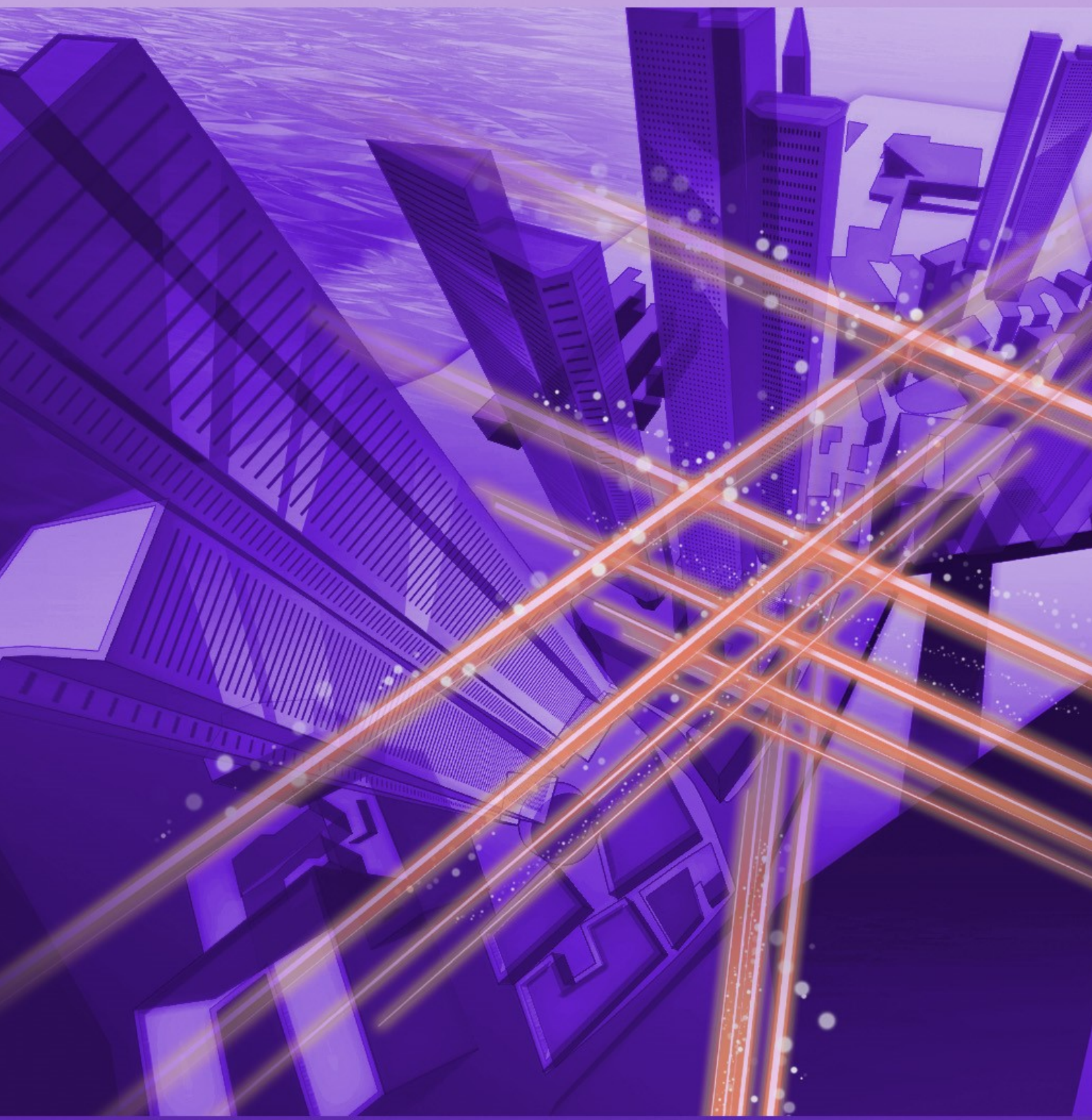
# NTT Technical Review

12
2019



December 2019 Vol. 17 No. 12

**NTT Technical Review**

## December 2019 Vol. 17 No. 12

**View from the Top**

- Seiji Maruyama, Senior Executive Vice President, NTT DOCOMO

**Feature Articles: Establishment of NTT Research, Inc. toward the Strengthening and Globalization of Research and Development**

- NTT Research, Inc. Launched to Strengthen and Globalize R&D
- Mission of Physics & Informatics Laboratories
- Research of Cryptography & Information Security Laboratories
- Launch of the Medical & Health Informatics Laboratories
- Establishing a Cryptography Research Lab in 2019

**Regular Articles**

- Data-coding Approaches for Organizing Omni-ambient Data

**Global Standardization Activities**

- Meeting Report of the 31st Asia-Pacific Telecommunity Standardization Program (ASTAP-31) and the Asia-Pacific Telecommunity (APT) Preparatory Meeting for WTSA-20

**Practical Field Information about Telecommunication Technologies**

- Efforts in Preventing Gas Leakage Caused by Movement of Conduit-enclosed Metallic Cables in Bridge Sections

**Information**

- Opening Ceremony of NTT Research, Inc.

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

# Enthusiasm Creates Surprise and Excitement—With the Spirit of DOCOMO, 5G Will Build a Richer Future

*Seiji Maruyama*
*Senior Executive Vice President,*
*NTT DOCOMO*

## Overview

Japan has reached the point in its advancement that it has to urgently and thoroughly address contemporary problems such as energy consumption, deterioration of infrastructure, and other social issues, including a declining birthrate and aging population. NTT DOCOMO is tackling these social issues using fifth-generation mobile communication systems (5G). At the same time as the Rugby World Cup 2019™ held in Japan this fall, NTT DOCOMO launched a 5G pre-commercial service, and such 5G services are expected to be applied in various scenarios. We asked Seiji Maruyama, Senior Executive Vice President, NTT DOCOMO, about NTT DOCOMO's endeavor to collaboratively create new value through contributions to industry, solutions to social issues, and expansion of its business.

*Keywords: 5G, social issues, open collaboration*

## 5G pre-commercial service has started. We want to support communication

*—5G pre-commercial service started in conjunction with the Rugby World Cup 2019™ that took place in Japan. How was the reaction?*

We are sensing expectations from everyone. We targeted starting the 5G pre-commercial service in conjunction with the opening of the Rugby World Cup 2019™*. I want as many people as possible to experience the splendor of fifth-generation mobile communication systems (5G).

5G has three features: high speed and large capacity, low latency, and multiple-terminal connection. We can say that 5G is a delightful way to watch sports that require a sense of presence and reality. We proposed and offered a new viewing style, such as multi-angle viewing, by which users were able to freely switch and watch footage captured from several cameras located in the stadiums and view additional information (such as player data) during some games of the Rugby World Cup 2019™. Taking advantage of the experience we gained through this pre-commercial service, we plan to start a 5G commercial service in the spring of 2020.

In the 5G era, the way you use your smartphones

* Rugby World Cup 2019™: "Rugby World Cup 2019" and its logo are trademarks or registered trademarks of Rugby World Cup Limited.

will change too. NTT DOCOMO is advocating the My Network Concept that allows 5G smartphones to be used as hubs for various peripheral devices and services linked to them in a 5G environment. Collaboration with partners is also very important. DOCOMO is promoting the DOCOMO 5G Open Partner Program for creating new usage scenarios for 5G in collaboration with over 3000 partners (as of September 2019), including companies, universities, and local governments. At the 5G pre-commercial service presentation held on September 18, we exhibited eighteen examples of our efforts in various fields, including manufacturing, medical care, and education, and environments such as work and public areas.

One example, which is an initiative with Takenaka Corporation, is remote operation of tower cranes used in the construction of high-rise buildings. A tower crane cannot work unless the operator climbs to the operator's cabin at the top of the crane, and once the operator has climbed to the cabin, it is said to be troublesome to come down to the ground again. To alleviate this work burden, we plan to conduct a trial demonstration of 5G remote control. It will be possible to transmit on-site audio and video, as well as crane-vibration data, which is important for making appropriate operational decisions, by using 5G. Consequently, the crane can be remotely operated as if the operator were in the actual cabin.

The rollout of 5G has attracted the attention of various fields and represents a huge technological advancement. It will be one of the pillars of digital transformation. Although new mobile communication technologies and services have been introduced approximately every 10 years—starting from the first (analog) generation in the early days of mobile phones, to the second generation (digitized from the first generation), to the third generation (oriented to mobile multimedia), and to the fourth generation (based on LTE: Long Term Evolution), 5G is attracting unprecedented attention.

Said to be an advanced country in terms of issues to be solved, Japan is facing various social issues such as the declining birthrate and aging population, depopulation in rural areas and regional disparity, labor shortage, and foreign workers, and these have become hot topics. Under these circumstances, 5G, artificial intelligence (AI), and the Internet of Things can be used to provide telemedicine and medical support, remote operation of construction machinery, and automatic operation of agricultural machinery. With such potential, 5G can be supplemented with a variety of added value in a manner that makes it useful for solving social issues.

*—It seems that 5G will help solve the problems facing Japan.*

Regarding the 5G pre-commercial service, through our DOCOMO 5G Open Lab, which we have expanded from four to eleven locations, NTT DOCOMO is providing 5G base-station equipment and video-transmission equipment connected to mobile stations free of charge to partners undertaking verification. We hope that partners who want to use 5G will use this testbed and deepen their collaboration with us in creating new 5G services. Aiming to solve the social issues that I mentioned earlier, we will accelerate our endeavors through the activities of our DOCOMO 5G Open Partner Program and DOCOMO 5G Open Lab.

For example, the revitalization of regional communities is promoted as a countermeasure against depopulation. In addition to creating industries using 5G, it is important to support the lives of people living in regions to be revitalized. If a new telemedicine infrastructure is put in place by connecting medical services in depopulated areas with hospitals in other areas via 5G, it would be possible to nurture a sense of security in residents with regard to being able to receive high-quality medical care, and that sensibility may lead to attracting more residents.

Regional revitalization tends to be a story of a particular region; however, as in the above example of telemedicine, cooperation among regions is vital. Communication between "people and people," "people and systems," and "systems and systems" is essential for this collaboration. 5G excels at communication providing a high sense of reality, real-time

information, and expanded networks, and providing communication services and infrastructure with such features is one of DOCOMO's major missions, which goes hand-in-hand with another of our major missions: providing solutions to social issues.

## The marketing environment has entered a period of change

*—Would you tell us about the present environment surrounding DOCOMO?*

The revised Telecommunications Business Law came into effect in October 2019. It has thus become necessary to review our sales methods, including adaptation to the separation of communication charges and device charges. In addition, a fourth operator was allowed to enter the market by the Japanese government to promote competition. It is rare for a large over-the-top player to enter a market as a mobile operator; accordingly, the Japanese mobile communication industry is attracting attention worldwide. Since that player is expected to enter the market with technologies and methods that differ from the methods we have cultivated thus far, we will study them thoroughly and adopt their good points.

The market also demands price competition among service providers, and by anticipating such changes in the environment, we introduced a new billing plan in June. Under a simple and easy-to-understand mechanism, the charges paid by certain customers will be cut by up to 40%. I want our customers to understand the features of DOCOMO services and continue to use them for as long as possible.

*—It seems that various services will be created according to the changing times and needs.*

We announced our medium-term management strategy in October 2018. To achieve sustainable growth in the 2020s, we are developing our business based on the basic policies of "transformation to business structure centered on customer membership programs" and "rollout of 5G and business creation." To implement those policies, we are focusing on creating revenue opportunities based on our customer base, growth with 5G, and rewarding customers and evolving customer contact points.

I explained the rollout of 5G and business creation earlier. Regarding transformation to business structure centered on customer membership programs, the definition of *customer* has changed. In the past, only subscribers to our mobile phone service have been defined as customers, but now all users of any of our services are defined as customers. For example, among our members of d POINT CLUB (customer loyalty program), nearly 20 million have contracts with other mobile phone service providers. Those people are also our customers, and together with customers having a mobile phone contract with DOCOMO, the number of customers is close to 70 million.

We are promoting marketing activities tailored to each individual so that all our customers can use various services more conveniently and actively. Our business operations centered on customer membership programs are steadily expanding, and the number of members is also increasing. Payment methods such as d CARD (credit card) and d PAYMENT (mobile payment service) are also spreading. By leveraging a wealth of assets, we will expand the number of members and partner companies and link them through digital marketing in a manner that forms continuous relationships with customers and provides new value.

This information of nearly 70 million members represents valuable big data. We currently have about 30,000 pieces of data per person, and we have accumulated those data for 70 million people. However, some customers may be worried about how these big data are used. Accordingly, to guarantee customer security and gain their trust while providing new value through data utilization, we announced DOCOMO's data-utilization policy in August 2019 as a personal data charter. In December, a personal data dashboard will be launched so that our customers can check their permission status concerning

different types of data and change their settings as desired.

An example of using another form of big data is our service called Mobile Spatial Statistics. This service allows the user to track or obtain anonymized information and see the distribution of people's movements on a map in a specific area in real time. Combined with AI, it is used for predicting demand of visiting commercial stores, optimally rearranging bicycles for bicycle-sharing services, and predicting traffic congestion on expressways.

Moreover, various sensors and cameras are installed in smartphones, so by linking these features with AI, many unique services are being created such as estimating concentration and mental state as well as selecting food from food packages and labels according to what food cannot be eaten for religious reasons. Some of these services have been put to practical use based on excellent ideas proposed in the Challenge Project that employees put forth voluntarily.

## The NTT Group's DNA: exerting its strength during challenging moments

*—In addition to new services, the mechanisms of DOCOMO seem to be structured to motivate young people and make them meet their potential in the company. Can you give a word to researchers and engineers inside and outside the company?*

It is my job to create an environment in which employees are motivated. This is a great opportunity for us when the 5G and information and communication technology (ICT) revolutions gather pace. I want to create a company in which employees can work proactively in this era. I think this situation is the same for each company in the NTT Group. So many opportunities are being formed, so I'd like our employees to grab them as many as possible. It is therefore important to work with enthusiasm. If we keep working with enthusiasm and a sense of purpose, chances will come in any environment.

Since joining NTT, I have been saying, "I want to do that," or "Let me do this." The first time was when I was assigned to the Mobile Communications Division. At that time, I belonged to the department responsible for developing services in the era of car phones. However, I didn't know the elements of the technology, so I requested to be assigned to a research center to study the technology more thoroughly. I applied for a transfer and was allowed to conduct

research and development of wireless communications. However, when I was doing this, I wanted to know more about the entire business, so I applied again for another transfer. Thinking back now, I was probably being a bit out of line, but I am very grateful to my seniors who fulfilled my request.

Again, I think we are in the midst of changing the world through the use of ICT. The NTT Group is at the very center of that change, and I think this is very fortunate. NTT Group employees can take advantage of this opportunity. I believe that by working with enthusiasm and purpose, our achievements will surely be useful to the world.

*—What is the source of your enthusiasm?*

When I was in charge of developing handsets, I was very happy to actually see that what I had been working on was out in the world. I was delighted to see people pointing to a cell phone and saying, "It's cool!" or when I saw a cell phone actually being used. In my case, that feedback may be a source of my enthusiasm.

Moreover, I think that the work hard/play hard mentality, which is now called "work-life balance," is another source of my enthusiasm. On weekends and holidays, I get a good rest by doing some reading. Most of the books I read are novels because I think it is important to just let your mind go. It is good for people to do things they like to reset the body and mind and tackle things without worrying. Such actions will also be a source of energy.

What's more, a sense of mission may be a source of enthusiasm. An example is a story about recovery from a communication failure caused by Typhoon Faxai that hit Chiba Prefecture in September. Due to

a power outage, it was difficult to use mobile phones, or they could not be used at all over a wide area. Although the restoration took time and inconvenienced our customers, our employees from Chiba and all over the country worked together tirelessly to restore communication services. NTT Group's cohesion accompanies such unforeseen disasters, and the response is a spirit that has been handed down from generation to generation. That spirit comes from a sense of mission to provide infrastructure that is crucial to society. If an incident occurs, a system is in place to respond to it immediately. The president and other executives gather at the disaster-response headquarters, and all employees—not only the executives—are prepared to respond. I think this commitment is both NTT's DNA and a source of enthusiasm.

**Interviewee profile**

■ Career highlights

Seiji Maruyama joined NTT in 1985. In 2010, he became NTT DOCOMO General Manager of the Product Department; in 2016, he became Senior Vice President and General Manager of the Human Resources Management Department; and in 2018, he became Executive Vice President and General Manager of the Corporate Strategy & Planning Department, Responsible for Mobile Society Research Institute and Preparation for the 2020. He assumed his current position in June 2019.

# NTT Research, Inc. Launched to Strengthen and Globalize R&D

*Kazuhiro Gomi and Kei Karasawa*

**Abstract**

A plan to establish a new company, NTT Research, Inc., was announced in November 2018 as part of NTT Group's Your Value Partner 2025 medium-term management strategy. NTT Research will conduct basic research to lay the groundwork for new technologies with the aim of creating new business in five to ten years. The first three fields of basic research to be tackled—quantum physics, mathematical information theory, and medical informatics—form the basis of NTT's IOWN (Innovative Optical and Wireless Network) initiative announced in May 2019. NTT Research aims to *Upgrade Reality*—we intend to bring an even greater transformation (Upgrade) of the real world (Reality).

*Keywords: basic research, IOWN, Upgrade Reality*

## 1. NTT's global businesses

NTT is strengthening its global business competitiveness—one of the pillars of growth in the NTT Group's Your Value Partner 2025 medium-term management strategy (**Fig. 1**). As one source of competitiveness, it is fostering innovation through the establishment of three new companies.

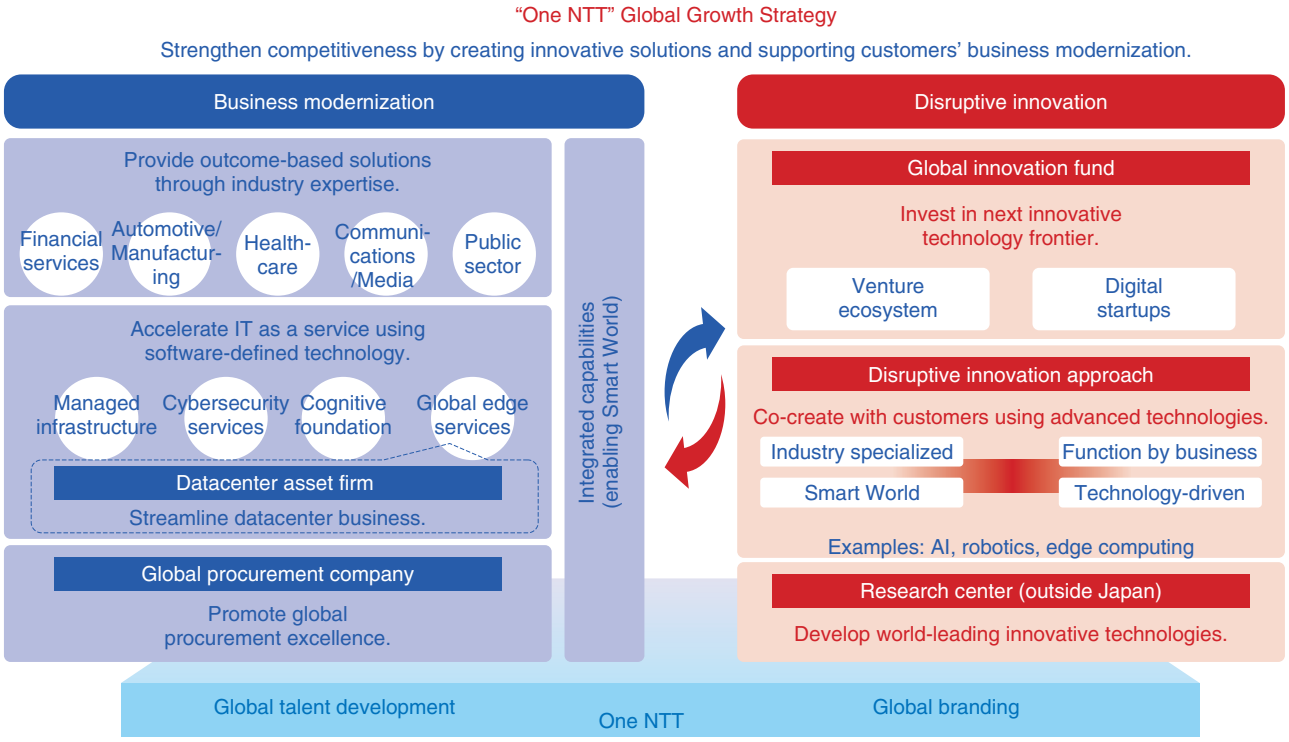
The first new company, NTT Disruption, aims to commercialize new technologies in a short timeframe of roughly one to three years through proof of concept and other development activities. The second new company, NTT Venture Capital, will invest in startups with the aim of bringing new technologies to market in about three to five years. The third new company is our company, NTT Research, Inc. Our mission is to conduct basic research to lay the groundwork for new technologies with the aim of creating new business in five to ten years.

