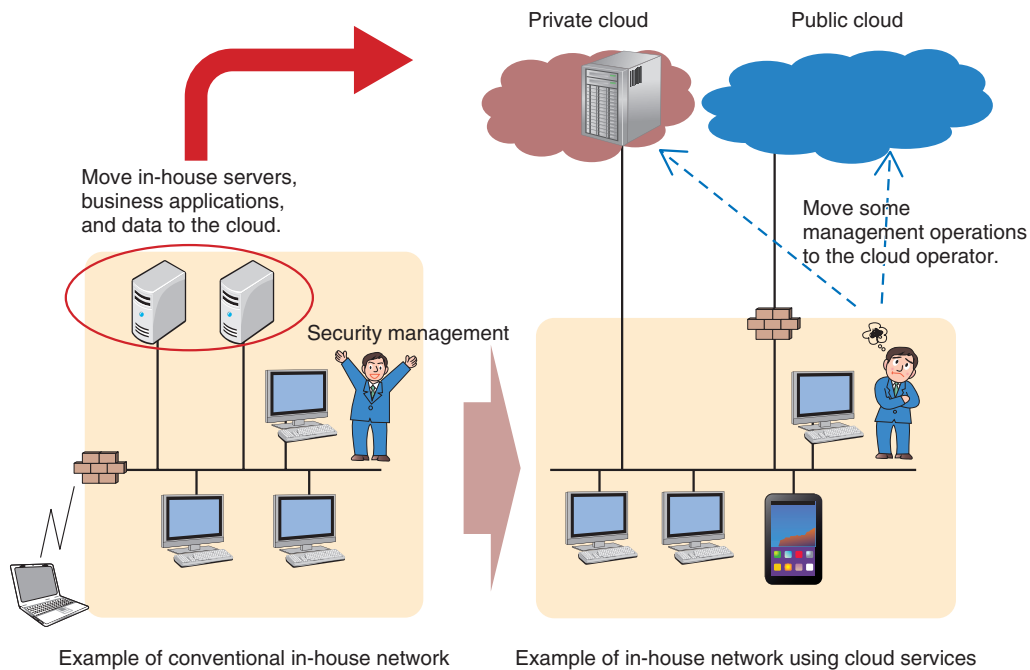


Fig. 2. Concerns about security in the cloud.

name Stuxnet notorious.

But public and corporate infrastructures are also social systems, and as such, they simply cannot come to a halt. The effects of an attack on such a system can be very great, but, as is the case with ordinary information systems, it is difficult to implement security countermeasures after a system has been brought down.

2. Countermeasures to new cyber attacks

The targets of ever-evolving cyber attacks are expanding on a daily basis, so attempting to tackle them with a conventional mindset is ineffective. There is an urgent need to fortify the development and deployment of anti-attack technologies on the basis of a new way of thinking and to enhance all security-related operations from the early detection of attacks and abnormal events that portend attacks to the restoration of a system damaged by an attack [1].

As new attack techniques appear in rapid succession and continue to evolve, it is essential to be able to detect a wide variety of attacks, including ones that are currently unknown, at an early stage. Up to now, it has taken much time to discover an attack, and the response to an attack has often been implemented

only after much damage had been caused. Dealing with attacks has therefore incurred much time and cost. If attacks and their indicators can be detected early and if early detection can be combined with effective countermeasures, it should be possible to curb the spread of damage.

In the cloud era in which data is routinely deposited and processed in the cloud, encryption is an absolute necessity. However, this is not just a matter of developing cryptographic technology that focuses on only confidentiality as in the past. It is also essential to develop cryptographic technology that places importance on the use and application of that data. If efforts were to be centered on only security at the sacrifice of convenience in everyday business and life, then security technologies would not be well received by users and corporate security administrators, and the level of security would actually drop as a consequence. From here on, there will be even greater demand for cryptographic technology that does not reduce usability from the user’s viewpoint.

For telecommunications operators like the NTT Group, accountability in relation to security events is also important. They must be able to give appropriate explanations to all business-related stakeholders including users, auditors, and even other operators.

In terms of strengthening security operations,

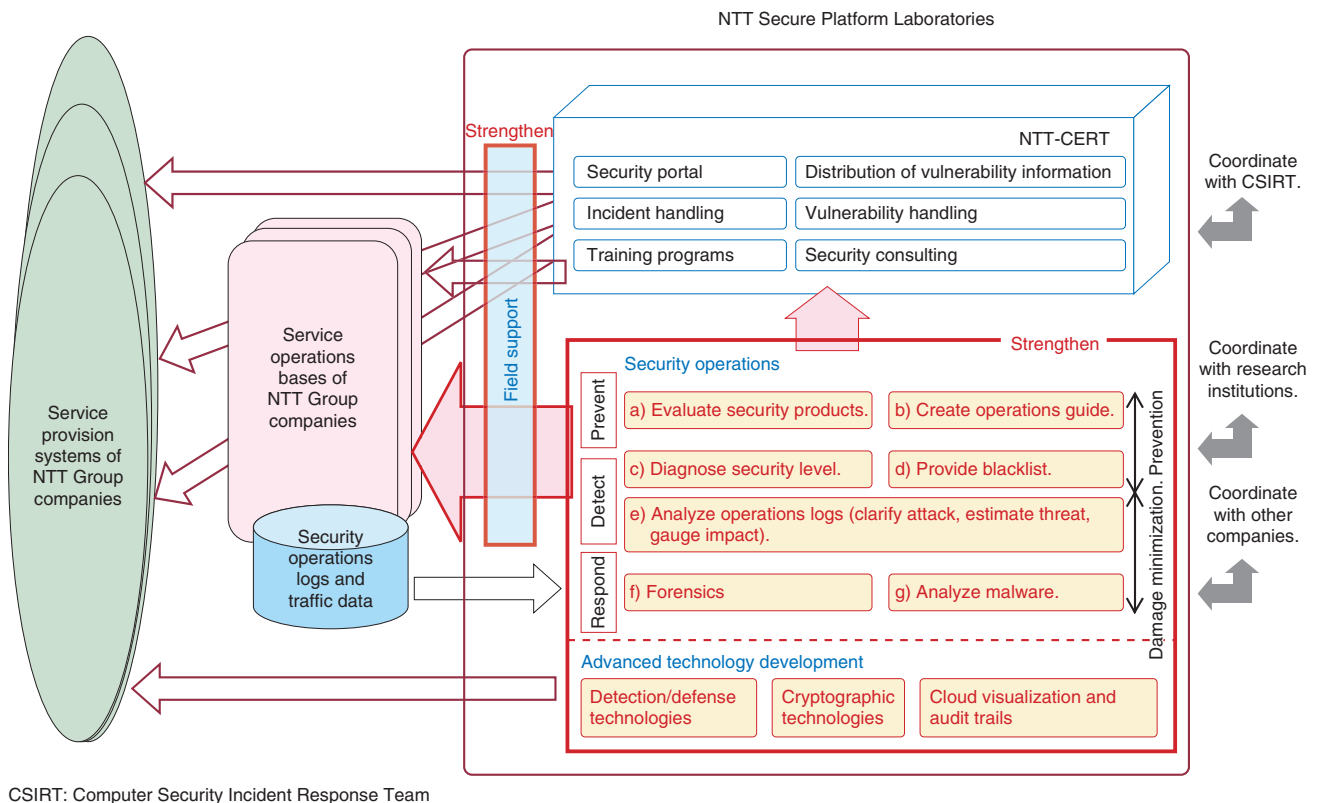


Fig. 3. Technology development and strengthening of security operations.

complete prevention of ever-evolving cyber attacks is difficult, which makes it important to prepare systems, accumulate know-how, and construct tools that can help discover and respond to attacks at an early stage. In this regard, importance should be placed on accumulating and systematizing know-how through daily security operations.

3. NTT's approach to cyber attacks

In NTT, researchers are taking a two-sided approach to dealing with new cyber attacks. First, they are developing advanced, security-related technologies, and second, they are developing techniques and accumulating know-how that can be put to immediate use in strengthening current security operations (Fig. 3).

In the development of advanced technologies, researchers are focusing their efforts in areas in which telecommunications operators feel that existing technologies are incapable by themselves of defending against new cyber attacks (Fig. 4). Specifically, the targets of these efforts can be divided into (1) detection, analysis, and countermeasure technologies; (2)

cryptographic technologies; and (3) cloud visualization and audit trails, as summarized below.

Detection, analysis, and countermeasure technologies for new cyber attacks have much to do with early detection of attacks and the ability to mount a prompt response. Two key points here are the large-scale collection and advanced analysis of attack-related data and the execution of countermeasures using the analysis results. NTT's laboratories coordinate with NTT Group companies to collect diverse types of security-log information from attack sensors located throughout the world. In the analysis of this information, those items deemed serious and requiring attention must be quickly extracted and passed on to the relevant system administrators. In the past, deciding what items required a response often depended on the judgment of skilled and experienced personnel. The aim now, however, is to use advanced technologies developed by NTT to automate the analysis of information about malicious applications, malicious websites, sources of attacks, etc. and to provide blacklists so that feedback can be provided promptly to operations. More details about these technologies are given

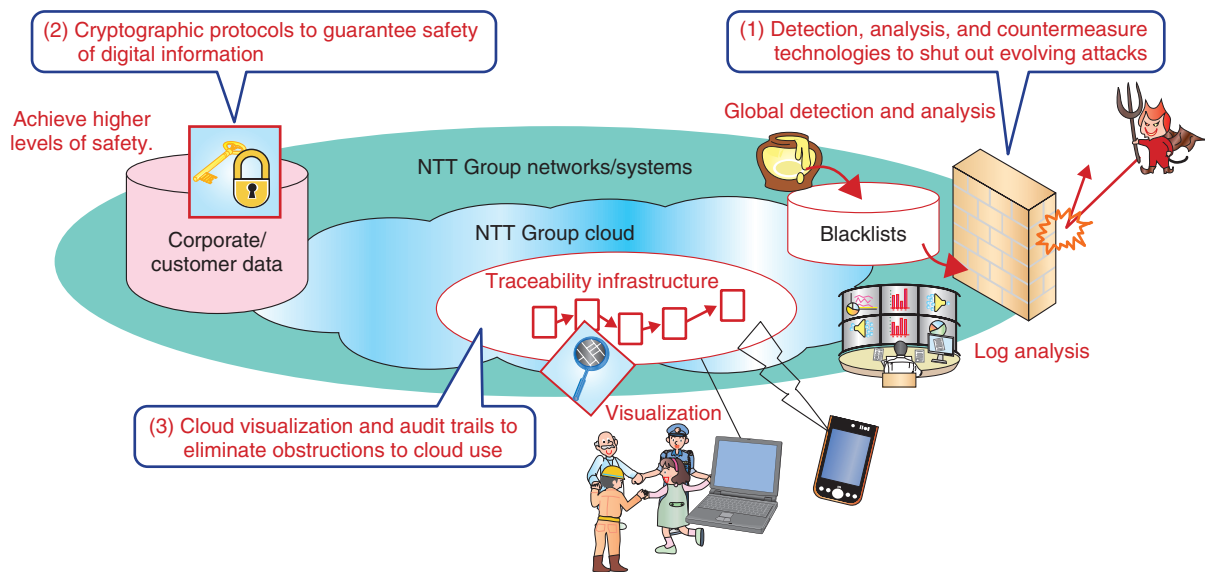


Fig. 4. Key fields in the development of advanced technologies.

in the Feature Article “Detection, Analysis, and Countermeasure Technologies for Cyber Attacks from Evolving Malware” [2] in this issue.

Next, in anticipation of the migration of data to a cloud infrastructure as systems convert to a cloud format, progress is being made in cryptographic technologies. NTT is promoting the formulation of new cryptographic theories, the creation of new cryptographic protocols, the application of cryptographic technologies to various types of systems, and the standardization of those technologies. More details about the development of new cryptographic technologies that take into account the environment surrounding security are given in the Feature Article “Cryptographic Techniques that Combine Data Protection and Ease of Utilization in the Cloud Computing Era” [3] in this issue.

The introduction of cryptography into a system does not guarantee safety from attacks on a permanent basis. Over time, the techniques used by attackers improve and attacks become more powerful, thereby making the cryptographic technology relatively vulnerable (cryptographic compromise). This means that cryptographic technologies that are currently in use must be reviewed periodically. NTT also provides information about the appropriate use of cryptography.

Finally, in the area of cloud visualization and audit trails, the plan is to develop a cloud-forensics function that can correctly interpret a history of operations

and events on the basis of operations information collected from the cloud. Such a function will help establish accountability in the provision of cloud services.

One more approach in addition to the development of advanced technologies is the development of techniques for strengthening security operations in the present. The NTT Computer Security Incident Response and Readiness Coordination Team (NTT-CERT) [4], [5] has been promoting methods for handling incidents and vulnerabilities, developing training programs, and supporting techniques for preventing the recurrence of attacks. Looking forward, NTT-CERT plans to develop a system for evaluating security technologies, create and disseminate an operations guide, and establish preventive measures such as security-diagnosis techniques for NTT Group websites. It also plans to provide information about malicious websites obtained from the abovementioned advanced technologies and to disseminate security-related know-how such as how to make early responses based on security-log analysis and how to collect and analyze Android malware. More details about techniques for strengthening security operations are given in the Feature Article “Tighter Security Operations to Help Provide Brands that are Safer and More Secure” [6] in this issue.

4. Concluding remarks

One question that is often asked in relation to security is “To what extent should I take measures to feel safe?” As described in this article, attacker expertise and attacking techniques are evolving quickly and the countermeasures to those attacks are expanding on a daily basis. In such an environment, there is no way that such evolving attacks can be dealt with effectively if today’s countermeasures are considered to be satisfactory. The technology infrastructure supporting information systems is also undergoing severe change together with the social environment, business environment, and technology trends. NTT Secure Platform Laboratories is moving forward with the development of cutting-edge technologies and seeks to contribute to enhanced system safety and the secure provision of services through the development of technologies that can strengthen security operations.

References

- [1] “Special Feature: Trend of Network Security Technologies,” NTT Technical Review, Vol. 8, No. 7, 2010.
<https://www.ntt-review.jp/archive/2010/201007.html>
- [2] T. Hariu, M. Akiyama, K. Aoki, T. Yagi, M. Iwamura, and H. Kurakami, “Detection, Analysis, and Countermeasure Technologies for Cyber Attacks from Evolving Malware,” NTT Technical Review, Vol. 10, No. 10, 2012.
<https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa2.html>
- [3] H. Fuji, A. Fukioka, T. Kobayashi, K. Chida, F. Hoshino, T. Miyazawa, and K. Suzuki, “Cryptographic Techniques that Combine Data Protection and Ease of Utilization in the Cloud Computing Era,” NTT Technical Review, Vol. 10, No. 10, 2012.
<https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa3.html>
- [4] M. Nagashima, Y. Sugiura, T. Abe, T. Yoshida, and A. Mukaiyama, “CSIRT Activities at NTT,” NTT Technical Review, Vol. 8, No. 7, 2010.
<https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201007sf5.html>
- [5] NTT-CERT. <http://www.ntt-cert.org/index-en.html>
- [6] 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>



Tohru Matsuno

Chief producer, NTT Research and Development Planning Department.

Since joining NTT in April 1990, he has contributed to the development of digital exchanges, systems engineering, human resource management, global sales, and the datacenter business. He is currently leading NTT's security R&D activities.



Hidetsugu Kobayashi

Project Manager, Network Security Project, NTT Secure Platform Laboratories.

Since joining NTT in April 1987, he has contributed to the development of a range of network-security-related products such as firewalls for IP-VPNs and authentication servers for the NGN. His research interests include network security and information networks.



Toru Kawamura

Producer, NTT Research and Development Planning Department.

Since joining NTT in April 1988, he has contributed to R&D-related data communication traffic control, a recommendation engine, and a 3D-GUI system for web browsing and some applications using cryptographic technology. He is currently promoting security R&D activities for the NTT Group.



Katsumi Takahashi

Project Manager, Information Security Project, NTT Secure Platform Laboratories.

He received the B.S. degree from Tokyo Institute of Technology in 1988 and the Ph.D. degree from the University of Tokyo in 2006. Since joining NTT in 1988, he has been working on information retrieval, data mining, cryptographic protocols, information security, privacy protection, and security social science.



Kazuhiko Ohkubo

Vice President, Project Manager, Security Management & Operations Project, NTT Secure Platform Laboratories.

He was engaged in operation system developments for intelligent networks and interactive multimedia systems in the 1990s. After receiving the MBA from MIT Sloan in 2000, he promoted R&D renovations by introducing exhaustive commercialization functions called the *producer system*. Recently, he has generalized security management related R&D such as CSIRT, SIEM, and cloud security platforms.



Shigeru Kayaguchi

Senior Research Engineer, Supervisor, Security Management & Operations Project, NTT Secure Platform Laboratories.

Since joining NTT, he has been engaged in operation system development for ISDN services, new business development, and the management of an Internet media venture company. His research interests include cloud security, smartphone security, and methods of compromising cryptosystems.

Detection, Analysis, and Countermeasure Technologies for Cyber Attacks from Evolving Malware

Takeo Hariu, Mitsuaki Akiyama, Kazufumi Aoki, Takeshi Yagi, Makoto Iwamura, and Hiroshi Kurakami

Abstract

After outlining trends in cyber attacks mounted mainly through the use of malicious software (malware), we describe technology for detecting malware infections and isolating infection sources and technology for analyzing malware and extracting the features of its functions; describe how information obtained from detection and analysis can be used by countermeasure technology to generate blacklists and defend against attacks on the network; and describe analysis techniques for tracing attacks by using logs kept by network devices.

1. Introduction

Cyber attacks that infect personal computers (PCs) and servers on the Internet to gain unauthorized access to personal information have become a serious problem in society. An example of malicious software (malware) infecting a PC via the web is shown in **Fig. 1**. A PC having a vulnerable web browser or plugin accesses a portal or relay site on which an attacker has prepared content for performing automatic transfers. As a result, the PC's Internet link is automatically transferred to an attack site on which attack code has been placed. The PC then receives this attack code and downloads and executes the related malware. The PC is now infected, enabling information to be sent from the PC to the attacker's command site and commands to be sent from the command site to the PC. Since attackers can exploit a wide variety of vulnerabilities to achieve malware infections, it is difficult to detect which vulnerabilities have been targeted and what caused the infection. Moreover, the continual appearance of new malware is making it more difficult to analyze the functions of each type of malware and gauge its threat.

To develop countermeasures to malware infections, research has been active in technology for detecting

infections and determining their causes and technology for analyzing malware. Detecting an infection requires an accurate understanding of the attack mounted at the time of infection, but this requires highly specialized knowledge in the use of detection technologies. Another problem is that new types of attacks and malware are now appearing in extremely short cycles. There is therefore a need to grasp attack trends and research and develop new technologies as early as possible.

2. Malware detection, analysis, and countermeasure technologies

To solve the above problems, NTT is researching and developing malware detection, analysis, and countermeasure technologies [1] in a three-phase manner, as shown in **Fig. 2**. These phases are described below.

In the first phase, detection technology is being developed to receive attacks using a *honeypot*, which is an undercover system for attracting attacks and collecting malware. Communications between the Internet and honeypot can be analyzed and useful information for preventing malware infections can be extracted.

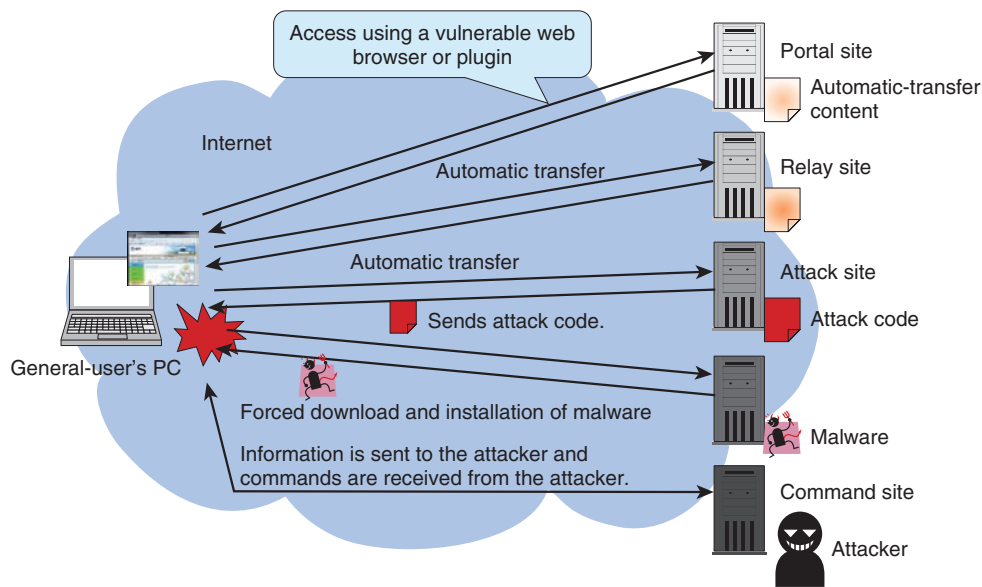


Fig. 1. Malware infection of PC (via web).

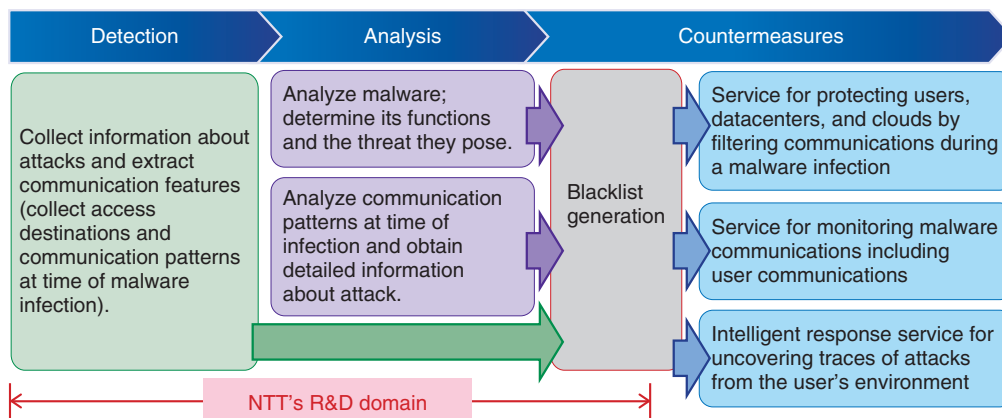


Fig. 2. R&D of malware detection, analysis, and countermeasure technologies at NTT.

