# NTT Technical Review

5
2018

May 2018 Vol. 16 No. 5

# NTT Technical Review

## May 2018 Vol. 16 No. 5

### Feature Articles: NTT Group Security Confronts Escalating Cyberattacks

- Research and Development of Advanced Security Measures to Protect Customers from Sophisticated and Large-scale Cyberattacks
- Collecting, Analyzing, and Leveraging Threat Intelligence at NTT-CERT
- Security Business Solutions for Customer Needs
- Cyberattack Countermeasure Technology to Support NTT’s Security Business

### Regular Articles

- Digital-preprocessed Analog-multiplexed Digital-to-analog Converter for Ultrahigh-speed Optical Transmitter
- Satellite Communications Modem Unit *COM-U*—Enhanced Maintenance, Operations, and Spectrum Utilization Efficiency of Satellite Transponders for Remote Island Satellite Communications and Disaster Relief Satellite Communications

### Global Standardization Activities

- Trends in Standardization of Blockchain Technology by ISO/TC 307

### Information

- Report on NTT R&D Forum 2018

### Short Reports

- Japan-Taiwan Joint Experiment Successfully Demonstrates White-box Based Carrier-grade Networking—International Service Provider Collaboration in Software-defined Networking Pushes Forward IP Packet Transport to Employ Commodity Products

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

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

# Research and Development of Advanced Security Measures to Protect Customers from Sophisticated and Large-scale Cyberattacks

*Kazuhiko Okubo*

## Abstract

The Feature Articles in this issue introduce recent trends and case studies of ever-escalating cyberattacks that are becoming increasingly sophisticated and large in scale, plus issues and needs in the security business of NTT Group companies. Additionally, new needs are arising for security measures for customers. These articles introduce the research and development of advanced technologies deemed necessary for countering cyberattacks and increasing business competitiveness.

*Keywords: security, cyberattack, MSS*

## 1. Changing environment in cyberspace and need for new security measures

Security threats continue to escalate due to a variety of factors. For example, cyberattack techniques are becoming increasingly sophisticated as reflected by malware with enhanced capabilities for autonomous operation. In addition, as Internet of Things (IoT) devices come to be connected in large numbers to the network despite their inherent vulnerability to security threats, large-scale distributed denial-of-service (DDoS) attacks are being carried out, with those devices used as stepping stones in their operation. Against this background, the need naturally arises for more advanced cyberattack countermeasure technologies, but there is also a need for technologies that can combat new types of security threats given the paradigm shift in the information and communication technology (ICT) environment accompanying the evolution of economic activity.

Furthermore, with Tokyo's major international sports event only about two years away, there are grave concerns about an increase in security threats against critical infrastructures and having insufficient measures to prevent and respond to incidents. Consequently, the development of technologies for securing critical infrastructures, the enhancement of comprehensive security risk management, and the development of more efficient security operations through the introduction of artificial intelligence are becoming urgent issues.

Moreover, in addition to the above *defensive* security, there is a growing need for so-called *offensive* security. This refers to the safe and secure use of data in business activities in the IoT era against the backdrop of the Japanese amended Act on the Protection of Personal Information enacted in May 2017. As a result, initiatives for avoiding risk using information security technologies including encryption and for creating new value toward economic revitalization hold great promise.

Against the background of such changes in the cyber environment and current market needs, NTT Secure Platform Laboratories has established four

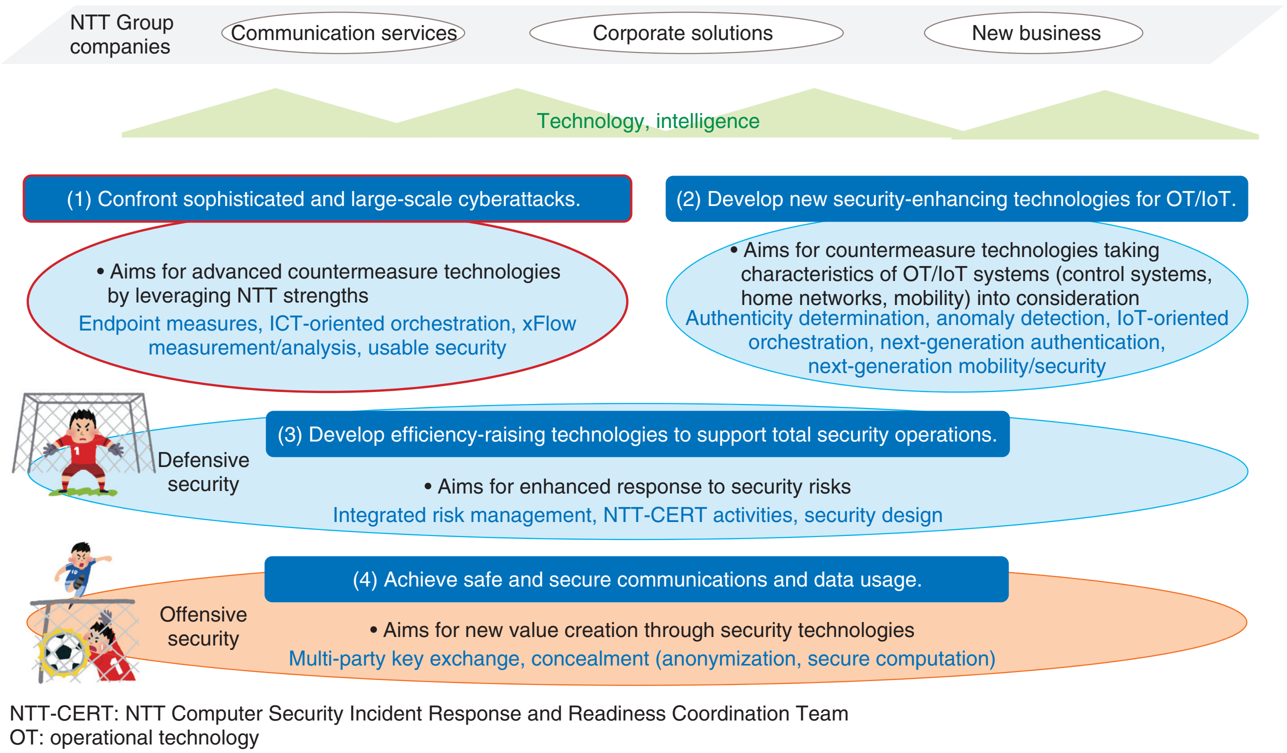

NTT Group companies
Communication services
Corporate solutions
New business
Technology, intelligence
(1) Confront sophisticated and large-scale cyberattacks.
• Aims for advanced countermeasure technologies by leveraging NTT strengths
Endpoint measures, ICT-oriented orchestration, xFlow measurement/analysis, usable security
(2) Develop new security-enhancing technologies for OT/IoT.
• Aims for countermeasure technologies taking characteristics of OT/IoT systems (control systems, home networks, mobility) into consideration
Authenticity determination, anomaly detection, IoT-oriented orchestration, next-generation authentication, next-generation mobility/security
Defensive security
(3) Develop efficiency-raising technologies to support total security operations.
• Aims for enhanced response to security risks
Integrated risk management, NTT-CERT activities, security design
Offensive security
(4) Achieve safe and secure communications and data usage.
• Aims for new value creation through security technologies
Multi-party key exchange, concealment (anonymization, secure computation)
NTT-CERT: NTT Computer Security Incident Response and Readiness Coordination Team
OT: operational technology

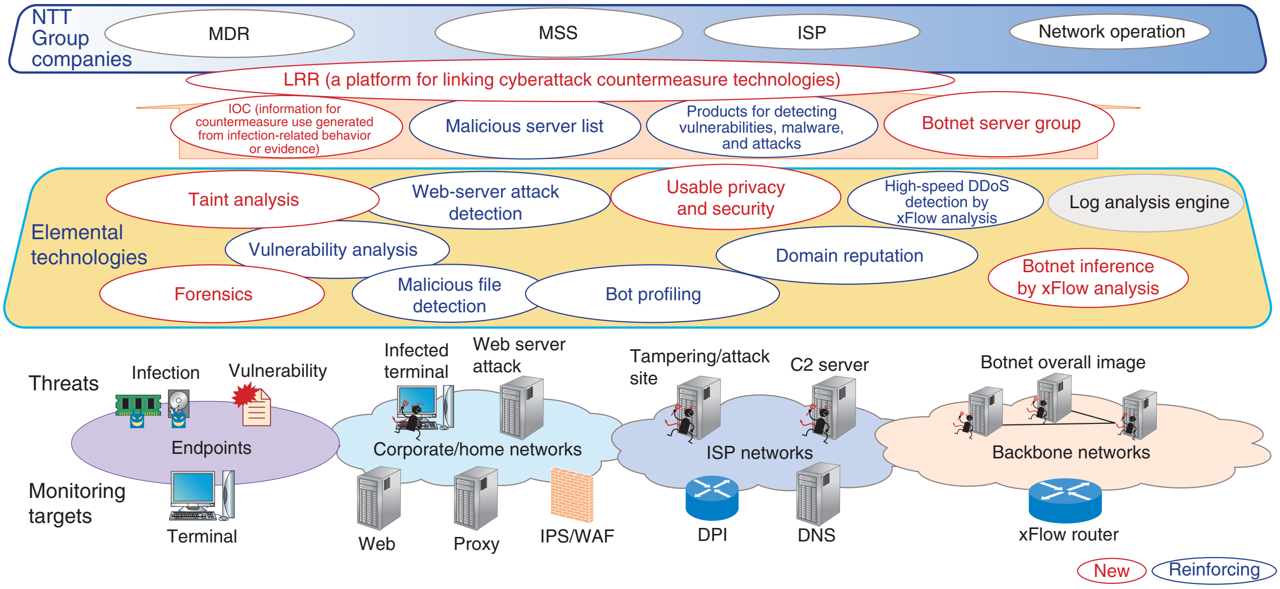
Fig. 1. Total view of security R&D.

objectives representing the pillars of its research and development (R&D) activities (**Fig. 1**). These are: (1) confront sophisticated and large-scale cyberattacks, (2) develop new security-enhancing technologies for operational technology (OT)/IoT, (3) develop efficiency-raising technologies to support total security operations, and (4) achieve safe and secure communications and data usage. Recent progress in pillars (2)–(4) was described in a previous publication [1]. Therefore, the Feature Articles in this issue focus on pillar (1) technologies for countering cyberattacks. We introduce, in particular, trends in security threats, issues and needs in business, as well as cutting-edge R&D activities to provide solutions [2–4].