The goal is to deploy new technologies globally by integrating these three companies with NTT Group's existing companies and research laboratories. The three companies are headquartered in the region in northern California known as Silicon Valley, an area of technical innovation. Establishing the companies there, a crucial nexus of people, money, and information, will help speed up the deployment of new technologies with our customers and partners. Another important reason for headquartering in Silicon Valley is that it offers a stimulating environment that attracts the best researchers engaging in basic research, precisely because of its nexus status.

## 2. Areas of research at NTT Research, Inc.

Our research areas at NTT Research were established through close collaboration with the NTT laboratories in Japan. By consistently supporting long-term research processes from fundamentals to applications across a wide range of research fields related to information and communication technologies, from optical communication devices to human psychology, NTT laboratories have produced a number of important results, some of which have been chosen as IEEE milestones.

NTT announced the IOWN (Innovative Optical and Wireless Network) initiative in May 2019 [1] to promote the development of technologies that further enhance humans beyond the boundaries of conventional communication services. To start with, NTT Research has established three laboratories focused on key research areas: quantum physics (the novelty of the IOWN initiative), mathematical information theory (which enables the secure use of various types of data, including personal information), and medical informatics (which deals with the basic biological data of humans). The respective labs are named as follows:




AI: artificial intelligence
IT: information technology

Fig. 1. Strengthening the competitiveness of NTT's global business.

(1) Physics & Informatics Laboratories (NTT PHI Labs)
(2) Cryptography & Information Security Laboratories (NTT CIS Labs)
(3) Medical & Health Informatics Laboratories (NTT MEI Labs)

These are the basic technological fields that NTT laboratories have cultivated in Japan for many years. However, our goal is to take these technologies in new directions by adding into the mix the best research outside Japan.

NTT PHI Labs will explore the interdisciplinary area between physics and informatics, focusing on basic physics research, particularly quantum-classical crossover physics and critical phenomena in neural networks. It will also pursue basic research to build new theories, which will include those that can be applied to information processing technologies. Its director is Yoshihisa Yamamoto, a professor emeritus of Japan's National Institute of Informatics and Stanford University. He is also program manager of Japan's ImPACT (Impulsing Paradigm Change through Disruptive Technologies) Program.

NTT CIS Labs will conduct basic research on cryptography and information security with the goal of building a safe and secure future. It will focus on theoretical topics such as cryptography in support of advanced functionality and security in decentralized environments that use technologies such as blockchain. The director is Tatsuaki Okamoto, an NTT fellow and one of the world's leading cryptography researchers.

NTT MEI Labs will work on the information processing technology that drives precision medicine, particularly focusing on data-driven medical technology for handling large multidimensional data sets of biological information, such as medical records and genomic information, as well as the electrical phenomena of the human body. The director is Hitonobu Tomoike, adviser to the Sakakibara Heart Institute, who has a track record of fruitful exchanges with world-class institutions.

NTT Research is taking advantage of the research networks and personal connections of these laboratory directors as we recruit new research teams to collaborate with NTT's Japanese researchers. We are

hiring the best external researchers from Japan and other countries in the areas that underlie the proprietary technologies developed by NTT laboratories. We want to introduce our customers and partners to the unique vision of the future that will inspire basic research at NTT Research. This showcases our value as a long-term business partner and highlights NTT Group's unique corporate assets, including our long-term vision and unparalleled depth of human resources. We hope that NTT Research along with these activities will contribute to the global development of the NTT Group businesses.

## 3. Future development

In the Feature Articles in this issue, the research lab directors explain the aims of their respective laboratories [2–4]. In addition, Brent Waters, a distinguished scientist in the area of basic cryptography theory, shares his thoughts on creating a new research lab [5].

NTT laboratories have a wide range of achievements, but globally, laboratories such as IBM and Samsung have achieved more results in terms of numbers of patents and papers. In addition, GAFA (Google, Amazon, Facebook, Apple) and other technology giants have invested in university laboratories to strengthen their research activities. In cooperation with NTT laboratories in Japan, NTT intends to further expand the advanced research network it has cultivated to universities and other organizations around the world. We will use our site in Silicon Valley as a base to build out a global research ecosystem starting from the basic research stage. Based on the digital society created by Xerox PARC and other pioneering research labs in Silicon Valley, we intend to bring an even greater transformation (Upgrade) of the real world (Reality). In short, NTT Research aims to *Upgrade Reality*.

## References


[1] NTT Technology Report for Smart World, https://www.ntt.co.jp/RD/e/techtrend/index.html

[2] Y. Yamamoto, "Mission of Physics & Informatics Laboratories," NTT Technical Review, Vol. 17, No. 12, pp. 9–16, 2019. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201912fa2.html

[3] T. Okamoto, B. Waters, and S. Matsuo, "Research of Cryptography & Information Security Laboratories," NTT Technical Review, Vol. 17, No. 12, pp. 17–20, 2019. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201912fa3.html

[4] H. Tomoike, "Launch of the Medical & Health Informatics Laboratories," NTT Technical Review, Vol. 17, No. 12, pp. 21–24, 2019. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201912fa4.html

[5] B. Waters, "Establishing a Cryptography Research Lab in 2019," NTT Technical Review, Vol. 17, No. 12, pp. 25–27, 2019. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201912fa5.html



**Kazuhiro Gomi**
President and CEO, NTT Research, Inc.


He joined NTT in 1985. Before taking up his current post in April 2019, he served as vice president (VP) of the Global Business Department of NTT Communications from 2001–2004, after which he served as VP of the Global IP Network Business Unit of NTT America (2004–2009), chief operating officer of NTT America (2009–2010), and president and chief executive officer of NTT America (2010–2019).


**Kei Karasawa**
Vice President of Strategy, NTT Research, Inc.


Kei Karasawa has been leading research and development (R&D) at NTT for more than 20 years. He is currently the vice president of strategy at NTT Research, Inc. From 2015–2019, he worked with the R&D planning department at NTT and built cooperative relationships with NTT operating companies around the world to deploy NTT R&D technology to global markets. He led applied R&D at NTT EAST from 2011–2015 and put the technology into practice in developing network services. Prior to that, he researched network software technologies, implemented patented software, such as security and distributed systems, and developed commercial services for the Next Generation Network. In 2005, he conducted basic research on cryptography and information processing as a visiting scholar, with Prof. Dan Boneh, in the Security Laboratory at Stanford University. He holds a doctorate of engineering in data-driven parallel computer technology. He has extensive knowledge and experience in information processing-related technologies from basic technology to applications.

# Mission of Physics & Informatics Laboratories

*Yoshihisa Yamamoto*

**Abstract**

At the Physics & Informatics Laboratories (PHI Labs) of NTT Research, Inc., we explore a new principle that will bring about a revolution in information processing technology in the interdisciplinary area between quantum physics and brain science, and it is here where we have positioned our research field. We will focus on quantum-classical crossover physics and critical phenomena in neural networks. We will concentrate, in particular, on optical implementation as a means of achieving a simple, elegant, and practical implementation of a computer that is based on this new principle, specifically on the optical parametric oscillator that can achieve quantum neural networks at room temperature. This article introduces the concepts, technologies, and target applications making up this research field at PHI Labs.

*Keywords: combinatorial optimization problem, quantum neural network, optical parametric oscillator*

## 1. Quantum neural networks using optical parametric oscillators

The development of new oscillators for generating coherent electromagnetic waves and the expansion of their application fields has a history marked by a rivalry between oscillators based on two different principles. In electrical engineering terms, one is a negative-resistance oscillator requiring no pump-source coherence, and the other is a nonlinear reactance oscillator requiring coherent pump waves. The development of oscillators for various frequency bands began with the emergence of negative-resistance oscillators that are easy to achieve. This was followed by the development of nonlinear reactance oscillators that generate a coherent wave with less noise.

The development of optical oscillators covering a broad wavelength band from ultraviolet to infrared is no exception to this historical rivalry. A laser, which is an optical negative-resistance oscillator, was developed in 1960 through the work of Theodore Maiman of Hughes Research Laboratories [1]. This was followed by the development of an optical nonlinear reactance oscillator as an optical parametric oscillator (in particular, an oscillator generating continuous waves for practical use) in 1968 by Stephen Harris and Robert Byer of Stanford University [2].

The foundation of optical communication technology, which blossomed in the 20th century, was the laser, but it is our future vision that the foundation of optical information processing technology of the 21st century will be the optical parametric oscillator. This type of parametric oscillator behaves like an analog device with strong quantum properties in the pump region below an oscillation threshold and like a digital device with strong classical properties in the pump region above the threshold. As described below, future information processing technology will require both quantum computing resources and classical computing resources, and the optical parametric oscillator is practically the only device that can simultaneously achieve this dual quantum-classical nature at room temperature.

We have been researching the neural networks using optical parametric oscillators as neurons and using such a configuration in an attempt to solve combinatorial optimization problems and quantum many-body problems that have posed a challenge to the modern computer [3] (**Fig. 1**). Regarding another element (synapse connections) making up a neural network, there are two methods of implementing a

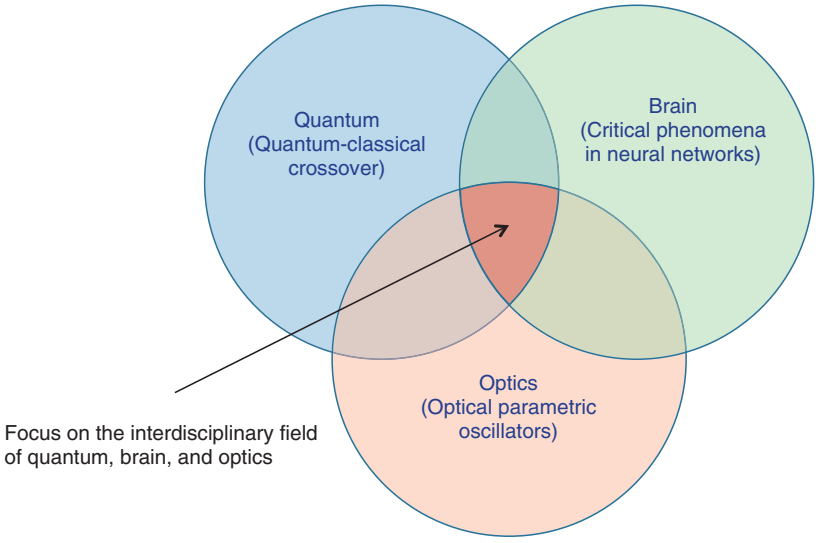
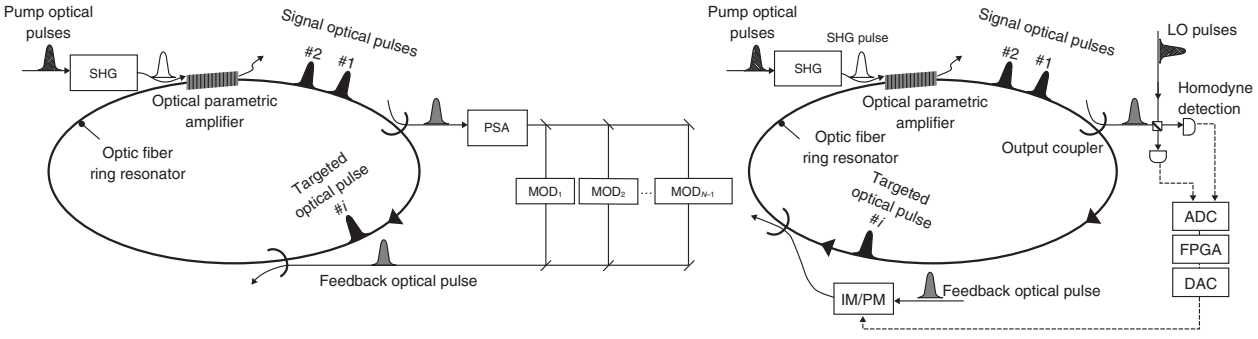



Fig. 1. Research fields at Physics & Informatics Laboratories (PHI Labs).




(a) Optical delay line coupling

(b) Measurement feedback coupling

ADC: analog-to-digital converter
DAC: digital-to-analog converter
FPGA: field-programmable gate array
IM/PM: intensity modulation/phase modulation
LO: local oscillator
MOD: optical modulator
PSA: phase sensitive amplifier
SHG: second harmonic generation

Fig. 2. Neural network configuration based on optical parametric oscillators.

fully connected neural network in which synapse connections are formed between all neurons (**Fig. 2**). These methods use $N$ optical parametric oscillator pulses circulating in an optical fiber ring cavity of 1 to 10 km for $N$ neurons instead of using $N$ optical parametric oscillators, a scheme that achieves $N$ defect-free uniform neurons simultaneously within a single cavity [4–6].

The optical delay line coupling method (Fig. 2(a)) can achieve $N$ ($N$–1) synapse coupling coefficients [$J_{ij}$] through ($N$–1) optical delay lines and the same number of optical modulators [4]. With this method, ($N$–1) input pulses $j$ simultaneously couple with a single target pulse $i$ at each time point via coupling coefficient $J_{ij}$, so $N$ ($N$–1) $J_{ij}$ coefficients are implemented for each round trip to achieve the above for all $N$ target pulses. This method has the advantage of simplifying the implementation of synapse coupling having directionality ($J_{ij} \neq J_{ji}$).

The measurement feedback coupling method

(Fig. 2(b)), on the other hand, can achieve $N$ ($N$–1) all-synapse coupling with just a single measurement feedback circuit [5, 6]. The former method is thought to be applicable to the implementation of large-scale, high-speed, and sparsely coupled neural networks and to quantum many-body problems. The latter method, however, is thought to be applicable to the implementation of medium-scale, high-order nonlinear coupling and densely coupled neural networks and to combinatorial optimization problems.

## 2. Application fields

This section introduces the application fields envisioned for quantum neural networks using optical parametric oscillators.

### 2.1 Combinatorial optimization problems

The Ising model is highly representative of combinatorial optimization problems. This model can be implemented through the use of degenerate optical parametric oscillators in which the signal wave and idler wave have identical frequencies [3]. As a result of recent improvements in hardware technology for achieving a degenerate optical parametric oscillator network together with the advancement in associated algorithms, the performance of the coherent Ising machine, a type of quantum neural network, is making significant gains. In fact, it is becoming superior to the quantum annealing machine—a type of quantum computer specialized for combinatorial optimization problems—and von Neumann computers implementing advanced algorithms such as Breakout Local Search [7, 8]. Expectations are high that the era of solving a variety of combinatorial optimization problems will eventually arrive by mapping them to the Ising model to achieve a general-purpose optimization solver. Application algorithms are now being developed for specific problems such as lead optimization in drug discovery and the development of optimum biocatalysts, resource allocation in wireless communication networks, scheduling and logistics, and sparse coding in compressed sensing.

The XY model, on the other hand, is highly representative of optimization problems involving continuous variables. A coherent XY machine for solving this type of problem can be implemented by a non-degenerate optical parametric oscillator network in which the signal and idler waves have different frequencies [9]. Application algorithms are being developed for specific optimization problems solvable using a coherent XY machine such as social network diagnosis (community detection) and portfolio optimization in the Fintech field.

Still another type of problem representative of combinatorial optimization problems is the satisfiability (SAT) problem. A coherent SAT solver that can solve this problem with good efficiency can be achieved by configuring a recurrent neural network with degenerate optical parametric oscillators [10]. One specific type of problem that could be solved by a coherent SAT solver is hardware/software verification.

The concept of quantum-inspired optimization has recently been attracting attention as a practical solver targeting combinatorial optimization problems. Instead of actually constructing an optical (or superconducting) parametric oscillator network, we apply this concept, which is aimed at obtaining optimal solutions by programming the quantum mechanical equations of motion that describe the experimental quantum neural network as an algorithm in a standard digital circuit such as a field-programmable gate array and conducting a type of numerical simulation [8, 11].

### 2.2 Quantum many-body problems

The development of new tools for achieving efficient numerical simulations with good accuracy of electron behavior within a solid, especially of correlated electron systems having strong interactions among electrons, is essential to searching for new materials (material informatics) and discovering new phenomena (topological physics). In particular, two-dimensional systems in which electrons are confined by two-dimensional potential forces exhibit novel quantum phenomena not found in ordinary three-dimensional systems. However, unlike three-dimensional systems, numerical simulations based on mean-field approximation tend to break down in two-dimensional systems, and it is also difficult to obtain exact solutions in two-dimensional systems as in one-dimensional systems.

This state of affairs led to the idea that the properties of a two-dimensional electron system could be understood by artificially implementing its electrons in a separate quantum system whose Hamiltonian could be easily controlled, then observing the behavior of this artificial two-dimensional quantum system. This is the concept of quantum simulation [12]. There has been much research on simulating electron properties in solids using a variety of physical systems such as cold atoms, trapped ions, and superconducting circuits.

The development of such a quantum simulator is

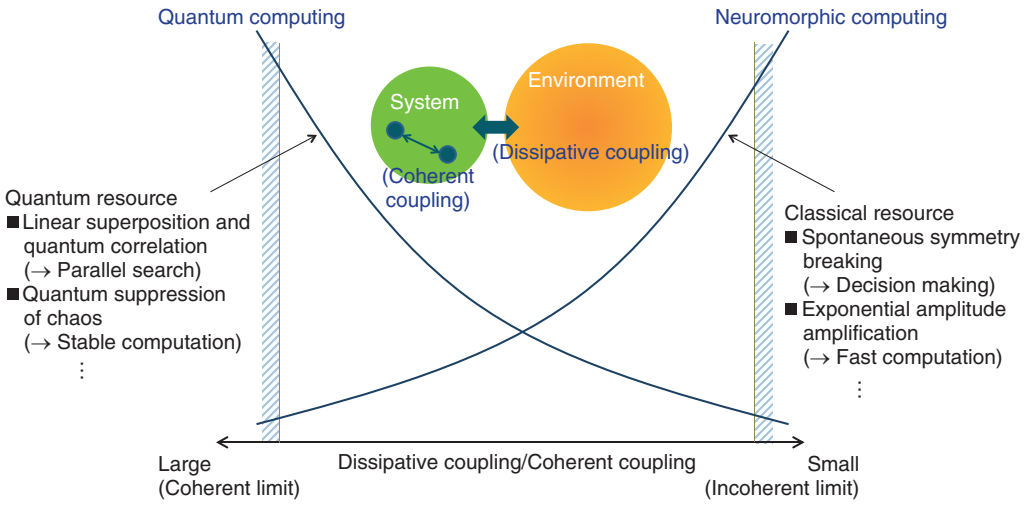



Fig. 3. Computing with quantum and classical resources.

still at the stage of basic research. In the future, however, we expect it to become competitive with traditional approaches in condensed matter physics and quantum chemistry that implement a variety of approximate numerical calculation techniques (such as dynamic or cluster mean-field theory, quantum Monte Carlo methods, and tensor network methods) as algorithms in high performance computing equipment. Diverse factors, such as simulation accuracy, speed, equipment size, cost, and ease of maintenance, will determine what approach survives as future technology.