Next, in the second phase, analysis technology is being developed to analyze the malware collected by the honeypot and the associated communication patterns. The aim is to understand the malware's functions and determine the threat that it poses, and in general, to acquire detailed information about the attack.

Finally, in the third phase, countermeasure technology is being developed to use the information obtained by the above detection and analysis technologies to generate blacklists in a format that can be used by services. Addresses of access destinations

appearing at the time of a malware infection extracted by detection technology can be used to generate blacklists consisting of URL (uniform resource locator) lists, IP (Internet protocol) address lists, etc. In the example in Fig. 1, the URLs of malicious sites—from the portal to the command site—can be added to a blacklist. Such a blacklist can be used as a communications filter to protect the user from malware infections during access to the Internet. Likewise, the addresses of access destinations appearing after a malware infection, as determined by analysis technology, can be used to generate a blacklist. Such

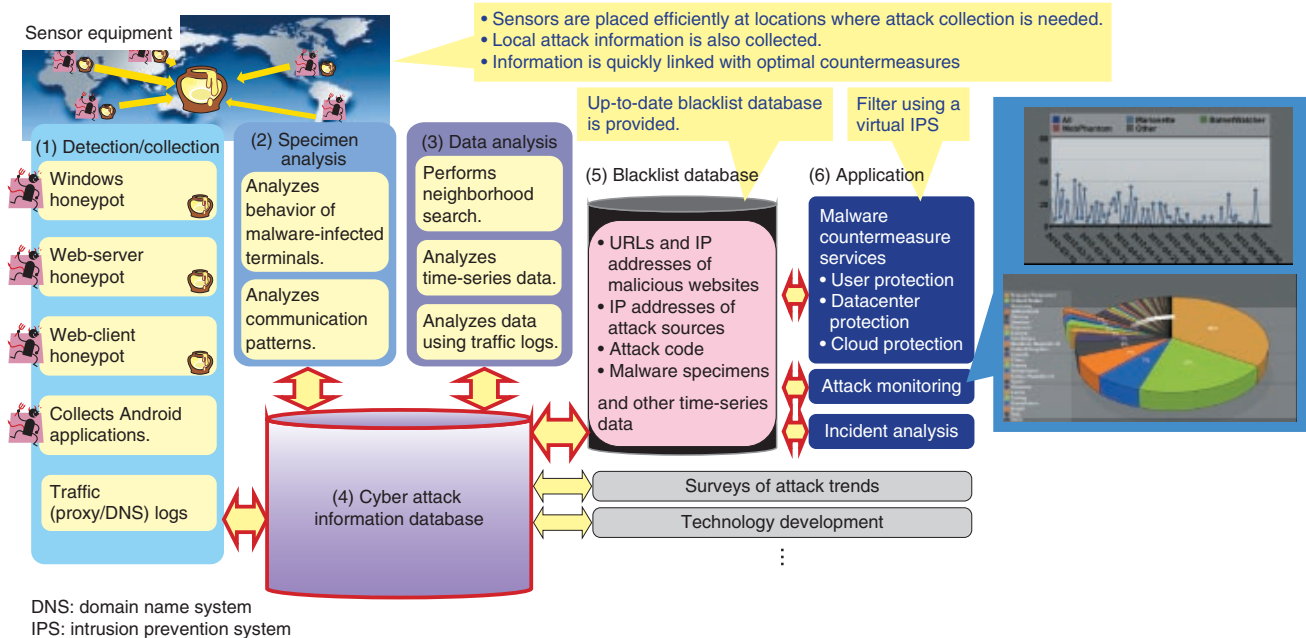


Fig. 3. Blacklist generation technology.

blacklists can be used by incident response services to check for the presence of malware infections or the occurrence of damage in a user’s environment. Section 3 describes blacklist generation technology in more detail.

3. Blacklist generation technology

Blacklist generation technology takes information about malicious URLs, IP addresses, etc. extracted or identified by detection and analysis technologies and converts it into blacklists in a form conducive to actual use (Fig. 3). These blacklists make it possible to conduct filtering based on malicious-site information without requiring the user to have extensive, specialized knowledge.

First, detection technology is used to collect malware-related information through the use of various types of honeypots that enable information about malware infections to be collected in a safe manner ((1) in Fig. 3). Honeypots are developed specifically for different types of malware infection methods that pose threats to society. For example, there are Windows honeypots targeting attacks that exploit vulnerabilities in the Windows operating system, web-server honeypots targeting attacks that exploit vulnerabilities in web applications [2], and web-client honeypots targeting attacks that exploit vulnerabilities in

web browsers [3].

NTT has developed analysis technology for analyzing malware specimens (2) consisting of open-environment-type malware dynamic analysis technology [4] and a debugger for analyzing the behavior of malware on a computer [5]. The former runs malware within an analysis environment that, while not allowing communications that would create more harm such as the spread of a malware infection, does allow communications with actual attackers on the Internet. This makes it possible to analyze behavior such as malware communication patterns on the network. The latter enables the behavior of malware to be analyzed without the malware itself being aware of the debugger’s existence. As advanced technologies unprecedented in Japan or abroad that can accurately grasp malware functions, these developments reflect NTT’s R&D strength.

Data analysis technology (3) consists of neighborhood search technology for automatically and efficiently discovering malicious URLs similar in structure to malicious URLs that have already been discovered [6], time-series data analysis technology for retrospectively analyzing the data collected by honeypots when a new attack or malware program is discovered, and data analysis technology for inspecting user access destinations by using traffic logs when a web-client honeypot was used. In particular,

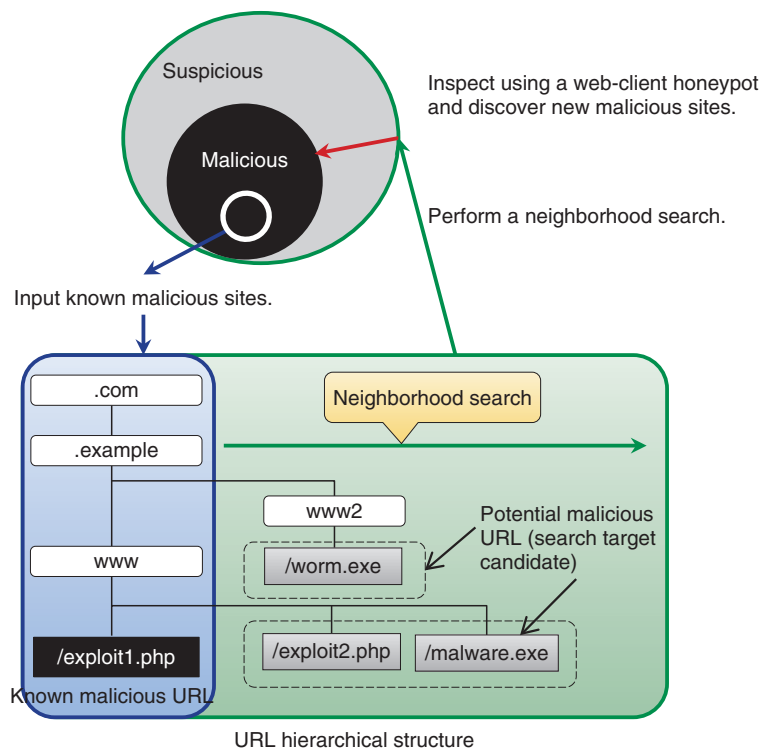


Fig. 4. Neighborhood search technology.

neighborhood search technology (**Fig. 4**) is an original development by NTT. It can discover information about malicious sites that has until now not been included in ordinary blacklists because of the difficulty of uncovering it. NTT has received a commendation for this technology at an IEEE international meeting.

The information obtained by these detection and analysis technologies is stored in a cyber attack information database (4). The idea is to continuously expand the information in the database by coordinating the detection and analysis technologies and repeating the information-collection and analysis processes. In addition to blacklist generation, the information stored in this database can be used to survey attack trends and develop new anti-malware technologies.

The information stored in this cyber attack information database is now used to generate specific blacklists, which are stored in the blacklist database (5). These include a list of URLs of malicious websites that, if accessed, will result in a malware infection, and a list of IP addresses of attack origins.

These blacklists are used to protect users, datacenters, and clouds (6). For example, they can be installed

and used as filters in anti-attack equipment composing a firewall, intrusion detection system (IDS), or intrusion prevention system (IPS). They can also be applied to the monitoring of traffic logs and other information to aid in discovering attacks and used as reference information in incident response. Section 4 describes methods for using these blacklists.

4. Methods for using blacklists

4.1 Methods

As shown in **Fig. 5**, the blacklist database stores four types of information, A–D, as effective data for an IDS/IPS to defend against attacks as well as two types, E and F, that will be provided to users. As an example of using type-A information, consider a list of URLs of malicious websites that would infect a client with malware if accessed by a vulnerable web browser. This list can be installed in an IDS/IPS filter on a user network to block access to malicious websites and protect the user's PC. Next, as an example of using type-B information, consider a list of URLs of malicious websites that web servers accessed at the time of a malware infection caused by an attack. This list can be installed in an IDS/IPS filter in a cloud

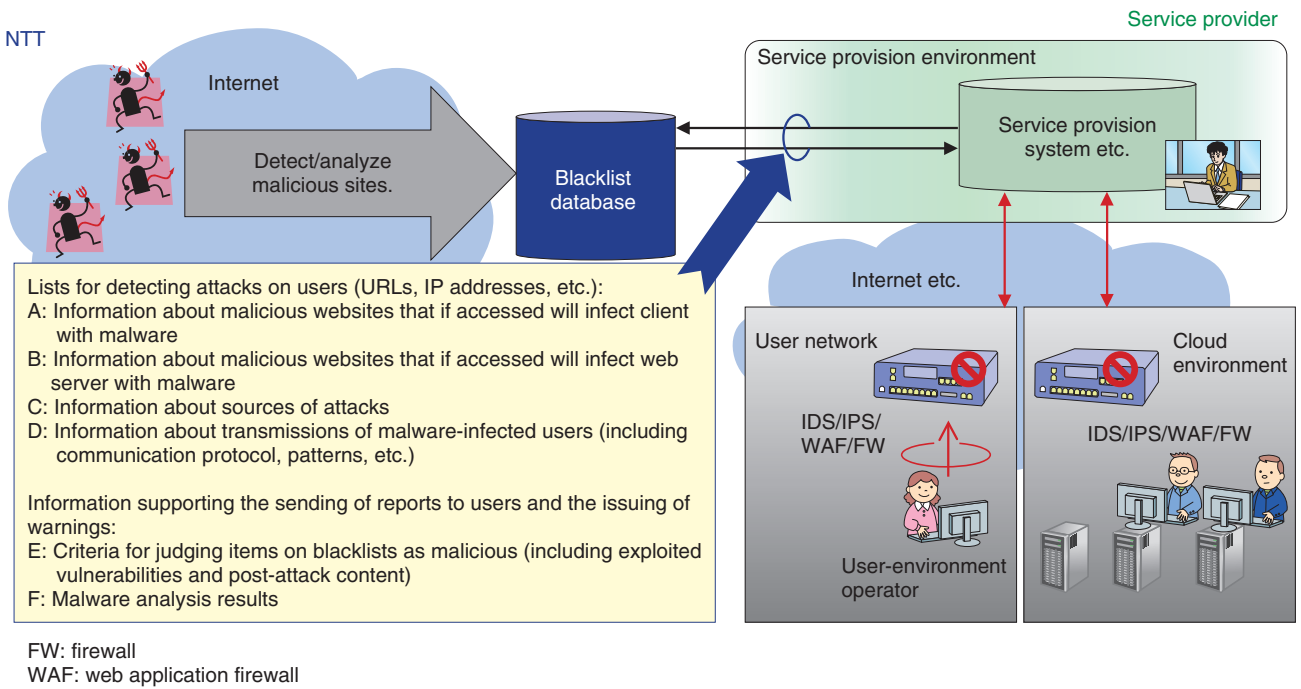


Fig. 5. Use of blacklists.

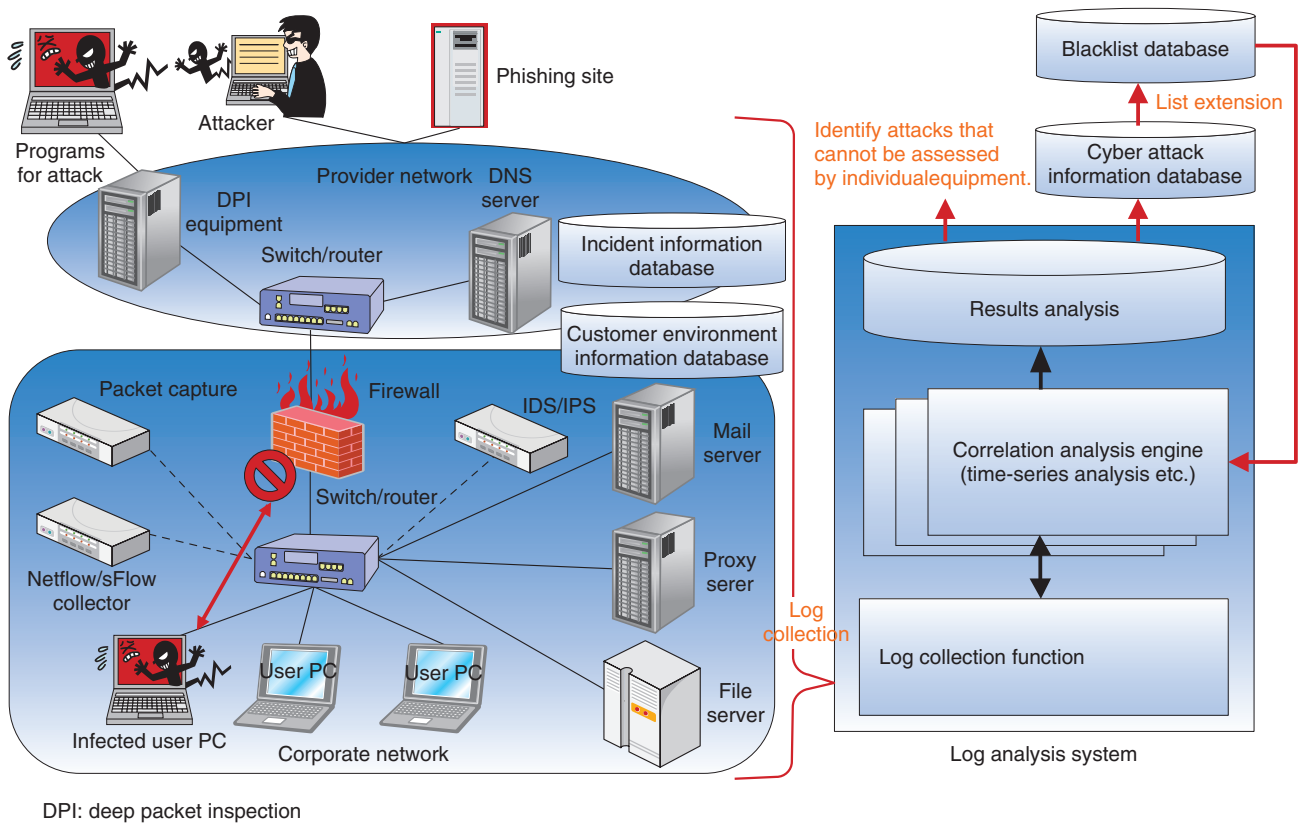


Fig. 6. Concept of log analysis.

environment to block further access to malicious websites and protect web servers. At this time, a list of IP addresses from which attacks are mounted against web servers (type-C information) can also be used in a filter to block access from IP addresses from which an attack is possible. Moreover, a list of access destinations uncovered during malware analysis (type-D information) can be installed in an IDS/IPS as a monitoring target to discover users susceptible to a malware infection. Information of types E and F can be used for services that create reports for users and issue warnings at the time of a security incident.

Blacklist generation technology can also be used for inspecting whether a specific website is malicious. For example, the logs of a user's proxy server or DNS (domain name system) server can be analyzed and websites found to be frequently accessed by the user can be periodically inspected so that malicious websites having a high possibility of being accessed by the user can be put on a blacklist early.

There are plans to extend the types of information stored in the blacklist database. Functions will eventually be extended with the aim of applying the data collected by honeypots and malware analysis to incident response.

4.2 Log analysis using blacklists

As shown in **Fig. 6**, blacklists can be used to perform correlation analysis with firewall, IDS, and IPS security-equipment logs, proxy/file server logs, logs output from client PCs, and logs of packet information to extract the behavior of attacks and information leaks on the network. Performing long-term log correlation analysis through a log analysis system makes

it possible to isolate abnormal behavior that cannot be identified by firewalls or IDS/IPS equipment alone. In this way, countermeasures to many types of attacks including targeted attacks can be formulated.

5. Future developments

NTT Secure Platform Laboratories plans to construct prototype tools for implementing detection, analysis, and countermeasure technologies and conduct diverse evaluation experiments to keep pace with quickly evolving cyber attacks.

References

- [1] M. Itoh, T. Hariu, N. Tanimoto, M. Iwamura, T. Yagi, Y. Kawakoya, K. Aoki, M. Akiyama, and S. Nakayama, "Anti-Malware Technologies," NTT Technical Review, Vol. 8, No. 7, 2010. <https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201007sf3.html>
- [2] T. Yagi, N. Tanimoto, T. Hariu, and M. Itoh, "Intelligent High-interaction Web Honeypots Based on URL Conversion Scheme," IEICE Trans. Commun., Vol. E94-B, No. 5, pp. 1339–1347, 2011.
- [3] M. Akiyama, M. Iwamura, Y. Kawakoya, K. Aoki, and M. Itoh, "Design and Implementation of High Interaction Client Honeypot for Drive-by Download Attacks," IEICE Trans. Commun., Vol. E93-B, No. 5, pp. 1131–1139, 2010.
- [4] K. Aoki, T. Yagi, M. Iwamura, and M. Itoh, "Controlling Malware HTTP Communications in Dynamic Analysis System Using Search Engine," Proc. of the 3rd International Workshop on Cyberspace Safety and Security (CSS2011), Milano, Italy, 2011.
- [5] Y. Kawakoya, M. Iwamura, and M. Itoh, "Memory Behavior-based Automatic Malware Unpacking in Stealth Debugging Environment," Proc. of the IEEE International Conference on Malicious and Unwanted Software (MALWARE2010), Nancy, France, 2010.
- [6] M. Akiyama, T. Yagi, and M. Itoh, "Searching Structural Neighborhood of Malicious URLs to Improve Blacklisting," Proc. of the 12th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT 2011), Munich, Germany, 2011.



Takeo Hariu

Senior Research Engineer, Supervisor, Network Security Project, NTT Secure Platform Laboratories.

He received the M.S. degree in electro-communications from the University of Electro-Communications, Tokyo, in 1991. Since joining NTT in 1991, he has been engaged in network security R&D. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and the Institute of Electrical Engineers of Japan (IEEJ).



Takeshi Yagi

Research Engineer, Network Security Project, NTT Secure Platform Laboratories.

He received the B.E. degree in electrical and electronic engineering and the M.E. degree in science and technology from Chiba University in 2000 and 2002, respectively. Since joining NTT in 2002, he has been engaged in network architecture R&D. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. His current research interests include network security and web security. He is a member of IEICE and IEEJ.



Mitsuaki Akiyama

Network Security Project, NTT Secure Platform Laboratories.

He received the M.E. degree in information science from Nara Institute of Science and Technology in 2007. Since joining NTT in 2007, he has been engaged in network security R&D. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of IEICE.



Makoto Iwamura

Research Engineer, Distinguished Researcher, Network Security Project, NTT Secure Platform Laboratories.

He received the B.E., M.E., and D.Eng. degrees in science and engineering from Waseda University, Tokyo, in 2000, 2002, and 2012, respectively. He joined NTT in 2002. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. His research interests include reverse engineering, vulnerability discovery, and malware analysis.



Kazufumi Aoki

Network Security Project, NTT Secure Platform Laboratories.

He received the M.S. degree in information science from Tohoku University, Miyagi, in 2006. Since joining NTT in 2006, he has been engaged in network security R&D. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of the Information Processing Society of Japan (IPSI) and IEICE.



Hiroshi Kurakami

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

He received the B.S. degree in physics from Tohoku University, Miyagi, in 1991. Since joining NTT in 1991, he has been engaged in R&D of ATM networks, IP VPNs, and network security. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories.

Cryptographic Techniques that Combine Data Protection and Ease of Utilization in the Cloud Computing Era

Hitoshi Fuji, Atsushi Fujioka, Tetsutaro Kobayashi, Koji Chida, Fumitaka Hoshino, Toshiyuki Miyazawa, and Koutarou Suzuki

Abstract

In this article, we introduce cryptographic techniques that protect data in the cloud computing era while being easy to use. Specifically, we describe secure computing technology—which can keep private information confidential while enabling anonymous statistical analysis—and intelligent encryption, a cloud-managed-key cryptographic scheme, and an authenticated key exchange technique that together can protect data in cloud storage and prevent the leakage of keys.

1. Introduction

In recent years, the quantity of data has been growing at an explosive rate, and the proportion of highly confidential data has also been increasing. According to one survey, the data generated or copied worldwide in 2010 amounted to 1.2 zettabytes (10^{21} bytes), of which 28% needed to be stored securely. This proportion is likely to increase in the future and is predicted to reach 33% by 2015 [1]. When critical data is stored and used in the cloud in such large quantities, we need technology to ensure that information is managed safely according to its degree of confidentiality and intended purpose and to ensure that it can be used safely (**Fig. 1**).