## 2. Solutions in response to customers' security needs

In August 2016, NTT established NTT Security to roll out worldwide consulting and managed security services (MSS). NTT Security brings together security experts, advanced analysis platforms, threat information, and specialized technologies in the NTT Group to gain a competitive advantage and achieve efficient security operations. Since its establishment, NTT Group companies, including Dimension Data, NTT Communications, and NTT DATA have been implementing domestically and internationally total solutions incorporating advanced technologies and services provided by NTT Security.

In the field of corporate risk management, importance is increasingly being placed on OT security measures for securing a business continuity plan in addition to conventional information technology (IT) security measures for protecting information assets. Given these current conditions, NTT Security has started providing security services for defending critical infrastructures such as factories, plants, power systems, and medical institutions. These include (1) consulting services that provide visualization of the components making up an industrial control system and their intrinsic risk, plus associated security measures, and (2) IT/OT integrated security services based on MSS for continuous monitoring of an industrial control network to detect, analyze, and immediately block cyberattacks.



C2 server: C&C (command and control) server
DNS: domain name system
DPI: deep packet inspection
IOC: indicators of compromise
IPS: intrusion prevention system
ISP: Internet service provider
MDR: managed detection and response
WAF: web application firewall

Fig. 2. Dealing with sophisticated and large-scale cyberattacks.

## 3. R&D of cyberattack countermeasure technologies for increasing competitiveness in security business

Cyberattacks are becoming increasingly sophisticated and large in scale, and more research needs to be done in order to develop technologies to cope with these attacks. At NTT Secure Platform Laboratories, the technologies now being focused on are categorized into *new technology* for providing new countermeasures to security threats and *reinforcing technology* for improving the effectiveness of existing countermeasure technologies. These technologies are outlined in **Fig. 2**.

Up to now, the monitoring targets in the case of defensive security have mostly been corporate and home networks and Internet service provider networks. However, to upgrade countermeasure technologies in order to keep up with the increasingly sophisticated and large-scale cyberattacks, monitoring targets must be expanded to include endpoints and backbone networks, and new technologies must be created with attention given even to the behavior and psychology of users exposed to a cyberattack.

Two examples of new technologies taken up by NTT Secure Platform Laboratories are taint analysis[*1] and forensics[*2]. These are elemental technologies used for generating indicators of compromise, which are used, in turn, as an aid in detecting endpoint infections and identifying tracks and evidence after an infection.

Additionally, analyzing flow[*3] in the backbone network will make it possible to detect a botnet master and infer the server group making up a botnet. This technology will enable security threats to critical infrastructures to be dealt with appropriately.

It will also become possible to detect elaborately designed cyberattacks that depend on user behavior and psychology through a new technique called *usable privacy and security* that has recently become a topic of interest worldwide. This technique, which is the outcome of interdisciplinary research not restricted to technology, efficiently achieves security and privacy protection together with high usability.

[*1] Taint analysis: A technique for analyzing the dependency between data by propagating a tag set in an item of data according to rules.

[*2] Forensics: Analysis of digital information and techniques for doing so with the aim of uncovering the causes of an incident, discovering evidence, etc.

[*3] Flow: A session identified by the combination of TCP (Transmission Control Protocol), UDP (User Datagram Protocol), or ICMP (Internet Control Message Protocol) destination/source Internet protocol addresses and port numbers.

## References

[1] "Feature Articles: Security Concerns—Growing Threats and Business Opportunities," NTT Technical Review, Vol. 15, No. 5, 2017.
https://www.ntt-review.jp/archive/2017/201705.html

[2] S. Konno, "Collecting, Analyzing, and Leveraging Threat Intelligence at NTT-CERT," NTT Technical Review, Vol. 16, No. 5, 2018.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201805fa2.html

[3] K. Matsuda, Y. Nagatake, F. Takeuchi, and K. Yozawa, "Security Business Solutions for Customer Needs," NTT Technical Review, Vol. 16, No. 5, 2018.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201805fa3.html

[4] T. Hariu, D. Chiba, M. Akiyama, T. Yagi, Y. Kawakoya, Y. Nagafuchi, and T. Koyama, "Cyberattack Countermeasure Technology to Support NTT's Security Business," NTT Technical Review, Vol. 16, No. 5, 2018.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201805fa4.html

**Kazuhiko Okubo**

Vice President and Head of NTT Secure Platform Laboratories.

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

# Collecting, Analyzing, and Leveraging Threat Intelligence at NTT-CERT

*Shunichi Konno*

**Abstract**

The use of threat intelligence is progressing in corporate-based security frameworks typified by computer security incident response teams (CSIRTs) in order to defend networks and systems against increasingly sophisticated cyberattacks. It is becoming necessary to obtain a deeper understanding of threat intelligence and to deal with more advanced forms of such information. This article presents an analysis of attacker motivation using threat intelligence. The usefulness of threat intelligence in actual on-site CSIRT activities is also explained.

*Keywords: NTT-CERT, CSIRT, threat intelligence*

## 1. Introduction to NTT-CERT

The NTT Computer Security Incident Response and Readiness Coordination Team (NTT-CERT) is involved in various activities associated with computer security incidents within the NTT Group as a computer security incident response team (CSIRT) in the NTT laboratories [1]. These activities include response, analysis, education and monitoring, and research and development (R&D) and were initiated on October 1, 2004, within NTT Information Sharing Platform Laboratories, the predecessor to NTT Secure Platform Laboratories. NTT-CERT is a member of the Forum of Incident Response and Security Teams (FIRST)* and a founding member of the Nippon CSIRT Association. It is involved in a variety of initiatives in conjunction with CSIRTs and security teams inside and outside NTT. The parent organization of NTT-CERT was moved to NTT Secure Platform Laboratories on April 1, 2012.

NTT-CERT has the following functions in its diverse activities in the NTT laboratories:

(1) Acts as an R&D organization for disseminating know-how and tools to NTT Group companies and customers based on its history of setting up and operating an advanced CSIRT in the NTT Group

(2) As the representative CSIRT in the NTT Group, serves as a point of contact for outside CSIRTs who wish to access the NTT Group

(3) Extracts needs from the field, feeds them back to the NTT laboratories, and conducts trial applications of research deliverables

With the huge scale of the NTT Group, NTT-CERT on its own is unable to provide technical support for all of the diverse incidents that occur within the group. There are presently more than ten CSIRTs within the NTT Group companies, all of which work in collaboration to prevent incidents and to minimize any incident-related damage.

## 2. Threat intelligence and CSIRT

Various types of information can be called *threat intelligence*. Simple examples are the source IP (Internet protocol) address of an attack observed in the past, characteristic character strings in transmissions at the time of an attack, and the targets of

* FIRST: An international confederation of CSIRTs and security teams founded by 11 organizations in 1990 as a framework spanning organizations, countries, and regions.

transmissions from a host infected with malware. There is also threat intelligence that compiles a series of attacks as a cyberattack campaign or that draws a correlation between an attack and a political event such as an election. In any case, threat intelligence constitutes knowledge extracted and processed in a variety of stages from basic data such as a network log in order to determine whether a threat is being posed to the recipient. For this reason, NTT-CERT devotes its efforts to analyzing and integrating a wide array of threat intelligence.

The main roles of a CSIRT are to provide security quality management services, proactive services, and reactive services [2]. In quality management, a CSIRT is involved in such activities as risk analysis, security consulting, and education, but the use of threat intelligence can improve the quality of quality management activities themselves. For example, analyzing the risk to one's company's security based on threat intelligence that has been obtained and reporting the analysis results to corporate management can produce a steering effect from the management layer. Here, to prevent this risk analysis from becoming just a *pie in the sky*, or an illusion, it is important that threat intelligence obtained from multiple routes be compared with examples of past incidents and with homemade threat intelligence obtained from Internet sensors and other sources to improve its reliability.

Threat intelligence used in quality management activities can also be useful in proactive services before the occurrence of incidents. For example, in addition to using it in filtering to prevent incidents from happening in the first place, threat intelligence can be used as input in efforts to hunt for undetected attacks in large volumes of log data.

## 3. Examples of using threat intelligence in reactive services: cyberattacks and motivation

Threat intelligence can also be quite useful in CSIRT reactive services if an incident should actually occur since it can facilitate a response to a sophisticated cyberattack and make incident response more efficient.

Cyberattacks are motivated for various reasons. Paolo Passeri, a Solutions Architect at Netskope, investigated the motivations for cyberattacks that occurred worldwide in 2016 as a percentage of incidents using the results of cyberattack analysis released by HACKMAGEDDON [3]. The results are given in **Fig. 1**.

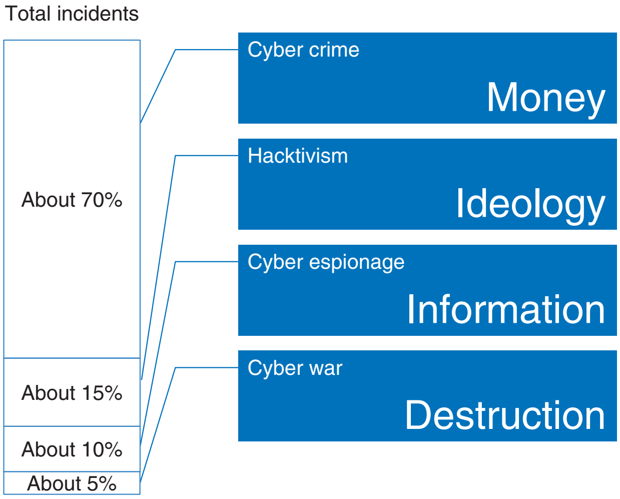


Fig. 1. Motivation behind cyberattacks.