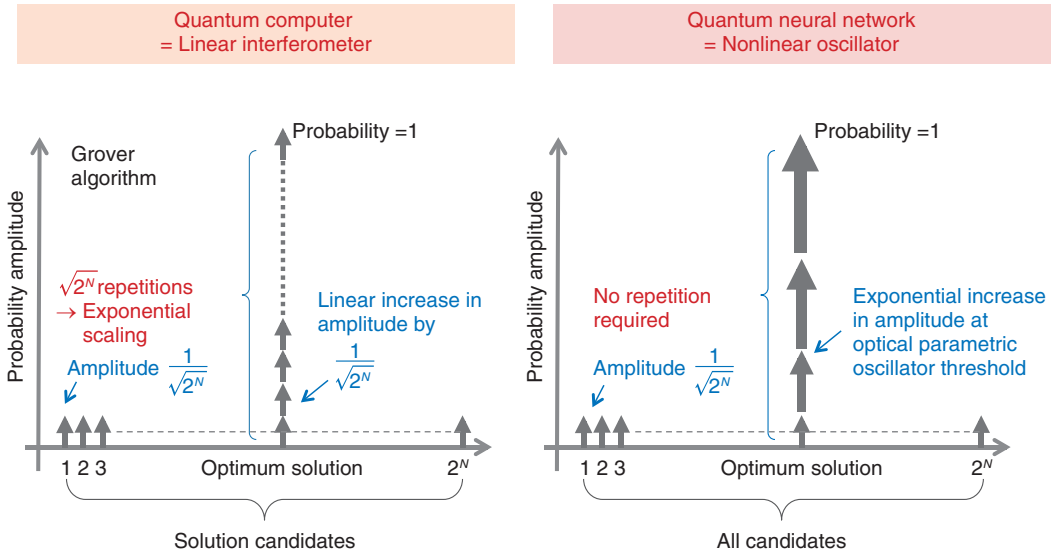
We consider equipment that uses light to simulate electrons to be the future vision of a quantum simulator that can achieve a competitive edge over traditional techniques [13].

## 3. Quantum-classical crossover physics

The quantum-classical crossover problem refers to the question of when and how quantum theory, which has been successful in describing the microscopic world, crosses over into classical theory, which rules over the macroscopic world. This question is the most fundamental theme for quantum physicists. One theoretical model that can make this problem easy to understand is an open system in which a system having a few degrees of freedom couples with an environment having many (or infinite) degrees of freedom [14]. As shown in **Fig. 3**, as dissipative coupling between the system and environment (decoherence) becomes smaller compared with the strength of coherent coupling within the system, quantum computing resources become more effective, such as quantum parallel search using linear superposition and quantum suppression of classical chaos using quantum interference. For this reason, it has been thought up to now that a quantum computer should be developed in a region that makes dissipative coupling with the environment as small as possible. Concepts such as quantum error correcting codes and topological quantum computers have emerged along this line of thinking.

As dissipative coupling with the environment becomes larger, however, there is an increase in the effectiveness of classical computing resources, such as irreversible decision making of a final solution by spontaneous symmetry breaking and exponential amplification of the amplitude of the selected final solution, as stable classical information. It has therefore been thought that a neuromorphic computer that mimics the function and mechanism of human nerve cells or acquires ideas based on human ways of thinking should be developed in a robust classical region that would make dissipative coupling with the environment as large as possible and completely remove quantum coherence in the system.

We consider that the computer of the future should be developed specifically in this quantum-classical crossover region in which the two types of computing resources—quantum and classical—can be used simultaneously. An optical parametric oscillator network is a unique hardware solution that can freely move about this quantum-classical crossover region




(a) Linear amplitude amplification in quantum computers

(b) Exponential amplitude amplification in quantum neural networks

Fig. 4. Two computational methods for combinatorial optimization problems.

by adjusting the pump rate. This approach has something in common with recent thinking by neuroscientists known as "computing at criticality" in which advanced functions of the human brain (consciousness, cognition, and decision-making) are based on types of phase transitions and critical phenomena in a massive neural network [15].

## 4. Why are classical computing resources also necessary?

A method for solving combinatorial optimization problems using only quantum computing resources is shown in **Fig. 4(a)**. This method first expresses all $(2^N)$ candidates of the solution of a given problem as linear superposition states, each having the same probability amplitude $(1/\sqrt{2^N})$. Then, after identifying the optimal solution by some methods such as the phase estimation algorithm, it amplifies the amplitude of that particular state from $1/\sqrt{2^N}$ to 1 and attenuates the amplitudes of all other states from $1/\sqrt{2^N}$ to 0. Finally, by conducting projective measurements of 0 or 1 against $N$ quantum bits, it determines an optimal solution with a probability close to 100%. The bottleneck with this method lies in how to amplify the amplitude of the optimal solution and how to attenuate the amplitudes of all other states that are not an optimal solution.

An optimal method for achieving this goal using a quantum computer was discovered by L. K. Grover [16]. Repeating this routine called Grover iteration a total of $\sqrt{2^N}$ times obtains the above final state. This means that exponential time must be spent in solving a combinatorial optimization problem using a quantum computer. The theoretical limits of the computational time needed to complete this Grover iteration for problem sizes of $N = 20$, 50, 100, and 150 bits are $4 \times 10^{-3}$ s, $6 \times 10^{2}$ s, $2 \times 10^{10}$ s, and $6 \times 10^{17}$ s. It is assumed that there is no decoherence and no gate error, and consequently no need for using quantum error correcting codes, and that fully connected bits are implemented so that non-localized two-bit gates can be freely implemented at a high speed of 1 ns. It is also assumed that the optimal solution to a given problem can be identified instantaneously by a new and independent algorithm, which is yet to be discovered. Yet, even with such an idealized quantum computer, the above result shows that it would take about 20 billion years to amplify the probability amplitude of the optimal solution from $1/\sqrt{2^N}$ to 1 for an extremely small problem of $N = 150$ bits.

What would be the computational time for solving the same type of problem with a coherent Ising machine? As shown in **Fig. 4(b)**, since $N$ optical parametric oscillator pulses below the oscillation threshold are in 0-phase and $\pi$-phase linear superposition

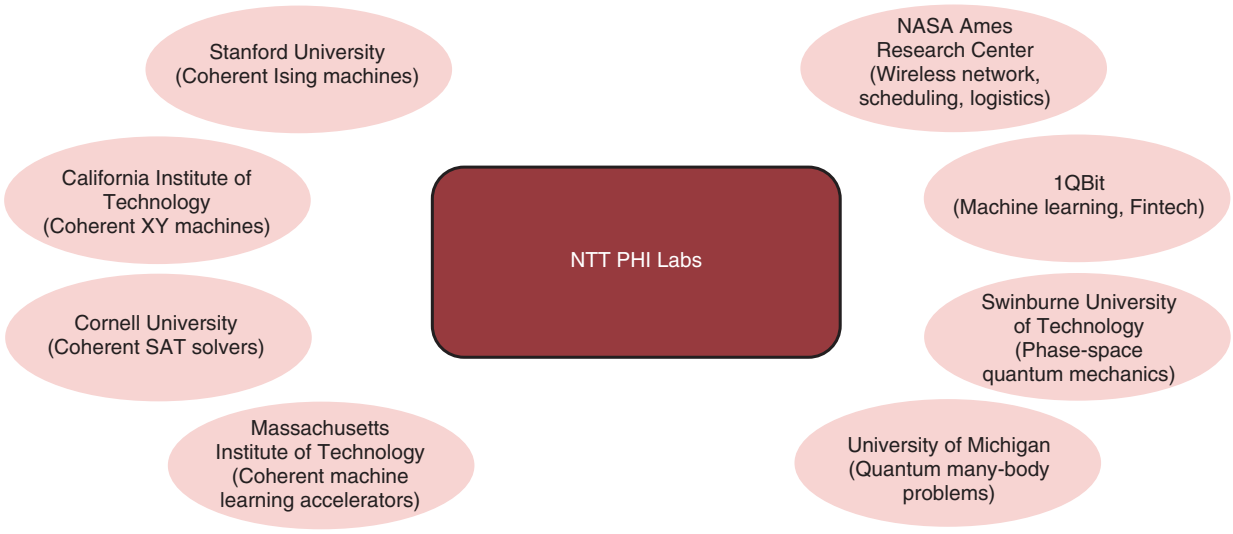



Fig. 5. PHI Labs and its partners.

states, all solution candidates can be expressed as linear superposition states, each having the same probability amplitudes ($1/\sqrt{2^N}$) in the same manner as the quantum computer. At this time, if the pump rate is increased to the oscillation threshold, the optimal solution having minimum network loss gives rise to single-mode oscillation, and that amplitude is exponentially amplified from its initial value ($1/\sqrt{2^N}$) to its final value (1) in a time comparable to a photon lifetime (on the order of μs–ms) at most [3]. This exponential amplification is a characteristic phenomenon in a classical (open) system that cannot be achieved in a quantum system. The computational times (experimental results) for obtaining optimal solutions to the same combinatorial optimization problem (Ising model) with a coherent Ising machine are 1.0 x $10^{-4}$ s, 3.7 x $10^{-4}$ s, 2.5 x $10^{-3}$ s, and 5.4 x $10^{-2}$ s [7].

With the exception of special problems having hidden periodicity (factorization, discrete logarithm, etc.), this example shows that classical computing resources, such as exponential amplitude amplification, will be essential to future computers for solving general combinatorial optimization problems at high speed in addition to quantum computing resources in the manner of linear superposition.

We emphasize that a quantum computing based on Grover iteration is an exact solver while a coherent Ising machine is a heuristic solver, for which the theoretical upper bound of computation time is not established for coherent Ising machines yet.

## 5. Research partners

The development of quantum neural networks using optical parametric oscillators targeting combinatorial optimization problems and quantum many-body problems is moving forward at NTT. PHI Labs is actively promoting joint research with outside research institutions to fulfill its responsibility of searching out new concepts and principles (**Fig. 5**).

The left side of the research partner diagram in Fig. 5 consists mainly of the experimental group. The Stanford University team (Professor Hideo Mabuchi, Professor Martin Fejer, Associate Professor Benjamin Lev, Associate Professor Surya Ganguli, Assistant Professor Amir Safavi-Naeini) is researching coherent Ising machines based on optical or superconducting parametric oscillator networks and critical phenomena in neural networks. The Cornell University team (Assistant Professor Peter McMahon) is researching coherent SAT solvers based on recurrent optical parametric oscillator networks. The California Institute of Technology team (Assistant Professor Alireza Marandi) is researching coherent XY machines based on non-degenerate optical parametric oscillator networks. The Massachusetts Institute of Technology team (Associate Professor Dirk Englund, Professor William Oliver) is researching

Table 1. Two quantum computational models.

| | Unitary quantum computation (Quantum computing) | Dissipative quantum computation (Quantum neural network) |
|---|---|---|
| Principles | Unitary rotation of state vectors in isolated quantum systems | Self-organization in open quantum systems |
| Proposals | Deutsch (1985): Quantum parallelism<br>Shor (1994): Factoring and discrete logarithm | Zurek (2003): Quantum Darwinism, Quantum chaos<br>Verstraete, Wolf and Cirac (2009): Universal quantum computation by dissipation |
| Resource | Quantum entanglement | Quantum discord |
| Merits | Transparent physics<br>Established theoretical limit | Robust against noise and gate error |
| Demerits | Sensitive to noise and gate error | Complicated physics<br>Theoretical limit unknown |
| Applications | Problems with hidden periods or structures | Problems without hidden periods or structures |

coherent accelerators (targeting deep machine learning) based on optical homodyne mixers and also fabrication of superconducting parametric oscillator networks.

The right side of the research partner diagram in Fig. 5 consists of the theoretical group. The NASA Ames Research Center team (Quantum Artificial Intelligence Laboratory: QuAIL Lead Eleanor Rieffel) is researching application algorithms for wireless networks, scheduling, logistics, and other areas. The 1QBit team (Group Head Pooya Ronagh) is researching application algorithms for machine learning. The Swinburne University of Technology team (Professor Peter Drummond, Professor Margaret Reid) is researching quantum stochastic differential equations by using the phase-space method. The University of Michigan team (Professor Franco Nori) is researching quantum simulations of non-Abelian anyon particles and topological physics.

Finally, **Table 1** summarizes the differences between conventional quantum computers and new quantum neural networks that we are researching.

## 6. Conclusion

The first AT&T-NTT executive meeting took place more than 30 years ago, and meetings were subsequently held annually at an AT&T or NTT research laboratory. At that time, I was one of the members from the NTT laboratories then headed by NTT senior executive vice president Yasusada Kitahara and remember well my visit to Bell Labs in New Jersey. The president of Bell Labs (to whom I was introduced) was British, the vice president in charge of research was German, and the executive director overseeing the physics department was Indian. The director of theoretical physics (commonly known as Physics 001) was American, and it was he who gave the keynote talk at this first AT&T-NTT executive meeting. I cannot forget the reprimand that he received at that time from Dr. Arno Penzias, the vice president of research (and recipient of the 1978 Nobel Prize in Physics), who said "If you speak that fast, you will lose half of your audience in the room!" My dream was to one day make the NTT laboratories into a place with such diversity and caliber—we stood at the starting line of that endeavor.

## References


[1] T. H. Maiman, "Stimulated Optical Radiation in Ruby," Nature, Vol. 187, pp. 493–494, Aug. 1960.

[2] R. L. Byer, M. K. Oshman, J. F. Young, and S. E. Harris, "Visible CW Parametric Oscillator," Appl. Phys. Lett., Vol. 13, No. 3, p. 109, Aug. 1968.

[3] Z. Wang, A. Marandi, K. Wen, R. L. Byer, and Y. Yamamoto, "Coherent Ising Machine Based on Degenerate Optical Parametric Oscillators," Phys. Rev. A, Vol. 88, No. 6, 063853, Dec. 2013.

[4] A. Marandi, Z. Wang, K. Takata, R. L. Byer, and Y. Yamamoto, "Network of Time-multiplexed Optical Parametric Oscillators as a Coherent Ising Machine," Nat. Photon., Vol. 8, pp. 937–942, Oct. 2014.

[5] T. Inagaki, Y. Haribara, K. Igarashi, T. Sonobe, S. Tamate, T. Honjo, A. Marandi, P. L. McMahon, T. Umeki, K. Enbutsu, O. Tadanaga, H. Takenouchi, K. Aihara, K. Kawarabayashi, K. Inoue, S. Utsunomiya, and H. Takesue, "A Coherent Ising Machine for 2000-node Optimization Problems," Science, Vol. 354, No. 6312, pp. 603–606, Nov. 2016.

[6] P. L. McMahon, A. Marandi, Y. Haribara, R. Hamerly, C. Langrock, S. Tamate, T. Inagaki, H. Takesue, S. Utsunomiya, K. Aihara, R. L. Byer, M. M. Fejer, H. Mabuchi, and Y. Yamamoto, "A Fully Programmable 100-spin Coherent Ising Machine with All-to-all Connections," Science, Vol. 354, No. 6312, pp. 614–617, Nov. 2016.

[7] R. Hamerly, T. Inagaki, P. L. McMahon, D. Venturelli, A. Marandi, T. Onodera, E. Ng, C. Langrock, K. Inaba, T. Honjo, K. Enbutsu, T. Umeki, R. Kasahara, S. Utsunomiya, S. Kako, K. Kawarabayashi, R. L. Byer, M. M. Fejer, H. Mabuchi, D. Englund, E. Rieffel, H. Takesue, and Y. Yamamoto, "Experimental Investigation of Performance Differences between Coherent Ising Machines and a Quantum Annealer," Sci. Adv., Vol. 5, No. 5, eaau0823, May 2019.
[8] T. Leleu, Y. Yamamoto, P. L. McMahon, and K. Aihara, "Destabilization of Local Minima in Analog Spin Systems by Correction of Amplitude Heterogeneity," Phys. Rev. Lett., Vol. 122, No. 4, 040607, Feb. 2019.
[9] Y. Takeda, S. Tamate, Y. Yamamoto, H. Takesue, T. Inagaki, and S. Utsunomiya, "Boltzmann Sampling for an XY Model Using a Non-degenerate Optical Parametric Oscillator Network," Quantum Sci. Technol., Vol. 3, No. 1, 014004, Nov. 2017.
[10] M. Ercsey-Ravasz and Z. Toroczkai, "Optimization Hardness as Transient Chaos in an Analog Approach to Constraint Satisfaction," Nat. Phys., Vol. 7, pp. 966–970, Oct. 2011.
[11] H. Goto, K. Tatsumura, and A. R. Dixon, "Combinatorial Optimization by Simulating Adiabatic Bifurcations in Nonlinear Hamiltonian Systems," Sci. Adv., Vol. 5, eaav2372, Apr. 2019.
[12] R. P. Feynman, "Simulating Physics with Computers," Int. J. Theoretical Physics, Vol. 21, Nos. 6/7, pp. 467–488, June 1982.
[13] M. D. Fraser, S. Höfling, and Y. Yamamoto, "Physics and Applications of Exciton–Polariton Lasers," Nat. Mater., Vol. 15, pp. 1049–1052, Sept. 2016.
[14] W. H. Zurek, "Decoherence, Einselection, and the Quantum Origins of the Classical," Rev. Mod. Phys., Vol. 75, No. 3, pp. 715–775, July 2003.
[15] J. Beggs, "Editorial: Can There Be a Physics of the Brain?", Phys. Rev. Lett., Vol. 114, No. 22, 220001, June 2015.
[16] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," Proc. of 28th Annual ACM Symposium on the Theory of Computing," pp. 212–219, Philadelphia, PA, USA, May 1996.

**Yoshihisa Yamamoto**
Director, Physics & Informatics Laboratories, NTT Research, Inc.

He received a Ph.D. from the University of Tokyo in 1978 and joined NTT Basic Research Laboratories. He became a Professor of Applied Physics and Electrical Engineering at Stanford University in 1992. He also became a Professor at the National Institute of Informatics (NII) in 2003. He is currently a Professor (emeritus) at Stanford University and NII, and an NTT R&D Fellow. He received many distinctions for his work, including the Carl Zeiss Research Award (1992), Nishina Memorial Prize (1992), IEEE/LEOS Quantum Electronics Award (2000), Medal with Purple Ribbon (2005), Hermann A. Haus Lecturer of MIT (2010), and Okawa Prize (2011). His research focuses on quantum information processing, quantum optics, and mesoscopic physics, especially quantum neural networks and coherent Ising machines.

# Research of Cryptography & Information Security Laboratories

*Tatsuaki Okamoto, Brent Waters, and Shin'ichiro Matsuo*

**Abstract**

One of the three laboratories of NTT Research, Inc. launched in July 2019 in Silicon Valley, USA, is Cryptography & Information Security Laboratories (CIS Labs). CIS Labs (Director: Tatsuaki Okamoto) is engaged in basic research on cryptography and has two research groups, Cryptography, and Blockchain (Head: Shin'ichiro Matsuo). The Cryptography group also includes Waters Laboratory (Head: Brent Waters), which focuses on deep and foundational research of cryptography. In this article, we describe the research targets and themes of CIS Labs.

*Keywords: cryptography, information security, basic research laboratories*

## 1. Introduction

In this article, we introduce Cryptography & Information Security Laboratories (CIS Labs), which is one of the three laboratories of NTT Research, Inc. launched in July 2019 in Silicon Valley, USA. CIS Labs is engaged in basic research of cryptography with the potential for having a long-term impact and has two research groups, Cryptography and Blockchain. The Cryptography group also includes the Waters Laboratory headed by Brent Waters, which focuses on deep and foundational research of cryptography. We discuss the research targets and themes of CIS Labs, mainly those of Waters Lab and the Blockchain group.

## 2. Research of Cryptography group, specifically Waters Lab

Waters Lab focuses on many areas of cryptography ranging from achieving new functionality that goes beyond what cryptographic primitives were previously achievable to achieving a better and deeper understanding of the foundations of cryptography. One initial focus area is on encryption systems. Encryption is the process of encoding data into a ciphertext such that only the intended recipient can decode and learn the data. Encryption systems are a cornerstone of our security ecosystem. They are used to encrypt sensitive web traffic, protect information on devices (e.g., laptops, phones) that could be physically stolen, as well as hide sensitive data stored on third-party cloud servers. Encryption can often end up at the forefront of news or public debates, as in the case of the 2015 San Bernardino shooting and the debate over whether Apple should be compelled to decrypt the culprit's iPhone.