In this article, we introduce secure computing technology that can process confidential information, such as personal details and business records, and enable anonymous statistical analysis while ensuring that privacy is maintained; intelligent encryption and a cloud-managed-key cryptographic scheme that protect data used in the cloud and prevent information from being leaked; and an authenticated key exchange

technique that can ensure confidential information is protected against leaks.

2. Technologies

2.1 Secure computing technology

With the changes in information processing platforms brought about by cloud computing, the management and practical application of confidential information is becoming more complex. One technique for protecting confidential information is secret sharing technology, which stores data in distributed form across multiple servers in such a way that safety is maintained even if data is leaked from any one of these servers [2]. NTT is researching and developing secure computing technology that can process shared secret information without restoring the original information. An outline of this processing technique is shown in **Fig. 2**.

A major feature of secure computing technology is that information processing is implemented cooperatively by multiple computers so that the data never exists intact on any one computer. This greatly

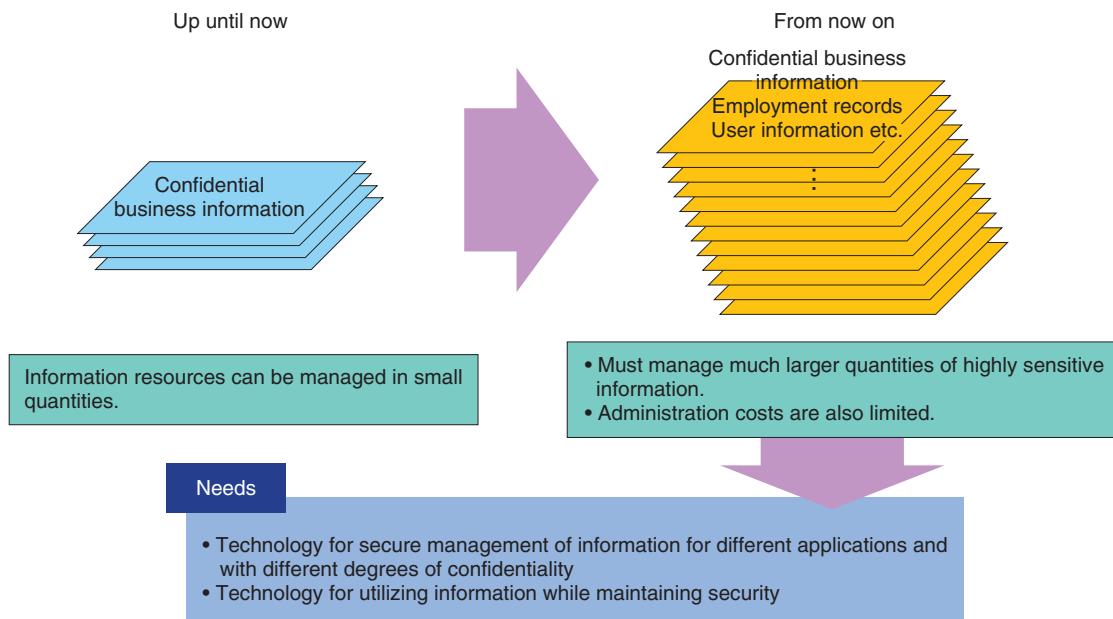


Fig. 1. Protecting information in the cloud computing era.

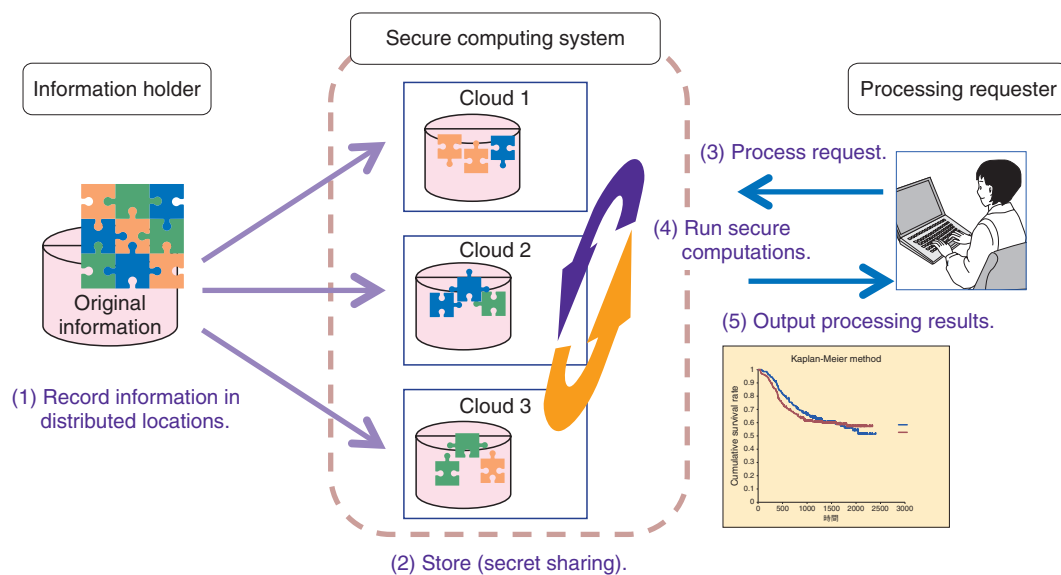


Fig. 2. Secure computing technology.

reduces the risk of information leaks and helps to dispel anxieties when information is provided to the cloud.

With the aim of facilitating the safe and secure utilization of clinical research data, the Japan Adult Leukemia Study Group and NTT were the first in the

world to demonstrate the feasibility of secure computing technology in the processing of medical statistics, as announced in a press release in February 2012 [3], [4]. In this demonstration, we were able to output the results of medical statistics processing while maintaining the confidentiality of patient data

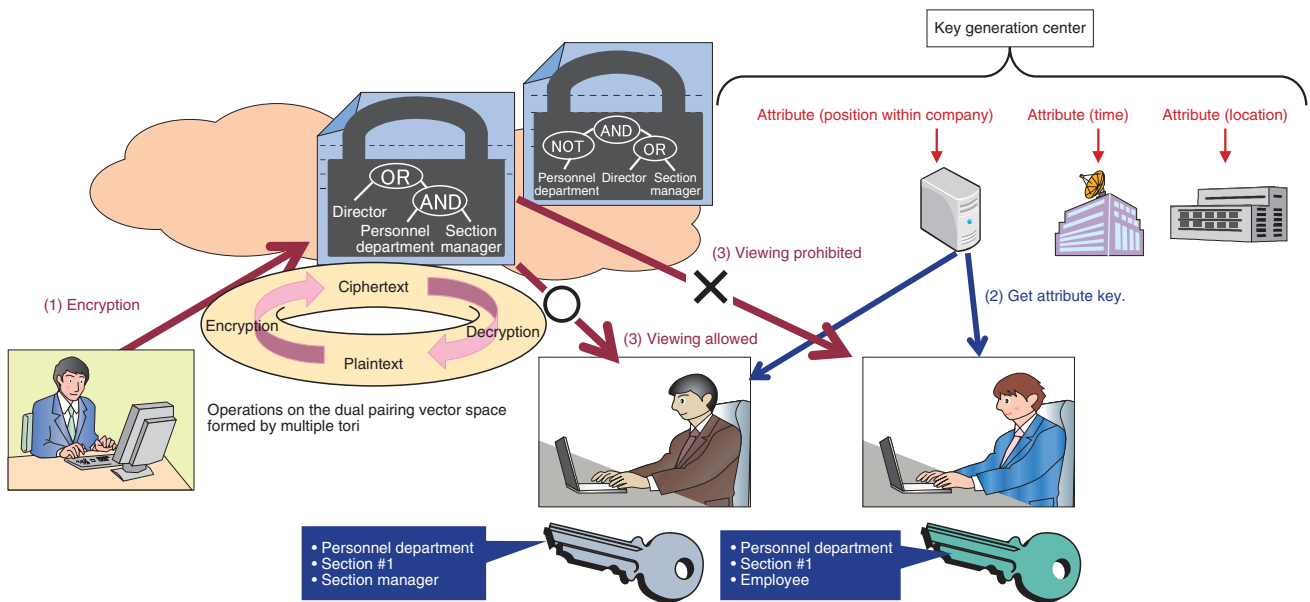


Fig. 3. Intelligent encryption.

registered from multiple medical facilities. This technology enables anonymous statistical analysis of confidential information held by various businesses.

Although secure computing technology is known to be secure in theory, its application to practical systems has been hindered by the limited processing speed. NTT’s secure computing system is the fastest of its kind anywhere in the world: it has achieved a speed of 1 million multiplication operations per second as a basic performance indicator. By developing data manipulation operations based on our proprietary algorithms, we have made it possible to perform a wide variety of information processing tasks in a practical amount of time, such as sorting 10,000 records in two seconds while maintaining the confidentiality of the information being sorted. The demonstration of medical statistics processing was implemented with approximately 1000 data records, but we are working on improvements to our algorithms and hardware that will enable a diverse variety of information processing to be performed in a practical amount of time on large-scale data sets.

2.2 Intelligent encryption

Besides secret sharing, another method for protecting confidential information is the use of encryption, which has the advantage of allowing data to be stored safely at one location. However, conventional cryptography has required that only one person (the

viewer) is authorized to see the clear content (plaintext) of the encrypted ciphertext. This makes it difficult for large numbers of people to access ciphertexts in the cloud. By contrast, intelligent encryption works by specifying, at the time of encryption, the conditions under which encrypted content can be viewed rather than the identity of the authorized viewer. This makes it possible to set up an access control system in which attribute keys corresponding to the attributes of each individual are distributed to viewers and viewing is allowed only when the viewing permission conditions and conditions related to the attribute keys held by the viewer (specified during encryption) have been met.

For example, consider the situation shown in Fig. 3, where access to confidential information is managed within a company. Conditions for viewing the information are incorporated into the ciphertext, and attribute information is applied to the decryption key so that decryption is possible only with a key that matches these conditions. If the data is encrypted with embedded conditions such as “[Director] OR [Personnel department AND Section manager]”, then it can be decrypted with a key containing the attributes [Personnel department, Section #1, Section manager], but not by a key containing the attributes [Personnel department, Section #1, Employee].

We have also developed an improved version of intelligent encryption that supports multiple attribute

key creation stations [5]. With this method, keys corresponding to various attributes associated with a particular individual (department, time, location, address, age, etc.) are issued separately by organizations that are able to verify these attributes, thereby enabling control of this individual's access to encrypted files subject to usage conditions such as the department, time, or location, regardless of where these files are located.

Intelligent encryption is complete in terms of encryption theory, and we are currently working to develop peripheral technologies, such as communication protocols and key management methods, and to improve its processing performance.

With regard to communication protocols, conventional public-key and shared-key encryption systems rely on standard protocols and a pre-established public key certification infrastructure (public key infrastructure), allowing people all over the world to use encryption according to standard methods. We are working with universities and other research organizations with the aim of preparing standards and infrastructures to make intelligent encryption easily available to everyone.

With regard to the management of attribute keys, there are still issues specific to intelligent encryption that need to be resolved, such as the authentication of attribute information and the invalidation of compromised keys, and we are continuing to study ways of resolving these issues.

With regard to processing performance, we are currently at the level where it is possible to perform encryption and decryption in about 1 s on an ordinary personal computer. In the future, we aim to speed up the processing to the same level even on mobile devices, which are likely to become much more prevalent in the future.

2.3 Cloud-managed-key cryptographic scheme

An issue that affects all encryption techniques is the inherent danger of allowing users to manage (store and distribute) decryption keys themselves. Furthermore, since a user who has obtained a decryption key is then able to decrypt ciphertexts at any time, there is another problem in that users can still view the content of ciphertexts in situations where they no longer have the authority to do so.

NTT has therefore developed a cloud-managed-key cryptographic scheme (referred to hereinafter as the cloud cryptographic scheme) that solves the issue of key management in public key cryptography [6]. The cloud cryptographic scheme is a technique where

decryption keys for public key cryptography are managed in the cloud (hereinafter referred to as a key management cloud), and the decryption processing is securely outsourced to the key management cloud. This allows users to make use of encrypted data without having to manage the decryption keys. Since the decryption processes can be enabled or disabled on the basis of authentication by the key management cloud, it is also possible to enable or disable the reading of a previously distributed ciphertext at a later time. This use of a key management cloud can provide a solution to the previous problem of needing a method for invalidating keys in intelligent encryption.

We are currently concluding our basic theoretical research on the cloud-managed-key cryptographic scheme, and we are also adding the final touches to a prototype system that can use highly confidential data in an online environment. To make this technology suitable for future business applications, we will press ahead with research aimed at practical applications and with the development of marketable systems. Specifically, we are continuing to investigate the availability of the key management cloud and the overall safety of the system, and we are conducting research and development aimed at specific services, such as applications to services that entrust data to the cloud (cloud storage services).

2.4 Authenticated key exchange

For secure exchange of information via public clouds or the Internet, there is a technique in which a secure communication channel is established by mutual authentication of two (or more) parties who want to exchange data by sharing keys used for confidential communication. This technique is called authenticated key exchange. An example of an authenticated key exchange scheme is SSL (Secure Socket Layer), which is upgraded whenever a vulnerability has been discovered.

As a result of its research on authenticated key exchange, NTT has developed an authenticated key exchange protocol [7] that satisfies the strongest level of safety and has been mathematically proven to be secure against all forms of key disclosure attack. An extended version of this protocol has been proposed to international standards organizations. In the above-mentioned intelligent encryption system, the person decrypting the information must have an attribute key for this purpose, but a technique for securely handing over attribute keys to the appropriate individuals in advance is also required. An authenticated key

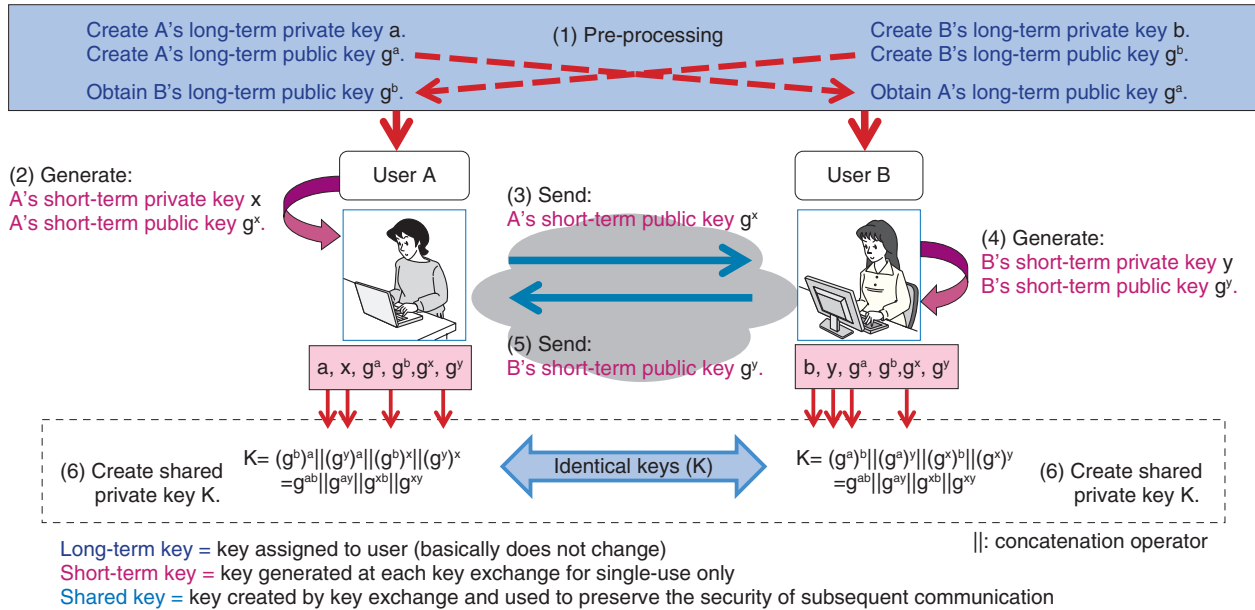


Fig. 4. Authenticated key exchange.

exchange can be used for this purpose.

An example of how authenticated key exchange is executed to share a shared key based on mutual authentication between two users over a public communication channel such as the Internet is shown in Fig. 4. Two users create shared keys as follows: each user performs exponential calculations based on his or her own long- and short-term private keys, called static and ephemeral keys, respectively, and the other user's long- and short-term public keys. The results are shared private keys that are guaranteed to be identical.

In this protocol, the long-term private keys are assigned to individual users and the short-term private keys are generated for each authenticated key exchange session. It is mathematically guaranteed that the confidentiality of the shared private keys is protected even if long- and short-term private keys are leaked in any combination (except in the case where both the long- and short-term private keys of the same user are compromised).

In addition to the public-key-based authenticated key exchange shown in Fig. 4, where authentication is performed between two users with public keys, there are also variants of authenticated key exchange such as a protocol where it is possible that a shared

private key is shared only when the other party fulfills certain specified conditions, as in intelligent encryption. We are continuing to research these advanced authenticated key exchange protocols.

References

- [1] J. Gantz and D. Reinsel, "Extracting Value from Chaos," IDC, 2011.
- [2] K. Chida and K. Takahashi, "Privacy Preserving Computations without Public Key Cryptographic Operation," Proc. of the 3rd IWSEC (IWSEC 2008), Kagawa, Japan, Lecture Notes in Computer Science, Vol. 5312, pp. 184–200, 2008.
- [3] Press release by NTT (in Japanese).
<http://www.ntt.co.jp/news2012/1202/120214a.html>
- [4] H. Shinohara, "R&D to Create the Future of ICT," NTT Technical Review, Vol. 10, No. 4, 2012.
<https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201204fa2.html>
- [5] T. Okamoto and K. Takashima, "Efficient Attribute-based Signatures for Non-monotone Predicates in the Standard Model," Proc. of the 14th International Conference on Practice and Theory in Public Key Cryptography (PKC 2011), Taormina, Italy, Lecture Notes in Computer Science, Vol. 6571, pp. 35–52, 2011.
- [6] G. Yamamoto and T. Kobayashi, "Self-correctors for Cryptographic Modules," Proc. of the 13th IMA International Conference on Cryptography and Coding (IMACC 2011), Oxford, UK, Lecture Notes in Computer Science, Vol. 7089, pp. 132–151, 2011.
- [7] A. Fujioka and K. Suzuki, "Designing Efficient Authenticated Key Exchange Resilient to Leakage of Ephemeral Secret Keys", Proc. of the CT-RSA 2011, San Francisco, CA, USA, Lecture Notes in Computer Science, Vol. 6558, pp. 121–141, 2011.



Hitoshi Fuji

Senior Research Engineer, Supervisor, Information Security Project, NTT Secure Platform Laboratories.

He received the B.E. and M.E. degrees in industrial engineering from Tokyo University of Science in 1991 and 1993, respectively, and the Ph.D. degree in informatics. Since joining NTT in 1993, he has been engaged in research on software engineering, network security, and information security. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).



Atsushi Fujioka

Senior Research Scientist, Supervisor, Information Security Project, NTT Secure Platform Laboratories.

He received the B.Eng., M.Eng., and D.Eng. degrees in electrical and electronic engineering from Tokyo Institute of Technology in 1985, 1987, and 1990, respectively. He joined NTT Communications and Information Processing Laboratories in 1990 and stayed at Swiss Federal Institute of Technology in Zurich, Switzerland, as an academic guest during 1993-1994. He is currently studying authenticated key exchange and identity-based identification. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of IEICE.



Toshiyuki Miyazawa

Research Engineer, Planning Section, NTT Secure Platform Laboratories.

He received the B.E. and M.S. degrees in mathematics from Waseda University, Tokyo, in 2000 and 2003, respectively. Since joining NTT Information Sharing Platform Laboratory in 2003, he has been engaged in R&D of information security, especially of public key cryptography and security protocols. As a result of organizational changes in April 2012, he is now in NTT Secure Platform Laboratories. He is a member of the Japan Society for Industrial and Applied Mathematics. He received the SCIS (Symposium on Cryptography and Information Security) Paper Award from IEICE in 2007.



Tetsutaro Kobayashi

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

He received the B.Eng. and M.Eng. degrees from Tokyo Institute of Technology in 1993 and 1995, respectively, and the Ph.D. degree from the University of Tokyo in 2005. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is currently engaged in research on information security. He received the SCIS (Symposium on Cryptography and Information Security) Paper Award in 2000.



Koutarou Suzuki

Senior Research Scientist, Information Security Project, NTT Secure Platform Laboratories.

He received the B.Sc., M.Sc., and Ph.D. degrees from the University of Tokyo in 1994, 1996, and 1999, respectively. Since joining NTT in 1999, he has been engaged in research on public key cryptography. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of IEICE and IPSJ. He received the SCIS Paper Award in 2002.



Fumitaka Hoshino

Research Engineer, Information Security Project, NTT Secure Platform Laboratories.

He received the B.Eng. and M.Eng. degrees from the University of Tokyo in 1996 and 1998, respectively. He joined NTT in 1998. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories.



Koji Chida

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

He received the B.S. and M.S. degrees in 1998 and 2000, respectively, and the Dr.Eng. degree in 2006, all from Waseda University, Tokyo. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of IEICE and IPSJ. He received the IPSJ Best Paper Award in 2011.

Tighter Security Operations to Help Provide Brands that are Safer and More Secure

Fumiyuki Tanemo, Ikuya Hayashi, Masaki Tanikawa, and Tsuyoshi Abe

Abstract

In this article, we review early work by NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team) and introduce the security research functions on which work has started with the aim of strengthening NTT's security response.

1. Introduction

1.1 Benefits and drawbacks of Internet growth

The Internet affects us all, and it is now closely connected to our everyday lives. With the falling cost of computers and network environments and the emergence and growing popularity of new personal devices such as smartphones, the Internet has become a means of communication that extends beyond its use merely as a tool for gathering information and providing services. For example, there are now many social networking services (SNSs) on the Internet. It is said that the 2010 Arab Spring pro-democracy movement was able to affect the governments of several countries because SNSs reach across international boundaries. This would have been inconceivable before the arrival of network technology.