(1) Cyber crime

The highest number of incidents falls within the category of cyber crime, at about 70% of all incidents. In general, these are attacks motivated by money. Ransomware such as WannaCry and NotPetya, which caused major issues in 2017, achieves the attacker's purpose by using encryption to make it difficult to read the content of the infected computer and intimidating the owner to pay a ransom to free up the data. In addition to ransomware, there are examples where money is demanded in the form of blackmail denial-of-service (DoS) attacks directed at Internet businesses whose continuous operation constitutes a lifeline. For example, an Internet-based foreign-exchange operator would be unable to profit from commissions if its website services came to a halt as a result of a DoS attack. Such an outcome would be a major blow to business.

(2) Hacktivism

The second type of motivation is hacktivism, accounting for about 15% of all incidents. This type of attack is carried out to proclaim the attacker's ideology. It may take the form of defacement of a website to display messages from the attacker or obstruction of the cyberspace activities of an organization at odds with the attacker's way of thinking. In Japan, well-known attacks of this type are associated with memorial days such as the *9/18 attack* that is mounted around September 18 every year recalling the Manchurian Incident of 1931. In addition, elements within the worldwide hacktivist group Anonymous have halted the website services of certain aquariums

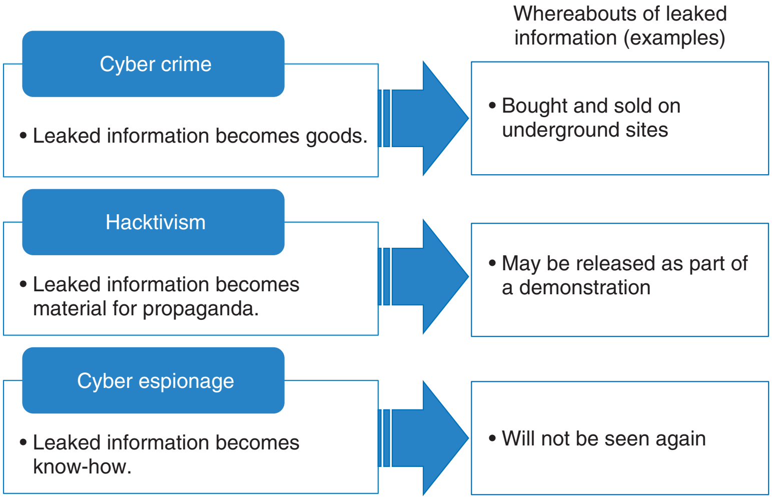

Whereabouts of leaked information (examples)
Cyber crime
• Leaked information becomes goods.
• Bought and sold on underground sites
Hacktivism
• Leaked information becomes material for propaganda.
• May be released as part of a demonstration
Cyber espionage
• Leaked information becomes know-how.
• Will not be seen again

Fig. 2. Whereabouts of leaked information.

by mounting a series of attacks as an operation called OpKillingBay, leveraging the strong opposition to dolphin hunting in Japan.

(3) Cyber espionage

The third type of motivation is cyber espionage, accounting for about 10% of all incidents. As the word *espionage* implies, this type of attack attempts to surreptitiously steal information. While the number of incidents of this type of attack is only one-seventh that of cyber crime, such attacks may involve the stealing of design information on developed products or equipment, so they cannot be disparaged simply because of the low number of incidents. One feature of this type of attack is that the victim may be completely unaware of the attack.

(4) Cyber war

The fourth type of motivation is cyber war, accounting for about 5% of all incidents. The purpose of such an attack is destruction of critical infrastructures. Such an attack, if mounted, could have a major impact on society.

In the above way, collecting examples of past attacks is advancing the analysis of attackers throughout the world, and accumulating information on TTP (tactics, techniques, and procedures), on attacker tools, and on evidence of attacks is proving useful for responding to incidents within a CSIRT.

## 4. Attacker motivation and CSIRT activities

Attacker analysis can also be important in cases where a CSIRT conducts a survey to determine how an organization's roster leaked to the outside may be used for malicious means. Even for incidents in which the same kind of information has been leaked, for example, a roster from company A and a roster from company B, the whereabouts of that leaked information may be completely different depending on the attacker's motivation (**Fig. 2**).

For an incident suspected of being a cyber crime, the leaked information may come to be bought and sold on underground sites on a darknet. In such cases, a CSIRT will conduct an investigation of underground spaces.

For an incident motivated by hacktivism, there should be concern that the leaked information could be leaked to the world as propaganda in support of the attacker's ideology.

Meanwhile, for an incident motivated by cyber espionage, a survey conducted by a CSIRT will often come to a dead end. For an attacker involved in cyber espionage, the stolen information is the embodiment of desperately needed know-how and constitutes secret information for which there is no desire to pass it on to another party.

It can be seen from the above that the approach taken in an investigation of leaked information will differ depending on the motivation of the attacker, which can often be inferred based on tools used in an attack or evidence left on a damaged terminal.

In this way, NTT-CERT collects and analyzes threat intelligence from a variety of information sources to enable more advanced responses to attacks and more efficient surveys.

## References

[1] Website of NTT-CERT, https://www.ntt-cert.org/index-en.html
[2] Software Engineering Institute, "CSIRT Services," 2002. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=53046
[3] HACKMAGEDDON, http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/

**Shunichi Konno**

Threat Intelligence Team Leader of NTT-CERT, and Senior Research Engineer, NTT Secure Platform Laboratories.

He received a Master of information science and technology from the University of Tokyo in 2003 and joined NTT the same year, where he studied operating system security, CSIRT operation, and virtualization. He is one of the founding members of NTT-CERT, which offers CSIRT services to the entire NTT Group throughout the world.

# Security Business Solutions for Customer Needs

*Koichi Matsuda, Yukiteru Nagatake, Fumitaka Takeuchi, and Kazunori Yozawa*

**Abstract**

The NTT Group strives to be a value partner to its customers by providing high-quality total security solutions utilizing NTT laboratories' technologies and intelligence. This article introduces two security business examples covering environmental and governmental trends related to cybersecurity.

*Keywords: digital transformation, risk management, proactive and reactive measures*

## 1. Initiatives for improving customer security capabilities

Cyber threats continue to evolve, and the methods now used for carrying out cyberattacks are becoming increasingly sophisticated. These methods include large-scale DDoS (distributed denial of service) attacks using vulnerable Internet of Things (IoT) devices as springboards. With the major sports events coming up in 2020, the number of cyberattacks on critical infrastructure is expected to increase, so improving security capabilities is becoming an urgent issue. The Ministry of Economy, Trade and Industry (METI) of Japan defines comprehensive security measures including both proactive (identify and protect) and reactive (detect, respond, and recover) functions in their report Cybersecurity Management Guidelines Ver. 2.0 published in November 2017 [1].

To protect our customers, the NTT Group provides total security solutions for integrated risk management, including proactive and reactive security measures. This article presents two cases in which the technologies and intelligence of our laboratories were applied to strengthen security. The first case is a security business initiative at NTT Communications that provides stronger protection and early response capabilities through indicator detection and utilization functions. The second case addresses issues in the operational technology (OT) domain and provides detection and response capabilities through business collaboration.

## 2. NTT Communications security measures and business development

Initiatives in the area of digital transformation are expanding. These initiatives involve finding solutions to existing issues and creating new business opportunities using newly emergent technologies such as IoT, big data, and artificial intelligence (AI). However, these new technologies also come with new risks. We are studying how these risks should be handled from the perspectives of risk mitigation, risk management, anomaly detection, business resilience, and organizational defense.

### 2.1 Ever-increasing security risks

Digital transformation in the information and communication technology (ICT) field has been attracting attention in enterprises and businesses that are actively using the latest technologies, discovering new knowledge, and creating new business. For example, the IoT is used to gather diverse data and to create big data, which is then analyzed using AI.

Digital transformation is an effective approach for enterprises, but it also requires awareness of new risks that arise. For example, when a new service is developed and launched on the market, it changes the environment, and careful thought must be given to any new risks that may appear. Also, with the advance