Traditionally, we have had an inert view of encryption where a user publishes a public key and keeps the corresponding secret key private. One can encrypt a data message using a public key to create a ciphertext. The data message can be decrypted by any holder of the secret key, but an attacker without this will learn nothing about the data.

Over time, we have discovered that this view of encryption may be too rigid for many applications. For example, suppose Alice's email server receives and stores emails encrypted under her public key. In addition to storing emails, she would like it to automatically discard spam (something current servers do on unencrypted emails) as well as send her a text alert if any email message with her child's name and the word "emergency" or "hospital" appears in it. To enable this functionality, she could hand over her secret key to the server, but this would allow a third party to read all her email messages; however, if Alice

holds it back then she cannot benefit from spam detection or emergency alerts. This is just one example of where we need to push beyond the confines of our traditional notions of encryption to obtain a desired result.

The research community has long recognized that doing this is important and there are various concepts of cryptosystems (some proposed by the PIs) that do this including: functional encryption, fully homomorphic encryption, identity-based encryption, attribute-based encryption, traitor tracing, and proxy re-encryption among others.

Our group's research will push the frontiers of what is achievable in this regime. We will focus on building encryption systems with advanced capabilities that have provable security under standard assumptions. We begin by focusing on three sub-areas.

### 2.1 Chosen ciphertext security

The chosen ciphertext security (indistinguishability under chosen-ciphertext attack: IND-CCA) is arguably the right notion of security both for traditional encryption systems as well as those with advanced functionality. However, most new results that push the envelope of functionality prove security in the indistinguishability against chosen plain-text attack (IND-CPA) model. We recently showed how to generically black-box convert any attribute-based encryption system that is IND-CPA secure into an IND-CCA one using a new tool called hinting pseudorandom generators (PRGs). We will build faster and smaller hinting PRGs from number theory and go beyond attribute-based encryption and discover CCA transformations for functional encryption and re-randomizable encryption. Finally, we will approach the classic problem of proving that IND-CPA implies IND-CCA with new ideas.

### 2.2 Tracing in encryption systems

Traitor tracing is the problem of determining the source of a decoder box in a broadcast system. We recently showed how to build *collusion-resistant* tracing systems with ciphertexts that scale in size with $lg(N)$ for $N$ users from the learning with errors (LWE) assumption. The previous best results from standard assumptions achieved $N^{1/2}$-sized ciphertexts. We explore challenging new problems including: obtaining trace and broadcast systems with $N^{1/c}$-sized ciphertexts for any constant $c$, achieving public traceability for the same parameters, and using tracing techniques for proving adaptive security.

### 2.3 New frontiers in LWE-based encryption

The LWE assumption is a well-regarded tool in cryptography due to its apparent resistance to quantum attacks as well as connections to worst case lattice problems. It has also turned into an exciting avenue for producing new functionality in cryptography from a well-studied assumption. Recent examples of primitives include fully homomorphic encryption, attribute-based encryption for circuits, and lockable obfuscation. None are currently realizable from any other standard number theoretic assumptions. We propose ambitious goals for building LWE-based cryptography. We first discuss a new concept of obfuscating pseudorandom functions (PRFs) and its applications. We then describe a program for constructing witness encryption from LWE beginning with an intermediate goal of building constrained PRFs for the bit-fixing functionality.

Our research lab is off to a good start in this area. Waters and Wichs (with co-authors) have a paper in CRYPTO 2019, the top conference in cryptography, that shows how to combine bilinear map broadcast encryption techniques from traitor tracing ideas from LWE to achieve trace and broadcast functionality with $N^{1/c}$-sized ciphertexts. Currently, Waters, Wichs, and Zhandry are collaborating to explore new techniques and limitations on achieving adaptive security for LWE-based attribute-based encryption systems.

## 3. Research of Blockchain group

After Satoshi Nakamoto published a paper on Bitcoin in 2009, blockchain technology gained a great deal of attention as a new data trust model based on cryptography, peer-to-peer (P2P) networks, game theory, economics, and other academic areas. Bitcoin is a mechanism to periodically revise a common ledger that records payment history by users who are parts of a P2P network without the existence of a trusted third party (TTP). It applies this technology to payment among users by treating the history of a record as money. Thus, Bitcoin is a system specialized as a payment application. However, the idea of updating a common ledger by users connected by a P2P network without TTP applies to a broader area than payment. Therefore, extensive research and development are being globally conducted on blockchain, the core protocol of Bitcoin, as a fundamental technology.

The most crucial keyword to understand the real impact of blockchain is *permissionless innovation*. The Internet enables multi-lateral and global

communication without a central party, providing everyone a chance to be a creator of innovation. Similarly, blockchain enables multi-lateral and global maintenance of *programmable* ledger(s) by multi-stakeholders without any permission; therefore, anyone can freely create new applications and innovations based on a shared ledger. It is not easy to answer the frequently asked question, "What is an excellent application of blockchain?" as in the case of the similar question, "What is an excellent application of the Internet?" There is currently no right answer to this question, but the real value of blockchain is that it creates a place for experiments where anyone can try to create new applications based on a programmable ledger.

In this sense, the main goal of research and development on blockchain technology is creating a situation such that anyone can freely develop an application based on a shared and programmable ledger. We might think that blockchain is *ready* technology from news on such technology; however, achieving the above goal is a considerable challenge and requires long-term fundamental and theoretical research and development.

Building blocks of blockchain technology have been confirmed and are not new. ECDSA (Elliptic Curve Digital Signature Algorithm), a digital signature algorithm used in Bitcoin and SHA-2, a cryptographic hash function, are standard cryptographic techniques with a long history. Digital time-stamping, which certifies the order of the existence of digital data by linking hash values, was proposed at CRYPTO in 1990. Sharing digital data by a large number of people via a P2P network is not new technology. There is a long history in the research of distributed computing on achieving a consensus of data by multiple networked computers. In Bitcoin, a proof of work technique is used as a secure consensus protocol, but this was invented as an example of the cryptographic puzzle to reduce spam email then established as a part of HashCash, which is hash-function-based digital money.

The real breakthrough of Bitcoin and blockchain is the capability to combine such well-confirmed technologies to develop a method of updating a ledger with certain business logic (e.g., payment) without a trusted server. Such a mechanism did not exist before Bitcoin. To make such a P2P network sustainable, Bitcoin implements an incentive mechanism that gives rewards (e.g., Bitcoins) to network participants who contribute to maintaining the network.

The security of blockchain relies not only on cryptography and network theory but also on a good incentive design. There are many trade-offs between its security and scalability. If we try to scale the blockchain technology naturally, its security degrades. Such trade-offs have not yet been theoretically clarified. Thus, we need to develop theories and conduct experiments to clarify the relationships and make blockchain technology usable to general users with satisfactory performance. This is a fundamental and long-term research issue.

Another fundamental issue of blockchain is scalability. The current Bitcoin network can process seven transactions per second worldwide. It is quite difficult to increase the number of transactions without compromising security. Top-level researchers are conducting extensive research on this issue.

The Blockchain group at CIS Labs focuses on fundamental research to achieve the goal described above. Specifically, it focuses on secure and scalable distributed consensus algorithms, a secure programming environment for the programmable ledger, and privacy protection for data processing over blockchain.

As mentioned above, theoretical research on blockchain technology is composed of different areas. Therefore, we need to form a team of top-level researchers with diverse backgrounds. Experts on cryptographic protocols, software engineering, formal verification, game theory, and economics are encouraged to join this group. Because blockchain research is in its very early stage, it is essential to gather young researchers such as post-docs and assistant professors from whom we can expect top-level research results.

Moreover, as regulators are concerned about Facebook's Libra, harmonization with future regulations is essential for making blockchain a social foundation. This harmonization should be considered by design, and we are planning joint research with a leading university in the United States on this topic.

## Trademark notes

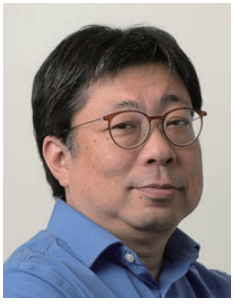
**Tatsuaki Okamoto**
Director, Cryptography & Information Security Laboratories, NTT Research, Inc.

He received a B.E., M.E., and Ph.D. from the University of Tokyo in 1976, 1978, and 1988. He has been working for NTT since 1978, and is an NTT Fellow. He is presently a Director of NTT Research in USA since 2019 and engaged in research on cryptography and information security. Dr. Okamoto served as President of the Japan Society for Industrial and Applied Mathematics (JSIAM), Director of International Association of Cryptology Research (IACR), and a program chair of many international conferences. Dr. Okamoto received the best and life-time achievement awards from the Institute of Electronics, Information and Communication Engineers (IEICE), the distinguished lecturer award from the IACR, the Purple Ribbon Award from the Japanese government, the RSA Conference Award, and the Asahi Prize.

**Brent Waters**
Distinguished Scientist, Cryptography & Information Security Laboratories, NTT Research, Inc.

Dr. Brent Waters received his Ph.D. in computer science from Princeton University, NJ, USA, in 2004. From 2004–2005, he was a postdoctoral researcher at Stanford University, CA, USA, then worked at SRI International as a computer scientist. In 2008 he joined the faculty at The University of Texas at Austin. In 2019 he joined NTT Research as a distinguished scientist. Dr. Waters' research interests are in the areas of cryptography computer security. His work has focused on identity-based cryptography, functional encryption, and code obfuscation. He is noted as a founder of functional encryption and attribute-based encryption.

Dr. Waters is a recipient of the National Science Foundation CAREER award, the Presidential Early Career Award for Scientists and Engineers (PECASE), and the 2015 ACM (Association for Computing Machinery) Grace Murray Hopper award. He has been a Microsoft Faculty Fellow, Sloan Research Fellow, a Packard Science and Engineering Fellow, and a Simons Investigator.



**Shin'ichiro Matsuo**
Head of Blockchain group, Cryptography & Information Security Laboratories, NTT Research, Inc.

He is the head of blockchain research at NTT Research. He is also a research professor at Georgetown University, Washington, D.C., USA, and works as a director and blockchain research lead of CyberSMART research center at Georgetown University. He has been engaged in research on cryptography and cryptographic protocols over 23 years. He was a program chair of Scaling Bitcoin workshop 2019 and program committee member of many blockchain related academic conferences such as IEEE S&B, CBT, Stanford Blockchain Conference and Crypto Economics and Security Conference. He is also a co-founder of BSafe.network, which is the global and neutral academic research testbed dedicated to blockchain research.

# Launch of the Medical & Health Informatics Laboratories

*Hitonobu Tomoike*

**Abstract**

NTT Research, Inc. has launched the Medical & Health Informatics Laboratories (MEI Labs) as a basic research institute for information technology in the medical and healthcare fields. This article gives a summary of environmental changes in clinical research in Japan and the prospects for MEI Labs in the globalization of medical and health informatics research.

*Keywords: precision medicine, regulatory science, data science*

## 1. Targets of biological information research

On November 28, 2018, NTT announced the establishment of three new research facilities responsible for basic research into next-generation technologies. Our stated policy is to focus on techniques such as artificial intelligence (AI) for analyzing biological information for precision medicine. The Medical & Health Informatics Laboratories (MEI Labs) was then launched on July 1, 2019.

The history of bioinformatics research dates back to the establishment of the Japan ME Society (currently, Japanese Society for Medical and Biological Engineering) in 1962. An increasingly broad range of biological information has recently become available due to the increased use of information and communication technology (ICT) in medicine. The fact that the scientific discipline known as *Translational Medicine* was renamed *Translational Bioinformatics* after just a few years is a testament to advancements in this field [1]. The explanation offered by the American Medical Informatics Association (AMIA) regarding what constitutes Translational Bioinformatics is perhaps the most canonical definition: "… *the development of storage, analytic, and interpretive methods to optimize the transformation of increasingly voluminous biomedical data and genomic data, into proactive, predictive, preventative, and participatory health. Translational bioinformatics includes research on the development of novel techniques for the integration of biological and clinical data and the evolution of clinical informatics methodology to encompass biological observations*."

There has been extensive research in this field, and the desired outcomes from such research are also being clarified. It could be argued that this definition is similar to that of *Smart World* advocated by NTT [2]. Therefore, the range of biological information that MEI Labs focuses on includes not only biological phenomena but also medical records, genome data, and information processing technology.

## 2. Approaches of bioinformatics in medicine and healthcare

Medical research has been conducted in three different areas: laboratory (experimental) studies, clinical research (non-invasive/invasive, observation/intervention), and epidemiological studies. Bioinformatics and recently advanced data science play key roles in these three areas as analysis tools. Apart from the MEI Labs, there are perhaps no other research institutes conceptualized as a center for basic research in information technology across multiple research fields.

### 2.1 Characteristics of data in medicine and healthcare

The diagnosis, treatment, and prevention of medical conditions are documented in medical records.

Since Japan provides universal health insurance, medical records can be regarded as official records. The use of this information for research and development has been prohibited since it was not intended to be used in this manner. Before collecting and using information in clinical research, researchers must obtain patients' written consent after they have been given a full explanation of how this information will be used. Researchers must also ensure that their research will be carried out honestly while complying with the obligation to correctly manage the collected information. Although health monitoring information can be provided through apps running on smartphones and other mobile devices, the collection and use of this information in research is governed by personal data protection rules and must therefore be handled with similar procedures as in clinical studies. When MEI Labs conducts basic clinical research, it will comply with the personal data protection laws of each country. In the United States, it is necessary to abide by the conditions of the Health Insurance Portability and Accountability Act (HIPAA), and in Europe, by the conditions of the General Data Protection Regulation (GDPR), which was revised and enforced on May 25, 2018.

The importance of innovation in medical and healthcare has also recently been emphasized. The patent application and associated intellectual property, which are regarded as important in business and industry, are also the primary responsibility of biological researchers. Carefully following procedures is necessary when dealing with intellectual property in matters such as device development and the discovery of new biological functions. Therefore, the broad understanding of norms and regulations regarding basic research at MEI Labs is necessary in planning and managing clinical or population research.

Regarding clinical data usage in Japan, we can see the steps in how the concept of personal information protection has been established in various directions. Discussions on how to go about digitizing medical and healthcare information began in 2001 by the Ministry of Health, Labor and Welfare, which published its grand design for the computerization of the healthcare field [3]. The Act on the Protection of Personal Information was fully enforced in 2005 [4] and revised in 2015. The Act on Anonymously Processed Medical Information to Contribute to Medical Research and Development (Next Generation Medical Infrastructure Act) came into effect in May 2018. This act relates to processes such as anonymizing data that will be shared [5]. Therefore, progress is being made in achieving a broad consensus on how to protect personal information when sharing medical data, conducting experiments, establishing laws, and allocating time for discussions and improvements.

A need has arisen for inter-regional healthcare cooperation and occasional mutual disclosure of information among different medical institutions by way of electronic health records (EHRs). To this end, the government has enacted the Health and Medical Strategy Promotion Act (Act No. 48 of 2014) to construct a digital infrastructure for the medical and healthcare field [6].

Basic research on biological information can thus be considered closely related to ethics, laws, and social implications (ELSI) [7]. Since these efforts are aimed at providing better health and medical care, it is important to approach the problem with ingenuity and from a social implementation perspective.

### 2.2 Data-driven era

Various concepts have been proposed as technical models of how industry and society should function in the future, e.g., Internet of Things (IoT), Society 5.0, and Industry 4.0. The basic principle is to increase productivity based on digital data, but there should also be a mechanism for sustainable development based on circulation, whereby information technology drives change through the gathering of new knowledge and evidence. This concept is having a major impact on healthcare reform. For example, it can be applied to data-driven circulation systems that automatically collect data generated during consultations, use ICT to extract new medical knowledge from these data, and use this knowledge to implement better medical care. In 2007, the Institute of Medicine, now the National Academy of Medicine, proposed the Learning Health System [8].

The importance of data gathering and information technology in the medical and healthcare fields is increasing yearly. Image diagnosis using AI and clinical applications of the human genome are regarded as major achievements. For this reason, big data and information technology have started to experience competition on a global scale. This sense of urgency is expressed in the strategic plan issued by the National Institutes of Health (NIH) in the United States in June 2018 ("Strategic Plan for Data Science"), whereby a specific plan was formulated at the national level [9]. This plan opens with the following sentence: "*As articulated in the National Institutes of Health (NIH)-Wide Strategic Plan and the Department of Health and Human Services (HHS) Strategic*

*Plan, our nation and the world stand at a unique moment of opportunity in biomedical research, and data science is an integral contributor*." This declaration is thought to originate from the precision medicine initiative set out by President Obama in his 2015 State of the Union address. Precision medicine is spreading from cancer treatment to medical treatment in general. Again, data science is essential for the creation of new concepts.

The quantity of information worldwide is growing exponentially in response to changes in the social environment of ICT. This amount is expected to increase by about 1.9 times between 2017 and 2020, and at a rate of 228 exabytes per month [10]. The number of IoT devices is expected to increase in the healthcare field (3 times more in 2020 compared with 2014), and a variety of information, such as genome information and medical images, are being digitized in the medical field. With the rapid expansion of medical IoT, it is expected that the amount of such information will increase even more in the future. A large medical institution has a large server for each modality for diagnostic imaging, but there are fears that this could result in the creation of information silos and memory depletion. Technological development, such as the application of *Innovative Optical and Wireless Networks (IOWN)*—on which NTT is actively working [2]—will be necessary to cope with this information explosion. At MEI Labs, we are constantly working on new ways to analyze, summarize, and use information.

### 2.3 Standardization in data science

Terminology can sometimes vary from one specialization to the next, with the same word having more than one definition. Furthermore, biological signals from different sources may have been gathered using equipment with different calibrations or subject to processing with different machines of undefined characteristics. Such differences can make it almost impossible to acquire new knowledge from the collected data. Therefore, data standardization is important for promoting data science in the medical field. Well-known examples include DICOM® (Digital Imaging and Communications in Medicine; a standard format for images) and SNOMED-CT (Systematized Nomenclature of Medicine Clinical Terms; a standard nomenclature for technical terms). Japan is promoting DPC (Diagnosis Procedure Combination), which standardizes the names of diagnosed illnesses according to International Classification of Diseases (ICD)-10. Information such as NDB (National Database) medical fee receipt information and the results of special health checks are maintained as big data, and there are high expectations from research using such data.

ICT has been used in the medical field for maintaining EHRs and personal health records (PHRs) and providing cooperative medical care. However, with the emergence of AI and big data, ICT is expected to play an increasingly important role. Again, the standardization of ICT must take place first. Legislation (HITEC Act: Health Information Technology for Economic and Clinical Health Act) and federal entities (ONC: Office of the National Coordinator for Health Information Technology) play an important role in the United States, where ICT has been rapidly deployed in clinical practice throughout the country.

The abovementioned US strategic plan states that medical research data should be findable, accessible, interoperable, and reusable (FAIR) [9]. This principle regarding the use and sharing of data is considered the basic attitude that should apply to all research involving the use of medical and healthcare data, where it is necessary to protect personal information and respect confidentiality.

## 3. MEI Labs initiatives

A principal concept of assessing variables in medical research is expanding from evidence-based medicine toward data-driven medicine that involves using large volumes of multidimensional data [11]. MEI Labs will be operated based on informatics, and we hope to generate knowledge and proposals that can contribute to the medical and healthcare fields. To carry out high-impact scientific research, we are conscious of the appropriateness of problem setting, quality of data (in terms of correctness, precision, and quantity), and highly sophisticated analysis. Our goals and the perspectives accord well with *IOWN* for *Smart World* and *Natural Technology* solutions [2].

There are at least three areas in medical and health informatics. These are: 1) sensor technology to measure the structure or function of a subject at rest during daily activity or under loaded conditions, 2) the accumulation and analysis of data for diagnosis, prevention, or treatment, and 3) EHRs or PHRs for lifelong care. As an extension of continued studies at NTT Basic Research Laboratories, MEI Labs in collaboration with Technical University of Munich will add a new research area focusing on nano- and/or micro-devices to efficiently sense biometric signals on the minute level and function as treatment modalities.