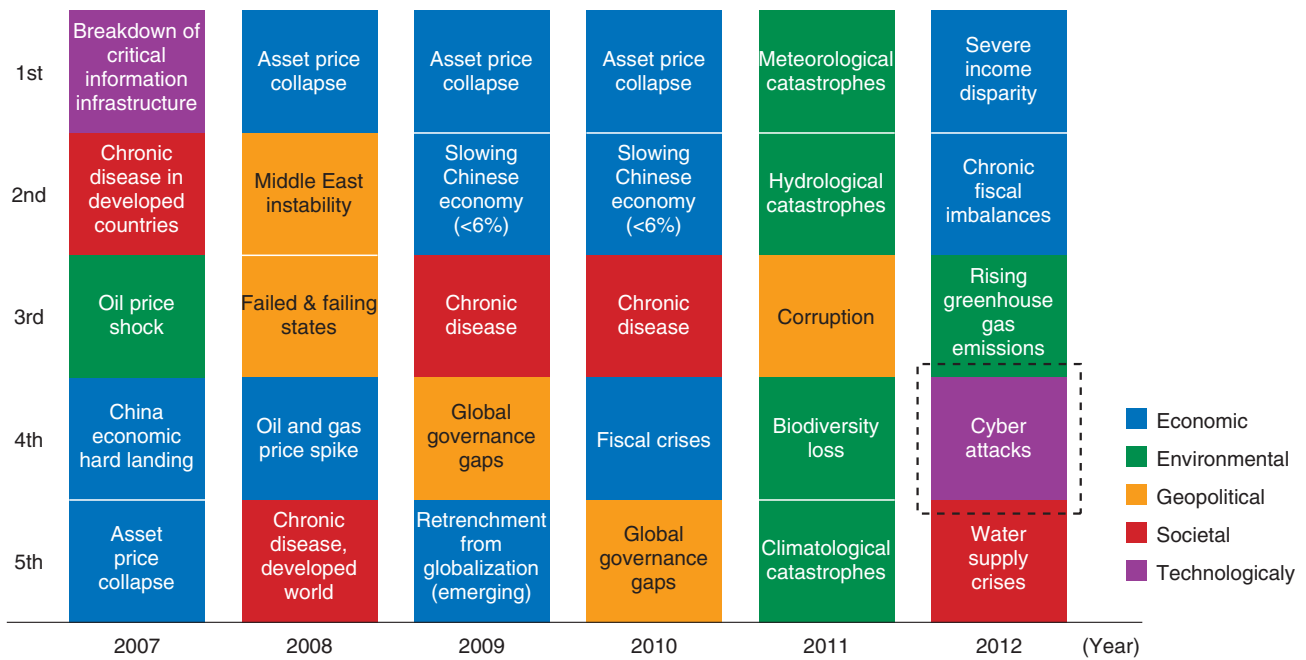
A drawback of this network development trend, however, is that it has allowed the perpetrators of cyber attacks and other malicious actions to use new methods of attack. Today, it is no longer unusual to see attackers clubbing together to launch systematic continuous attacks, and we are witnessing an increased threat of cyber attacks. The way in which the top five global risks have changed over the last few years according to the World Economic Forum is shown in **Fig. 1**. Cyber attacks were ranked fourth in 2012 despite having never appeared on this list before.

1.2 Increasingly sophisticated cyber attacks

To protect against these cyber attacks, most security administrators have generally made efforts to prevent damage from occurring in the first place by taking measures such as using antivirus software and firewalls and by performing maintenance to eliminate security vulnerabilities that can be exploited in cyber attacks. In recent years, however, we have not only seen a continuing increase in the number and severity of vulnerabilities requiring conventional maintenance, but also noticed attackers using new types of attack and new attack mechanisms. It is therefore becoming harder to protect against cyber attacks by conventional methods and ways of thinking.

For example, the spread of communication tools like smartphones and SNSs has made it easy for anyone to access information that would have been difficult to obtain before, such as a user's previous actions, thoughts, locations, and relationships. By combining the information handled by multiple communication tools, an attacker can easily engineer situations where it is possible to gain the trust of target individuals or organizations. This is why targeted attacks such as advanced persistent threat (APT) attacks pose such a major threat today.

It has also been reported that a succession of intrusion and information leakage incidents in the networks of various organizations including major corporations in 2011 was committed by a new group of



Source: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf

Fig. 1. Recent changes in the top five global risks.

attackers called *hacktivists*. Unlike conventional attackers who are motivated by financial gain, hacktivists use cyber attacks as a means of asserting their views, and their attack mechanisms vary widely. Hitherto, the concept of defense has been based on the reasoning that attackers will decide that an attack is not worth pursuing if they face sufficient preventative measures such as firewalls, which require considerable technological ability and time to overcome. However, if attacks are not financially motivated, then this approach is simply no longer applicable.

1.3 Proactive and reactive security

Owing to the appearance of advanced cyber attacks and new attack motivations, our approach to preventative measures is also changing. Specifically, the diverse nature of attacks means that it may not be possible to completely prevent all attacks. On the basis of this premise, it is now more important than ever to establish organized systems that can implement reactive security measures.

With preparation, it is possible to minimize damage by taking prompt measures to prevent secondary attacks instead of hurrying to resolve issues after an attack has already taken place. It is also possible to

make use of the resulting know-how to provide proactive feedback, such as preventing or detecting future incidents.

We believe that a thorough understanding of both proactive and reactive approaches is useful for handling security operations in modern Internet environments.

1.4 CSIRTs and reactive security measures

A computer security incident response team (CSIRT) is an organization that implements measures ranging from preventing security incidents to detecting them and applying countermeasures. Such organizations regard security incidents as inevitable occurrences and consider reactive measures as their main approach. They set up cooperative networks with other CSIRTs to share defense know-how and information about new attacks so that they can respond immediately to diverse attacks. Consequently, CSIRTs play a key role in reactive security measures.

To represent the NTT Group, NTT's Information Sharing Platform Laboratories (now called the Information Sharing Platform Laboratories) launched its own CSIRT called NTT-CERT (NTT Computer

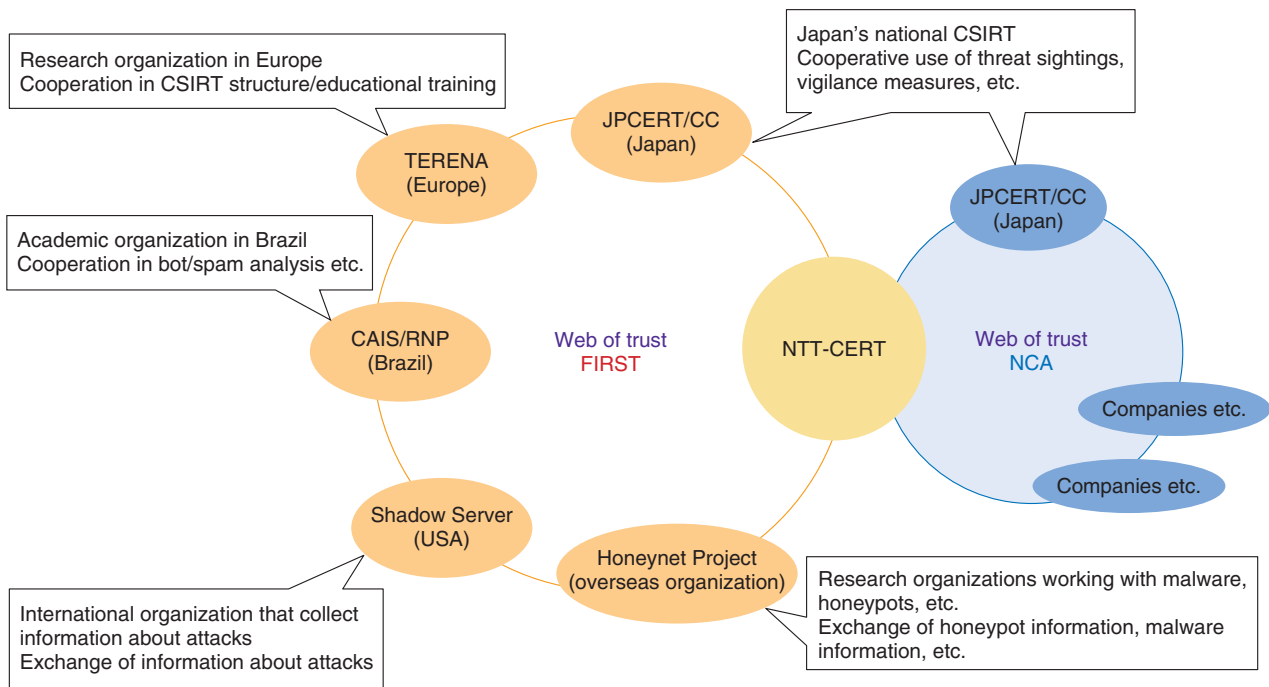


Fig. 2. Cooperation between NTT-CERT and other representative CSIRTs in Japan and overseas.

Security Incident Response and Readiness Coordination Team), which has been active since 2004 [1], [2].

CSIRTs originated from the CERT Coordination Center set up in the USA in 1988 to deal with a global malware pandemic [3]. Today, there are CSIRTs that have been set up by countries, businesses, and organizations all over the world, including Japan. In 1990, the CSIRT international forum FIRST (Forum of Incident Response and Security Teams) was set up by the principal CSIRTs at that time because of the need for a response to international concerns [4]. FIRST’s members include over 200 CSIRTs from all over the world, including NTT-CERT (as of April 2012). NTT-CERT is also an active founding member of the Nippon CSIRT Association (NCA), which was established in 2007 as a collection of Japanese domestic CSIRTs [5] (Fig. 2).

2. NTT-CERT

2.1 Activities

At NTT-CERT, we are building a worldwide cooperative circle of CSIRT organizations from different countries and organizations by taking advantage of communication forums such as FIRST and NCA

(Fig. 3). We also provide the following functions for the NTT Group:

- (1) Offering the trustworthy point of contact
- (2) Collecting, analyzing, and providing security-related information
- (3) Supporting the construction of CSIRTs
- (4) Providing training and educational activities
- (5) Conducting security-related research and development

Specifically, we provide support and information to all companies in the NTT Group, such as support for incident countermeasures and the discovering/reporting of vulnerabilities, and we collect information from external organizations including other CSIRTs as a point of contact with the NTT Group.

In addition to providing documentation such as reports on vulnerabilities verified at NTT and security configuration guidelines used when configuring servers, we actively provide information to each company in the NTT Group in an easily understood form, including holding workshops on various security-related themes.

We are also actively contributing to a wide range of outward-facing activities such as cooperating with the preparation of annual reports at the Information-technology Promotion Agency of Japan (IPA) and

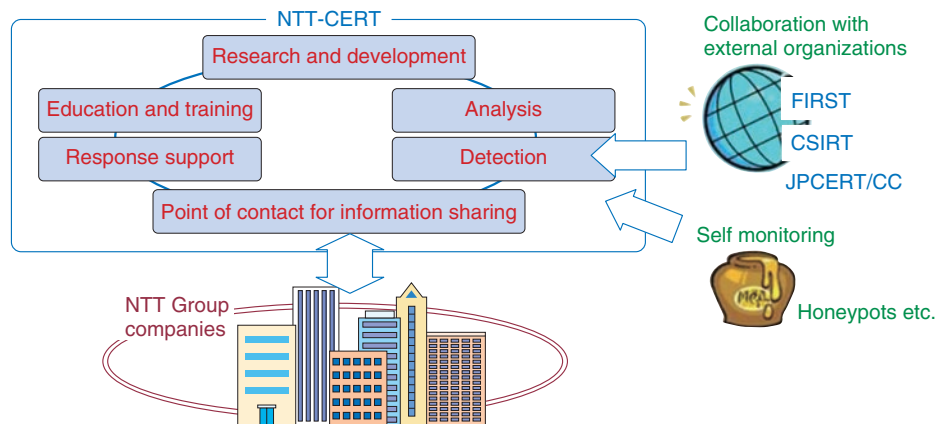


Fig. 3. Overview of NTT-CERT's activities.



Fig. 4. Our presentation at the FIRST meeting in March 2012.

giving various presentations and issuing research papers via FIRST and NCA (Fig. 4).

2.2 Challenges of security operations

As mentioned above, attacks against information systems and services are becoming more and more sophisticated, and they are likely to continue changing in the future. It is therefore important that our security operations keep in step with these changes with both proactive and reactive security measures.

In proactive security, measures for detecting and preventing attacks need to be appropriately reviewed according to changes in attack trends. From the viewpoint of APT attack countermeasures, it is now more important than ever to analyze log files as a way of detecting attacks.

In reactive security measures, there is an increasing need for advanced techniques and know-how to ana-

lyze the traces of attacks and correctly perceive what has happened in order to minimize the damage.

2.3 Security research functions

To meet the challenges faced by security operations, we launched a security research function that builds on the activities of NTT-CERT, and we started efforts to support the security operations of each company in the NTT Group (Fig. 5). We are working to support the NTT Group companies and improve our security operations technology across the following seven missions, ranging from proactive incident prevention measures to reactive damage mitigation measures.

1) Security product evaluation

Various security products and technologies target increasingly sophisticated attacks. We subject these products to technical appraisal before they are

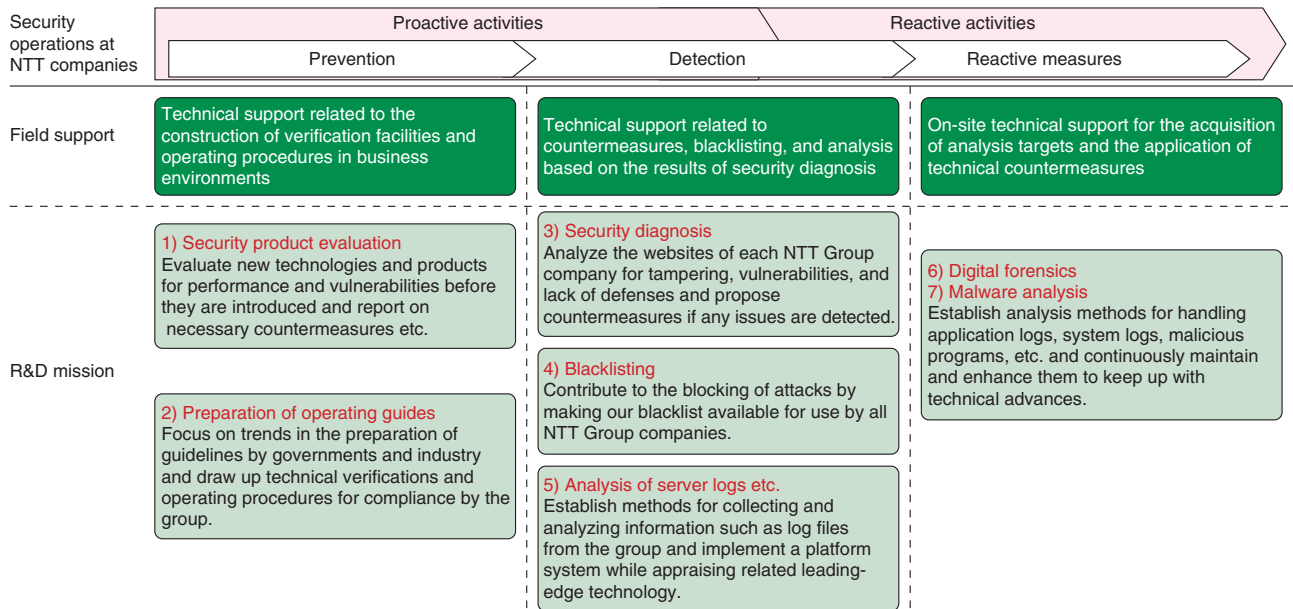


Fig. 5. Security research functions.

introduced for business use, and we are continuing to develop more advanced product evaluation techniques for this purpose.

2) Preparation of operating guides

While keeping abreast of trends in the formulation of guidelines (e.g., cloud security guidelines) by government and industry bodies, we prepare guidelines for use within the NTT Group for the defense of servers, Android platforms, and so on.

3) Security diagnosis

On the websites of NTT Group companies, we periodically search for tampering, vulnerabilities, and lack of defenses, and we issue reports on the trend of any problems discovered and the countermeasures taken.

4) Blacklisting

Using advanced malware detection technology developed at NTT, we are creating a blacklist of higher quality than those of existing providers, such as antivirus vendors, and we are providing this blacklist to companies in the NTT Group.

5) Analysis of server logs etc.

We collect information such as large-scale server logs and security news from sources such as network equipment, servers and operating systems, and we are using a large-scale data processing platform to establish techniques for analyzing log files in order to

streamline our operations, including automatic extraction of incident-related information based on machine learning and automatic classification of security logs.

6) Digital forensics

To understand what occurred on compromised computers, we deeply investigate by examining system logs and other records on the computers and related systems.

7) Malware analysis

We also deeply analyze malicious programs that we can get from compromised computers or other sources.

It is difficult to implement items (6) and (7) at all NTT Group companies. To support them, we are working on detailed analysis methods for application and system logs, malicious programs, etc.

References

[1] NTT-CERT. <http://www.ntt-cert.org/index-en.html>
 [2] M. Nagashima, Y. Sugiura, T. Abe, T. Yoshida, and A. Mukaiyama, "CSIRT Activities at NTT," NTT Technical Review, Vol. 8, No. 7, 2010. <https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201007sf5.html>
 [3] CERT. <http://www.cert.org/>
 [4] FIRST. <http://www.first.org/>
 [5] Nippon CSIRT Association. <http://www.nca.gr.jp/en/>

**Fumiyuki Tanemo**

Senior Research Engineer, Supervisor, Security Management & Operations Project, NTT Secure Platform Laboratories.

He received the B.E. and M.E. degrees in information engineering from Nagoya University, Aichi, in 1991 and 1993, respectively. He joined NTT in 1993. He is engaged in network security R&D as the leader of NTT-CERT. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of the Information Processing Society of Japan and the IEEE Computer Society.

**Masaki Tanikawa**

Senior Research Engineer, Security Management & Operations Project, NTT Secure Platform Laboratories.

He received the B.E. and M.E. degrees in systems science from Tokyo Institute of Technology in 1993 and 1995, respectively. He joined NTT in 1995. He is engaged in network security R&D as a member of NTT-CERT. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

**Ikuya Hayashi**

Senior Research Engineer, Security Management & Operations Project, NTT Secure Platform Laboratories.

He received the B.S. degree in earth science from Hokkaido University in 1998. He joined NTT in 1988. He is currently engaged in network security R&D as a member of NTT-CERT. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories.

**Tsuyoshi Abe**

Senior Research Engineer, Security Management & Operations Project, NTT Secure Platform Laboratories.

He received the B.E. and M.E. degrees in mechanical engineering from Waseda University, Tokyo, in 1993 and 1995, respectively. He joined NTT in 1995. He is engaged in network security R&D as a member of NTT-CERT. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of IEICE.

Unraveling an Exotic Electronic State for Error-free Quantum Computation

Koji Muraki

Abstract

A recently proposed approach could lead to a totally new architecture for quantum computation with an exceedingly low error rate by exploiting *quasiparticles* that behave differently from fundamental particles in nature. Highly sensitive nuclear magnetic resonance measurements have unraveled an electronic state in a semiconductor device that is expected to host such exotic quasiparticles. The experimental results support the theory predicting that this state will have properties suitable for error-free quantum computation.

1. Introduction

Quantum computers are expected to possess computational capabilities far exceeding those of conventional computers. Their immense computing power stems from quantum parallelism. The classical, or digital, bit used by conventional computers can take only one value at a time: either 0 or 1. On the other hand, the qubit—the quantum analog of a bit—can encode any superposition of two quantum states $|0\rangle$ and $|1\rangle$. The state of a system comprising n qubits is thus described by a vector that spans an entire 2^n -dimensional space referred to as Hilbert space. Calculations are performed by executing a series of gate operations that transforms the state of the qubits and the result is read out by measuring their final state. Quantum parallelism arises because the time evolution of the qubits follows many different trajectories in the huge Hilbert space in parallel until the final state is projected by a measurement. During quantum computation, errors can occur just as they can in conventional computers, but the errors in quantum computation have a much greater impact and are a major obstacle to building a practical quantum computer. Errors can be induced by both intentional logic gate operations and unintentional interactions with the environment. For example, a gate operation intended to rotate a qubit by 90° may actually produce a 90.1° rotation. Likewise, uncontrolled interactions with the environment can cause the state to evolve in an unin-

tended way. Fortunately, error correction is possible for quantum computers; it is done by representing information redundantly so that errors can be detected without measuring the information, which would destroy it [1]–[4]. However, information redundancy inevitably implies a corresponding increase in the number of qubits required to implement the same algorithm. Furthermore, there is a threshold for the error rate above which error correction is no longer possible [5]–[8]; this imposes a stringent requirement on the admissible error rate.

Recently, a totally new architecture for quantum computation with an exceedingly low error rate has been proposed and it has attracted interest. The architecture, called topological quantum computation [9]–[14], exploits *quasiparticles*, which are elementary excitations of a many-particle system that behave like particles. However, the quasiparticles that can be used are restricted to those belonging to a specific class called non-Abelian quasiparticles or non-Abelian anyons, which behave distinctly differently from fundamental particles in nature. A state containing such quasiparticles is transformed into a different state distinguishable from the initial one when two quasiparticles are moved so that they exchange positions. However, topological quantum computation is still only a theoretical possibility: it is hypothetical in that no experimental evidence has yet been found for the existence of non-Abelian quasiparticles in a real physical system. A prime candidate for a physical

Table 1. Types of (quasi)particles and examples.