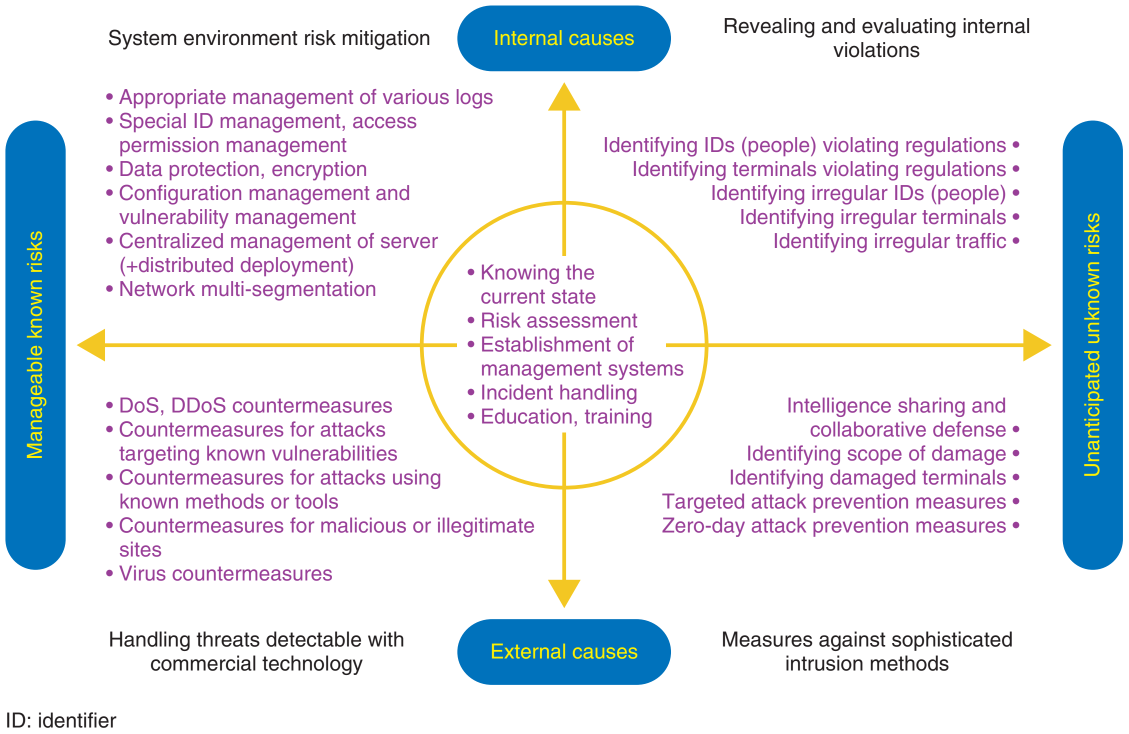

System environment risk mitigation
Internal causes
Revealing and evaluating internal violations
• Appropriate management of various logs
• Special ID management, access permission management
• Data protection, encryption
• Configuration management and vulnerability management
• Centralized management of server (+distributed deployment)
• Network multi-segmentation
Identifying IDs (people) violating regulations •
Identifying terminals violating regulations •
Identifying irregular IDs (people) •
Identifying irregular terminals •
Identifying irregular traffic •
Manageable known risks
Unanticipated unknown risks
• Knowing the current state
• Risk assessment
• Establishment of management systems
• Incident handling
• Education, training
• DoS, DDoS countermeasures
• Countermeasures for attacks targeting known vulnerabilities
• Countermeasures for attacks using known methods or tools
• Countermeasures for malicious or illegitimate sites
• Virus countermeasures
Intelligence sharing and collaborative defense •
Identifying scope of damage •
Identifying damaged terminals •
Targeted attack prevention measures •
Zero-day attack prevention measures •
Handling threats detectable with commercial technology
External causes
Measures against sophisticated intrusion methods
ID: identifier

Fig. 1. Cybersecurity issues in administrative environments.

of automation in production lines using new technologies such as IoT, the possibility increases that entire manufacturing processes may be affected by cyberattacks from outside the enterprise. It is important to be aware that such risks are inherent to digital transformation, and it is necessary to study measures to deal with them.

As the range of areas subject to cyberattacks expands, risks that were never imagined earlier are becoming real. The hacking of the San Francisco Municipal Railway system and the malware infection at a power plant in the Ukraine, which caused large-scale power outages, are good examples of this. We expect that power plant systems are designed with redundancy so that if there is a fault, the remaining systems can continue to operate. However, the fact that this situation occurred in spite of such preparation is an indication of how extremely clever the attack must have been. The recent WannaCry cyberattack also caused widespread damage. It was not particularly new in its methods, but it caused damage to hospital systems and prevented treatments and surgeries from proceeding in some cases. This also shows how extremely widespread the risk of cyberattacks has become.

### 2.2 Establishment of a cycle of improvement that anticipates unknown risks

Cybersecurity is already recognized as a management issue, and we are moving from an ICT management phase, which considers protection of individual systems, to a risk management phase, which considers protection of group management as a whole. These issues can be categorized into four quadrants according to internal and external causes, and whether they are known, manageable risks or unknown, unanticipated risks (**Fig. 1**). The issues in quadrants 1 to 4 interact and exacerbate each other according to changes in the environment, and key approaches to resolving these issues include risk mitigation, risk management, anomaly detection, business resilience, and organizational defense.

An important aspect of risk mitigation is to simply review the group ICT management environment. Risk is reduced by having only one connection to the Internet rather than having connections at every location. The point is to plan architecture simplifications such as this. This also requires consolidating usage regulations. Details are reviewed and decided from a perspective assuming malicious intent or vulnerability rather than a charitable nature, and also assuming

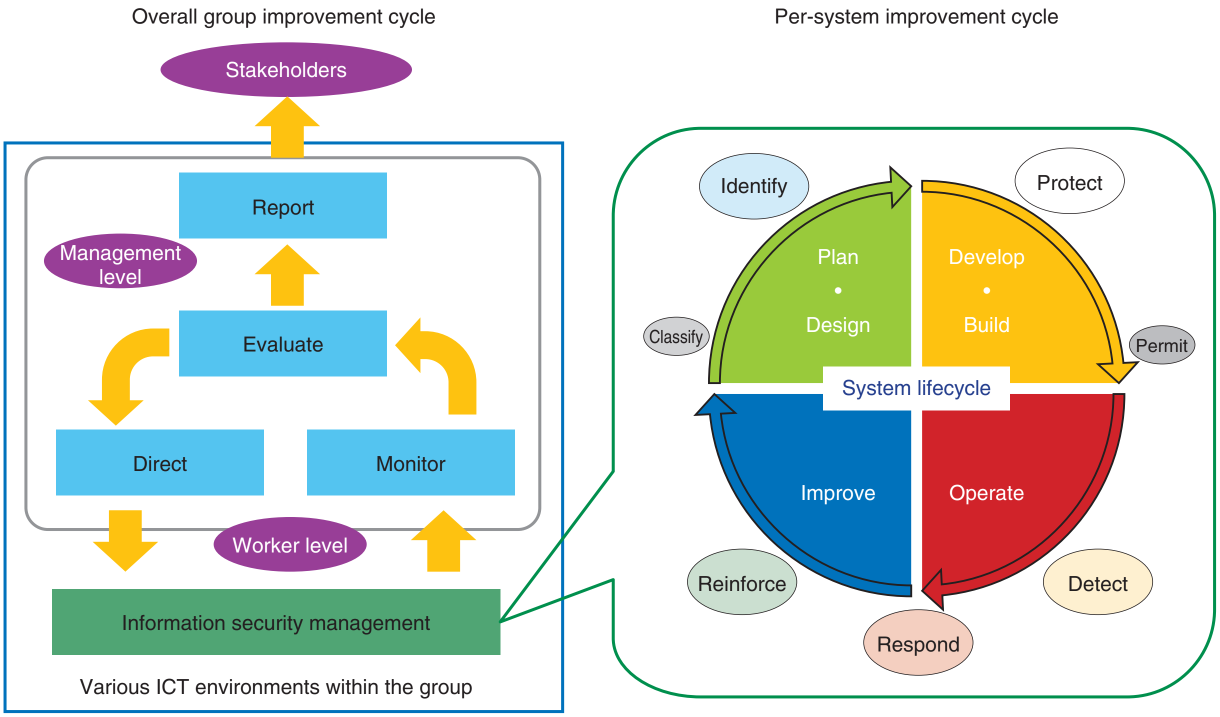


Fig. 2. Establishment of improvement cycle anticipating unknown risks (plan, do, check, act cycle).

that employees are susceptible, in order to cultivate a comprehensive culture of basic behavior. This is what is required for risk management in the digital transformation era.

A key point in risk management is to establish a cycle of improvement that anticipates unknown risks. In addition to information security management at the level of practical workers, an improving cycle of monitoring, evaluation, direction, and reporting at the management level is needed (**Fig. 2**). Information must be regularly shared with stakeholders. If trust can be built with stakeholders, any incidents that occur can be resolved without resulting in insecurity or mistrust. This is important work at all times, and not just when an incident occurs.

System lifecycles, from development and construction to operation, improvement, planning, and design, are determined for individual systems. If a security perspective is incorporated into these cycles, it is possible to unify security levels in these systems. Furthermore, security levels can be improved by establishing rules for managing system vulnerabilities, security logs, and monitoring mechanisms during the operation phase, by disallowing full operation until they are satisfied, and by setting explicit, comprehensive rules for approval during preparation.

It is important to establish such fair security-level metrics and put standards in place. As an example, it is conceivable to create models for measuring levels of maturity from the perspectives of processes, people, organizations, and technologies, and to evaluate them based on the models. Evaluating levels of maturity each year would give an appropriate understanding of conditions and provide useful guidelines for considering practical measures that need to be taken. Using such security levels as criteria for investing in security could also be effective by deciding, for example, that systems handling customer information must be Level 4 or higher, while strictly internal systems must be Level 2 or higher. Deciding priorities for security investment in this way also contributes to efficient investment.

### 2.3 Role of computer security incident response team (CSIRT) in risk management

Risk management systems are also an important element of risk management. Taking a strategic, long-term view is the core concept of risk management, and measuring the degree of impact on business that would result from a cyberattack on these systems is

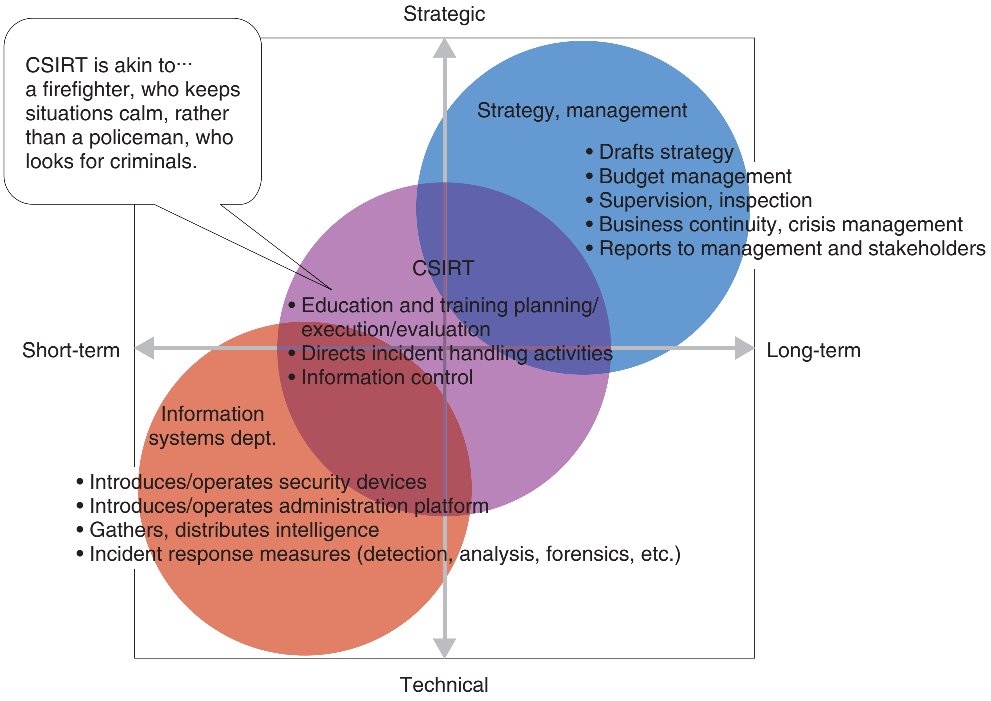

Strategic
Technical
Short-term
Long-term
CSIRT is akin to···
a firefighter, who keeps situations calm, rather than a policeman, who looks for criminals.
Strategy, management
• Drafts strategy
• Budget management
• Supervision, inspection
• Business continuity, crisis management
• Reports to management and stakeholders
CSIRT
• Education and training planning/execution/evaluation
• Directs incident handling activities
• Information control
Information systems dept.
• Introduces/operates security devices
• Introduces/operates administration platform
• Gathers, distributes intelligence
• Incident response measures (detection, analysis, forensics, etc.)