We will take advantage of our location in North America and quickly adapt to global standards while fostering a productive research environment for young researchers in Japan, the United States, and around the world. MEI Labs contributed to the proposal and implementation of at least seven of the eleven technical innovations advocated for NTT's *Smart World* vision [2]. The realization of *Bio Digital Twins* [12] would be ideal for accurate real-time diagnosis and high-quality treatment, and we hope to pursue this as one of our research targets.

## References


[1] Translational Bioinformatics, AMIA (American Medical Informatics Association), https://www.amia.org/applications-informatics/translational-bioinformatics

[2] NTT Technology Report for Smart World, https://www.ntt.co.jp/RD/e/techtrend/index.html

[3] Press release issued by the Ministry of Health, Labour and Welfare on Dec. 26, 2001 (in Japanese). https://www.mhlw.go.jp/shingi/0112/s1226-1.html

[4] The Act on the Protection of Personal Information (in Japanese), https://www.ppc.go.jp/files/pdf/290530_personal_law.pdf

[5] The Act on Anonymously Processed Medical Information to Contribute to Medical Research and Development (in Japanese), https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=429AC0000000028

[6] Health and Medical Strategy Promotion Act (in Japanese), https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=426AC0000000048

[7] T. Kamisato, "The Possibility of Applying Ethical, Legal and Social Implications (ELSI) to Information Technology—A Historical Background," Journal of Information Processing and Management, Vol. 58, No. 12, pp. 875–886, Mar. 2016.

[8] The Learning Health System, National Academy of Medicine, https://nam.edu/programs/value-science-driven-health-care/learning-health-system-series/

[9] NIH Strategic Plan for Data Science, https://datascience.nih.gov/sites/default/files/NIH_Strategic_Plan_for_Data_Science_Final_508.pdf

[10] Ministry of Internal Affairs and Communications, Japan, "White Paper on Information and Communications in Japan," http://www.soumu.go.jp/johotsusintokei/wp_eng.html

[11] N. H. Shah and J. D. Tenenbaum, "The Coming Age of Data-driven Medicine: Translational Bioinformatics' Next Frontier," J. Am. Med. Inform. Assoc., Vol. 19, pp. e2–e4, 2012.

[12] Press release issued by NTT Research, Inc., "World-class Research Center Opens in Palo Alto," July 8, 2019. https://www.ntt-research.com/2019/07/08/world-class-research-center-opens-in-palo-alto/



**Hitonobu Tomoike**

Director & Senior Vice President, Medical & Health Informatics Laboratories, NTT Research, Inc.; Research Professor, Bio-Medical Informatics Research Center, NTT Basic Research Laboratories.

He received a Bachelor of Medicine from Kyushu University, Fukuoka in 1969. Before taking on his current positions, he held several senior positions at universities and research institutes, including serving as associate professor at the Research Institute of Angiocardiology and Cardiovascular Clinic in the medical department of Kyushu University; professor in the First Department of Internal Medicine of Yamagata University; hospital director (Director General) at the National Cerebral and Cardiovascular Center; director emeritus at the National Cerebral and Cardiovascular Center; and hospital director at the Sakakibara Heart Institute.

# Establishing a Cryptography Research Lab in 2019

*Brent Waters*

**Abstract**

On July 1, 2019, NTT launched NTT Research, Inc. in Silicon Valley as part of a larger reorganization. NTT Research consists of three research labs in the areas of cryptography, quantum computing, and healthcare, where each lab is directed by a prominent researcher from Japan. I am very excited to be part of the cryptography research group. I was involved with kicking off this endeavor by recruiting several researchers. In this article, I share my thoughts on establishing a successful corporate research lab.

*Keywords: reorganization, cryptography, collaboration*

## 1. Introduction

While there is much reason for enthusiasm in starting a new research lab, it is also important to reflect on the challenges facing this endeavor. One sobering thought is that over the course of my career I have seen several vibrant cryptography research groups come and go. When I use the term "research," I mean basic research that can be published at top conferences or in journals. While some amount of change and turnover is inevitable; however, there does seem to be less permanence to corporate research labs in computer science than in university departments. One looming issue facing almost all corporate labs in basic research is the eventual pressure to produce and articulate their business value to the company. This comes with challenges. First, most good research in many fields has an impact along a longer time line, which can be at times difficult to align with the near-term goals of a company. Second, good research from any group will be publicly disseminated, will build upon research from people outside the organization, and will be used by other groups and organizations. This typically means that the returns of creating a strong research group are implicitly shared with the broader community. One path, of course, is to curtail outside publication and collaboration, but I have not seen this approach produce top quality research—at least not in my time in my field. It should be noted that by having a strong research group, a company is conversely positioned to build upon and capitalize on the innovations of outside researchers as well.

Despite these challenges, the opportunity of starting and joining a new lab can far outweigh the risks for both researchers and the organization if done the right way. Below I impart a few thoughts on how to establish a successful research lab. I emphasize that the perspective I share below is centered on creating a research lab with the primary goal of producing top-tier publications in computer science—that is, producing the *best* research—and some of these ideas might apply differently to different goals.

**Be elite.**

"Do it right or don't do it." It is fairly easy to start a mediocre research lab, but starting a great one is where the challenge and excitement lays.

This starts with hiring the right people. The difference between a top-tier researcher and an average hire is quite significant. It therefore makes sense to strategize on how to attract the best people. A good starting point is salary and compensation. Given the large value difference in acquiring top people, one has to do what it takes to get the right person. One comparison point is professional sports in which a team may be eager to trade several athletes to acquire a superstar. The resources for compensation will be finite. I suggest they be focused on quality over quantity.

Another way to recruit a regular stream of top talent is to begin by recruiting top talent. Top researchers will want to collaborate with each other (On the other side of the coin, not making the right hires can negatively affect future recruiting). One thing a corporate lab can do is to create an environment in which several people can work together. This also works well with recruiting interns and postdocs. If you can get a critical mass of senior researchers, the lab will become a destination that graduate students will flock to over the summer.

**Let researchers do what they are good at.**

If fortunate enough to hire the right people, let them do what they are best at. Top researchers have a special ability and will want to focus on basic research. The best way to manage them is really just to give them space to "do their thing." Of course, it is reasonable to have occasional requirements such as asking researchers to explain their ideas to a developer who is putting those ideas into practice. I suspect most researchers will be happy to meet such requirements. However, if the group's vision of what a researcher should be doing is much different than letting them stick to what they are good at, then I would argue that the vision wasn't compatible with basic research to begin with.

It is also important to ensure researchers have the right amount of time to do their research. Minimizing the amount of additional meetings or other activities with overhead is important. Gaining external exposure of the lab's achievements is important, although much of this will happen organically as researchers travel to present papers at conferences and invited talks. Generally, researchers will already have a good feel of where their time is best spent.

**Know the competition and what is needed to compete.**

Let's say we subscribe to the ideology of obtaining very strong researchers. We next need to look at the competition. Let's focus on faculty positions at research universities. As a faculty member, a researcher will have access to eager graduate students, have the opportunity to achieve lifetime job security through tenure, have a large amount of independence in pursuing his/her interests, be able to conduct research on a college campus with a nice office, and gain the prestige of being recognized as a professor.

It is important to keep this in mind when recruiting people who already have academic jobs or have just completed their Ph.D. studies and are considering university positions. There are certain things, of course, that just cannot be matched. If someone wishes to teach, be on a university campus, and be called professor, then a university job is for them. However, there are other aspects where a corporate lab can meet or exceed an academic position. Let's start with office space. Many company working environments are *open offices* where engineers work either at desks or cubicles. After speaking to many potential recruits for NTT Research, Inc. (as well as consulting my own personal feelings), I can say with great confidence that such a setup will not be popular with researchers. Researchers desire private, individual offices where they can concentrate on their ideas. This is what any computer science faculty member will be given, and if the same is not offered, it will be considered a significant minus to anyone deciding between offers. There is also a certain prestige associated with offices (and a corresponding lack of prestige associated with not having them). If you want to make a recruit feel special, this is critical.

There are other points at which a corporate lab can exceed an academic offer.

- Compensation: At universities, there are political and other pressures to keep salaries relatively uniform and lower. A corporate lab should ideally have the ability to pay more as well as have more flexibility in achieving its hiring goals.
- Number of colleagues in an area: At NTT Research we have the opportunity to hire several cryptography researchers at the same location. In a well-balanced computer science department, the hiring will be more spread out among different areas. This provides a special opportunity to researchers in a lab.
- Less overhead: At a corporate research lab, one does not have to teach, serve on committees, or search for funding. The freedom to devote more time to pure research can be a huge draw. It is important not to lessen this advantage by having too many tasks, meetings, etc.

**Make collaboration and publication easy.**

A surefire way to stymie the growth of an elite research lab is to put up excessive barriers to publication or collaboration. Researchers must be able to enter into collaborations with others outside the company without any barriers. Also, there should be few to no barriers to publishing or posting a research paper online. Otherwise, the best people will simply find someplace else to work. Of course, a company

should have the ability to patent research that comes out of the lab, but this should be done in a way with minimal impediment to the core research goals.

Everything above should be doable if the right resources and management style are in place. If there is a single takeaway, I would say that basic research is simply different from product development, and academically focused researchers are different from engineers. To establish a successful research lab, a company needs to develop a distinct approach.

## 2. Concluding remarks

I'd like to conclude by describing the many benefits of having a corporate lab that produces groundbreaking research. An obvious one is that researchers who create new ideas can help build up a company's intellectual property portfolio. In addition, having in-house expertise can be very useful for evaluating emerging technologies. However, the most important role by far is that a corporate research lab is the source for transformative and novel ideas. Embracing change and new ideas is necessary for companies to stay at the top. At NTT Research's kick-off event, I was interested to learn that less than 20% of NTT's current revenue comes from voice (including voice from mobile)—this is from a company with the words "telephone" and "telegraph" in its name. To stay relevant, a company will have to evolve over time. Big ideas in research can come from unplanned and unexpected places. For instance, one of the research contributions I am best known for is attribute-based encryption—a way of encrypting to a policy as opposed to targeting specific individuals. However, this concept sprouted out of a work (with Amit Sahai) where we were initially investigating how to encrypt biometric identities. It is precisely this ability to tap into fundamentally new ideas and technologies that make running a successful research lab a pillar to a company's future growth. I am very encouraged by the solid launch of NTT Research and excited to see where things go from here.

**Brent Waters**
Distinguished Scientist, Cryptography & Information Security Laboratories, NTT Research, Inc.

Dr. Brent Waters received his Ph.D. in computer science from Princeton University, NJ, USA, in 2004. From 2004–2005, he was a post-doctoral researcher at Stanford University, CA, USA, then worked at SRI International as a computer scientist. In 2008 he joined the faculty at The University of Texas at Austin. In 2019 he joined NTT Research as a distinguished scientist. Dr. Waters' research interests are in the areas of cryptography computer security. His work has focused on identity-based cryptography, functional encryption, and code obfuscation. He is noted as a founder of functional encryption and attribute-based encryption.

Dr. Waters is a recipient of the National Science Foundation CAREER award, the Presidential Early Career Award for Scientists and Engineers (PECASE), and the 2015 ACM (Association for Computing Machinery) Grace Murray Hopper award. He has been a Microsoft Faculty Fellow, Sloan Research Fellow, a Packard Science and Engineering Fellow, and a Simons Investigator.

# Data-coding Approaches for Organizing Omni-ambient Data

*Seishi Takamura*

**Abstract**

Various information sensors are currently deployed to generate data such as images, video, audio, and temperature. The amount of such multi-modal data is rapidly increasing compared to the development of information and communication technology (such as storage, transmission, and processing technology). This means a considerable amount of important Internet-of-Things data has to be abandoned since such data cannot be stored, transmitted, or processed. In this article, I describe our approaches for fully using the huge amount of multi-modal data.

*Keywords: video coding, multi-modal signal handling, IoT data handling*

## 1. Introduction

An increasing amount of data is becoming available with advances in technology and the expansion of the Internet of Things (IoT). The potential advantages of having such data available are described in this section.

### 1.1 Growth in IoT data

It has been reported [1] that the growth in storage devices is expected to increase 10 fold per decade, which is estimated to reach 100 zettabytes (ZB) (1 ZB = $10^{21}$ bytes) by 2030 and 1 yottabyte (YB) (1 YB = $10^{24}$ bytes) by 2040. However, the growth in information generated by sensors is expected to increase 40 fold per decade, which is estimated to reach 1 YB by 2030 and 40 YB by 2040 (**Fig. 1**).

Reflecting this rapid growth in IoT data generation and awareness of issues in their processing, a number of international standardization projects, such as Big Media [2], Internet of Media Things [3, 4], Network-Based Media Processing [5, 6], and Network Distributed Media Coding [7], have recently been initiated.

### 1.2 New opportunities via large-scale multi-modal data

Multi-modal IoT sensors are expected to be deployed around the world to obtain data of the entire earth (**Fig. 2**), which will make various applications possible. For example, in agriculture:

- Monitoring field crops based on super-wide-area video analysis
- Optimizing the timing and amount of fertilizer, water, and agrichemicals
- Maximizing crops and quality of the harvest based on precipitation, temperature, and moisture data.

Weather forecasting, disaster prevention, smart cities, surveillance/security, intelligent transport systems, logistics, infrastructure maintenance/inspection, tourism, etc., may benefit from the data of the entire earth.

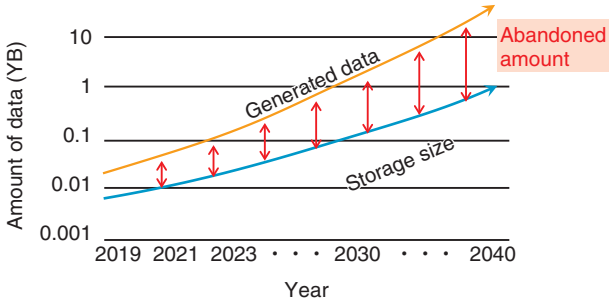



Fig. 1. Growth in generated data and storage size.

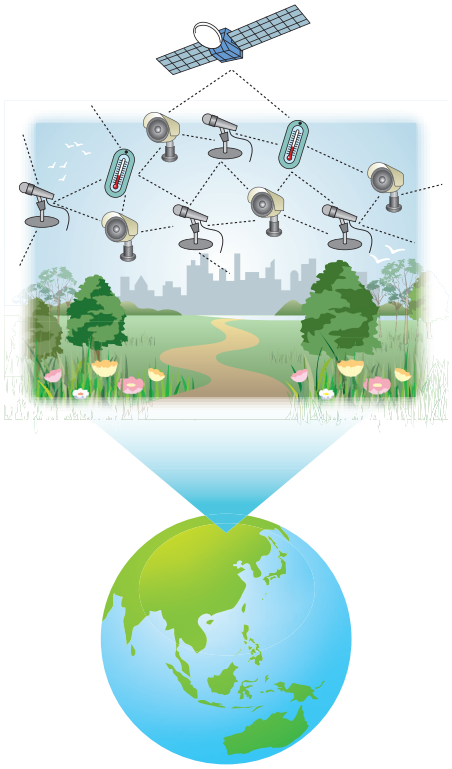


Fig. 2. Multi-modal sensor network over the entire earth.

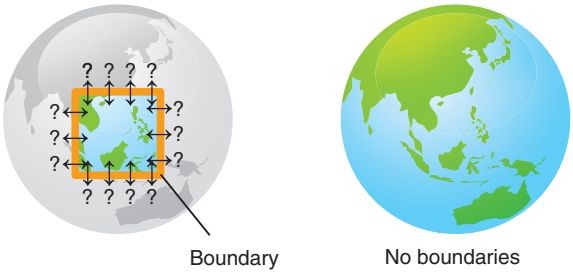



Fig. 3. Partial-earth sensing limitation (left) and entire-earth sensing advantage (right).

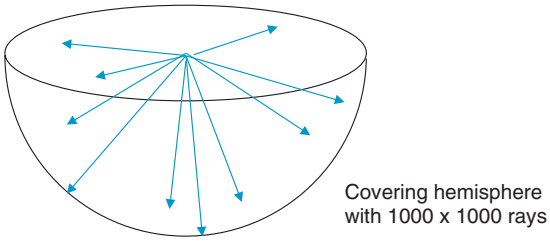



Fig. 4. Light-field-density image covering one hemisphere.

## 2. Omni-ambient data: data that cover the entire earth

Hereafter, the multi-modal data that cover the entire earth are referred to as omni-ambient data. Let us estimate the data size of omni-ambient data.

### 2.1 Number of sensors

If we were to observe the entire earth, we would have to deploy multi-modal sensors at every 10-m mesh point at, say, 10 m above the earth's surface. Since the surface area of the earth is $5.1 \times 10^8$ km$^2$, the number of sensors to cover the earth (S) would be $5.1 \times 10^{12}$. The rationale of covering the entire earth with sensors is as follows. If only a part of the earth is sensed, there will always be boundaries, which may cause uncertainty in data flux/interaction across them. If the entire world is covered, there would not be any boundaries; hence, no uncertainty would arise (**Fig. 3**).

### 2.2 Visual data

A hemisphere should be covered by about 1000 × 1000 light rays (**Fig. 4**) to capture the earth's light field. This resolution is about half the full high definition (HD) resolution (1920 × 1080). With this configuration, one ray covers a solid angle of $6.3 \times 10^{-6}$ sr (steradian). If we assume that video is captured at 30 frames per second and each pixel has 8-bit red (R), green (G), and blue (B) information, the total amount of raw (uncompressed) video data from a single camera becomes 90 Mbit/s, but these data can be compressed with an existing video coding scheme (such as MPEG-H* or High Efficiency Video Coding (HEVC) [8]) to 1/350 its size, which is V (the total amount of compressed video data from a single camera) = 257 kbit/s. The total visual amount of omni-ambient data is S × V = 1.41 Ebit/s (1 exabyte (EB) = $10^{18}$ bytes), which is 41 YB per year. This amount is equivalent to all data that will be generated by 2040 (Fig. 1).

### 2.3 Audio data

Compact disc quality single-channel audio is assumed for capturing audio, which is 44.1 kHz × 16

* MPEG-H: International standards for video and audio compression developed by the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Moving Picture Experts Group (MPEG).

bits = 88 kbit/s. Let it be compressed with a conventional audio coding scheme (such as Advanced Audio Coding) to 1/20 its size, which is 4.4 kbit/s. The total audio amount of omni-ambient data is S × A = 45 Pbit/s (1 petabyte (PB) = $10^{15}$ bytes), which is 1.4 YB per year.

### 2.4 Importance of visual data

The amount of audio data is about 30 times less than that of light data in omni-ambient data. The amounts of other data, such as depth, temperature, and moisture, may be comparable or even less. Therefore, the majority of the data is visual data. This is analogous to the visual data in Internet protocol (IP) traffic. It has been reported that mobile video traffic accounted for 59% of all worldwide mobile data traffic in 2017 and will be 79% by 2022 [9]. IP video traffic accounted for 75% of all worldwide IP traffic in 2017 and will be 82% by 2022 [10].

## 3. Challenges with organizing omni-ambient data

Some of the challenges with and opportunities for organizing omni-ambient data are discussed in this section. In addition to the example techniques described below (3.1–3.4), there should be many techniques to enable such organizing, such as pattern recognition, non-visual signal compression, large-scale archiving, ultrafast database construction, distributed computing, broadband IoT connection, and communication security.

### 3.1 Further compression via multi-modal synergic coding

Suppose there are two random variables X and Y. We then have the following equation

$$I(X; Y) = H(X) + H(Y) - H(X, Y),$$

where I(X; Y) is the mutual information of X and Y, H(X) and H(Y) are the marginal entropies of X and Y, and H(X, Y) is the joint entropy of X and Y. Since I(X; Y) is non-negative, the above equation can be rewritten as

$$H(X, Y) \geqq H(X) + H(Y).$$

This means that in terms of compression, it is always better to compress two (or even more) sources together. This encourages us to abandon conventional single-modal data coding for multi-modal data coding. One of the possibilities of efficient multi-modal data compression is depicted in **Fig. 5**. Conventionally, depth data and two-dimensional (2D) video data are encoded independently (sizes A and B, respectively, in figure). Since there is a non-negative relationship between depth and the captured image, 3D-shape-aware collaborative video coding may have less compressed data (size B'), which is smaller than B. This applies to not only two but also more than two modalities.