Type	Particles		Quasiparticles	Statistics
	Fundamental particles	Composite particles		
Fermion	Electron	Proton, neutron	Hole	Abelian
Boson	Photon	Helium atom	Phonon	
Anyon (only in two dimensions)			1/3 quasiparticle	Non-Abelian
			(5/2 quasiparticle)	

system that is expected to host such quasiparticles is the $\nu = 5/2$ fractional quantum Hall (FQH) state [15], [16], an exotic electronic state that emerges in a pristine semiconductor heterostructure at millikelvin temperatures (ν : filling factor); however, its exact nature is not yet fully understood. My colleagues and I have recently performed nuclear magnetic resonance (NMR) measurements on the $\nu = 5/2$ state and unraveled its nature [17]. The experimental results support the theory [18], [19] predicting that the state will have properties suitable for error-free quantum computation. This article outlines the basic idea of topological quantum computation and reviews our experiment.

2. Topological quantum computation

2.1 Non-Abelian quasiparticles

Fundamental particles in nature are classified as either fermions or bosons according to how their wave function changes sign with the interchange of two identical particles. Taking the most familiar examples: electrons are fermions and photons are bosons. Interestingly, the behavior of a system consisting of many particles interacting with each other is often well understood by using the notion of quasiparticles—elementary excitations behaving like particles but with properties different from the parent particles that support the quasiparticle excitations. Examples include holes in a semiconductor and phonons in a crystal lattice. Quasiparticles are also classified according to their behavior upon quasiparticle exchange in terms of whether more than one quasiparticle can be created at the same location. Holes are fermions and phonons are bosons.

Intriguingly, in a two-dimensional space, the statistical properties of quasiparticles are no longer restricted to the fermion/boson dichotomy. For a specific class of quasiparticles termed *anyons*, the

exchange of two quasiparticles adds a complex phase ϕ to their wave function, through multiplication by a factor $e^{i\phi}$ instead of ± 1 for ordinary fermions (-1) or bosons ($+1$) [20], [21]. The generosity of nature in allowing the existence of such exotic quasiparticles comes as a surprise, but they are not very different from fermions or bosons in that the exchange of these quasiparticles does not alter the state itself. That is, the phase of the wave function acquired after (quasi)particle exchange is factored out by a measurement. Alternatively, it can be said that they are all Abelian, meaning that successive (quasi)particle exchanges in a series are commutative; i.e., the result is independent of the order of (quasi)particle exchanges.

In topological quantum computation, quasiparticles of yet another kind with exceedingly unusual properties are relevant. For these quasiparticles, dubbed *non-Abelian quasiparticles* or *non-Abelian anyons*, [11], [12], [22] quasiparticle exchange does alter the state; it transforms the state from one of several degenerate ground states to another. Such an operation can be described by a unitary transformation, so it can form the basis for quantum logic gates. A necessary condition for such quasiparticle exchange to be a nontrivial unitary transformation is that the ground state is degenerate. In the simplest example, a system containing two quasiparticles should have a degeneracy of 2, which then form a qubit. When the system has $2n$ quasiparticles, there is a 2^{n-1} -dimensional space of degenerate states, which can be viewed as $n - 1$ qubits [11]. **Table 1** summarizes the classification of (quasi)particles and gives examples of them.

2.2 Topological quantum computation

The ground state of a system containing $2n$ non-Abelian quasiparticles has a 2^{n-1} -dimensional space of degenerate states, which serves as $n - 1$ qubits.

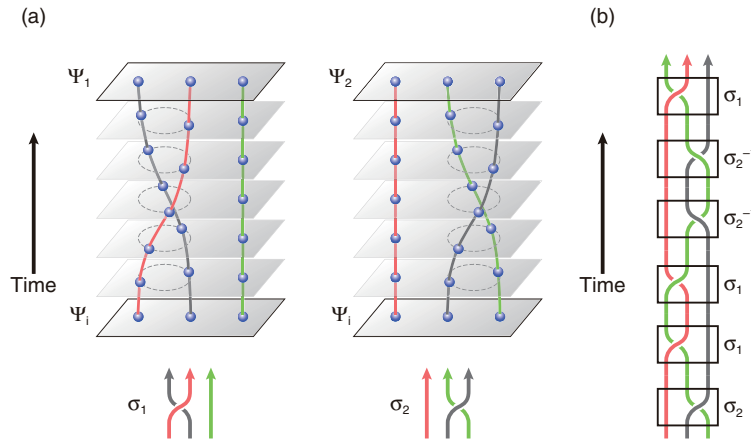


Fig. 1. Schematic illustrations of quasiparticle exchanges and topological quantum computation. (a) Basic operations (σ_1 and σ_2) on a system containing three quasiparticles. Top: illustrations of the temporal evolution of the system from the initial state ψ_i to the final state $\psi_{1(2)} = \sigma_{1(2)}\psi_i$. Bottom: diagrammatic representations of the quasiparticle exchange operations. (b) Example of logic gate operations consisting of the basic operations σ_1 and σ_2 shown in (a) and their inverses σ_1^{-1} and σ_2^{-1} .

Topological quantum computation exploits the unitary transformation of a state that accompanies an exchange of two non-Abelian quasiparticles as a basis for quantum logic gates. The result of the calculation depends solely on the order of the quasiparticle exchanges and does not depend on the details of the quasiparticles' trajectories. This unique property makes topological quantum computation immune to errors. By using a $(2 + 1)$ -dimensional space-time representation, we can express quasiparticle trajectories as world lines and express quasiparticle exchange as the braiding of two world lines around each other. An example is schematically illustrated in **Fig. 1(a)**. Two of three quasiparticles confined to a two-dimensional plane are manipulated in such a way that they exchange positions via relative motion in the counter-clockwise direction. The thick solid lines that trace the position of the quasiparticles in this space-time representation form the quasiparticles' world lines. The quantum information is encoded in the braid's topology, that is, the way the world lines are braided. Similar to a braided cord or hair, which can be loosened but not undone, the quantum information is not affected when the quasiparticle trajectories are locally perturbed. The quantum information is thus said to be *topologically protected*. **Figure 1(b)** shows an example of logic gate operations consisting of the basic operations shown in Fig. 1(a) and their inverses.

3. $\nu = 5/2$ FQH state

3.1 Quasiparticles in FQH states

A prime candidate for a physical system expected to host non-Abelian quasiparticles is an exotic state of a two-dimensional electron system (2DES), called the $\nu = 5/2$ FQH state [15]. This state emerges in a pristine semiconductor heterostructure under extreme conditions of millikelvin temperature and high magnetic field of several tesla. FQH effects are characterized by the quantization of Hall resistance that occurs when the applied field B and the electron density n take particular ratios [23]. Hall resistance R_{xy} is usually related to n and B as $R_{xy} = B/ne$, where e is the elementary charge. As a consequence of electron-electron interaction, an energy gap forms at the Fermi level for particular values of B/n , around which R_{xy} is pinned at a constant value over a finite range of n and B [24]. The energy gap also leads to the vanishing of longitudinal resistance R_{xx} .

Because of the energy gap that forms at particular values of B/n , the electron system tries to preserve the same B/n ratio to minimize the interaction energy when B or n is slightly detuned. The resultant mismatch is accommodated by introducing *point defects* around which the local electron density is higher or lower than in the surrounding area. These point defects, which carry electric charge and behave like charged particles, are quasiparticles in FQH systems [24]. FQH quasiparticles have been shown to have a

fraction of the electron charge [25], [26] and are believed to be anyons [21]. Their properties, including their charge and statistics, are derived from the properties of the FQH state hosting them. The FQH state that emerges at $\nu = 5/2$, where $\nu = (h/e)n/B$ (h : Planck's constant), is believed to have the distinctive property that its quasiparticles are non-Abelian [18].

3.2 Theoretical models for the $\nu = 5/2$ state

The $\nu = 5/2$ FQH state [15], [16] and its particle-hole counterpart $\nu = 7/2$ are the only FQH states with even-denominator ν observed in a single-layer 2DES. Unlike other FQH states with odd-denominator ν , the exact mechanism responsible for the energy gap formation at $\nu = 5/2$ has not yet been established. In the standard theory of FQH effects [24], [27], [28], the fermionic nature of electrons requires ν to have an odd denominator. Thus, the breaking of the odd-denominator rule suggests a paired state of fermions [19], [29]. Various theoretical models have been proposed and examined [18], [19], [29]–[36], including both those with non-Abelian statistics and those with Abelian statistics.

Experiments reported thus far have neither demonstrated the non-Abelian nature of $\nu = 5/2$ quasiparticles nor pinned down precisely which theoretical model correctly describes the $\nu = 5/2$ ground state. The quasiparticle charge of $e/4$ observed in shot noise [37], [38] and local compressibility [39] measurements indicates that the $\nu = 5/2$ state is indeed a paired state, but does not discriminate among different types of paired states which all have charge- $e/4$ quasiparticles. Notably, quasiparticle tunneling between FQH edges through a narrow constriction [40], [41] has allowed the screening of different model wave functions through detailed comparison with theory. However, the likely candidates that emerged through these experiments include an undesirable Abelian wave function.

3.3 Spin polarization of the $\nu = 5/2$ state

Most theories of topological quantum computation using the $\nu = 5/2$ state as a platform to manipulate non-Abelian quasiparticles [11], [42] are based on the premise that the state is described by the wave function proposed by Moore and Read [18], which is considered to host non-Abelian quasiparticles. An important feature of the Moore-Read theory is that it assumes that all the electrons have their spins—an internal degree of freedom of electrons making them behave like tiny magnets—aligned along the same direction. Numerical studies have shown that the

ground state at $\nu = 5/2$ is spin polarized [43]–[45]. However, experiments reported thus far have indicated conflicting results for the spin polarization of the $\nu = 5/2$ state [46], [47]. The addition of an in-plane magnetic field to increase the spin-splitting energy is known to weaken the $\nu = 5/2$ state [48], [49], which hinted at an unpolarized or only partially polarized state. On the other hand, under a perpendicular magnetic field, the $\nu = 5/2$ state persists over a wide range of magnetic field, even up to 10 T [50], suggesting full polarization. Recent optical measurements using photoluminescence [51] and inelastic light scattering [52] indicated an unpolarized state or an inhomogeneous state consisting of unpolarized or partially polarized domains, respectively. It is therefore of paramount importance to determine the spin polarization with a high level of confidence.

4. Highly sensitive resistively detected NMR measurements

4.1 NMR

NMR spectroscopy is one of the most powerful and sophisticated analytical tools for investigating the electronic and structural properties of matter. It exploits the resonant absorption of electromagnetic waves by nuclei placed in a strong magnetic field. When the electron system surrounding the nuclei has non-zero spin polarization, the hyperfine interaction between the electron spins and the nuclear spins acts as an effective magnetic field for the nuclei: this field shifts the nuclear resonance frequency by a small amount (Knight shift) proportional to the electron spin polarization. Thus, the electron spin polarization can be deduced by measuring the Knight shift of nuclei placed in contact with a 2DES. All three nuclides, ^{69}Ga , ^{71}Ga , ^{75}As , constituting the GaAs quantum well, where a 2DES resides, have nuclear spin $I = 3/2$ and can consequently serve as NMR probes.

The challenge in applying NMR to 2DESs is the low signal level resulting from the small number of nuclei in contact with the 2DES and the overwhelming background coming from the thick substrate. Resistively detected NMR (RD-NMR) [53], [54] provides a way to overcome these issues of sensitivity and selectivity, thereby allowing us to perform NMR on a single sheet of a 2DES. Instead of probing inductive signals via a pickup coil or directly measuring the absorption, in RD-NMR we measure the change in the electrical resistance of the sample that occurs when the frequency of the applied radio-frequency

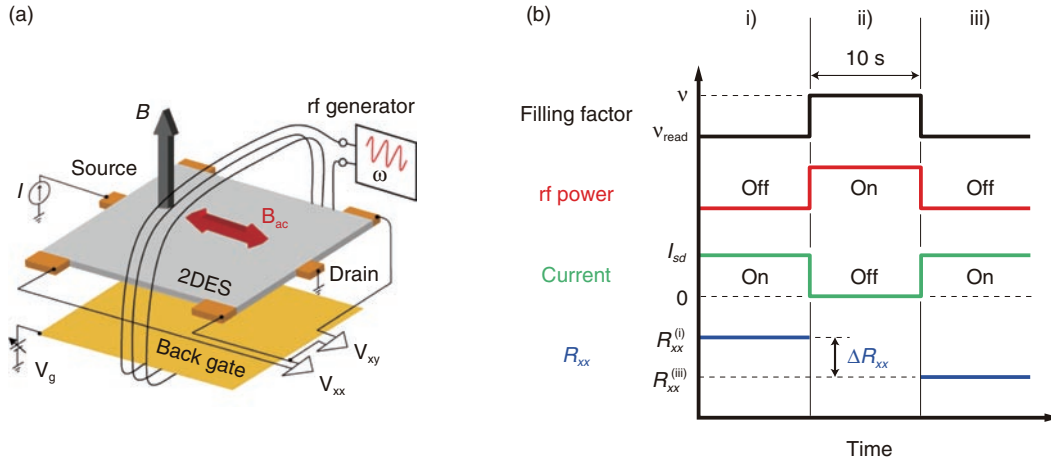


Fig. 2. (a) Experimental setup and (b) measurement sequence of resistively detected nuclear magnetic resonance.

(rf) wave matches the resonance frequency of the nuclei. In return for its high sensitivity, the conventional RD-NMR has the drawback of being applicable only under a particular set of conditions such that the electron system has measurable finite electrical resistance and is sensitive to a tiny change in the electronic Zeeman energy. The former implies that the method is not applicable to a well-developed quantum Hall state, where the sample's resistance exponentially vanishes at low temperatures; the latter condition is necessary because resistive detection relies on the hyperfine coupling between electron spins and nuclear spins, which acts as an effective magnetic field modifying the electronic Zeeman energy.

4.2 Sample and method

The sample used in our study was a 27-nm-wide GaAs quantum well with $\text{Al}_{0.25}\text{Ga}_{0.75}\text{As}$ barriers grown by molecular beam epitaxy. The structure was doped with Si on one side (front) of the quantum well at a setback distance of 90 nm, which provided the 2DES with density $n = 1.55 \times 10^{11} \text{ cm}^{-2}$ and mobility $\mu = 5.8 \times 10^6 \text{ cm}^2/\text{Vs}$ in the as-grown condition. The sample was processed into a 100- μm -wide Hall-bar device. A degenerately Si-doped GaAs buffer layer 1 μm below the 2DES served as a back gate [55], which allowed us to tune the electron density n over a wide range: from $0.5 \times 10^{11} \text{ cm}^{-2}$ to $4.2 \times 10^{11} \text{ cm}^{-2}$. The mobility exceeded $1.0 \times 10^7 \text{ cm}^2/\text{Vs}$ for $n \geq 2.8 \times 10^{11} \text{ cm}^{-2}$, reaching a maximum value of $1.15 \times 10^7 \text{ cm}^2/\text{Vs}$ at around $n = 3.9 \times 10^{11} \text{ cm}^{-2}$. To observe a well-developed $\nu = 5/2$ state, it is essential to control

the disorder potential due to the remote ionized impurities in the Si doping layer. Details of the sample optimization are given in [56].

Our measurement setup is schematically shown in **Fig. 2(a)**. A Hall-bar device mounted on a DIP (dual in-line package) chip carrier is cooled in the mixing chamber of a dilution refrigerator with a base temperature of 10 mK. A three-turn coil is wound around the sample and connected to an rf generator. Electrical measurements are performed by driving a low-frequency (17 Hz) ac current I_{sd} through the sample and measuring the voltages V_{xx} and V_{xy} that appear in the longitudinal and transverse directions using lock-in amplifiers. The longitudinal and Hall resistances are obtained as $R_{xx} = V_{xx}/I_{sd}$ and $R_{xy} = V_{xy}/I_{sd}$.

Our measurement sequence consists of three steps, i) to iii), as schematically shown in **Fig. 2(b)** [17]. The salient feature of our measurement scheme is that we exploit an electronic state (designated by filling factor ν_{read}) that is different from the electronic state of interest (designated by filling factor ν) to read out the change in R_{xx} that results from the rf irradiation on the state ν . As shown in Fig. 2(b), this is done by switching the gate voltage V_g at a fixed magnetic field B while alternately turning on and off the current and the rf wave [57]. Our signal is the difference ($\Delta R_{xx} = R_{xx}^{(i)} - R_{xx}^{(iii)}$) in R_{xx} measured in periods i) and iii), right before and after the period ii). By repeating this sequence for different frequencies, we obtain a resonance spectrum. It is important to note that, although we measure R_{xx} of the state ν_{read} , the spectral information contained in the resultant NMR spectrum reflects only the electronic properties of the state ν . It is also

important to note that while the state ν_{read} needs to satisfy the conditions required for conventional RD-NMR, the state ν does not. This eliminates the restrictions imposed on conventional RD-NMR, allowing RD-NMR to be performed for any electronic state accessible via gate voltage. Specifically, we used $\nu_{\text{read}} = 0.59$; in this range of filling factor, the electronic system is very sensitive to a small change in the Zeeman energy [58], [59]. Below, the filling factor ν refers exclusively to the value during step ii).

4.3 Experimental results

R_{xx} and R_{xy} of our sample as a function of magnetic field B are shown in **Fig. 3**. Fractional quantum Hall effects at Landau-level filling factor $\nu = 8/3$, $5/2$, and $7/3$ are manifested as plateaus in R_{xy} and minima in R_{xx} , indicating high sample quality. The RD-NMR spectra of ^{75}As nuclei measured at $B = 6.4$ T are shown in **Fig. 4**. As shown in the inset, the magnetic field splits the energy levels of ^{75}As nuclear spins $I = 3/2$ into four levels with $I_z = \pm 3/2$ and $\pm 1/2$. Here, we focus on the transition between $I_z = 1/2$ and $-1/2$. (Other transitions, which are split off by quadrupole interactions, are outside the frequency range shown in the figure.) In **Fig. 4**, spectra taken at three different filling factors $\nu = 2$, $5/2$, and $5/3$ are shown. As explained below, the spectra for the $\nu = 2$ and $5/3$ states, whose spin polarizations are known, are necessary to deduce the Knight shift at $\nu = 5/2$ and convert it into spin polarization.

The electron configurations at these filling factors are schematically shown in **Fig. 5**. When a 2DES is subjected to a strong perpendicular magnetic field B , the cyclotron motion of electrons is quantized and their energy spectrum splits into a set of equally spaced discrete levels (Landau levels) designated by the orbital quantum number N ($= 0, 1, 2, \dots$), with energy separation $\hbar\omega_c$, where $\omega_c = eB/m^*$ is the cyclotron frequency (m^* : effective mass). Each Landau level is further split into spin-up (\uparrow) and spin-down (\downarrow) levels separated by the Zeeman energy $E_Z = |g|\mu_B B$, where $\mu_B = e\hbar/2m_e$ is the Bohr magneton (m_e : electron mass in vacuum) and g is the g -factor. The ratio of the Zeeman energy to the Landau level separation (m^*/m_e) $\cdot|g|/2$, which is unity for electrons in vacuum, is significantly reduced in GaAs, by a factor of ~ 70 owing to the small effective mass $m^* = 0.067m_e$ and the small g -factor ($g = -0.44$).

Each spin-split Landau level has a degeneracy of $n_\phi = eB/h$, so that Landau-level filling factor ν , defined as $\nu = nh/eB$, represents the number of occupied levels. The electron configurations for Landau-level

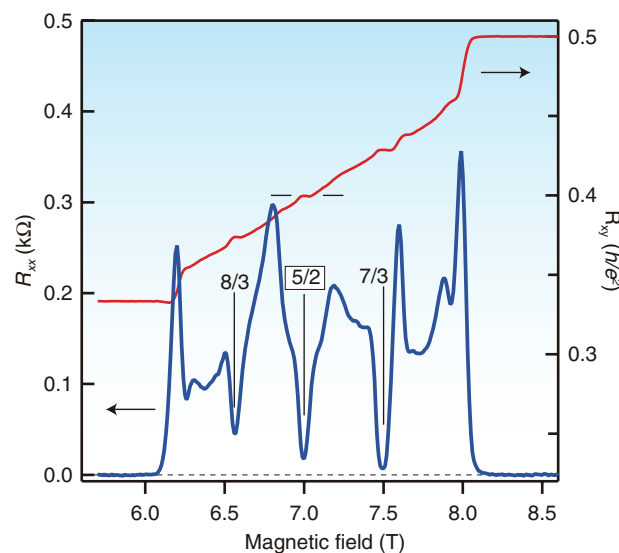


Fig. 3. Magnetotransport properties of the sample used for the resistively detected nuclear magnetic resonance measurements.

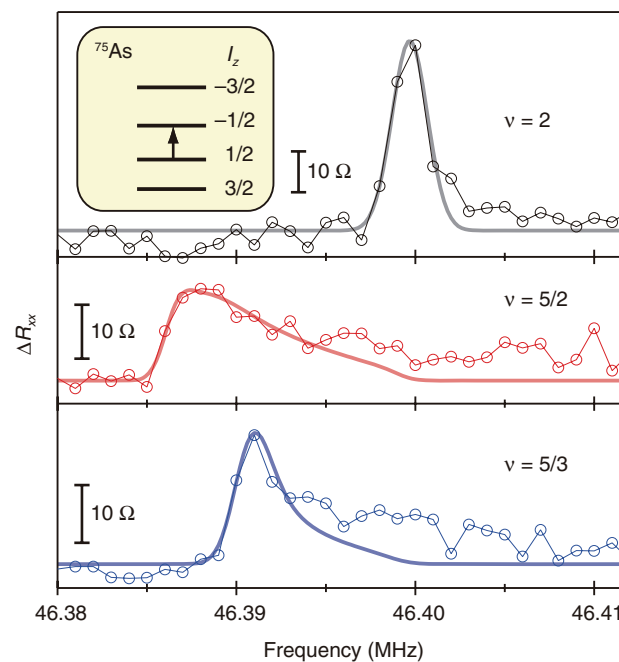


Fig. 4. Resistively detected nuclear magnetic resonance spectra of ^{75}As nuclei taken at $B = 6.4$ T. The top, middle, and bottom panels show spectra taken at Landau-level filling factor $\nu = 2$, $5/2$, and $5/3$. The thick solid lines show the fitting based on model calculations. The inset shows the nuclear spin levels.