Fig. 3. Overall image of risk management system.

the point of assessment in risk management. As such, the strategic management group assesses risk from the perspective of business continuity and crisis management, considers whether such risk is permissible, and if not, determines what sort of investment is necessary.

In conventional cybersecurity, the information systems department took the central role, but now that security is considered a management responsibility, the strategic management group and the information systems department must proceed together. However, these two parts of an organization are often opposite in various ways. For example, their priorities for handling incidents are different, and they even use different terminology. Consequently, even if a system is created, communication difficulties can cause delays and prevent incidents from being handled appropriately. A way of bridging these two parts of an organization and preventing such dysfunction is needed, and this can be provided by a CSIRT (**Fig. 3**).

The CSIRT acts as the firefighter in the ICT environment, quickly extinguishing the fire if a problem occurs and working to keep the situation calm. It does not play the part of a policeman, who actively investigates crimes. This group also conducts and evaluates ongoing education and training to prevent incidents from occurring in the first place. Members are acquainted with the work of the enterprise or group, and are also very proficient with the technologies involved. If these people function in a leadership role when incidents occur, the CSIRT will play a vital role in risk management for the organization.

### 2.4 Role of Security Information Event Management (SIEM) in detecting attacks

The next point is anomaly detection. No matter what cybersecurity measures are taken and to what extent systems are prepared, a cyberattack is still a possibility. Detecting cyberattacks quickly is important in order to deal with them. An essential first step is knowing what could potentially occur.

NTT Communications provides intelligence services using wide-ranging, high-quality information sources in cooperation with KELA Corp. of Israel. It combines NTT Communications' intelligence support with the RaDark intelligence service provided by KELA, which collects and summarizes darknet information. This service is very effective in finding out about external trends.

It is important to detect anomalies as early as possible, and the WideAngle managed security service (MSS) is designed to do this. The MSS provides

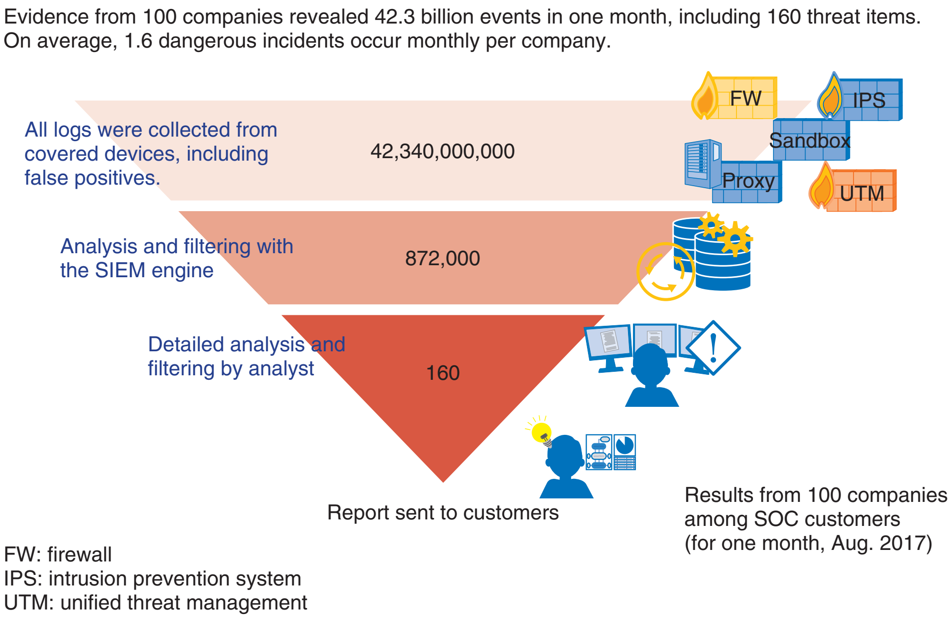

Evidence from 100 companies revealed 42.3 billion events in one month, including 160 threat items.
On average, 1.6 dangerous incidents occur monthly per company.
All logs were collected from covered devices, including false positives.
42,340,000,000
FW
IPS
Sandbox
Proxy
UTM
Analysis and filtering with the SIEM engine
872,000
Detailed analysis and filtering by analyst
160
Report sent to customers
Results from 100 companies among SOC customers (for one month, Aug. 2017)
FW: firewall
IPS: intrusion prevention system
UTM: unified threat management

Fig. 4. SIEM effectiveness (August 2017 results).

functionality that gathers logs from customers' ICT environments in a central location and detects cyberattacks and related symptoms. This information is provided by the security operations center (SOC). This service is offered by NTT Security, which operates SOCs in ten locations in and outside of Japan. Analysis is done automatically using the SIEM system developed by NTT Security, with detailed analysis by an analyst, who selects threats that are difficult to discriminate using security devices. During the month of August in 2017, the Tokyo SOC processed 42.3 billion events in the traces (logs) from 100 companies (**Fig. 4**). This was filtered down to 872,000 events by the SIEM engine, which NTT Security developed, and 160 events were deemed dangerous after detailed analysis by a specialist. Without this type of initiative—using the extremely advanced SIEM engine and specialized analysts working 24 hours a day—it would not be possible to know what is actually happening in detail. This is the sort of response needed today. The fact that 160 events related to threats were found in the logs of 100 companies—companies having strong awareness of security and using SIEM—in just one month, suggests that at least one or two threats went undetected per company. This indicates that cyberattacks are extremely frequent.

Note that proxy server logs are particularly useful for the SIEM log analysis. When we selected 13 of the companies from our customers in Tokyo and analyzed the observation results, by far the most threats detected were in the proxy servers themselves, or in the combination of proxy and security devices. Reasons for this include that time sequences of communication states can be detected, and that the logs contain useful information such as the referrer, which is an HTTP (Hypertext Transfer Protocol) header field that identifies the address of the webpage.

Considering these conditions, NTT Communications has begun providing an option to analyze only proxy logs using SIEM, which was not possible earlier. We want customers to understand that beyond security products, logs from network devices and proxy servers are extremely important for security.

SIEM first collects logs and packets and automatically visualizes potential risks using the analysis engine. These are then analyzed in detail by an analyst to determine danger levels and identify false positives. In the automatic analysis process, there is a check for communication with malicious sites using a malware countermeasure blacklist (RELIEF) developed by NTT Secure Platform Laboratories (SC Labs). The RELIEF blacklist is SC Labs' own threat information platform. It was generated using honeypots and dynamic analysis and contains malicious sites that other companies have difficulty detecting. To further increase our ability to detect malicious sites, we have also cooperated with SC Labs regarding domain analysis technology. The analysis engine also actively utilizes AI technologies and is able to detect domain names automatically generated by malware with 99.5% accuracy.

### 2.5 Proactive use of intelligence

The final two points are business resilience and organizational defense. Increasing business resilience involves building a process that rapidly identifies personal computers (PCs) infected with malware, quarantines and analyzes them, prevents spreading and eradicates the virus, and recovers the PCs. The difficult part is the quarantine, which requires that work stops. Determining who must make such decisions, and by what process, is not something to think about when an incident occurs and must be considered beforehand.

Strengthening capabilities for restoration and recovery from incidents is also a continuous process that ends with final reports to the customer. This involves technical aspects, but also includes how communication should be handled to increase resilience.

Consideration must also be given to organizational protection. In particular, newly established subsidiaries and enterprises acquired through merger and acquisition may have low levels of security. Attackers will target such parts of an organization that have low security, so corresponding measures must be considered.

One possible alternative to the parent company attempting to impose security measures is to build a common group platform such as a proxy server, which subsidiaries would use to connect to the Internet for a fee. This could be provided at low cost so that even group companies with small security budgets would have adequate access. Any threats can then be detected by analyzing the logs from these proxies using SIEM. Such active utilization of intelligence would be effective for organizational defense.

The actions of performing URL (uniform resource locator) filtering on a common group platform and blocking communication with malicious sites also have significant security benefits. To meet this need, NTT Communications offers the Active Blacklist Threat Intelligence service. This service provides a real time blacklist of malicious sites discovered by the Tokyo SOC as it performs security monitoring for Japanese enterprises and government agencies. Introducing this service into network devices reduces risk by quickly blocking communication with newly created black sites.

As mentioned earlier, NTT Communications has also created an environment that enables it to obtain information from the darknet, where attackers share and exchange information, and it provides such information to customers. Thus, defenses can pinpoint particular attacks using accurate prior information. In the past, attackers were overwhelmingly superior, and the gap between them and defenders was increasing. However, by utilizing intelligence for preventative maintenance, we can implement measures not possible previously.