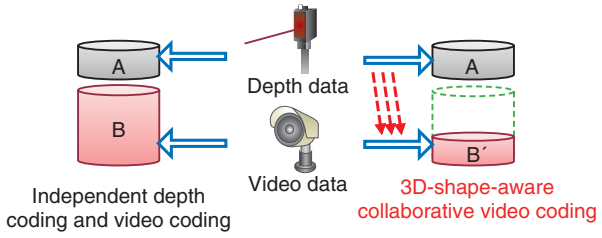



Fig. 5. Example of efficient multi-modal data compression.

### 3.2 Removing noise via real-entity mining

Sensed data are not always collected under ideal conditions, i.e., acquired data are deemed to contain noise, which is unpredictable and uncompressible by nature. Therefore, from the coding, storing, processing, and transmitting points of view, noise should be removed. Conventionally, acquired pixel values are targeted for encoding. However, the original objects should be behind the acquired pixel values. Therefore, being reminded of the existence of original objects (real-entity-oriented approach) may work better in signal processing, data compression, etc., than not taking care of it (observed-signal-oriented approach) (**Fig. 6**).

One such example is still-camera video coding. By processing such a video sequence and obtaining a real-entity image of the background, the video can be further compressed. Compared to the state-of-the-art video coding standard H.265/HEVC (reference software HEVC test model (HM)16.4) [8], bit-rate savings of 32.40% on average and 56.92% at maximum in terms of the Bjøntegaard Delta rate (BD rate) [11] were observed. It was also observed that the decoded video contains less camera noise than the original, which means the decoded video is even subjectively better than the original (**Fig. 7**). It also provides 21.17% faster encoding [12].

Noise is inevasible in any type of sensed data and it is uncompressible by nature. Therefore, noise reduction from data is crucial for compression efficiency. By tracking noisy rigid objects and temporally aligning

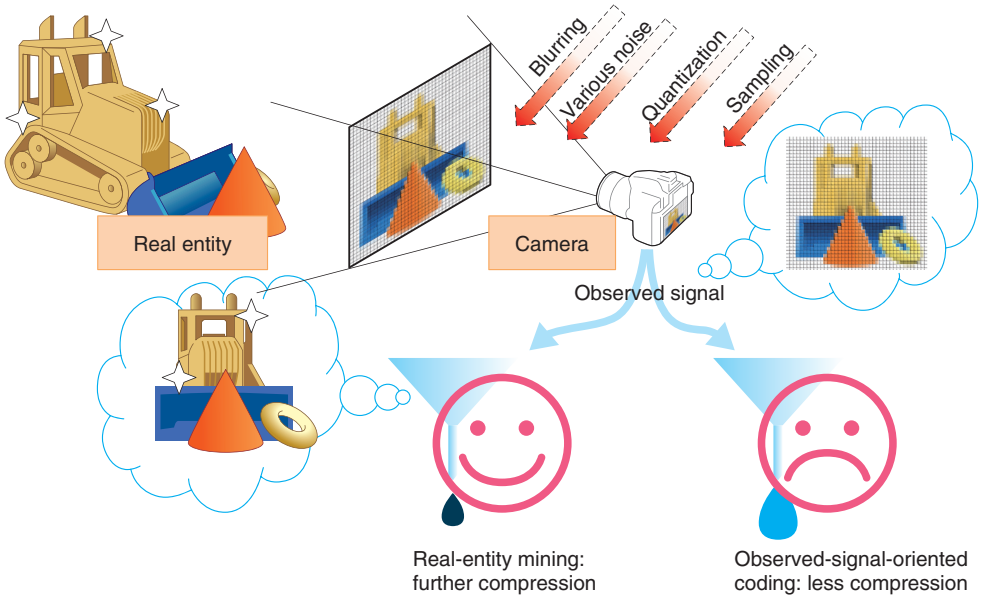



Fig. 6. Observed-signal-oriented coding vs. real-entity mining.

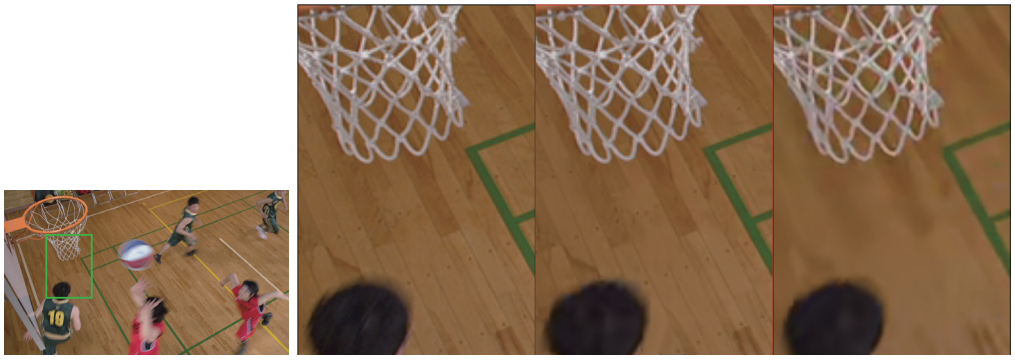



Fig. 7. Still-camera video-coding results based on real-entity background [12]. (a) Original image. Green box is magnified area, (b) original (noisy), (c) real-entity background based coding (Y-PSNR (peak signal-to-noise ratio) = 36.99 dB) 1/330 compression, and (d) H.265/HEVC (HM16.4) (Y-PSNR = 33.60 dB) 1/330 compression.

them and filtering out camera noise, coding efficiency greatly improves. The filtered image can be considered as the real entity of the rigid object and will be used as a reference frame for input video coding. In our experiments, this processing worked well for both objective and subjective metrics (**Fig. 8**). There was a 19–47% increase in the BD rate against H.265/HEVC (HM16.6) and 13–30% against preliminary Versatile Video Coding (VVC) [14] (JEM5.0). In terms of subjective video quality, the decoded video looked even better than the original video while only using 141–229 times fewer bits than JEM5.0 [13].

Another example is water-bottom video coding. Video content through the water surface is generally quite difficult to encode efficiently because of random movement and nonlinear deformation of objects seen through the moving water surface. By generating one additional frame from the input video sequence, which represents the real-entity image of bottom objects (**Fig. 9**), and additionally encoding the

Fig. 8. Rigid-object video-coding results based on real-entity mining approach [13]. (top-left) Former Versatile Video Coding (VVC); experimental model JEM5, rate = 1,857,505 bytes (noisy, similar to original), (top-right) real-entity mining based coding with super-low-rate mode, rate = 13,169 bytes (no noise and crisp), (bottom-left) H.265/HEVC (HM16), rate = 15,061 bytes (distorted), (bottom-right) JEM5, rate = 13,617 bytes (distorted).

(a) (b) (c) (d)

Fig. 9. Real-entity extraction example [15]. (a) Original water-bottom video frame under moving water surface (skewed), (b) temporal median filter result (blurred), (c) real-entity mining based (crisp and not skewed), (d) original water-bottom image under still water surface (ground truth).

frame and storing it as a long-term reference frame, a BD-rate reduction of 12–42% compared to the next-generation standard VVC under development (reference software VVC Test Model (VTM)1.1) [14] and 13–48% compared to VTM4.0, were achieved [15].

### 3.3 Indexing via machine-to-machine (M2M)-oriented image coding

Adding annotations to the obtained signal is essential for organizing omni-ambient data, and of course it should be done using machines (not by humans). Therefore, information coding that maximizes subjective quality may be less important than coding that maximizes machine recognition. One such M2M-oriented image-coding approach is that by Suzuki et al. [16]. The importance of this concept is reflected in the recent initiation of a new standardization project called Video Coding for Machines [17].

### 3.4 Reducing amount of original source data via compressed sensing

The above-estimated naïve data amount could become burdensome for initial-stage transmission. Sometimes it may be necessary to reduce the data rate at the sensor and (in return) restore the data by additional data processing. To achieve this, a compressed sensing technique [18] will be applied.

## 4. Conclusion

An overview was given of the rapidly increasing amount of data generated by ubiquitously deployed multi-modal devices, standardization trends to cope with such data, and possible applications by fully using the data that cover the entire world, i.e., omni-ambient data. The physical amount of such data was evaluated, and it was noted that visual data are dominant; therefore, efficient compression is crucial. Then the possibility of such compression by using mutual information among multi-modal signals was

discussed. How real-entity mining would help reduce noise, enable further compression, and improve subjective video quality was also discussed. We will continue investigating and tackling the challenges and taking advantage of the opportunities of this research, expanding the potential for more applications.

## References


[1] H. Muraoka, "Yottabyte-scale Massive Data and Its Impact—Breaking Through a Wall of Ever-increasing Amounts of Information," Presentation material at Tohoku Forum for Creativity Symposium, pp. 11–12, Aug. 2017 (in Japanese), https://www.tfc.tohoku.ac.jp/wp-content/uploads/2017/08/2017EPP_03_Hiroaki_Muraoka.pdf

[2] MPEG Exploration Part 21, Big Media, https://mpeg.chiariglione.org/standards/exploration/big-media

[3] ISO/IEC 23093: "Internet of Media Things (IoMT)."

[4] ISO/IEC JTC 1/SC 29/WG 11, N 18910, "Technology under Consideration for IoMT," Oct. 2019.

[5] ISO/IEC 23090-8: "Network-Based Media Processing (NBMP)."

[6] ISO/IEC JTC 1/SC 29/WG 11, N 18848, "Technologies under Consideration for NBMP."

[7] MPEG Exploration Part 25, Network Distributed Media Coding, https://mpeg.chiariglione.org/standards/exploration/network-distributed-media-coding

[8] ISO/IEC 23008-2:2015: "Information technology – High efficiency coding and media delivery in heterogeneous environments – Part 2: High efficiency video coding," 2015.

[9] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022 White Paper, updated on Feb. 2019. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html

[10] Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper, updated on Feb. 2019. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

[11] G. Bjøntegaard, "Calculation of Average PSNR Differences between RD-curves," ITU-T VCEG-M33, Apr. 2001.

[12] S. Takamura and A. Shimizu, "Simple and Efficient H.265/HEVC Coding of Fixed Camera Videos," Proc. of the 23rd IEEE International Conference on Image Processing (ICIP 2016), TP-L1.3, pp. 804–808, Phoenix, AZ, USA, Sept. 2016.

[13] S. Takamura and A. Shimizu, "Efficient Video Coding Using Rigid Object Tracking," Proc. of Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) 2017, FP-04.5, Kuala Lumpur, Malaysia, Dec. 2017.

[14] ISO/IEC 23090-3 MPEG-I Versatile Video Coding.

[15] S. Takamura and A. Shimizu, "Water-bottom Video Coding Based on Coding-oriented Reference Frame Generation," Proc. of 2019 IEEE International Conference on Visual Communications and Image Processing (VCIP 2019), Sydney, Australia, Dec. 2019.

[16] S. Suzuki, M. Takagi, K. Hayase, T. Onishi, and A. Shimizu, "Image Pre-Transformation for Recognition-Aware Image Compression," Proc. of the 26th IEEE International Conference on Image Processing (ICIP 2019), TP.PG.7, Taipei, Taiwan, Sept. 2019.

[17] ISO/IEC JTC 1/SC 29/WG 11, N18772, "Draft Evaluation Framework for Video Coding for Machines," Oct. 2019.

[18] D. L. Donoho, "Compressed Sensing," IEEE Trans. Inf. Theory, Vol. 52, No. 4, pp. 1289–1306, Apr. 2006.

**Seishi Takamura**

Senior Distinguished Engineer, Signal Modeling Technology Group, Universe Data Handling Laboratory, NTT Media Intelligence Laboratories.

He received a B.E., M.E., and Ph.D. from the Department of Electronic Engineering, Faculty of Engineering, the University of Tokyo, in 1991, 1993, and 1996. His current research interests include efficient video coding and ultrahigh-quality video processing. He has fulfilled various duties in the research and academic community in current and prior roles, including serving as associate editor of the Institute of Electrical and Electronics Engineers (IEEE) Transactions on Circuits and Systems for Video Technology (2006–2014), editor-in-chief of the Institute of Image Information and Television Engineers (ITE), executive committee member of the IEEE Region 10 and Japan Council, and director-general of ITE affairs. He has also served as chair of ISO/IEC Joint Technical Committee (JTC) 1/Subcommittee (SC) 29 Japan National Body, Japan head of delegation of ISO/IEC JTC 1/SC 29, and as an international steering committee member of the Picture Coding Symposium. From 2005 to 2006, he was a visiting scientist at Stanford University, CA, USA.

He has received 51 academic awards including ITE Niwa-Takayanagi Awards (Best Paper in 2002, Achievement in 2017), the Information Processing Society of Japan (IPSJ) Nagao Special Researcher Award in 2006, Picture Coding Symposium of Japan (PCSJ) Frontier Awards in 2004, 2008, 2015, and 2018, the ITE Fujio Frontier Award in 2014, and the Telecommunications Advancement Foundation (TAF) Telecom System Technology Awards in 2004, 2008, and in 2015 with highest honors, the Institute of Electronics, Information and Communication Engineers (IEICE) 100-Year Memorial Best Paper Award in 2017, the Kenjiro Takayanagi Achievement Award in 2019, and Industrial Standardization Merit Award from Ministry of Economy, Trade and Industry of Japan in 2019.

He is an IEEE Fellow, a senior member of IEICE and IPSJ, and a member of Japan Mensa, the Society for Information Display, the Asia-Pacific Signal and Information Processing Association, and ITE.

# Meeting Report of the 31st Asia-Pacific Telecommunity Standardization Program (ASTAP-31) and the Asia-Pacific Telecommunity (APT) Preparatory Meeting for WTSA-20

*Noriyuki Araki and Hideyuki Iwata*

**Abstract**

The 31st Asia-Pacific Telecommunity Standardization Program (ASTAP-31) was held in Tokyo in June 2019 with the aim of strengthening standardization activities in the information and communication technology field in the Asia-Pacific Telecomunity (APT) and contributing to the regional formulation of international standards. This article reports the results of ASTAP-31 and the status of the first APT preparatory meeting for WTSA (World Telecommunication Standardization Assembly) planned in 2020.

*Keywords: ASTAP, WTSA, ITU-T*

## 1. The 31st Asia-Pacific Telecommunity Standardization Program (ASTAP) meeting

The Asia-Pacific Telecomunity (APT) was established in 1979 and is an international organization promoting the development of information and communication technology (ICT) in the Asia-Pacific region. It currently has 38 member countries. ASTAP consists of an APT standardization committee that meets every 10 months or so. The 31st ASTAP meeting (ASTAP-31) was held in Tokyo (Akihabara) in June 2019. The Ministry of Internal Affairs and Communications (MIC) of Japan hosted this meeting with the support of NTT and other Japanese member companies in order to strengthen cooperation with major Asian countries and coordinate proposals reflecting Japan's opinions. The meeting had 108 participants from 20 countries. The meeting opened with speeches given by Ms. Areewan Haorangsi, APT Secretary General, and Ms. Yukari Sato, then State Minister of MIC, who spoke on behalf of the host country.

## 2. First APT preparatory meeting for World Telecommunication Standardization Assembly 2020 (WTSA-20)

The first meeting of the APT Preparatory Group for WTSA-20 (APT WTSA-20) was held in conjunction with ASTAP-31. WTSA-20 is one of the most important meetings of the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T). The purpose is to decide the study group structure of ITU-T, the chair and vice-chair of each study group, and the study theme on the latest technology such as artificial intelligence and Internet of Things (IoT) in the study period from 2021 to 2024.

In WTSA deliberations, it is common to divide the world into six regions (Asia and the Pacific, the

Table 1. Structure of APT WTSA-20.

| Organization / Working Group (WG) | Chair | Vice-chair |
|---|---|---|
| APT WTSA-20 | Mr. Yoichi Maeda (TTC, Japan) | Dr. Hyoung Jun Kim (Korea)<br>Mr. Xu Heyuan (China)<br>Mr. Arvind Chawla (India) |
| WG1: ITU-T Working methods | Dr. Kangchan Lee (Korea) | Ms. Miho Naganuma (NEC, Japan)<br>Mr. Ashutosh Pandey (India)<br>Proposed (China) |
| WG2: ITU-T Work organization | Mr. Noriyuki Araki (NTT, Japan) | Mr. Nguyen Van Khoa (Vietnam)<br>Mr. P. K. Singh (India)<br>Proposed (Korea)<br>Proposed (China) |
| WG3: Regulatory/policy and standardization related issues | Dr. Cao Jiguang (China) | Ms. Eriko Hondo (KDDI, Japan)<br>Ms. Arezu Orojlu (Iran)<br>Mr. Premijit Lal (India)<br>Ms. Nguyen Thi Khanh Thuan (Vietnam) |

Americas, Europe, Russia (Commonwealth of Independent States), the Arab states, and Africa) and to have common proposals for each region. This is done to improve the efficiency of consensus building. Therefore, the APT WTSA-20 preparatory meetings are crucial for discussing the course of action for WTSA-20. For example, if we try to reflect Japan's proposals, it will be possible to negotiate with other regions at the regional level by making them an APT common proposals as the Asia-Pacific region.

This was the first meeting leading up to WTSA-20, and the selection of the APT WTSA-20 chair, vice-chair, and other officials in charge of the management of the meeting and approval of the meeting structure were made. The structure of the APT WTSA-20 is indicated in **Table 1**. Mr. Yoichi Maeda, chief executive officer and senior vice president of the Telecommunication Technology Committee (TTC), was elected as chair of APT WTSA-20. In addition, three Working Groups (WGs) were established to discuss ITU-T working methods (WG1), ITU-T work organization (WG2), and regulatory/policy and standardization related issues (WG3). Japan has established a strong support system to reflect its intentions, with three members from Japan selected as the chair or vice-chair of the WGs to promote substantive discussions at meetings. In the future, discussions toward an agreement on the APT common proposals will be held at the preparatory meetings, taking into account the trend of discussions held in ITU-T Telecommunication Standardization Advisory Group (TSAG).

## 3. Industry workshops

An industry workshop was held on the afternoon of the first day of the meeting. Seven speakers from four countries gave lectures on disaster response ICT in the first half and smart cities and IoT in the second. The industry workshop programs are listed in **Table 2**. Promising items for future study in the Expert Groups (EGs) of ASTAP were reported at this workshop.

## 4. Organizational structure of ASTAP

The structure of ASTAP and the respective office bearers are shown in **Fig. 1**. ASTAP consists of 11 EGs and 3 WGs that organize EGs by technical field. Substantial technical discussions are conducted by each EG, and the outcome documents from each EG are approved by the WG and then finally discussed at the ASTAP Plenary so that efficient discussions can be conducted at each meeting level.