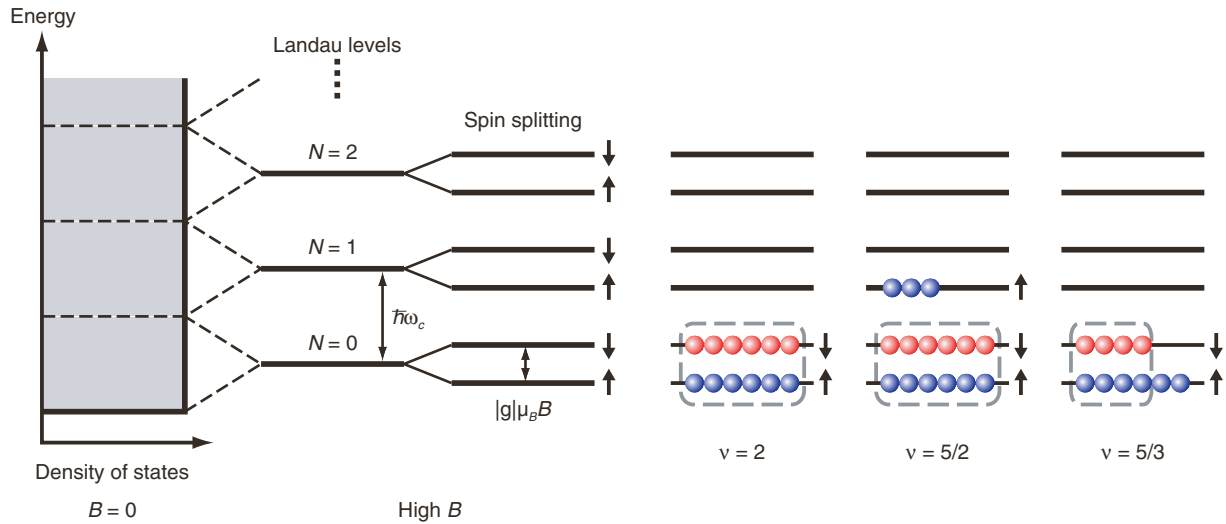


Fig. 5. Schematic illustrations of energy level splitting and electron configurations in a high magnetic field at different filling factors. Note that the energy splitting is not to scale.

filling factor $\nu = 2$, $5/2$, and $5/3$ are shown schematically in Fig. 5 with the simplistic model that each spin-split Landau level can accommodate only six electrons. The electrons enclosed by the dashed lines have equal numbers of up and down spins, so they do not contribute to the net spin polarization.

At $\nu = 2$, the two lowest levels, ($N = 0$, \uparrow) and ($N = 0$, \downarrow), are fully occupied with equal numbers of spin-up and spin-down electrons, so the net spin polarization is zero. Thus, the peak position of the RD-NMR spectrum taken at $\nu = 2$ marks the bare resonance frequency of the ^{75}As nuclei without a Knight shift.

At $\nu = 5/2$, the $N = 0$ Landau levels are fully occupied with equal numbers of spin-up and spin-down electrons, so only those electrons in the $N = 1$ Landau level contribute to the spin polarization and hence to the Knight shift. The resonance spectrum for $\nu = 5/2$ appears in the frequency range lower than the resonance frequency at $\nu = 2$. The Knight shift measured from peak to peak is about 12 kHz. The finite Knight shift observed for $\nu = 5/2$ clearly indicates that the electrons in the $N = 1$ Landau level forming the $\nu = 5/2$ FQH state have non-zero spin polarization.

To convert the measured Knight shift into spin polarization, we need a control spectrum for a state with known (non-zero) polarization. For this purpose, we use the spectrum at $\nu = 5/3$. As schematically shown in Fig. 5, $5/3$ filling of electrons is equivalent to $1/3$ filling of holes in the $N = 0$ Landau level. Since the $\nu = 1/3$ state is fully polarized, the $\nu = 5/3$ state is

as well [60], which implies the electron configuration shown in Fig. 5. Note that we accessed different values of ν by changing the number of electrons while keeping B constant. Thus, the ratio of the number of electrons that contribute to spin polarization in the $\nu = 5/2$ and $5/3$ states is 3:2 if the $\nu = 5/2$ state is fully polarized, and this is indeed what we observed. To determine the spin polarization more accurately, we fitted the measured spectra by taking into account the local electron density that varies along the direction normal to the 2D plane (solid lines in the figure). The simulation reproduces the observed spectral shape and confirms that the $\nu = 5/2$ FQH state is fully polarized.

5. Concluding remarks

Our NMR experiments have demonstrated maximal spin polarization for the $\nu = 5/2$ FQH state. These measurements are consistent with the Moore-Read theory, which predicts the existence of non-Abelian quasiparticles [18]. Most importantly, with our results, the unpolarized (331) state [34], which had been the most likely Abelian contender [40], [41], [11], can be unambiguously ruled out, thus lending strong support to the $\nu = 5/2$ state being non-Abelian. We must note that our measurements probe the ground-state property of the system at $\nu = 5/2$, but not that of its quasiparticles. Thus, the exciting prospect of topologically protected quantum operations using

the $\nu = 5/2$ FQH state awaits direct experimental demonstration of the quasiparticles' non-Abelian nature. One candidate is quasiparticle interference experiments [61]–[65].

Acknowledgments

I would like to thank Dr. Lars Tiemann (Japan Science and Technology Agency, now at ETH Zurich, Switzerland) and Dr. Gerardo Gamez (now at Bell Laboratories, Alcatel-Lucent, USA), who conducted the experiments described in this article with my NTT colleague Dr. Norio Kumada and I. These experiments were performed through joint research with the Japan Science and Technology Agency as part of the ERATO nuclear spin electronics project.

References

- [1] P. W. Shor, "Scheme for Reducing Decoherence in Quantum Computer Memory," *Phys. Rev. A*, Vol. 52, No. 4, pp. R2493–R2496, 1995.
- [2] A. R. Calderbank and P. W. Shor, "Good Quantum Error-correcting Codes Exist," *Phys. Rev. A*, Vol. 54, No. 2, pp. 1098–1105, 1996.
- [3] A. M. Steane, "Error Correcting Codes in Quantum Theory," *Phys. Rev. Lett.*, Vol. 77, No. 5, pp. 793–797, 1996.
- [4] A. Steane, "Multiple-particle Interference and Quantum Error Correction," *Proc. of R. Soc. London Ser. A*, Vol. 452, No. 1954, pp. 2551–2577, 1996.
- [5] D. Aharonov and M. Ben-Or, "Fault Tolerant Quantum Computation with Constant Error." [arXiv:quant-ph/9611025v2]
- [6] J. Preskill, "Reliable Quantum Computers," *Proc. of R. Soc. London Ser. A*, Vol. 454, No. 1969, pp. 385–410, 1998. [arXiv:quant-ph/9705031v3]
- [7] E. Knill, R. Laflamme, and W. H. Zurek, "Resilient Quantum Computation," *Science*, Vol. 279, No. 5349, pp. 342–345, 1998.
- [8] E. Knill, R. Laflamme, and W. H. Zurek, "Resilient Quantum Computation: Error Models and Thresholds," *Proc. of R. Soc. London Ser. A*, Vol. 454, No. 1969, pp. 365–384, 1998.
- [9] A. Y. Kitaev, "Fault-tolerant Quantum Computation by Anyons," *Ann. Phys.*, Vol. 303, No. 1, pp. 2–30, 2003. <http://arxiv.org/abs/quant-ph/9707021v1>
- [10] M. H. Freedman, A. Kitaev, M. J. Larsen, and Z.-G. Wang, "Topological Quantum Computation," *Bull. Amer. Math. Soc.*, Vol. 40, No. 1, pp. 31–38, 2003.
- [11] C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. Das Sarma, "Non-Abelian Anyons and Topological Computation," *Rev. Mod. Phys.*, Vol. 80, No. 3, pp. 1083–1159, 2008.
- [12] S. Das Sarma, M. Freedman, and C. Nayak, "Topological Quantum Computation," *Physics Today*, Vol. 59, No. 7, pp. 32–38, 2006.
- [13] G. P. Collins, "Computing with Quantum Knots," *Scientific American*, Vol. 294, pp. 56–63, April, 2006. [doi:10.1038/scientificamerican0406-56]
- [14] J. Preskill, "Lecture Notes for Physics 219: Quantum Computation." <http://www.theory.caltech.edu/~preskill/ph219/topological.pdf>
- [15] R. Willet, J. P. Eisenstein, H. L. Störmer, D. C. Tsui, A. C. Gossard, and J. H. English, "Observation of an Even-Denominator Quantum Number in the Fractional Quantum Hall Effect," *Phys. Rev. Lett.*, Vol. 59, No. 15, pp. 1776–1779, 1987.
- [16] W. Pan, J.-S. Xia, V. Shvarts, D. E. Adams, H. L. Stormer, D. C. Tsui, L. N. Pfeiffer, K. W. Baldwin, and K. W. West, "Exact Quantization of the Even-Denominator Fractional Quantum Hall State at $\nu = 5/2$ Landau Level Filling Factor," *Phys. Rev. Lett.*, Vol. 83, No. 17, pp. 3530–3533, 1999.
- [17] L. Tiemann, G. Gamez, N. Kumada, and K. Muraki, "Unraveling the Spin Polarization of the $\nu = 5/2$ Fractional Quantum Hall State," *Science*, Vol. 335, No. 6070, pp. 828–831, 2012.
- [18] G. Moore and N. Read, "Nonabelions in the Fractional Quantum Hall Effect," *Nucl. Phys. B*, Vol. 360, No. 2-3, pp. 362–396, 1991.
- [19] M. Greiter, X. G. Wen, and F. Wilczek, "Paired Hall States," *Nucl. Phys. B*, Vol. 374, No. 3, pp. 567–614, 1992.
- [20] B. I. Halperin, "Statistics of Quasiparticles and the Hierarchy of Fractional Quantized Hall States," *Phys. Rev. Lett.*, Vol. 52, No. 18, pp. 1583–1586, 1984.
- [21] D. Arovas, J. R. Schrieffer, and F. Wilczek, "Fractional Statistics and the Quantum Hall Effect," *Phys. Rev. Lett.*, Vol. 53, No. 7, pp. 722–723, 1984.
- [22] A. Stern, "Non-Abelian States of Matter," *Nature*, Vol. 464, pp. 187–193, 2010.
- [23] D. C. Tsui, H. L. Stormer, and A. C. Gossard, "Two-dimensional Magnetotransport in the Extreme Quantum Limit," *Phys. Rev. Lett.*, Vol. 48, No. 22, pp. 1559–1562, 1982.
- [24] R. B. Laughlin, "Anomalous Quantum Hall Effect—An Incompressible Quantum Fluid with Fractionally Charged Excitations," *Phys. Rev. Lett.*, Vol. 50, No. 18, pp. 1395–1398, 1983.
- [25] R. de Picciotto, M. Reznikov, M. Heiblum, V. Umansky, G. Bunin, and D. Mahalu, "Direct Observation of a Fractional Charge," *Nature*, Vol. 389, No. 6647, pp. 162–164, 1997.
- [26] L. Saminadayar, D. C. Glatzli, Y. Jin, and B. Etienne, "Observation of the $e/3$ Fractionally Charged Laughlin Quasiparticle," *Phys. Rev. Lett.*, Vol. 79, No. 13, pp. 2526–2529, 1997.
- [27] F. D. M. Haldane, "Fractional Quantization of the Hall Effect—a Hierarchy of Incompressible Quantum Fluid States," *Phys. Rev. Lett.*, Vol. 51, No. 7, pp. 605–608, 1983.
- [28] J. K. Jain, "Composite-fermion Approach for the Fractional Quantum Hall Effect," *Phys. Rev. Lett.*, Vol. 63, No. 2, pp. 199–202, 1989.
- [29] N. Read and D. Green, "Paired States of Fermions in Two Dimensions with Breaking of Parity and Time-reversal Symmetries and the Fractional Quantum Hall Effect," *Phys. Rev. B*, Vol. 61, No. 15, pp. 10267–10297, 2000.
- [30] X. G. Wen, "Non-Abelian Statistics in the Fractional Quantum Hall States," *Phys. Rev. Lett.*, Vol. 66, No. 6, pp. 802–805, 1991.
- [31] B. Blok and X. G. Wen, "Many-body Systems with Non-Abelian Statistics," *Nucl. Phys. B*, Vol. 374, No. 3, pp. 615–646, 1992.
- [32] M. Levin, B. I. Halperin, and B. Rosenow, "Particle-hole Symmetry and the Pfaffian State," *Phys. Rev. Lett.*, Vol. 99, No. 23, 236806, 2007.
- [33] S.-S. Lee, S. Ryu, C. Nayak, and M. P. A. Fisher, "Particle-hole Symmetry and the $\nu = 5/2$ Quantum Hall State," *Phys. Rev. Lett.*, Vol. 99, No. 23, 236807, 2007.
- [34] B. Halperin, *Helv. Phys. Acta*, "Theory of the Quantized Hall Conductance," Vol. 56, No. 1-3, pp. 75–102, 1983.
- [35] J. Overbosch and X.-G. Wen, "Phase Transitions on the Edge of the $\nu = 5/2$ Pfaffian and anti-Pfaffian Quantum Hall State." [arXiv:0804.2087v1]
- [36] C. Töke and J. K. Jain, "Understanding the $5/2$ Fractional Quantum Hall Effect without the Pfaffian Wave Function," *Phys. Rev. Lett.*, Vol. 96, No. 24, 246805, 2006.
- [37] M. Dolev, M. Heiblum, V. Umansky, A. Stern, and D. Mahalu, "Observation of a Quarter of an Electron Charge at the $\nu = 5/2$ Quantum Hall State," *Nature*, Vol. 452, No. 7189, pp. 829–834, 2008.
- [38] M. Dolev, Y. Gross, Y. C. Chung, M. Heiblum, V. Umansky, and D. Mahalu, "Dependence of the Tunneling Quasiparticle Charge Determined via Shot Noise Measurements on the Tunneling Barrier and Energetics," *Phys. Rev. B*, Vol. 81, No. 16, 161303(R), 2010.
- [39] V. Venkatachalam, A. Yacoby, L. Pfeiffer, and K. West, "Local Charge of the $\nu = 5/2$ Fractional Quantum Hall State," *Nature*, Vol. 469, No. 7329, pp. 185–188, 2011.
- [40] I. P. Radu, J. B. Miller, C. M. Marcus, M. A. Kastner, L. N. Pfeiffer, and K. W. West, "Quasi-particle Properties from Tunneling in the $\nu = 5/2$ Fractional Quantum Hall State," *Science*, Vol. 320, No. 5878, pp. 899–902, 2008.

- [41] X. Lin, C. Dillard, M. A. Kastner, L. N. Pfeiffer, and K. W. West, "Measurements of Quasiparticle Tunneling in the $\nu = 5/2$ Fractional Quantum Hall State," *Phys. Rev. B*, Vol. 85, No. 16, 165321, 2012.
- [42] S. Das Sarma, M. Freedman, and C. Nayak, "Topologically Protected Qubits from a Possible Non-Abelian Fractional Quantum Hall State," *Phys. Rev. Lett.*, Vol. 94, No. 16, 166802, 2005.
- [43] R. Morf, "Transition from Quantum Hall to Compressible States in the Second Landau Level: New Light on the $\nu = 5/2$ Enigma," *Phys. Rev. Lett.*, Vol. 80, No. 7, pp. 1505–1508, 1998.
- [44] I. Dimov, B. I. Halperin, and C. Nayak, "Spin Order in Paired Quantum Hall States," *Phys. Rev. Lett.*, Vol. 100, No. 12, 126804, 2008.
- [45] A. E. Feiguin, E. Rezayi, K. Yang, C. Nayak, and S. Das Sarma, "Spin Polarization of the $\nu = 5/2$ Quantum Hall State," *Phys. Rev. B*, Vol. 79, No. 11, 115322, 2009.
- [46] S. Das Sarma, G. Gervais, and X. Zhou, "Energy Gap and Spin Polarization in the $5/2$ Fractional Quantum Hall Effect," *Phys. Rev. B*, Vol. 82, No. 11, 115330, 2010.
- [47] J. K. Jain, "The $5/2$ Enigma in a Spin?," *Physics*, Vol. 3, p. 71, 2010.
- [48] J. P. Eisenstein, R. Willett, H. L. Stormer, D. C. Tsui, A. C. Gossard, and J. H. English, "Collapse of the Even-Denominator Fractional Quantum Hall Effect in Tilted Fields," *Phys. Rev. Lett.*, Vol. 61, No. 8, pp. 997–1000, 1988.
- [49] C. R. Dean, B. A. Piot, P. Hayden, S. Das Sarma, G. Gervais, L. N. Pfeiffer, and K. W. West, "Contrasting Behavior of the $5/2$ and $7/3$ Fractional Quantum Hall Effect in a Tilted Field," *Phys. Rev. Lett.*, Vol. 101, No. 18, 186806, 2008.
- [50] C. Zhang, T. Knuuttila, Y. Dai, R. R. Du, L. N. Pfeiffer, and K. W. West, " $\nu = 5/2$ Fractional Quantum Hall Effect at 10 T: Implications for the Pfaffian State," *Phys. Rev. Lett.*, Vol. 104, No. 16, 166801, 2010.
- [51] M. Stern, P. Plochocka, V. Umansky, D. K. Maude, M. Potemski, and I. Bar-Joseph, "Optical Probing of the Spin Polarization of the $\nu = 5/2$ Quantum Hall State," *Phys. Rev. Lett.*, Vol. 105, No. 9, 096801, 2010.
- [52] T. D. Rhone, J. Yan, Y. Gallais, A. Pinczuk, L. Pfeiffer, and K. W. West, "Rapid Collapse of Spin Waves in Nonuniform Phases of the Second Landau Level," *Phys. Rev. Lett.*, Vol. 106, No. 19, 196805, 2011.
- [53] W. Desrat, D. K. Maude, M. Potemski, J. C. Portal, Z. R. Wasilewski, and G. Hill, "Resistively Detected Nuclear Magnetic Resonance in the Quantum Hall Regime: Possible Evidence for a Skyrme Crystal," *Phys. Rev. Lett.*, Vol. 88, No. 25, 25680, 2002.
- [54] O. Stern, N. Freytag, A. Fay, W. Dietsche, J. H. Smet, K. von Klitzing, D. Schuh, and W. Wegscheider, "NMR Study of the Electron Spin Polarization in the Fractional Quantum Hall Effect of a Single Quantum Well: Spectroscopic Evidence for Domain Formation," *Phys. Rev. B*, Vol. 70, No. 7, 075318, 2004.
- [55] A. Valeille, K. Muraki, and Y. Hirayama, "Highly Reproducible Fabrication of Back-gated GaAs/AlGaAs Heterostructures Using AuGe-Ni Ohmic Contacts with Initial Ni Layer," *Appl. Phys. Lett.*, Vol. 92, No. 15, 152106, 2008.
- [56] G. Gamez and K. Muraki, " $\nu = 5/2$ Fractional Quantum Hall State in Low-mobility Electron Systems: Different Roles of Disorder," <http://arxiv.org/abs/1101.5856>
- [57] N. Kumada, K. Muraki, and Y. Hirayama, "NMR Evidence for Spin Canting in a Bilayer $\nu = 2$ Quantum Hall System," *Phys. Rev. Lett.*, Vol. 99, No. 7, 076805, 2007.
- [58] J. H. Smet, R. A. Deutschmann, F. Ertl, W. Wegscheider, G. Abstreiter, and K. von Klitzing, "Gate-voltage Control of Spin Interactions between Electrons and Nuclei in a Semiconductor," *Nature*, Vol. 415, No. 6869, pp. 281–286, 2002.
- [59] S. Kraus, O. Stern, J. G. S. Lok, W. Dietsche, K. von Klitzing, M. Bichler, D. Schuh, and W. Wegscheider, "From Quantum Hall Ferromagnetism to Huge Longitudinal Resistance at the $2/3$ Fractional Quantum Hall State," *Phys. Rev. Lett.*, Vol. 89, No. 26, 266801, 2002.
- [60] R. R. Du, A. S. Yeh, H. L. Stormer, D. C. Tsui, L. N. Pfeiffer, and K. W. West, "Fractional Quantum Hall Effect Around $\nu = 3/2$ —Composite Fermions with a Spin," *Phys. Rev. Lett.*, Vol. 75, No. 21, pp. 3926–3929, 1995.
- [61] A. Stern and B. I. Halperin, "Proposed Experiments to Probe the Non-Abelian $\nu = 5/2$ Quantum Hall State," *Phys. Rev. Lett.*, Vol. 96, No. 1, 016802, 2006.
- [62] P. Bonderson, A. Kitaev, and K. Shtengei, "Detecting Non-Abelian Statistics in the $\nu = 5/2$ Fractional Quantum Hall State," *Phys. Rev. Lett.*, Vol. 96, No. 1, 016803, 2006.
- [63] R. L. Willett, L. N. Pfeiffer, and K. W. West, "Measurement of Filling Factor $5/2$ Quasiparticle Interference with Observation of Charge $e/4$ and $e/2$ Period Oscillations," *Proc. of Natl. Acad. Sci.*, Vol. 106, No. 22, pp. 8853–8858, 2009.
- [64] R. L. Willett, L. N. Pfeiffer, and K. W. West, "Alternation and Interchange of $e/4$ and $e/2$ Period Interference Oscillations Consistent with Filling Factor $5/2$ Non-Abelian Quasiparticles," *Phys. Rev. B*, Vol. 82, No. 20, 205301, 2010.
- [65] S. An, P. Jiang, H. Choi, W. Kang, S. H. Simon, L. N. Pfeiffer, K. W. West, and K. W. Baldwin, "Braiding of Abelian and Non-Abelian Anyons in the Fractional Quantum Hall Effect." [arXiv:1112.3400v1]



Koji Muraki

Senior Research Scientist (Distinguished Researcher) and Group Leader of the Quantum Solid State Physics Research Group, NTT Basic Research Laboratories.