Obtaining information regarding new attack tools quickly and sharing it among enterprises can also inflict significant damage on attackers, increasing their costs and reducing the effectiveness of attacks. Intelligence is being shared in this way, within the group and in society as a whole. This type of practice is necessary for risk management in the age of digital transformation.

### 2.6 Security measures needing special attention today

As mentioned earlier, cybersecurity issues can be categorized into four quadrants according to internal and external causes and whether they are known, manageable risks or unanticipated, unknown risks (Fig. 1). Till now, cyberattacks from outside (external causes) have increased in sophistication and quantity, and priority has been given to dealing with them, but the handling of internally caused and unknown risks (first quadrant) is also beginning to emerge as an issue. This includes maintenance work and detection of abnormal behavior from malware that is introduced with data on media such as universal serial bus (USB) memories.

There are two measures that can be taken to deal with such issues.

(1) Managed detection and response (MDR)

MDR refers to a range of services and technologies deployed to actively detect abnormal behavior of unknown malware on PCs and other endpoints in real time, remotely and quickly isolate infected terminals before the infection or damage can expand or spread, assess the damage, and eliminate it. WideAngle MSS offers MDR functions that go beyond detecting and notifying users of security threats. Those functions can also reduce the risk of security incidents occurring through rapid response at endpoints based on highly accurate decisions made by analysts using SIEM.

Another important technical element of MDR is the indicator of compromise (IoC) definition file, which is the basis for detecting malicious behavior of malware on endpoints. This file incorporates a wealth of knowledge from NTT Security in addition to the custom IoC from SC Labs.

(2) User and entity behavior analytics (UEBA)

UEBA is a field attempting to detect suspicious or unauthorized behavior of ordinary users (i.e., employees) at the earliest possible stage. Internal misbehavior can result in security incidents directly related to management responsibilities and that threaten business continuity, so they must be given sufficient attention with risk countermeasures.

With the arrival of the IoT era, preserving security in the IoT/OT domain is becoming increasingly important, and countermeasures can also be explained in relation to Fig. 1. In the IoT/OT domain, most threats must initially be considered as coming from the second quadrant, so it is necessary to start by understanding the state of systems that integrate information technology (IT) and OT, potential threats, and risks by monitoring security during design, construction, and operation of security measures, and by promoting measures to deal with internal threats.

With the WideAngle MSS provided jointly by NTT Communications and NTT Security, we are actively expanding security solutions using various technologies to counter cyberattacks as they continue to advance. For example, in May 2017, NTT Security announced a total security solution to detect unknown malware and ransomware. This solution combines the Cybereason AI-driven cyberattack countermeasure platform from Cybereason Japan Corp. and the MSS platform operated by NTT Security. Security solutions are also being actively developed in the OT domain. NTT Security provides the IT/OT Integrated Security Service for industrial control systems and is also developing a program to train security personnel for the IoT domain in collaboration with ICS Laboratory Co. Ltd. and NTT Communications.

## 3. Joint development of real-time anomaly detection technologies for OT domain

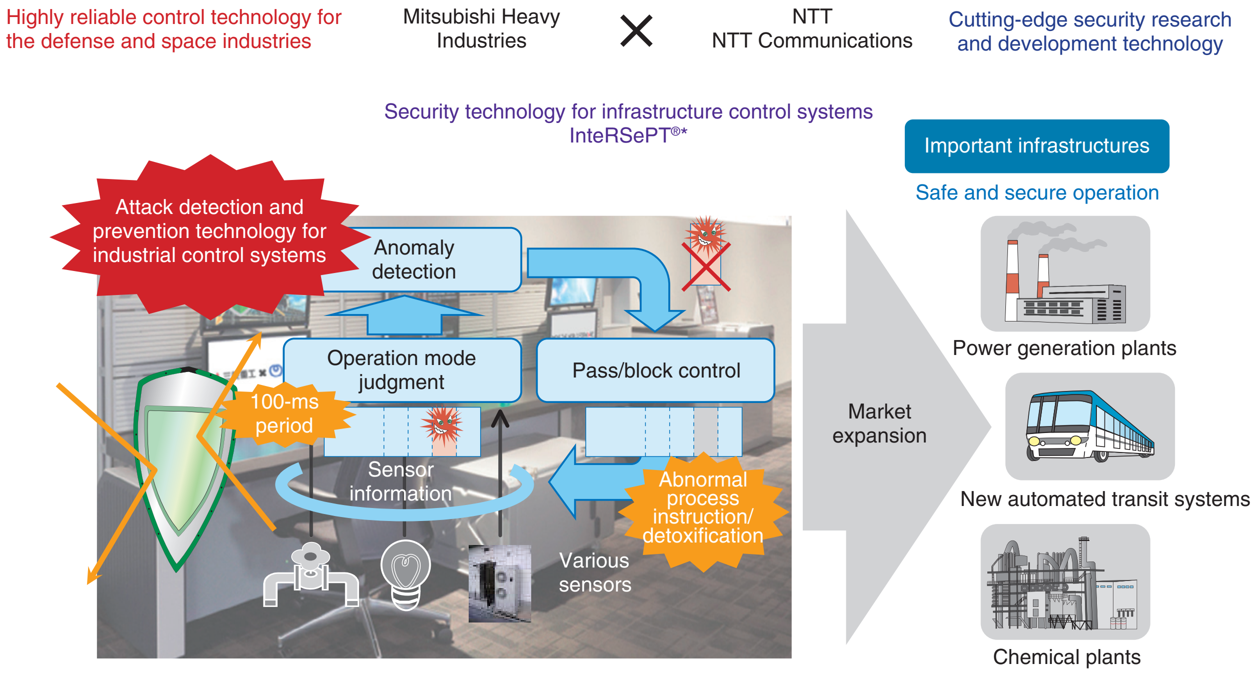
A critical infrastructure system consists of the ICT domain (information systems) and the OT domain (industrial control systems). Industrial control systems are operated (and have been for decades) 24 hours a day, 7 days a week, and they require high availability. In contrast, information systems are operated mainly during business hours with relatively short interval system updates, and they require confidentiality. Conventionally, industrial control systems have been safe because their networks were isolated from the Internet. However, with digital transformation, the latest technologies are being applied even in the OT domain for expanding and optimizing industrial business operations. Consequently, new risks are emerging such as cyberattacks through USB memory devices and via maintenance networks. For instance, incidents such as the previously mentioned hacking of a transit system and a malware infection at a power plant have been detected.

NTT is working in collaboration with Mitsubishi Heavy Industries Ltd. (MHI) to develop cybersecurity technologies in industrial control systems. We have developed a prototype for an industrial control system that automatically detects cyberattacks and responds with protection measures (**Fig. 5**). This prototype has unique functions designed especially for the protocol characteristics of industrial control systems such as variations and frequencies of control commands and sensor signals. One function is a partial revising capability that can handle only abnormal commands even if the signal has hundreds of both legitimate and cyberattack commands. We believe this function will contribute to improving the business continuity of industrial control systems.

In the future, the NTT Group aims to expand the security business into areas such as power generation plants, chemical plants, and other fields requiring high availability by using our security technologies and the control technologies of MHI for the defense and aerospace fields.

## 4. Future prospects

By providing high quality total security solutions using technologies and intelligence from our laboratories, the NTT Group aims to meet our customers' needs as their enterprises grow and to continue to be chosen as a value partner.


Highly reliable control technology for the defense and space industries
Mitsubishi Heavy Industries
×
NTT
NTT Communications
Cutting-edge security research and development technology
Security technology for infrastructure control systems InteRSePT®*
Important infrastructures
Safe and secure operation
Attack detection and prevention technology for industrial control systems
Anomaly detection
Operation mode judgment
Pass/block control
100-ms period
Sensor information
Abnormal process instruction/ detoxification
Various sensors
Market expansion
Power generation plants
New automated transit systems
Chemical plants

* “InteRSePT” stands for “Integrated Resilient Security and Proactive Technology” and is a registered trademark of Mitsubishi Heavy Industries, Ltd. in Japan.

Fig. 5. Safe and secure operation of critical infrastructures.

## Reference

[1] METI, “Cybersecurity Management Guidelines Ver. 2.0,” Nov. 2017. http://www.meti.go.jp/policy/netsecurity/mng_guide.html

## Trademark notes

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

**Koichi Matsuda**

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

He received an M.E. in information science from Nara Institute of Science and Technology in 2000. He joined NTT WEST in 2000, where he was engaged in developing security solutions for enterprise customers. He has been with the R&D Planning Department at NTT headquarters since 2014, where he has been promoting security related business and technologies. He contributed to the establishment of the Cross Sectors Forum and has promoted cross-sector collaboration for cybersecurity workforce development.

**Yukiteru Nagatake**

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

He received a B.E. and M.E. in information engineering from Kyushu University, Fukuoka, in 1996 and 1998. He joined NTT Network Service Systems Laboratories in 1998 and was involved in practical research of the Advanced Intelligent Network. He worked on the development of the NGN (Next Generation Network) from 2007 to 2010 and helped develop the Integrated IT Infrastructure and cloud services such as DaaS and application virtualization at NTT WEST from 2010 to 2017. Since 2017, he has been in his current department, where he has been promoting security related business and technologies.

**Fumitaka Takeuchi**

Vice President, Security Evangelist, Managed Security Service Taskforce Corporate Planning Department, NTT Communications Corporation.

He developed an anti-virus service in 2001 and was in charge of its operation. In 2003, he established a security operations center and was involved in managing the overall security business. In 2013, he became president and CEO of NTT Com Security Co. (which merged with other NTT security operations to become NTT Security in 2016), where he developed and launched the WideAngle managed security services of NTT Communications. He has been in his current position since 2016.

**Kazunori Yozawa**

Chief Technology Officer and Regional CEO, Japan, NTT Security.