## 5. Main results of ASTAP-31

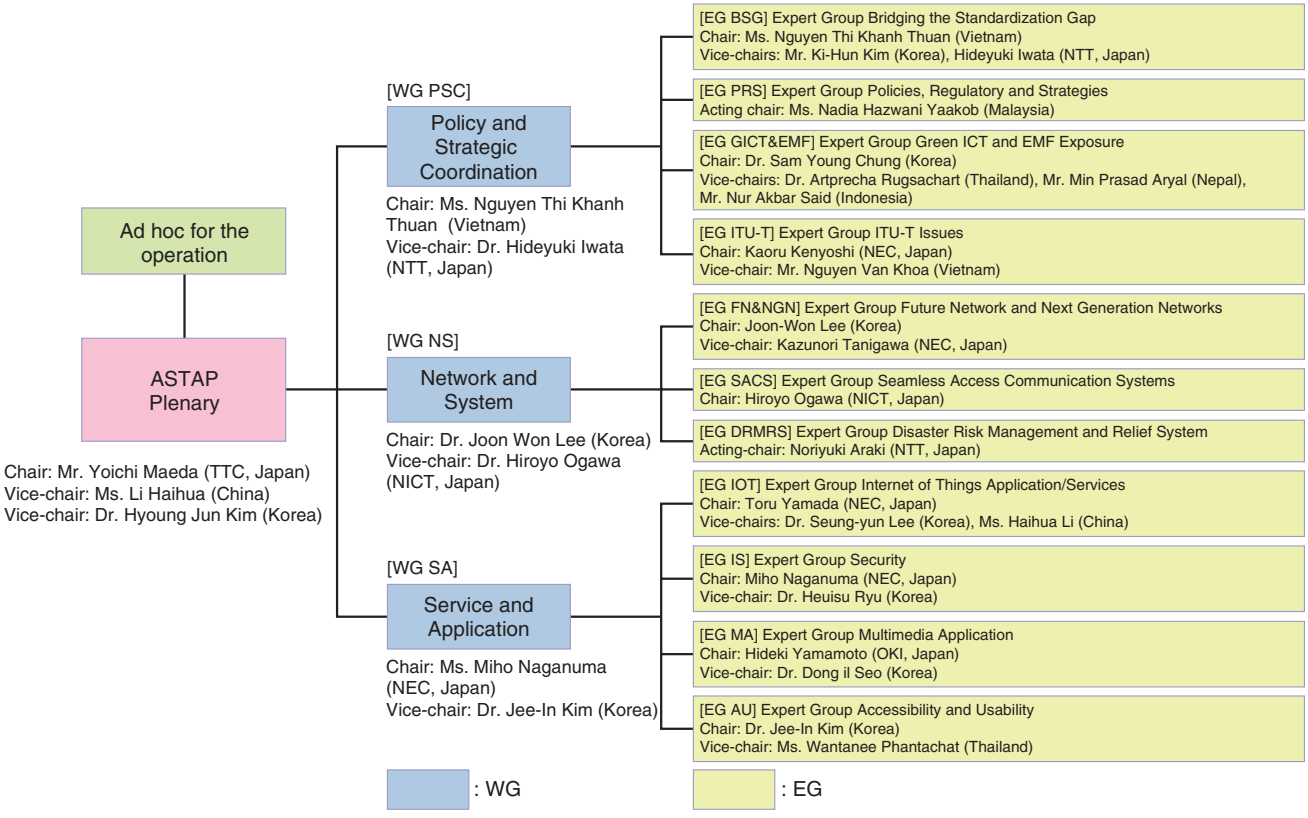
At the ASTAP meeting, 11 APT reports, 1 guideline document, 4 survey questionnaires, and 3 liaison statements to other standardization bodies were approved. The main output documents are listed in **Table 3**.

In the EG DRMRS (Disaster Prevention and Recovery System) session, the discussion progressed on the technical report on the use cases of portable emergency communication systems that had been studied based on the proposal from NTT. The use case of portable ICT resource units (MDRU: movable and deployable ICT resource units) [1] during the 2016 Kumamoto earthquake was incorporated into the APT report. The APT report was finally approved

Table 2. Industry workshop programs.

| |
|---|
| Opening Remarks: Ms. Yuki Naruse (NICT, Japan)<br>Workshop program committee member |
| **Part I: Disaster Response**<br>Chair: Dr. Seungyun Lee, ETRI, Korea |
| ●Development of Unmanned Aerial Vehicle Sensor-based Smart Eye Technology for Local Disaster Monitoring and Situational Response<br>by Dr. Yong-Tae Lee, ETRI, Korea<br>●About V2X that Utilized Route Bus in Kobe<br>by Mr. Yasuo Oishi, Honda Motor Co., Ltd., Japan<br>●Disaster Resilient Communications and Information Systems using the New V-Hub Standard<br>by Prof. Gregory L. Tangonan, Ateneo de Manila University, Philippines |
| **Part II: Smart Cities and IoT**<br>Chair: Mr. Kaoru Kenyoshi, NICT, Japan |
| ●Smart City and IoT Projects of ASEAN IVO<br>by Dr. Hiroshi Emoto, NICT, Japan<br>●NEC's Smart City Solutions Employed in APT Member Countries<br>by Dr. Toru Yamada, NEC Corporation, Japan<br>●Tuberculosis Laboratory Data System in Myanmar<br>by Dr. Ikuma Nozaki, Bureau of International Health Cooperation, National Center for Global Health and Medicine, Japan<br>●5G Internet of Vehicle Outlook and Practice<br>by Dr. Chen Xiao, ZTE Corporation, China |

ASEAN: Association of Southeast Asian Nations
ASEAN IVO: ICT Virtual Organization of ASEAN Institutes and NICT
ETRI: Electronics and Telecommunications Research Institute
5G: fifth-generation mobile communications
NICT: National Institute of Standards and Technology
V2X: vehicle-to-everything




EMF: electromagnetic field

Fig. 1. Structure of ASTAP and office bearers.

Table 3. Main output documents approved at ASTAP-31.

| WG | Document title |
|---|---|
| WG PSC | Handbook to Introduce ICT Solutions for the Community in Rural Areas |
| | Report on Regulatory Matters and Implementation Practices of Quality of Experience in Mobile Communications |
| | APT Report on Efforts to Achieve Green Data Centers in the ICT/telecommunications Sector in APT Member Countries |
| | APT/ASTAP Report on EMF Information Platform |
| | Asia-pacific Regional Activities on Human Exposure to EMF (Ed.1) |
| | Questionnaire to Collect Data on the Measurement Scenarios and Sampling Methodologies to Assess Quality of Popular Mobile Services |
| | Questionnaire on Compliance Label of Communication Devices |
| | Questionnaire for Requirements on ICT Standardizations |
| | Liaison Statement to SG11 to Share Information on Combating Counterfeit and Stolen Mobiles |
| WG NS | Draft APT Report on Case Studies for Portable/Movable Emergency Telecommunication System in APT Region |
| | Draft New APT Report on Field Trial of Wireless Access WDM-PON Deployment based on Radio over Fiber Technology |
| | Draft New APT Report on Power over Fiber System for Radio over Fiber Network |
| | Draft New APT Report on Broadband Railway Communication Systems Using Radio over Fiber Technologies |
| | Draft New APT Report on Description of Radio over Fiber Technologies for Seamless Access Communication Systems |
| | Draft Liaison Statement to ITU-T SG15 |
| WG SA | The Security Guideline: Guidelines for Secure Use of IT Devices and Services (Version 2) |
| | APT Report "Harmonization of S2ST (Speech-to-Speech Translation) Standardization" |
| | Draft Questionnaire for Traffic Accident Record and Its Analysis Method's Guidelines in Asia-Pacific Region |
| | Liaison Statement to ITU-T SG16 Q21and Q24 and ISO/IEC JTC1 SC35/WG5: Approval of APT Report "Harmonization of S2ST Standardization" |

IEC: International Electrotechnical Commission
ISO: International Organization for Standardization
IT: information technology
JTC1: Joint Technical Committee 1
Q: question
WDM-PON: wavelength division multiplexing passive optical network

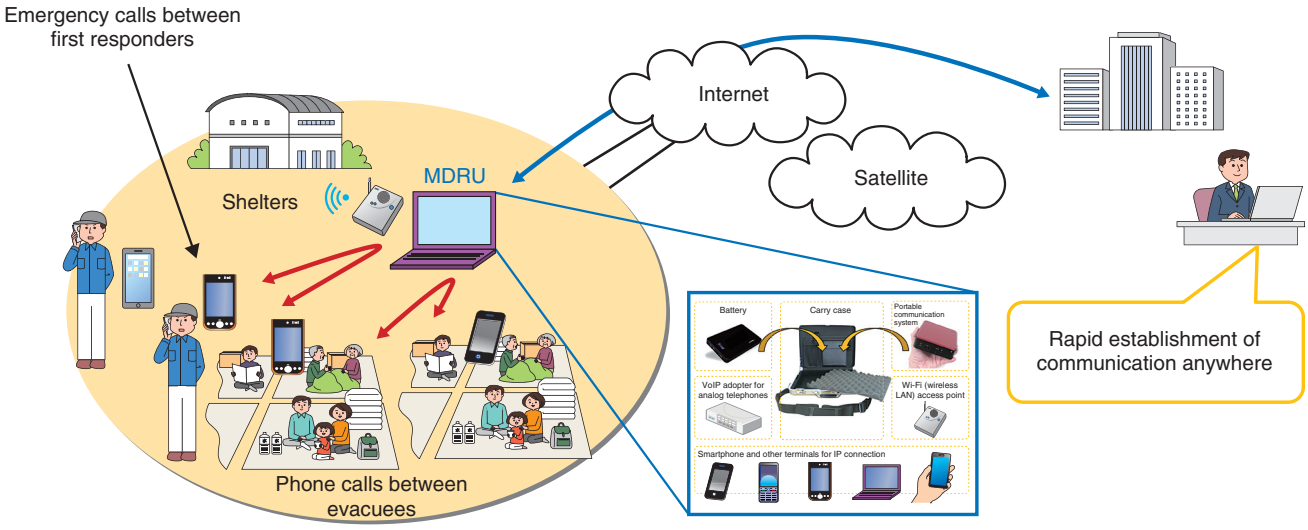
by adding the examples of emergency communication systems in China and the Philippines, and the standardization status of disaster response ICT related technology and communication services in other standardization organizations such as ITU (**Fig. 2**). In the future, it is expected that the use of portable emergency communication systems such as MDRUs will expand in the Asia-Pacific region.

In addition, it was reported that the Information and Communication System using Vehicle during Disaster (V-HUB), of which the APT Recommendation process had been agreed to move forward with at the previous ASTAP-30 meeting, was approved as an APT Recommendation at the 41st APT Management Committee meeting held in October 2018. The voting requirement for an APT Recommendation is that a 25% majority (10 countries) of votes in favor of the Recommendation is received by member countries, and there is no opposition from 2 or more countries.

In the EG ITU-T (ITU-T Issues) session, APT member countries, including developing countries, share information and reports on the latest standardization topics, technical trends, and deliberation status in each study group (SG) of the ITU-T. All the SGs of ITU-T gave presentations this time, and APT member countries were able to share information on the current status of each SG and new issues for discussion at WTSA-20.

## 6. Future plans and issues

ASTAP is a meeting to promote standardization activities in the APT region. The ASTAP chairman is from Japan, and the Japanese delegates are office bearers in many of the WGs and EGs. The participants from NTT and Japan also play leading roles in the deliberations of technical documents. Japan is a major country in the APT; and thus, expectations and trust in Japan are extremely high. In a large-scale international standardization conference such as WTSA-20, proposals as a region rather than an individual country are often emphasized, so it is important to always show a presence in the APT region and to deepen cooperation with APT members. For ITU-T, ASTAP as well as APT preparatory meetings will be a valuable opportunity for this purpose. The next




LAN: local area network
IP: Internet protocol
VoIP: voice over IP

Fig. 2. Features of attaché case type MDRU.

APT WTSA-20 preparatory meeting will be held in April 2020, and the 32nd ASTAP meeting will be held in May or June 2020.

## Reference

[1] T. Sakano, S. Kotabe, and T. Komukai, "Overview of Movable and Deployable ICT Resource Unit Architecture," NTT Technical Review, Vol. 13, No. 5, 2015.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201505fa1.html

**Noriyuki Araki**
Senior Research Engineer, Access Network Media Project, NTT Access Network Service Systems Laboratories.

He received a B.E. and M.E. in electrical and electronic engineering from Sophia University, Tokyo, in 1993 and 1995. He joined NTT Access Network Service Systems Laboratories in 1995, where he researched and developed operation and maintenance systems for optical fiber cable networks. He has been contributing to standardization efforts in ITU-T SG6 since 2006. He was the Rapporteur of Question 6 in ITU-T SG6 from 2006 to 2008 and the Rapporteur of Question 17 in ITU-T SG15 from 2008 to 2012. He also served as the chairman of the ITU-T Focus Group on Disaster Relief Systems and Network Resilience and Recovery. He has been a vice-chair of ITU-T SG15 since 2013. He also contributes to the activities of the International Electrotechnical Commission (IEC) TC86 (Technical Committee 86: Fibre optics). He received the ITU-AJ Award from the ITU Association of Japan in 2012. He is a member of the Institute of Electronics, Information and Communication Engineers.

**Hideyuki Iwata**
General Manager, Standardization Strategy, Research and Development Planning Department, NTT.

He received a Ph.D. in electrical engineering from Yamagata University in 2011. From 1993 to 2000, he conducted research on high-density and aerial optical fiber cables at NTT Access Network Service Systems Laboratories. Since 2000, he has been responsible for standardization strategy planning for NTT research and development. He has been a delegate of IEC Subcommittee 86A (optical fiber and cable) since 1998 and of ITU-T TSAG since 2003. He is a vice-chair of the Working Group on Policy and Strategic Coordination and the Expert Group on Bridging the Standardization Gap in ASTAP. He received an award from the IEC Activities Promotion Committee of Japan in 2004, the ITU-AJ International Activity Encouragement Award in 2005, an ITU-AJ International Cooperation Award in 2012, an award for contributions to an ICT development project at the APT ICT Ministerial Meeting in 2014, the ITU-AJ Accomplishment Award in 2018, and the TTC Chairman's Prize in 2019.

# Efforts in Preventing Gas Leakage Caused by Movement of Conduit-enclosed Metallic Cables in Bridge Sections

*Technical Assistance and Support Center, NTT EAST*

**Abstract**

In this article, we introduce our efforts to prevent gas leakage caused by cable movement in conduits attached to bridges, for which no effective measures have conventionally been available. This is the fifty-fifth article in a series on telecommunication technologies.

*Keywords: metallic cable, underground conduit, closure*

## 1. Introduction

The NTT EAST Technical Assistance and Support Center is continuously working to resolve various failures of communication equipment. There have been no effective countermeasures against leakage of gas* from closures at cable connection points, which occurs when metallic cables laid in conduits in bridge sections move due to vibrations, etc. In this report, our efforts to prevent such cable movement are introduced.

## 2. Countermeasures for cable movement in underground conduits

For communication cables laid in underground conduits, a phenomenon called creeping, where the entire cable moves in conjunction with its surroundings, may occur. The following three factors are said to be related to this phenomenon:

(i) vibration caused by vehicle traffic (easily generated under a road surface frequently used by large vehicles);
(ii) inclination of underground conduits (which are prone to move downward);
(iii) ground hardness (i.e., cable movement is likely to occur in soft ground).

The cable movement puts a load on the cable inlet of the closure and causes gas leakage. Accordingly, two types of fixtures (A and B in **Photo 1** and **Fig. 1**) are attached to the cable to prevent cable movement based on the standard implementation method. These fixtures prevent movement of the cable in one direction by supporting it via the concrete wall of the manhole duct. These fixtures must be supported by a strong and stable structure (such as a concrete wall) near the underground conduit.

## 3. Issues concerning bridge sections

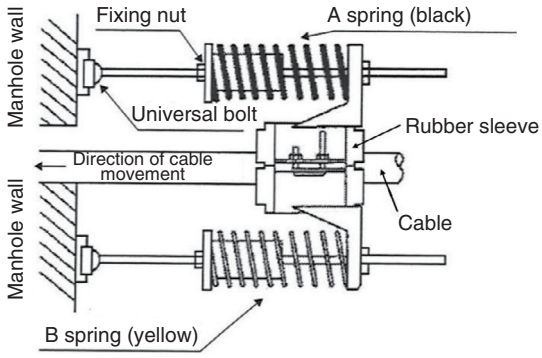
The metallic cable of a bridge section is laid in a conduit attached to the bridge (e.g., bridge floor). For

* In many underground conduits of metallic cables, dry air is constantly injected into the cable, and pressure is applied from the inside of the cable to prevent water from entering the cable and its connection points. That dry air is called *gas* hereafter.

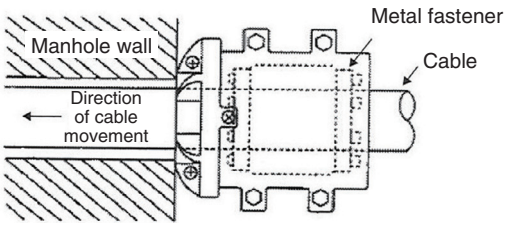
A-type cable-movement-prevention fixture
(holding force: 2000 N or less)

B-type cable-movement-prevention fixture
(holding force: 2000 to 6000 N)

Photo 1. Metal fixtures for preventing cable movement.




A-type cable-movement-prevention fixture




B-type cable-movement-prevention fixture

Fig. 1. Installation of fixtures for preventing cable movement.

long-span bridges, closures used as connection points of cables are installed at intervals of a few meters in the conduit. Even in such a bridge section, the cable moves due to vibrations caused by vehicle traffic, etc., and that movement causes gas to leak from the closure. However, strong and stable structures, such as underground manholes, do not exist in these bridge sections, and the conduit itself is not firmly fixed to the bridge; consequently, fixtures for preventing cable movement have not been used effectively.

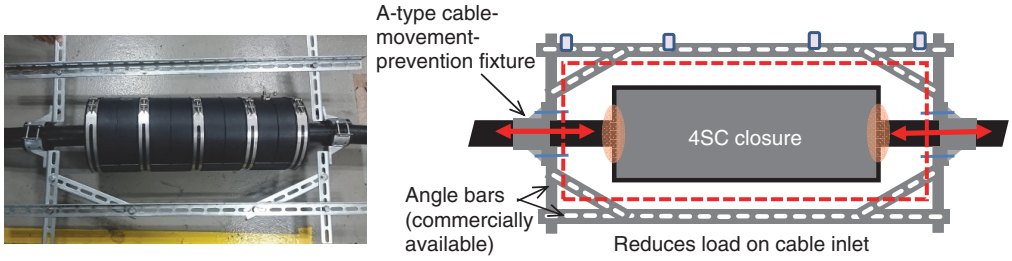
## 4. Devising countermeasure product and trials

In light of the above-described circumstances, the Technical Assistance and Support Center has devised a countermeasure product that can be used even in places where there are no rigid structures. This product (**Fig. 2**) combines an A-type cable-movement-prevention fixture (Photo 1) and commercially available angle bars. By providing cable grips at both ends of the closure, gripping the cable at regular intervals to bypass the closure, and maintaining the intervals while retaining the shape of the countermeasure product, the product is expected to reduce the load caused by cable movement on the cable inlet of the closure. We therefore installed it on an actual bridge-attached cable and subjected it to a trial.

## 5. Issues concerning countermeasure product and improvements

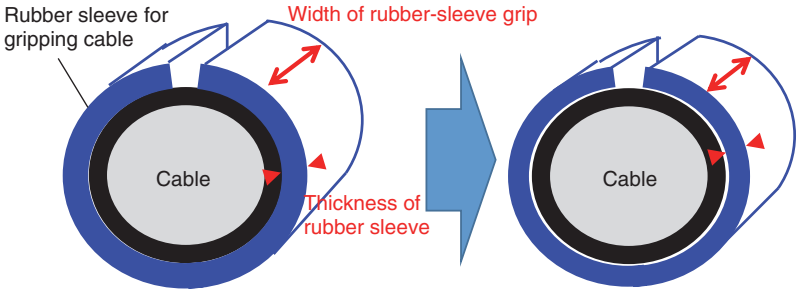
During trials in Hokkaido, where several units of the countermeasure product were installed, it was confirmed that cable movement was not prevented in winter, and after conducting a field survey and verification, the following two facts were revealed.