He received the B.E., M.E., and Ph.D. degrees in applied physics from the University of Tokyo in 1989, 1991, and 1994, respectively. He joined NTT Basic Research Laboratories in 1994. From 2001 to 2002, he was a visiting researcher at the Max Planck Institute for Solid State Research, Stuttgart, Germany. His research interests are focused on many-body effects in low-dimensional semiconductor structures. He is a member of the Physical Society of Japan and the Japan Society of Applied Physics.

Digital Signage Standardization

Kenichi Muramoto

Abstract

In this article, we discuss a vision for digital signage in the future and standardization activities toward this vision, which incorporates insights and know-how gained through the experience of last year's Great East Japan Earthquake. Digital signage utilizing broadband networks has already begun to spread in industrialized regions, mainly in Europe, America, and Japan, and more installations are expected in a variety of locations. For digital signage to develop further as a next-generation infrastructure for distributing information, there is a need to ensure compatibility among products from different manufacturers and interconnectivity for communications, so international standardization is becoming more important.

1. Introduction

After the Great East Japan Earthquake on March 11, 2011, and the power supply problems due to the ensuing nuclear power plant incident, digital signage systems were temporarily shut down to save power, and planned new installations were delayed or cancelled one after another. These measures had a major effect on the digital signage market in Japan. However, directly after the earthquake, the usual programming schedule changed, and digital signage was used as an effective tool for distributing information to people unable to return home and confined indoors, by displaying news broadcasts from NHK (Japan Broadcasting Corporation). There were many positive cases in which urban signage was used effectively to provide information helpful for daily life after the earthquake, such as disaster news and information about survivors and radiation. This led to greater recognition of the value and importance of digital signage.

Most companies operating digital signage experienced new issues such as not having operation manuals that anticipate disaster and other emergency situations, no analysis of content required at specific locations during a disaster, and no preparation of such content for distribution beforehand. Taking these into consideration, the Production Department of the Digital Signage Consortium has analyzed the types of content needed when a disaster occurs, dividing the time-line following a disaster into three periods

(disaster, initial recovery, and post-recovery) and defining three types of region (disaster-hit, partially damaged, and safe). It then summarized the results and proposed the following regarding content needed in times of disaster.

- (1) Local information, using the local characteristics of the digital signage, is essential.
- (2) Train and bus operation information is needed (in urban areas).
- (3) NHK is a useful source of information directly after a disaster.
- (4) Use of public advertising for televising during a disaster must be arranged beforehand.
- (5) Content and operation must be integrated.

To provide the content needed at the time of a disaster, we need a digital signage platform for disaster response such as that shown in **Fig. 1**. For the implementation of such a platform, cooperation and discussion among government, academia, and the private sector is very important.

For situations such as disasters and emergencies, the NTT Group has developed the "Hikari Signage" digital signage solution, with solar signage incorporating solar panels and batteries so that information can still be provided when the power supply is unreliable. We are promoting the deployment of these systems first in highly public locations. In October, 2011, we introduced examples of using digital signage as a tool for distributing information in the aftermath of the Great East Japan Earthquake at Telecom World 2011, held in Geneva, Switzerland. The

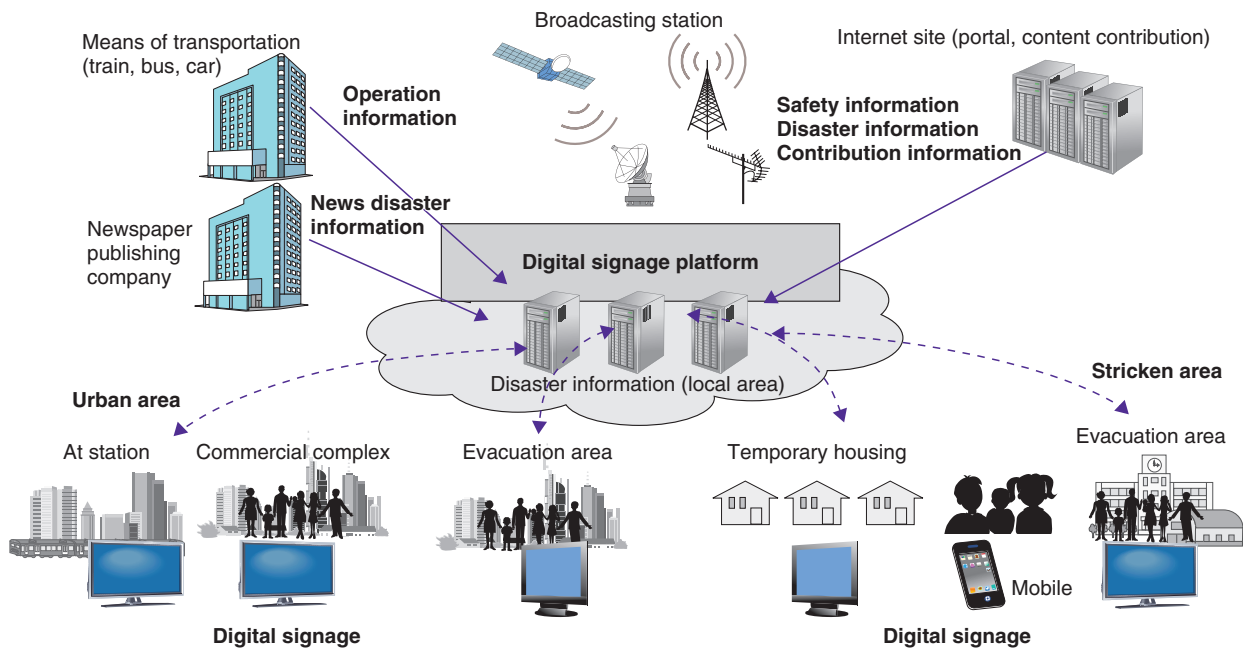


Fig. 1. Digital signage platform for disaster response.



Fig. 2. Solar signage.

solar signage exhibits (Fig. 2) attracted much interest from government-agency-related attendees from various countries. This demonstrated a high level of awareness of the importance of providing information in public places and of using natural energy sources, and it reinforced our impression, common

around the world, that addressing these issues is essential for disaster prevention.

2. Trends in digital signage systems

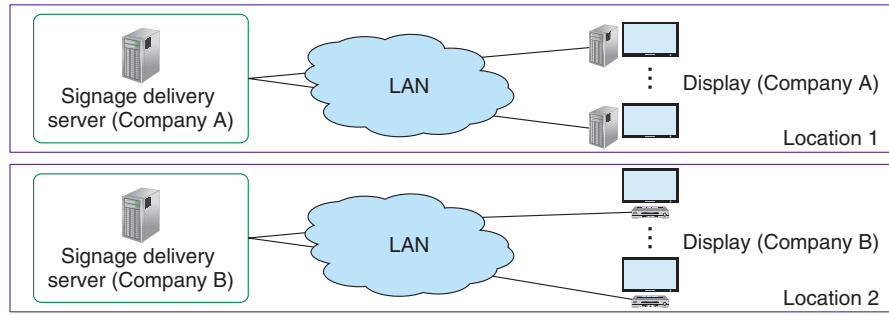
Next, we discuss some trends in digital signage systems. This includes the transition from dedicated systems, which have been dominant until now, to remote controlled systems utilizing networks, and the development of systems applying next-generation web technologies. These systems can be divided into three generations (Fig. 3).

- 1st generation: Dedicated systems with distribution servers and terminals provided as a set.
- 2nd generation: Distribution servers located in a datacenter and systems controlled remotely over a network.
- 3rd generation: Systems utilizing next-generation web technologies.

First-generation systems were dominant until a few years ago, but second-generation systems have recently overtaken them, providing the benefits of improved usability, decreased installation and operating costs, and no need for dedicated operators, even for large-scale installations on tall buildings or in airports. These merits are also clearly effective for medium- and small-scale applications, so use of this technology where it can be applied easily, mainly for

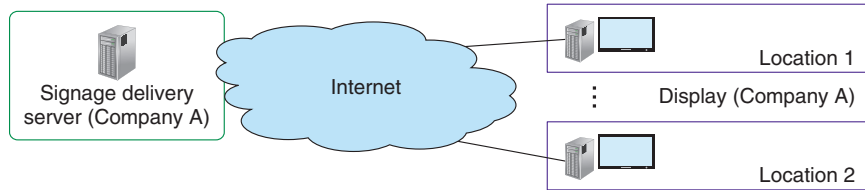
1st generation

- Different specifications for each vendor/maker
- Operated in the same location
- Mainly SI type



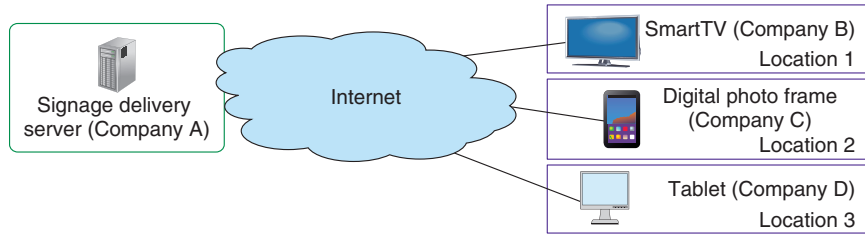
2nd generation

- Different specifications for each vendor/maker
- Remote operation via the Internet
- Emergence of SaaS type



3rd generation and onwards

- Multiple devices based on international standards
- Remote operation via the Internet
- Cloud type utilizing SmartTV etc.



LAN: local area network
 SaaS: software as a service
 SI: systems integration

Fig. 3. Trends in digital signage systems.

informational and sales promotion applications in enterprise, is growing.

3. Systems applying next-generation web technology

Next-generation web technology refers to HTML5 (hypertext markup language version 5), which is being standardized by the organization that creates web technology standards, the World Wide Web Consortium (W3C) [1]. HTML5 is not only for document design, but also defines standards for graphics, communications, databases, and other functions and is implemented as a standard in all browsers. The significance of this is that the browser provides a common application platform for various devices, including smartphones, tablets, and smart TVs. This eliminates the need to create individual applications for each device, as was the case with earlier technologies. Applying HTML5 to create content for digital signage systems also allows smartphones, tablets, and smart TVs to be used as signage displays using only

their general functionality (Fig. 4).

Applying this type of next-generation web technology for digital signage systems can be expected to yield many benefits. Firstly, it should result in reduced overall system costs. Ordinary web servers and devices such as those mentioned above can be used for distribution servers and terminals. In terms of content creation, it is relatively easy to retain HTML coders and it is not necessary to create content for each type of device, as was the case earlier.

Next, using standard technologies makes new services possible. One characteristic function enabled by next-generation web technology is realtime communication between a distribution server and terminal, through WebSocket technology. Thus, in times of disaster and other emergencies, information on display devices can be changed through updates pushed from the distribution server. Though pushed changes were possible before, specifications differed among manufacturers. Since disaster applications must be usable over broad areas, this was recognized as a significant obstacle to the use of this earlier technology.

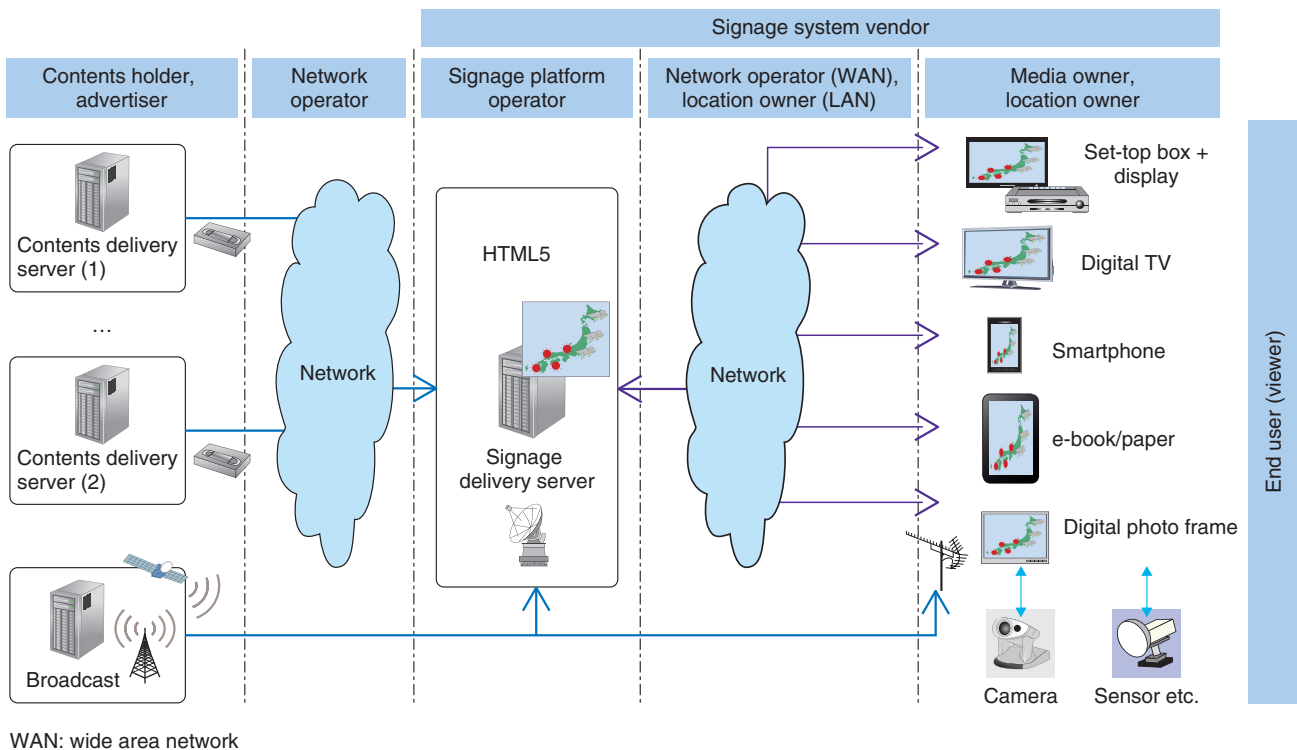


Fig. 4. Systems applying next-generation web technology.

Furthermore, linking with the already abundant content on the Internet can increase expressive power. It has become easy to link with community and informational sites on the Internet through application programming interfaces, so content relevant to the location can be separated out and displayed on signage effectively.

This type of environment provides fertile ground for developing new businesses given the right idea, as has been true with Internet businesses, so it can play a major role in stimulating markets, with new investment from venture companies and other sources.

4. International standardization trends

Regulation and standardization are being conducted in forums such as (1) POPAI (point-of-purchase advertising international), which is an organization in the USA related to digital signage that has established a set of application specifications for digital signage and is standardizing aspects of advertising content such as screen media type and (2) the Digital Place-based Advertising Association (DPAA), which has published viewer-measurement guidelines to mea-

sure the effectiveness of advertising placement. However, standardization of signage systems architectures is not being examined. Moreover, though various other countries such as the USA and China have broadband proliferation strategies that give some consideration to digital signage, there are no clear policies that apply specifically to the digital signage field.

By contrast, various documents such as the “Digital Signage Standard System Guidelines 1.0” have been published by the Digital Signage Consortium in Japan, and consensus among the major related vendors was reached in 2008, so, through its domestic market, Japan can be said to be leading the world in standardization efforts in this field.

5. International standardization trends in digital signage led by Japan

In consideration of these international standardization trends and as part of its effort to strengthen Japan’s international competitiveness, the Telecommunications Bureau of the Ministry of Internal Affairs and Communications (MIC) established

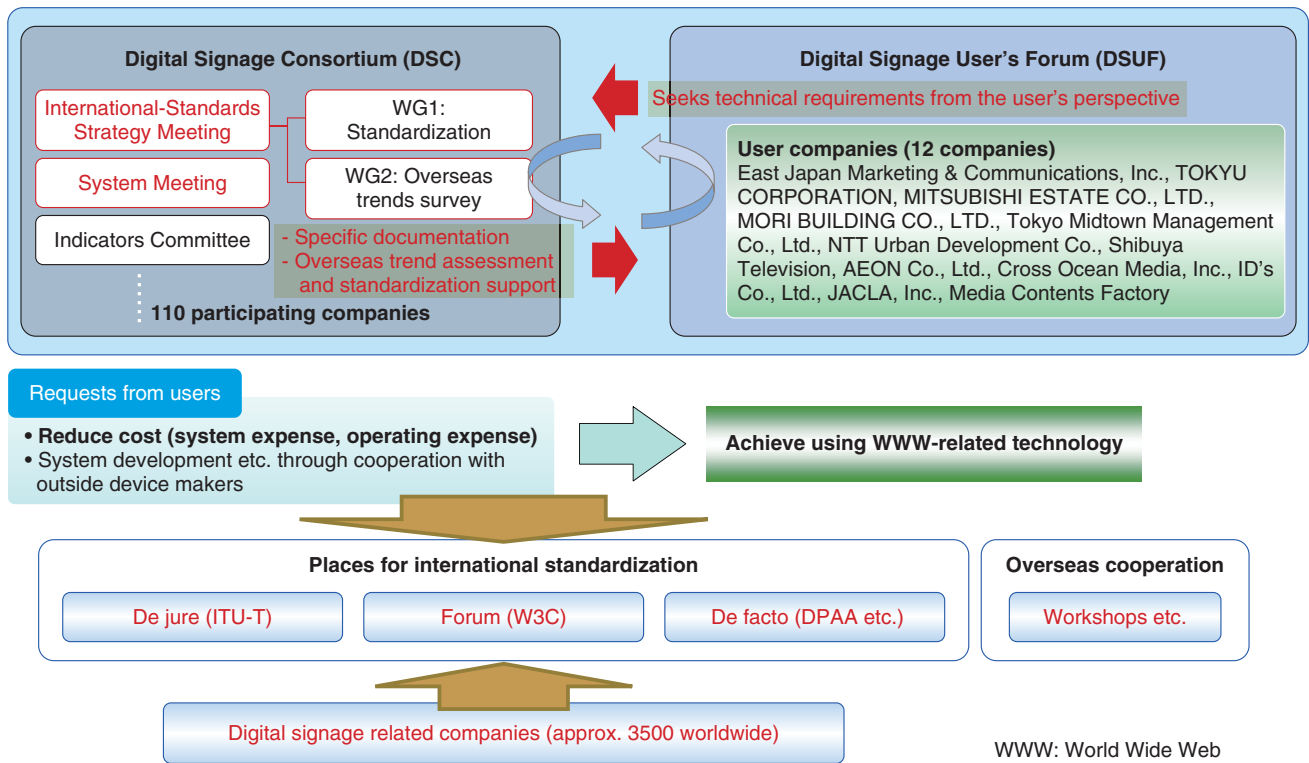


Fig. 5. Organizations promoting standardization of digital signage systems.

digital signage as an important field for standardization in its “Interim Report on Standardization Policies in the Information and Telecommunications Fields (Feb. 2011)”. To promote this standardization activity, a new Digital Signage Users Forum was established, with membership including a dozen or more Japanese businesses using digital signage, such as location owners and signage providers. This has provided a system for reflecting input from actual users of the services, rather than from only the infrastructure providers when setting standard specifications for signage systems, by promoting cooperation with the Digital Signage Consortium, which is composed mainly of providers (Fig. 5).

The standard specifications resulting from study under this system will be proposed for international standardization. Until now, MIC has been working to establish *de jure standards*, typified by activities of the International Telecommunication Union (ITU), by reaching agreement among national governments. However, considering international trends such as accelerating standardization work and changes in technical standardization fields, activity on *forum standards* like those of the W3C will also become

prominent in the future, with related businesses cooperating to create a plan and using it as the standard.

With this sort of strong backing from the government, standardization work was begun, through a joint proposal from NTT and Japanese manufacturers, at a meeting of ITU-T SG16 (International Telecommunication Union, Telecommunication Standardization Sector, Study Group 16) held in March 2011. To promote this activity, the ITU Digital Signage Workshop was held in Akihabara, Tokyo, in December 2011, sponsored by ITU and backed by the Digital Signage Consortium. It attracted many attendees from government agencies in various countries, standardization organizations, and related companies, who engaged in active discussion of international standardization of digital signage. This activity yielded results, and in July 2012, “ITU-T H.780: Digital signage: Service requirements and IPTV-based architecture” was approved [2] (IPTV: Internet protocol television).

Moreover, regarding venues for forum standardization, at the W3C TPAC2011 (Technical Plenary/Advisory Committee meeting), which started on October 31, 2011, NTT proposed web-based signage

based on next-generation web technology as a form of digital signage for the multiscreen era. Then, in April 2012, the Web-based Signage Business Group was established with a chairman from Japan, and discussion toward standardization began. Furthermore, the first W3C workshop on digital signage was held on June 14 and 15, 2012, in Japan (Makuhari Messe, Chiba), bringing together many related participants for the discussion.

6. Concluding remarks

Among industrialized countries, Japan is one of the most advanced in terms of digital signage prolifera-

tion, related technologies, knowledge, and know-how. We have also studied practical applications of digital signage during times of disaster, incorporating experience from the Great East Japan Earthquake. We are confident that this will be a source for strengthening Japan's international competitiveness in the future, and we are using various standardization avenues to continue our activities that will enable Japan to lead the global digital signage marketplace.

References

- [1] <http://www.w3.org/community/websignage/>
- [2] <http://www.itu.int/rec/T-REC-H.780-201206-P>



Kenichi Muramoto

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

He received the B.E. and M.E. degrees in electronics from Tokyo University of Science in 1995 and 1997, respectively. After first working for a telecommunication service company, he joined NTT Communications in 2001 and took charge of the consulting service for corporation users about the system and network for digital content delivery. He was transferred to NTT in 2009. He is currently engaged in production activities related to the digital signage business of the NTT Group.

Case Studies of Using the Gigabit-compatible Protocol Checker as a Troubleshooting Tool for Home IP Systems

Abstract

This article introduces case studies of using the gigabit-compatible protocol checker as a troubleshooting tool for home Internet protocol (IP) systems. It is the thirteenth in a bimonthly series on the theme of practical field information about telecommunication technologies. This month's contribution is from the Network Interface Engineering Group, Technical Assistance and Support Center, Maintenance and Service Operations Department, Network Business Headquarters, NTT EAST.