He received a B.S. in electrical engineering in Japan in 1979 and an MBA from Stanford University, USA, in 1995. He joined NTT in 1979. He has been a member of the supervisory board at NTT Com Security since 2009. He served in senior executive and board roles at various companies in the NTT Group, including holding a senior position at the US subsidiary. He also introduced new service initiatives including enterprise hosting and managed IT. He is experienced in leading major mergers and acquisitions and integration initiatives.

# Cyberattack Countermeasure Technology to Support NTT's Security Business

*Takeo Hariu, Daiki Chiba, Mitsuaki Akiyama, Takeshi Yagi, Yuhei Kawakoya, Yukio Nagafuchi, and Takaaki Koyama*

## Abstract

NTT Secure Platform Laboratories is researching and developing the world's most advanced technologies for countering cyberattacks to support NTT's security business. In this article, we introduce domain name analysis technology that can effectively detect and defend against malware infections, malware analysis technology to support managed detection and response services, and unified threat management solutions that use a resilient security engine and anti-malware blacklists.

*Keywords: domain name analysis, MDR services, security orchestration*

## 1. Domain name analysis technology

Domain names and the domain name system (DNS) are considered to be essential elements of today's Internet. A domain name is information written in the form "example.com" that is used for identifying the destination of communications when accessing a website or sending/receiving email. The DNS, meanwhile, is a mechanism for obtaining a mapping between a domain name and an Internet protocol (IP) address that is required for actual communications.

Unfortunately, in addition to this important use on the Internet, domain names and the DNS are also exploited for use as an infrastructure for mounting cyberattacks. For example, an attacker may generate new domain names daily to distribute malicious software (malware) or create a domain name similar to that of a legitimate service to deceive users through a phishing attack. An attacker may also manipulate a command-and-control server to issue malware-controlling instructions and use domain names and the DNS to mount cyberattacks such as a DDoS (distributed denial-of-service) attack, spam-mail distribution, or information theft.

NTT Secure Platform Laboratories has been researching and developing various technologies to create information related to malware infections (security intelligence), with the aim of contributing to the NTT Group's global security business [1]. These include various types of decoy systems (honeypots) for accurately and safely observing malware behavior at the time of an infection and malware dynamic analysis technology for analyzing malware behavior after an infection by having the system manipulate that malware. However, the ever-evolving nature of cyberattacks indicates that attackers have been devising measures to avoid such analysis technologies and countermeasures. As a result, attacks that cannot be identified by these technologies have emerged.

Consequently, to continue responding to cyberattacks as they become more advanced and sophisticated, NTT Secure Platform Laboratories has initiated the research and development (R&D) of attack analysis techniques that focus on the properties of malicious domain names exploited by an attacker as

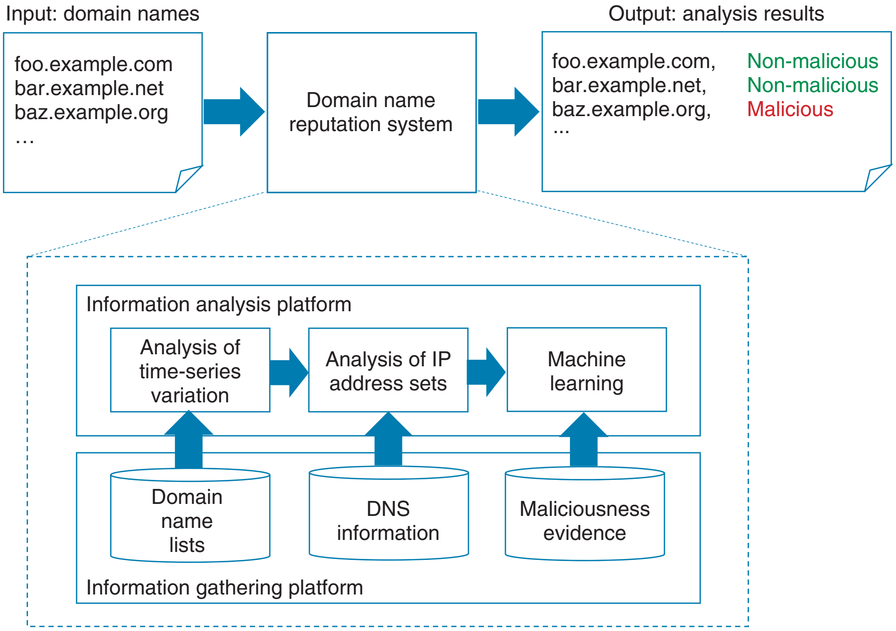

Input: domain names
foo.example.com
bar.example.net
baz.example.org
…
Domain name reputation system
Output: analysis results
foo.example.com, Non-malicious
bar.example.net, Non-malicious
baz.example.org, Malicious
...
Information analysis platform
Analysis of time-series variation
Analysis of IP address sets
Machine learning
Domain name lists
DNS information
Maliciousness evidence
Information gathering platform

Fig. 1. Domain name reputation system.

an attack infrastructure, and has also begun acquiring more security intelligence. These R&D efforts include developing a domain name reputation system that can identify malicious domain names and a domain name categorization system that can generate information for effectively preventing cyberattacks based on malicious domain names. Cyberattack countermeasures including infection defense for preventing malware infections and identification of malware-infected hosts can be further improved using the security intelligence acquired by exploiting these two systems.

### 1.1 Domain name reputation system

At NTT Secure Platform Laboratories, we make use of information we collect as well as publicly available information to evaluate domain-name maliciousness from many angles. The domain name reputation system that we have developed enables us to identify and output malicious domain names used by attackers from input domain names (**Fig. 1**).

An attacker may generate new malicious domain names daily and may regularly change the domain name used in attacks to mount cyberattacks while evading countermeasures. For example, an attacker may attempt to evade countermeasures by generating a large number of malicious domain names that are valid for only a short period of time using a mechanism called a domain generation algorithm (DGA) or by reregistering legitimate domain names originally used for other purposes.

Amid such activity, this reputation system focuses on domain-name lifecycles from registration to expiration and analyzes domain-name characteristics that change due to cyberattacks as a time-series variation pattern. This approach enables accurate identification of domain names owned and used by an attacker. For example, we consider the case in which an attacker reregisters the domain name “example.com” originally used as a legitimate site as soon as it expires and then uses it as a malware distribution site. Our reputation system can detect the expiration of a domain name and subsequent changes in its use to identify a malicious domain name before the occurrence of an attack (**Fig. 2**).

In addition, this reputation system simultaneously performs analysis based on sets of IP addresses corresponding to a domain name. For example, given the input domain name “foo.example.com” and its parent domain name “example.com,” this system examines sets of IP addresses corresponding to these domain names (**Fig. 3**). In particular, the use of security intelligence accumulated by NTT Secure Platform Laboratories makes it possible to refer to information on IP addresses used in past cyberattacks and to identify trends unique to attackers who operate malicious

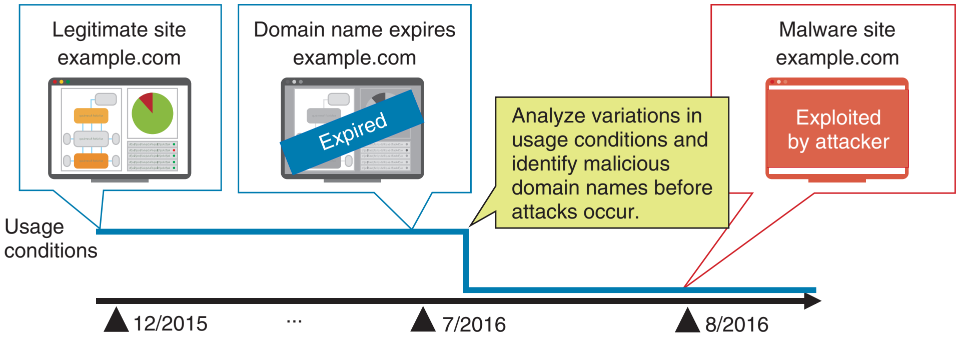


Fig. 2. Time-series variation analysis of domain name usage.

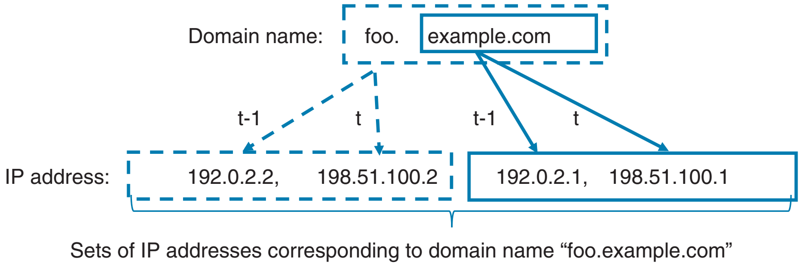


Fig. 3. Analysis of IP address sets corresponding to domain name.

domain names. Consequently, by using machine-learning techniques based on the results of analyzing IP address sets in this way and the results of analyzing time-series variation patterns as described above, we have achieved a system for calculating and predicting the possibility that a domain name is being exploited for malicious purposes.

As a result of performing a large-scale evaluation using malicious domain names used in actual cyberattacks, this reputation system has been successful in predicting with good accuracy malicious domain names that have not been able to be identified using conventional techniques. The paper describing this system was presented at a prestigious international conference [2].

### 1.2 Domain name categorization system

This categorization system determines the history and circumstances behind domain-name generation and indicates the countermeasure that should be taken against individual malicious domain names. The domain name categorization system that we have achieved outputs the specific type of countermeasure that should be taken against each input malicious domain name to prevent cyberattacks (**Fig. 4**).

An attacker can avoid uniform countermeasures by generating malicious domain names with different characteristics. For example, malicious domain names include those that are generated by abusing mechanisms that are used by legitimate Internet services. As a result, if such domain names were to be simply blacklisted and blocked, legitimate users or the use of legitimate services might be mistakenly disturbed. However, some malicious domain names are prepared exclusively for the purpose of cyberattacks using techniques such as DGAs. In this case, blocking communications in units of domain names is the most effective approach. With the above information taken into account, even if many malicious domain names can be specified based on their use by attackers, the fact that those malicious domain names may have different generation structures means that those domain names themselves cannot be used effectively as security intelligence.