(1) As temperature drops, the rubber of the cable grip contracts, and the expected gripping force




| | |
|---|---|
| Strength test | Check that there is no movement of the cable or damage to the product under a load of 2000 N at air temperature of 20°C (compliant with gripping-force specification of A-type cable-movement-prevention fixture). |
| | Conduct vibration test at 10 Hz one million times to confirm that the bolts do not loosen and that the product does not rattle (compliant with the airtightness test specifications of the 4SC closure). |

Fig. 2. Appearance and structure of countermeasure product.




| Temperature | 21°C | 0°C | –10°C | –20°C | –30°C |
|---|---|---|---|---|---|
| Thickness of rubber sleeve | 8.6 mm | 8.5 mm | 8.4 mm | 8.3 mm | 8.2 mm |
| Width of rubber-sleeve grip | 75.3 mm | 75.3 mm | 75.2 mm | 75.0 mm | 74.9 mm |

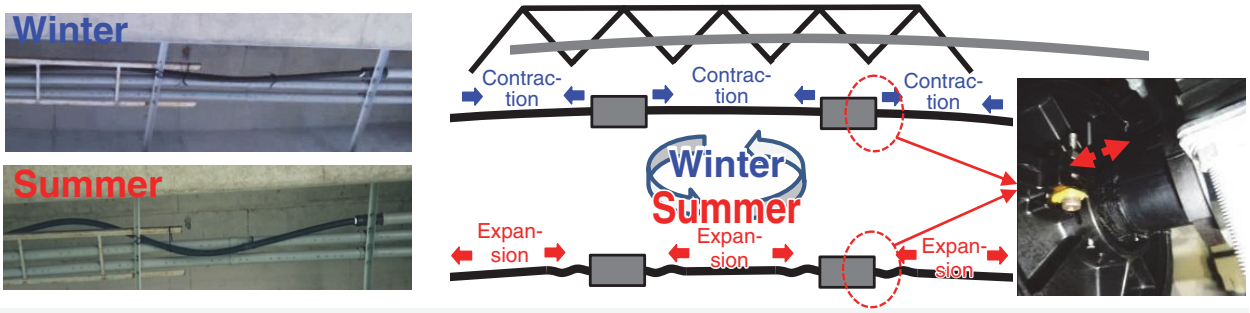
Fig. 3. Temperature drop and shrinkage of rubber sleeve for gripping cable.

cannot be maintained.

(2) The entire cable does not move, however, the cable significantly expands and contracts in places due to temperature changes.

Regarding fact (1), due to the shrinkage of the gripping material as the temperature decreases (**Fig. 3**), the gripping force decreases, the cable cannot be gripped, and the cable near the cable inlet repeatedly moves. Regarding fact (2), even at the same installation location, cable expansion and contraction are large in summer and winter and are particularly noticeable in exposed parts of the cable (i.e., cable not covered by the conduit) where the closures are installed (**Fig. 4**).

Unlike cable movement in one direction due to vibrations, expansion and contraction caused by this temperature change is repeated in both directions. It is estimated that it is highly likely that gas leaks owing to the increased load on the cable inlet of the closure are caused by the cable entering and exiting the inlet. Therefore, to cope with expansion and contraction due to low temperature or temperature change, two A-type cable-movement-prevention fixtures for gripping were combined (**Fig. 5**), and a trial is being continued to evaluate the following improvement, namely, increasing the gripping area to ensure that a constant gripping force is maintained even if the gripping material contracts.




Notes: Estimated expansion and contraction of cable-jacket material (low-density polyethylene)
$\Delta L$ (expansion/contraction) = $\alpha$ [$10^{-6}$/°C] (thermal-expansion coefficient) × $\Delta T$ (temperature change) × L (length)
Low-density polyethylene coefficient (170) × 40°C × connection point (200 m) = 136 cm
*Friction in conduits is not taken into account.

Fig. 4. Expansion/contraction of cables installed at the same location.

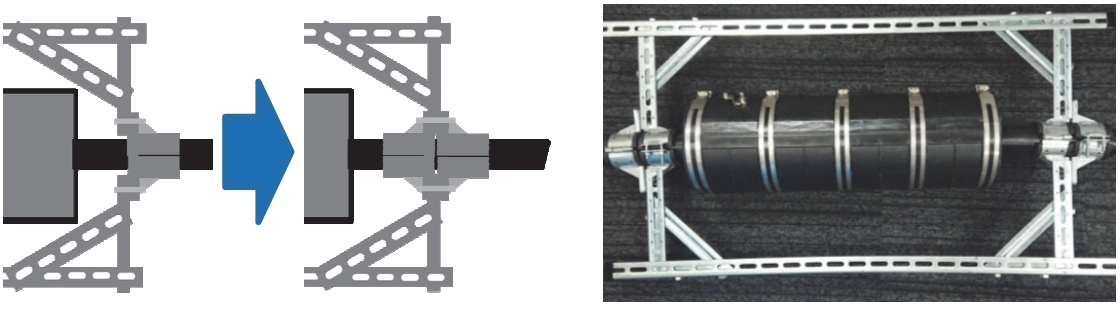


Fig. 5. Gripping area expanded by combining two A-type cable movement-prevention fixtures.

## 6. Future efforts

Five units of the improved countermeasure product fixture were installed in 2018 (in two locations and more installed in 2019), and we will continue to check their functionality, durability, and safety while monitoring changes in temperature throughout the years.

We also aim to reduce weight and improve workability of the improved countermeasure product by unifying several components into a single unit and thereby reducing the number of bolted parts to ensure its popularization while planning to create an installation manual to instruct maintenance personnel on how to install this product.

## 7. Concluding remarks

In this article, we introduced our efforts to prevent gas leakage caused by cable movement in bridge sections, for which no effective measures have conventionally been available. This countermeasure is aimed at reducing maintenance operations that have always been difficult to handle and avoiding having to renew cables in the said sections. This will contribute to reducing metallic cable investment and maintenance costs. The Technical Assistance and Support Center will continue promoting efforts to improve the reliability of communication facilities and reduce failures on the basis of our accumulated knowledge and experience as well as application of new technologies.

# Opening Ceremony of NTT Research, Inc.

*Atsuyuki Muramoto*
*Research and Development Planning Department, NTT*

**Abstract**
NTT and NTT Research, Inc. held a ceremony to open NTT Research, Inc. in the suburbs of Palo Alto, California, USA, on July 8, 2019. This article describes what took place at the ceremony.

*Keywords: global, security, quantum*

## 1. Introduction

The opening ceremony of NTT Research, Inc. was attended by about 280 people, including customers of NTT Group companies, analysts, people from academia worldwide, business partner enterprises, and representatives of the press and the U.S. government. The event offered an overview of the future activities of NTT Research, Inc., which was founded on April 1, 2019, and the three laboratories newly established within it (**Photos 1** and **2**).

## 2. Address by NTT president and chief executive officer (CEO)

NTT President and CEO Jun Sawada started his address by explaining the intention behind the founding of NTT Research, Inc. (**Photo 3**). The NTT Group has the vision of being *Your Value Partner* and aims to resolve global social issues through collaboration with various partners. For this purpose, it considers human resources as central to its activities and has selected *connect*, *trust*, and *integrity* as shared


Photo 1. The event took place at Rosewood Sand Hill in Menlo Park.

Photo 2. Inside the venue.


Photo 3. Jun Sawada, President and CEO, NTT.

Photo 4. Kazuhiro Gomi, President and CEO, NTT Research, Inc.

values for its employees. To achieve *One NTT*, the group is pressing ahead with its four initiatives: full stack/advisory, integrated solutions IT (information technology) as a service, disruptive innovation, and next-generation innovation. As part of its initiative in disruption innovation, it founded NTT Research, Inc., through which it will promote research and development (R&D) that will transform the world and strengthen basic research at global sites. Starting with the establishment of NTT Research, Inc. in Silicon Valley, the NTT Group intends to expand its R&D base to other areas, including Munich and Boston.

President Sawada said that the NTT Group is striving to achieve a *natural world* in which anyone can benefit from technology without conscious effort and that to achieve such a world, the group embraces a next-generation vision, called Innovative Optical and Wireless Network (IOWN). The vision consists of three elements: *an all-photonic network*, which features low power consumption, high quality/high capacity, and low latency; *digital twin computing*, which creates new value by synthesizing the digital twins of humans and objects; and *cognitive foundation*, which optimally combines requirements from a variety of ICT (information and communication technology) resources and centrally manages their configurations. His address ended to resounding applause.

## 3. Address by NTT Research, Inc. president and CEO

The address by NTT Research, Inc. President and CEO Kazuhiro Gomi began with a presentation of the vision of NTT Research, Inc. (**Photo 4**).

To rapidly expand its global business in collaboration with its global partner enterprises and global human resources, NTT needs to support this expansion from the R&D side. The starting point is here in Silicon Valley. NTT Research, Inc. has already recruited top researchers in the U.S. It also has access to research results from Japan obtained by NTT R&D. It additionally works with global partners. The output of NTT Research, Inc. will be produced by integrating all of these and is intended to help create a better world together with its valued partners.

President Gomi then described the three research areas that will be the focus of NTT Research, Inc. He used *digital twin computing*, introduced by President Sawada, as an example. When *bio digital twin computing*, which is an extension of the former concept, becomes a reality, it may become possible to simulate what will soon happen to one's cyberspace avatar, thereby predicting that one will suffer an illness within, say, the next three weeks. He added that NTT Research, Inc. focuses on three technologies that are needed to bring about such innovation: quantum computing, secure computing, and medical informatics. This is the reason three laboratories have been established within it. He then introduced Director Yoshihisa Yamamoto of the Physics & Informatics Laboratories, Director Tatsuaki Okamoto of the Cryptography & Information Security Laboratories, and Director Hitonobu Tomoike of the Medical & Health Informatics Laboratories.

Besides NTT Research, Inc., which focuses on basic research, the NTT Group's innovation portfolio includes two more organizations newly established abroad. NTT Disruption concentrates on showcasing

Photo 5. Some NTT R&D results were exhibited.

the digital transformations likely to reach the market in the near future. NTT Venture Capital looks for investment partners for startups. He concluded his address by saying that together with those in the audience, "The world will be as one," citing the lyrics of John Lennon's 'Imagine.'

## 4. Presentations by guest speakers and a concert

There were guest lectures by Professor Kathryn Moler from Stanford University and Dr. Rupak Biswas from NASA's Ames Research Center. Lectures were also given by Professor Robert L. Byer from Stanford University, who is also a researcher at NTT Research, Inc., and Dr. Brent Waters, who has moved to NTT Research, Inc. from a professorship at the University of Texas.

After the lectures, violinist Ryu Goto gave a special performance to enliven the ceremony. In addition, NTT's optical Ising machine, LASOLV™, and a fabric that when worn as a shirt—known as hitoe™—can collect biosignals from the body, were exhibited, and the activities of the Cryptography & Information Security Laboratories and the Medical & Health Informatics Laboratories were introduced on display panels at the venue (**Photo 5**). The ceremony was followed by free time for social interaction by attendees and guests.

## 5. Conclusion

A large number of senior members of enterprises and academia attended the ceremony, indicating their high expectations of the NTT Group in the coming years. NTT Research, Inc. will accelerate its R&D from Silicon Valley, to respond to valuable opinions and requests given by the guests, support global business and global partners, and contribute to creating a better world in collaboration with them.

# External Awards

### Distinguished Service Award
**Winner:** Hideki Maeda, NTT Network Service Systems Laboratories
**Date:** September 11, 2019
**Organization:** The Institute of Electronics, Information and Communication Engineers (IEICE)

For his distinguished services for planning and operations in Communications Society.

### Female Analyst Award
**Winner:** Yuko Ueno, NTT Basic Research Laboratories
**Date:** September 12, 2019
**Organization:** The Japan Society for Analytical Chemistry

For her research on the creation of molecular recognition functional materials and their application to microanalysis.

### Young Scientist Presentation Award
**Winner:** Hiroki Miyazako, NTT Basic Research Laboratories
**Date:** September 18, 2019
**Organization:** The Japan Society of Applied Physics

For "Directed Aggregation of Cardiomyocytes by Topographical Guides in Co-culture System."
**Published as:** H. Miyazako, T. Teshima, and Y. Ueno, "Directed Aggregation of Cardiomyocytes by Topographical Guides in Co-culture System," The 66th JSAP Spring Meeting 2019, Tokyo, Japan, Mar. 2019.

### Young Scientist Presentation Award
**Winner:** Yuki K. Wakabayashi, NTT Basic Research Laboratories
**Date:** September 18, 2019
**Organization:** The Japan Society of Applied Physics

For "$J_{eff}$=3/2 Ferromagnetic Insulating State above 1000 K in a Double Perovskite Osmate $Sr_3OsO_6$."
**Published as:** Y. K. Wakabayashi, Y. Krockenberger, N. Tsujimoto, T. Boykin, S. Tsuneyuki, Y. Taniyasu, and H. Yamamoto, "$J_{eff}$=3/2 Ferromagnetic Insulating State above 1000 K in a Double Perovskite Osmate $Sr_3OsO_6$," The 80th JSAP Autumn Meeting 2019, Sapporo, Japan, Sept. 2019.

### Outstanding Paper Award
**Winner:** Munekazu Date, Shinya Shimizu, and Hideaki Kimata, NTT Media Intelligence Laboratories
**Date:** September 19, 2019
**Organization:** 3D-Conf

For "Table-top Photographic-image 3D Display Using Visually Equivalent Light Field 3D."
**Published as:** M. Date, S. Shimizu, and H. Kimata, "Table-top Photographic-image 3D Display Using Visually Equivalent Light Field 3D," Proc. of 3D-Conf, P-2, Kanagawa, Japan, July 2019.

### Best Paper Award
**Winner:** Toshiaki Miyazaki, The University of Aizu; Kazuya Anazawa, NTT Network Innovation Laboratories; Yasuyuki Maruyama, Seiya Kobayashi, Toku Segawa, Peng Li, The University of Aizu
**Date:** October 2, 2019
**Organization:** The Luxembourg Institute of Science and Technology (LIST)

For "Resilient Information Management for Information Sharing in Disaster-affected Areas Lacking Internet Access."
**Published as:** T. Miyazaki, K. Anazawa, Y. Maruyama, S. Kobayashi, T. Segawa, and P. Li, "Resilient Information Management for Information Sharing in Disaster-affected Areas Lacking Internet Access," The 18th International Conference on Ad Hoc Networks and Wireless (AdHoc-Now 2019), Luxembourg, Oct. 2019.

### Industrial Standardization Merit Award
**Winner:** Seishi Takamura, NTT Media Intelligence Laboratories
**Date:** October 8, 2019
**Organization:** Ministry of Economy, Trade and Industry

For his technical contribution to and leadership in standardization efforts in ISO/IEC JTC 1/SC 29 (International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1/Subcommittee 29)—Coding of audio, picture, multimedia, and hypermedia information.

# Papers Published in Technical Journals and Conference Proceedings

### Experimental Evaluation of WaveRNN Predictor for Audio Lossless Coding

S. Amada, R. Sugiura, Y. Kamamoto, N. Harada, T. Moriya, T. Yamada, and S. Makino

Proc. of the 2019 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP2019), pp. 315–318, Honolulu, HI, USA, March 2019.

This paper describes a new scheme of speech and audio lossless coding. MPEG-4 Audio Lossless Coding (ALS) is the international standard lossless compression scheme of audio signals. It uses linear predictor and compresses the signal by converting the signal into information such as prediction residuals and prediction coefficients. In the compressed signal with MPEG-4 ALS, the prediction residuals occupy a large amount of such information. Improving the performance of the predictor is directly related to improving compression performance. Using non-linear predictors in lossless coding may enable flexible prediction and improve prediction performance. A WaveRNN is a deep neural network performing non-linear prediction. The output of a WaveRNN is the predicted probability distribution of the target sample. Arithmetic coding can generate an optimal code for a set of arbitrary symbols and probabilities. A WaveRNN is trained to minimize the bitrate after encoding when using arithmetic coding for the output of the WaveRNN. This paper proposes a scheme of speech and audio lossless coding that combines a WaveRNN with arithmetic coding. Experimental evaluation confirmed that the proposed scheme reduced the number of bits by around 0.7 bits per sample compared to MPEG-4 ALS in speech coding. DNN-based speech and audio coding techniques are expected to transcend the international standard technologies.

### Pilot Study on Semi-automated Patch Diffing by Applying Machine-learning Techniques

A. Nakajima

Proc. of ROOTCON 13, Tagaytay, The Philippines, September 2019.

When developing a 1-day exploit code, patch diffing (binary diffing) is one of the major techniques to identify the part of the code to which security fixes are applied. This technique is well-known among reverse engineers; thus, to support diffing, various tools such as BinDiff, TurboDiff, and Diaphora have been developed. Although these tools effectively support analysis, patch diffing is still difficult because it requires extensive knowledge and experience. To address this issue, we conducted a pilot study to achieve semi-automated patch diffing by applying machine-learning techniques. Based on the hypothesis that "similar types of vulnerabilities will be fixed in a similar manner," we applied an unsupervised machine-learning technique to extract patterns and considered an approach to achieve semi-automated patch diffing. In the talk, we will give details of our pilot study and share the insights that we have gained. We believe that our insights will help other researchers conduct similar research in the future.

### Shape Control of Discrete Generalized Gaussian Distributions for Frequency-domain Audio Coding

R. Sugiura, Y. Kamamoto, and T. Moriya

IEEE/ACM Trans. Audio, Speech, Language Process., October 2019.

Entropy coding, which is an essential component of audio compression, is required to manage the tradeoffs between compression efficiency and computational complexity, and the strategy to achieve entropy coding highly depends on the distributions of inputs. We present a coder for controlling distributions of input numbers to enhance the compression efficiency of Golomb-Rice (GR) encoding, one of the simplest entropy coding methods optimal for Laplacian distributions. We argue that the proposed coder enables GR encoding to assign nearly the optimal code length for a wider range of distributions, generalize Gaussian distributions, and maintain low computational cost. A simulation using random numbers revealed that the proposed coder works about 6 times faster than the state-of-the-art arithmetic coder for Gaussian-distributed integers by maintaining the increase in relative redundancy to around 2.6%, which is much lower than that of a conventional GR coder. We also present an application of our coder to a practical speech and audio coding scheme. An objective evaluation for real speech and audio signals confirms the advantages of the proposed coder in compression. This coder is expected to widen the capability of low-complexity entropy coding, providing us with more flexible codec designs.

### Quantum Key Distribution with Simply Characterized Light Sources

A. Mizutani, T. Sasaki, Y. Takeuchi, K. Tamaki, and M. Koashi

npj Quantum Information, Vol. 5, Article no. 87, October 2019.

To guarantee the security of quantum key distribution (QKD), security proofs of QKD protocols have assumptions on devices. Commonly used assumptions are, for example, each random bit of information chosen by a sender needs to be precisely encoded on an optical emitted pulse and the photon-number probability distribution of the pulse needs to be precisely known. These typical assumptions imposed on such light sources are rather strong and would be difficult to verify in practical QKD systems. Our goal was to replace those strong assumptions on light sources with weaker ones. We adopted the differential-phase-shift (DPS) QKD protocol and drastically reduced the requirements on light sources, while assuming trusted and photon-number-resolving detectors for the measurement unit. Specifically, we only assume the independence among emitted pulses, independence of the vacuum emission probability from a chosen bit, and upper bounds on the tail distribution function of the total photon number in a single block of pulses for single, two, and three photons. Notably, no other detailed characterizations, such as the amount of phase modulation, are required. Our security proof significantly relaxes the demands for light sources, which paves the way to guarantee implementation security with simple verification of devices.

### Understanding Community Structure in Layered Neural Networks

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

Neurocomputing, Vol. 367, pp. 84–102, November 2019.

A layered neural network is now one of the most common choices for predicting high-dimensional practical data sets, where the relationship between input and output data is complex and cannot be represented well with simple conventional models. This network's effectiveness has been shown in various tasks, such as image recognition and natural language processing; however, the lack of interpretability of the trained result by such a network has limited its application area. In our previous studies, we proposed methods for extracting a simplified global structure of a trained layered neural network by applying a network analysis method and classifying the units into communities according to their connection patterns with adjacent layers. These methods provided us with knowledge about the strength of the relationship between communities from the existence of bundled connections, which are determined by the threshold processing of the connection ratio between pairs of communities. However, it has been difficult to precisely understand the role of each community by observing the resulting modular structure with these previous methods. We could only determine to which sets of the input and output dimensions each community was mainly connected by tracing the bundled connections from the community to the input and output layers. Another problem is that the finally obtained modular structure is highly dependent on the setting of the threshold hyperparameter used for determining bundled connections, leading to a different result to the discussion about the role of each community. We propose a method called Community Analysis for Modular Neural Networks (CA-MNN) for quantitatively interpreting the role of each community regarding inference, which we extracted using our previously reported methods, by defining the effect of each input dimension on a community and the effect of a community on each output dimension. We experimentally show that CA-MNN can reveal the role of each component of a layered neural network by applying the neural networks to three types of data sets, extracting communities from the trained network, and applying CA-MNN to the community structure.