1. Introduction

Customer needs are changing as access lines become faster and a wide range of application services come to be provided. There is demand for high-quality Internet protocol (IP) services with even higher levels of reliability than in the past. However, the range of configuration patterns for IP equipment within customers' residences has been growing. As a result, the Technical Assistance and Support Center has been receiving many inquiries concerning faults having low reproducibility, such as ones that occur once a day or once a week, as well as enquiries about unusual faults for which a solution cannot be found without analyzing the packets flowing in the customer's home network.

This article presents case studies of using the gigabit-compatible protocol checker, which can easily capture the packet data needed for fault analysis.

2. Overview of gigabit-compatible protocol checker

The gigabit-compatible protocol checker (**Fig. 1**) [1] has two local area network (LAN) ports for mirroring and one LAN port for management. It can be installed within the Ethernet segment in a residence



Fig. 1. External view of gigabit-compatible protocol checker.

as a packet-capture tool that obtains packet data and stores it in a built-in memory. Although it is compact, it provides long-term file acquisition and storage so it is effective for low-reproducibility faults because it can capture data when the fault reappears; the captured data can be analyzed using a LAN analyzer such as Wireshark. Its main functions are: support for packet capture at about 200 Mbit/s over gigabit Ethernet, an operation panel for starting and stopping packet capture without the need to attach a personal computer (PC), and support for remote control from a maintenance center and automatic transfer of data.

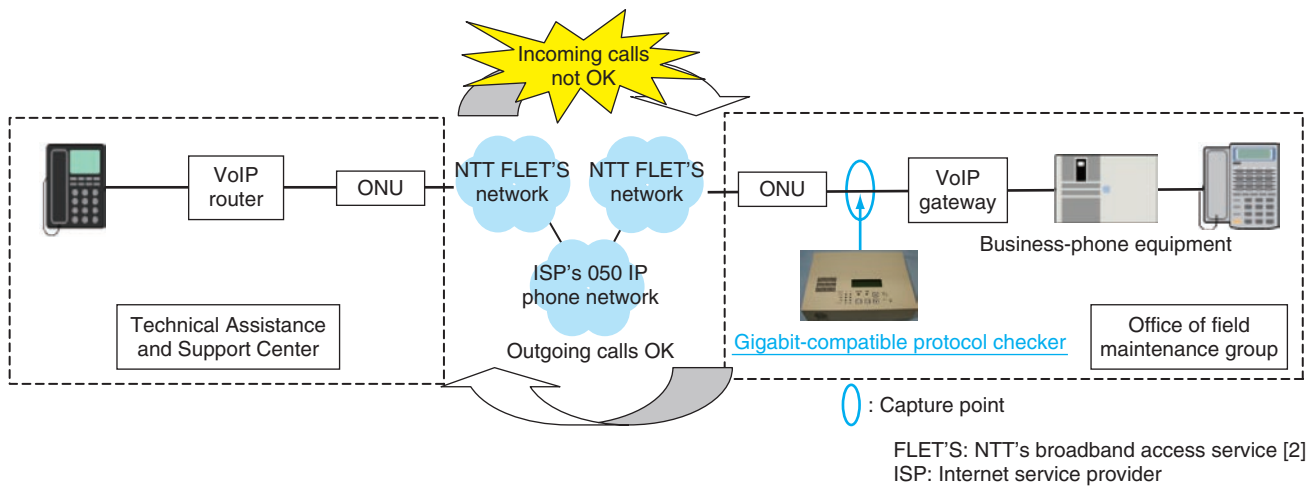


Fig. 2. Customer's home configuration and measurement system.

3. Case studies

3.1 Incoming calls disabled on 050 IP phone service

3.1.1 Description of fault

A customer using NTT EAST's B FLET'S service and an ISP's 050 IP phone service upgraded the VoIP-gateway from model A to model B, but then found that incoming calls were disabled even though outgoing calls could be made as usual (VoIP: voice over IP). At the time of the fault, the party making the call simply heard a busy signal although the receiving party (the NTT customer) was not using the line. Even when the new model-B gateway equipment was replaced, the problem persisted.

3.1.2 Inspection method

To troubleshoot this problem, we duplicated the customer's system configuration in the office of a field maintenance group and conducted a test to inspect calls made from the Technical Assistance and Support Center to that office. In this test, we inserted the gigabit-compatible protocol checker between the optical network unit (ONU) and the VoIP gateway in the customer's premises to analyze call conditions at the time of the fault (incoming calls not OK) and we investigated any differences in the session initiation protocol (SIP) sequence for two cases: (1) when the VoIP gateway was model A and (2) when it was model B. The test setup is shown in Fig. 2.

3.1.3 Inspection results

We found that calls could be received normally when the VoIP gateway was model A (Fig. 3). However, when it was model B, after returning a 100Try-

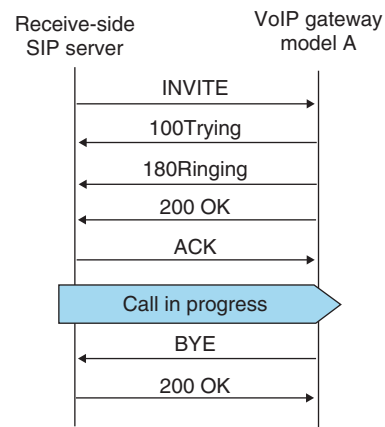


Fig. 3. Incoming-calls OK sequence.

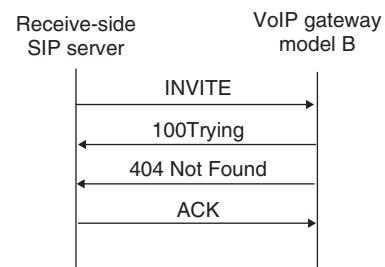


Fig. 4. Incoming-calls not OK sequence.

ing message in response to an INVITE message from the receive-side SIP server, the gateway returned an

```

2011/2/3 22:34:31 PPPoE セッション解放[接続先1]
2011/2/3 21:55:34 PPPoE セッション解放[接続先1]
2011/2/3 20:51:11 PPPoE セッション解放[接続先1]
2011/2/3 20:29:48 PPPoE セッション解放[接続先1]
2011/2/3 20:15:25 PPPoE セッション解放[接続先1]
2011/2/3 19:49:26 PPPoE セッション解放[接続先1]
2011/2/3 18:51:32 PPPoE セッション解放[接続先1]
    
```

Fig. 5. Router log.

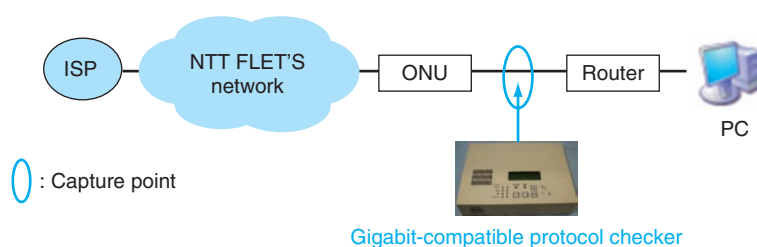


Fig. 6. Customer's home configuration and measurement system.

error “404 Not Found” (Fig. 4). This error is returned whenever the called party cannot be detected, which means that the model-B VoIP gateway had judged that the terminal targeted by the incoming call did not exist.

3.1.4 Cause of fault

The results of this inspection led us to consider that although the model-B VoIP gateway received the dial-in number contained in the INVITE message, it could not recognize the terminal targeted by it and returned “404 Not Found”. When the model-B VoIP gateway was designed, no assumptions were made about the provider of the 050 IP telephone services; consequently, the maintenance manual did not describe how to set the additional dial-in numbers for a particular provider. This lack of settings caused this problem.

3.1.5 Countermeasure and results

We solved this problem by creating settings for additional dial-in numbers in the model-B VoIP gateway. We also concluded that no problems occurred with incoming calls in the model-A VoIP gateway because it does not refer to settings of additional dial-in numbers in the INVITE message of the ISP's 050 IP phone service.

3.2 Occasionally slow Internet access

3.2.1 Description of fault

A customer using a FLET'S optical line reported

that Internet access slowed down sometimes. Upon checking the customer's router log, we found frequent occurrences of the message “PPPoE^{*1} session released” (Fig. 5). Even when the router and ONU were replaced and the accommodation line was changed, the problem remained.

3.2.2 Inspection method

We inserted the gigabit-compatible protocol checker between the ONU and router installed in the customer's residence and proceeded to capture and analyze packets. The system configuration at that time is shown in Fig. 6.

3.2.3 Inspection results

Upon analyzing the router log and data captured at the time of this phenomenon, we found that the reception of a PPP (point-to-point protocol) Termination Request from the network side was followed by a PPPoE Active Discovery Termination (PADT) request. Furthermore, upon checking the packet data captured at times other than when this phenomenon occurred, we found that in all cases the reception of a PPP Termination Request was preceded by an idle state with the Internet service provider (ISP) lasting about 10 minutes (Fig. 7).

*1 PPPoE: Point-to-point protocol (PPP) over Ethernet; a protocol specifically for establishing, setting, and terminating a PPP session between an access concentrator and a terminal device on an Ethernet network.



Fig. 7. Captured data.

3.2.4 Cause of fault

The PPPoE session was terminated when the idle state with the ISP lasted longer than 10 minutes, and it took about 6 seconds for the session to be reestablished. Therefore, we concluded that the customer would have experienced a slow response when attempting to access the Internet during this 6-s period.

3.2.5 Coping

When we contacted the customer's ISP, we were advised that a PPP session is terminated if the idle time exceeds 10 minutes to prevent unnecessary distribution of global IP addresses. We therefore told the customer that the problem was not caused by NTT equipment and we asked the customer to consult with the ISP.

3.3 Failure of LAN communications between fax and PC

3.3.1 Description of fault

A customer with a home fax machine receives images via a FLET'S optical line and uses a function for automatically transferring those images from the fax to a PC via a LAN. The customer reported that this transfer occasionally failed. Replacing devices within the customer's home did not solve the problem.

3.3.2 Inspection method

To examine the image-data transmission conditions between the fax and PC, we inserted a gigabit-com-

patible protocol checker between the fax and switch in the customer's home and analyzed the captured data. The system configuration at that time is shown in Fig. 8.

3.3.3 Inspection results

Upon analyzing the captured data, we found that communications between the fax and PC were conducted in the form of a TCP (transmission control protocol) session. During normal operation, the session was established on the basis of a TCP 3-way handshake*2 (Fig. 9) and communications proceeded without any problems. However, when the fault occurred, no Syn/Ack packets were returned from the PC in response to a Syn packet sent from the fax. As a consequence, no session was established and normal communications were not performed. Data captured during normal operations is shown in Fig. 10 and data captured when the fault occurred is shown in Fig. 11.

3.3.4 Cause of fault

Upon inspecting the customer's PC, we found that the firewall settings of the security software installed on it had been modified from their standard values: the settings closed the TCP port, which disrupted communications.

3.3.5 Countermeasure and results

The firewall settings modified by the customer

*2 3-way handshake: A procedure for establishing a connection in TCP. The name derives from the fact that packets are passed three times, as shown in Fig. 9.

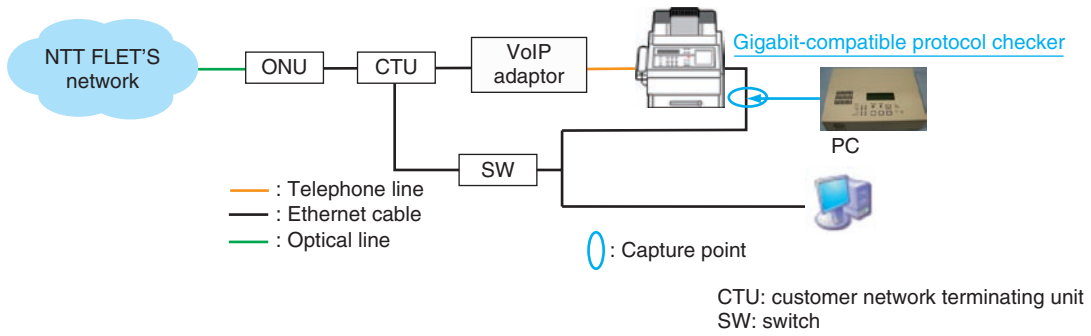


Fig. 8. Customer's home configuration and measurement system.

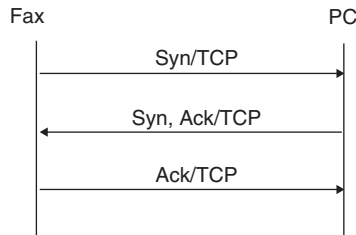


Fig. 9. TCP 3-way handshake.

Time	Source	Destination	Size	Protocol	Info
10:04:11.421	192.168.24.A	192.168.24.B	60	TCP	2803 > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:04:11.421	192.168.24.B	192.168.24.A	60	TCP	2869 > 2803 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
10:04:11.422	192.168.24.A	192.168.24.B	60	TCP	2803 > 2869 [ACK] Seq=1 Ack=1 Win=4380 Len=0
10:04:11.424	192.168.24.A	192.168.24.B	284	TCP	2803 > 2869 [PSH, ACK] Seq=1 Ack=1 Win=4380 Len=230
10:04:11.424	192.168.24.B	192.168.24.A	261	TCP	2869 > 2803 [PSH, ACK] Seq=1 Ack=1 Win=4380 Len=230
10:04:11.424	192.168.24.B	192.168.24.A	1259	TCP	2869 > 2803 [FIN, PSH, ACK] Seq=2 Ack=1 Win=0 Len=1259
10:04:11.426	192.168.24.A	192.168.24.B	60	TCP	2803 > 2869 [ACK] Seq=231 Ack=206 Win=0 Len=0
10:04:11.436	192.168.24.A	192.168.24.B	60	TCP	2803 > 2869 [ACK] Seq=231 Ack=1414 Win=3175 Len=0
10:04:11.438	192.168.24.A	192.168.24.B	60	TCP	2803 > 2869 [FIN, ACK] Seq=231 Ack=1414 Win=4380 Len=0
10:04:11.438	192.168.24.B	192.168.24.A	60	TCP	2869 > 2803 [ACK] Seq=1414 Ack=232 Win=65305 Len=0

During normal operations, a TCP 3-way handshake is successfully performed.

*IP addresses are partially shown. 192.168.24.A: FAX, 192.168.24.B: PC

Fig. 10. Fax LAN port communications during normal operations.

Time	Source	Destination	Size	Protocol	Info
10:09:05.038	192.168.24.A	192.168.24.B	60	TCP	2804 > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:09:05.496	192.168.24.A	192.168.24.B	60	TCP	2804 > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:09:07.076	192.168.24.A	192.168.24.B	60	TCP	2805 > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:09:07.546	192.168.24.A	192.168.24.B	60	TCP	2805 > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:09:14.274	192.168.24.A	192.168.24.B	60	TCP	2806 > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:09:14.719	192.168.24.A	192.168.24.B	60	TCP	2806 > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:14:17.297	192.168.24.A	192.168.24.B	60	TCP	2807 > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
10:14:17.736	192.168.24.A	192.168.24.B	60	TCP	2807 > 2869 [SYN] Seq=0 Win=4380 Len=0 MSS=1460

Fax sends a Syn packet to the PC but receives no response.

*IP addresses are partially shown. 192.168.24.A: FAX, 192.168.24.B: PC

Fig. 11. Fax LAN port communications at time of fault occurrence.

were restored to their standard values. This action eliminated the fault.

4. Concluding remarks

This article presented case studies of using a gigabit-compatible protocol checker to troubleshoot faults. Packet analysis is becoming an essential tool for investigating IP-related faults, and it is hoped that

the reader has found the case studies described here to be informative and useful.

References

- [1] "Gigabit-compatible Protocol Checker," NTT Technical Review, Vol. 10, No. 7, 2012.
<https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201207fa3.html>
- [2] FLET'S services. <http://flets.com/english/>

Papers Published in Technical Journals and Conference Proceedings

Double-branched 1×29 Silica-based PLC Switch with Low Loss and Low Power Consumption

T. Watanabe, Y. Hashizume, and H. Takahashi

Proc. of the 17th Microoptics Conference (MOC'11), Sendai, Japan, 2011.

We propose a novel double-branched circuit configuration for a 1×N optical switch. This compact configuration offers a high port count without greatly increasing power consumption. The fabricated 4-arrayed 1×29 silica-based PLC (planar lightwave circuit) switch exhibits an insertion loss as low as 2.6 dB.

Liquid Deposition Patterning of Conducting Polymer Ink onto Hard and Soft Flexible Substrates via Dip-Pen Nanolithography

H. Nakashima, M. J. Higgins, C. O'Connell, K. Torimitsu, and G. G. Wallace

Langmuir, American Chemical Society, Vol. 28, No. 1, pp. 804–811, 2012.

Ink formulations and protocols that enable the deposition and patterning of a conducting polymer (poly(3,4-ethylenedioxythiophene) poly(styrenesulfonate) or PEDOT:PSS for short) in the nanoscale domain have been developed. Significantly, we demonstrated the ability to pattern onto soft substrates such as silicone gum and polyethylene terephthalate (PET), which are materials of interest for low cost, flexible electronics. The deposition process and dimensions of the polymer patterns were found to be critically dependent on several parameters, including the pen design, ink properties, time after inking the pen, dwell time of the pen on the surface, and the nature of the material substrate. By assessing these different parameters, we obtained an improved understanding of the ability to control the dimensions of individual PEDOT:PSS structures down to 600 nm in width and 10–80 nm in height within patterned arrays. This applicability of dip-pen nanolithography for simple and nonreactive liquid deposition patterning of conducting polymers could lead to the fabrication of organic nanoelectronics or biosensors and complement existing printing techniques such as inkjet and extrusion printing by scaling down conductive components to submicrometer and nanoscale dimensions.

Compact Wavelength Tunable Filters Fabricated on a PLC Chip that Construct a Colorless/Directionless/Contentionless Drop Function in an Optical Cross-Connect

T. Niwa, R. Hirako, H. Hasegawa, K. Sato, M. Okuno, and T. Watanabe

Proc. of the Optical Fiber Communication Conference (OFC), p. OTh3D.6, Los Angeles, USA, 2012.

We demonstrate an efficient colorless/directionless/contentionless add/drop configuration utilizing newly proposed tunable filters to develop flexible optical cross connects (OXC) and reconfigurable optical add-drop multiplexers (ROADMs). The filters were compactly fabricated on a 15×70 mm² PLC (planar lightwave circuit) chip and the performance was verified.

Silica-based PLC Transponder Aggregators for Colorless, Directionless, and Contentionless ROADM

T. Watanabe, K. Suzuki, and T. Takahashi

Proc. of the Optical Fiber Communication Conference (OFC), p. OTh3D.1, Los Angeles, USA, 2012.

We describe a silica-on-silicon PLC (planar lightwave circuit) transponder aggregator based on a splitter-switch architecture. This integrated aggregator enables us to make a colorless, directionless, and contentionless multidegree reconfigurable optical add-drop multiplexer (ROADM) cost-effectively with a small footprint.

Constructing a Class-Based Lexical Dictionary using Interactive Topic Models

K. Sadamitsu, K. Saito, K. Imamura, and Y. Matsuo

Proc. of the 8th International Conference on Language Resources and Evaluation (LREC), pp. 2590–2595, Istanbul, Turkey, 2012.

This paper proposes a method of constructing arbitrary class-based related word dictionaries on interactive topic models; we assume that each class is described by a topic. We propose a semi-supervised method that uses the simplest topic model yielded by the standard EM (expectation maximization) algorithm; model calculation is very rapid. Furthermore, our approach allows a dictionary to be modified interactively and the final dictionary has a hierarchical structure.

This paper makes three contributions. First, we propose a word-based semi-supervised topic model. Second, we apply the semi-supervised topic model to interactive learning; this approach is called the Interactive Topic Model. Third, we propose a score function; it extracts related words that occupy the middle layer of the hierarchical structure. Experiments showed that our method can appropriately retrieve the words belonging to an arbitrary class.

Suppression of Polarization Dependence of Gain in Distributed Raman Amplifier System with Compact Pump Depolarizer

H. Kawakami, K. Mori, H. Yamamoto, and H. Miyamoto

Proc. of the 10th International Conference on Optical Internet (COIN2012), Vol. TuF3, Yokohama, Japan.

This paper tackles the polarization dependence of gain (PDG) in a distributed Raman amplifier system with orthogonal polarization multiplexed pump lights. We show that polarization mode dispersion in a transmission line degrades the orthogonality of pump lights and induces PDG. We propose a compact pump depolarizer to suppress PDG.

Hardware implemented network time protocol (HwNTP) based synchronization for digitized radio over fiber systems

S. Kuwano, Y. Yamada, K. Hisadome, and M. Teshima

IEICE Communications Express, Vol. 1, No. 1, pp. 4–9, 2012.

This paper reports on the synchronization performance of a hardware implemented network time protocol (HwNTP) module for a digitized radio over fiber (DROF) system. In experiments, the

HwNTP client was synchronized with the HwNTP server via an asynchronous packet network, and it provided highly accurate time and frequency references compared with software-based NTP. The accuracy achieved for a commercial Ethernet service is sufficient to satisfy the DROF requirements.

**Quantum repeaters and computation by a single module:
Remote nondestructive parity measurement**

K. Azuma, H. Takeda, M. Koashi, and N. Imoto

Physical Review A, Vol. 85, 062309, 2012.

We introduce a simple photonic probing scheme of remote nondestructive parity measurement (RNPM) on a pair of matter qubits. The protocol works as a single module for key operations such as entanglement generation, Bell measurement, and parity check measurement, which are sufficient not only for working toward a quantum repeater but also for equipping it with entanglement distillation. Moreover, the RNPM protocol can also be used for generating cluster states toward measurement-based quantum computation.