Under these conditions, we have come to realize the importance of indicating what type of action should be taken as a countermeasure to each malicious domain name in addition to simply indicating

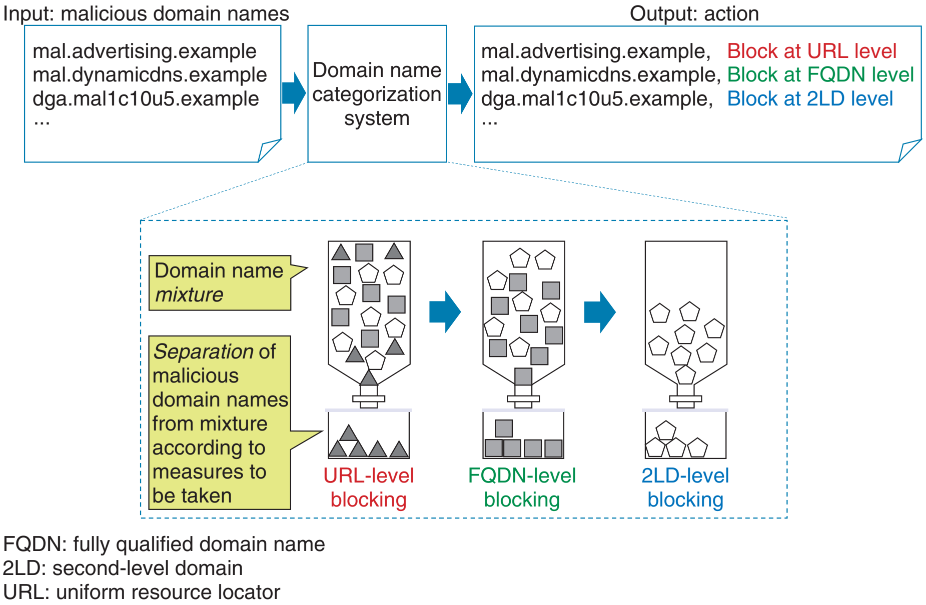

Input: malicious domain names
mal.advertising.example
mal.dynamicdns.example
dga.mal1c10u5.example
...
Domain name categorization system
Output: action
mal.advertising.example, Block at URL level
mal.dynamicdns.example, Block at FQDN level
dga.mal1c10u5.example, Block at 2LD level
...
Domain name mixture
Separation of malicious domain names from mixture according to measures to be taken
URL-level blocking
FQDN-level blocking
2LD-level blocking
FQDN: fully qualified domain name
2LD: second-level domain
URL: uniform resource locator

Fig. 4. Domain name categorization system.

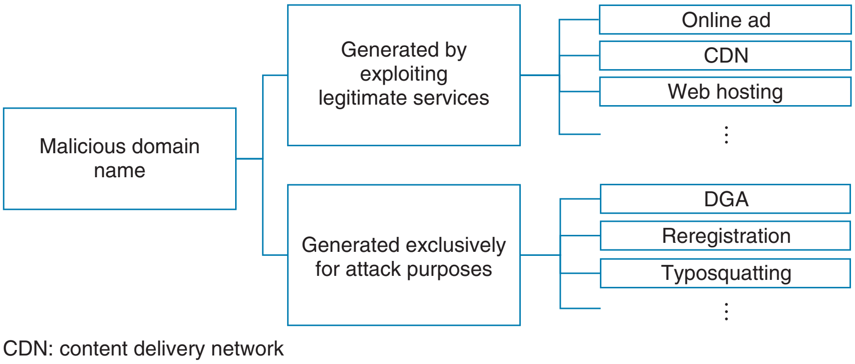
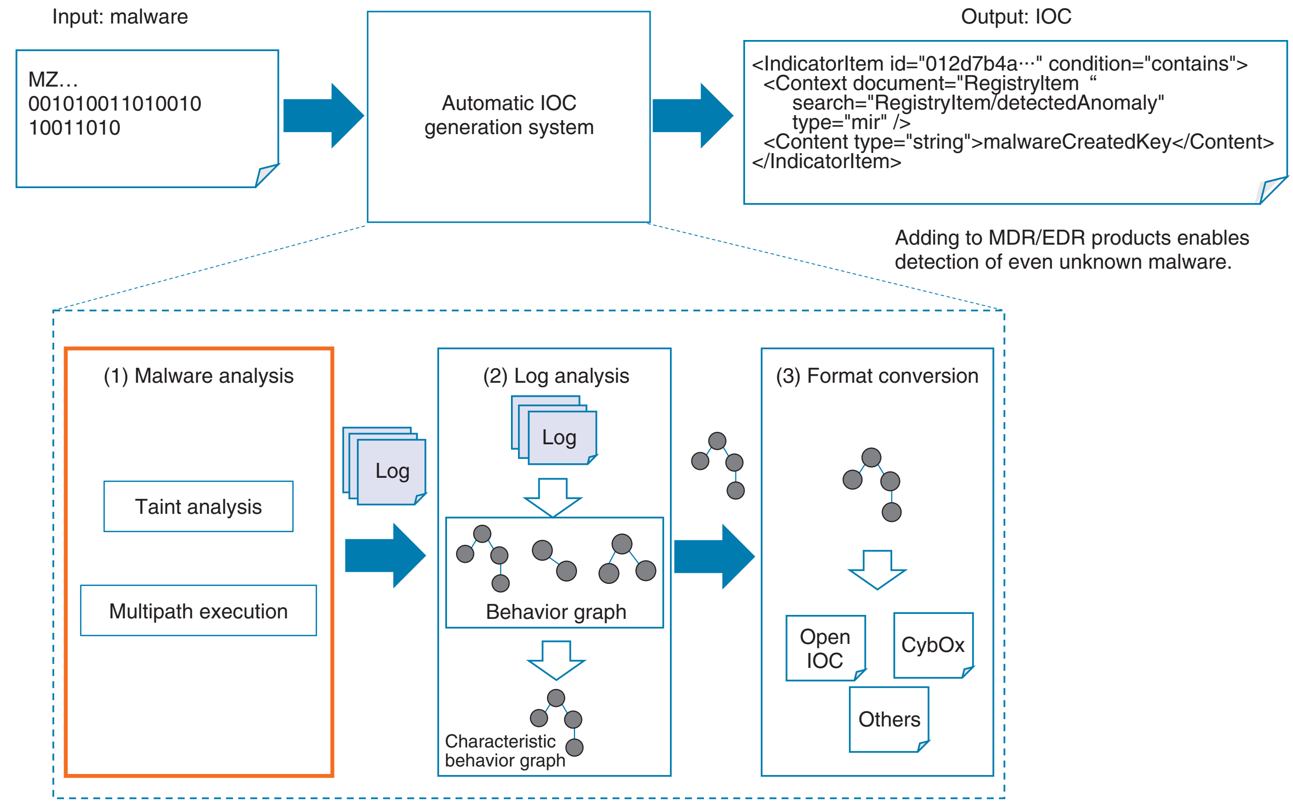

Malicious domain name
Generated by exploiting legitimate services
Online ad
CDN
Web hosting
⋮
Generated exclusively for attack purposes
DGA
Reregistration
Typosquatting
⋮
CDN: content delivery network

Fig. 5. Analysis of generation structure of malicious domain names.

malicious domain names. We therefore set out to develop a domain name categorization system that systematically identifies the generation structure of each malicious domain name specified by the reputation system.

This categorization system systematically determines the generation structure of a malicious domain name that should be taken into account when applying a countermeasure (**Fig. 5**). Specifically, it divides malicious domain names into two main categories. The first category consists of malicious domain names generated by the malicious use of legitimate services. For example, the attacker may exploit online advertising services, CDN (content delivery network) services, or web hosting services for this purpose. Since a domain name used by such a service is inherently established in order to provide a legitimate service, it is necessary here to generate countermeasure information in units of URLs (uniform resource locators) instead of simply blocking certain domain names altogether to avoid erroneous interference with legitimate services.

The second category consists of malicious domain names generated exclusively for attack purposes. These would correspond, for example, to domain names generated by a DGA, domain names reregistered



```
<IndicatorItem id="012d7b4a···" condition="contains">
  <Context document="RegistryItem  “
      search="RegistryItem/detectedAnomaly"
      type="mir" />
  <Content type="string">malwareCreatedKey</Content>
</IndicatorItem>
```

Fig. 6. Automatic IOC generation system.

by the attacker, or domain names generated by typosquatting, which targets user mistyping. For such malicious domain names used only for attacks, damage from attacks can be prevented by proactively blocking those domain names.

With this categorization system that correctly determines the generation structure of malicious domain names, we have achieved a system that presents the optimal actions to be taken against specific domain names included in a so-called *mixture* consisting of a large number of malicious domain names having various generation structures. This system can provide the most effective countermeasures as security intelligence without having a negative effect on legitimate services.

Implementing the actions generated by this categorization system against actual malicious domain names has effectively prevented cyberattacks without inflicting any damage on legitimate services. The paper describing this system was presented at a major academic conference [3].

## 2. Malware analysis technology supporting managed detection and response (MDR)

The increasing sophistication of malware as seen in its use in targeted attacks is driving the expansion of conventional security monitoring at the network level and focusing attention on MDR, which includes response measures to attacks, and on endpoint detection and response (EDR), which includes the monitoring of behavior in a host.

To improve MDR services, NTT Secure Platform Laboratories has been researching and developing technology for automatically generating indicators of compromise (IOCs) as definition files that become the grounds for detecting the malicious behavior of malware in a host. This technology analyzes input malware using advanced malware analysis technology ((1) in **Fig. 6**), extracts characteristic behaviors of that malware ((2) in Fig. 6), and generates an NTT proprietary custom IOC based on that behavior ((3) in Fig. 6).

Applying such custom IOCs generated from malware collected from the networks of NTT customers

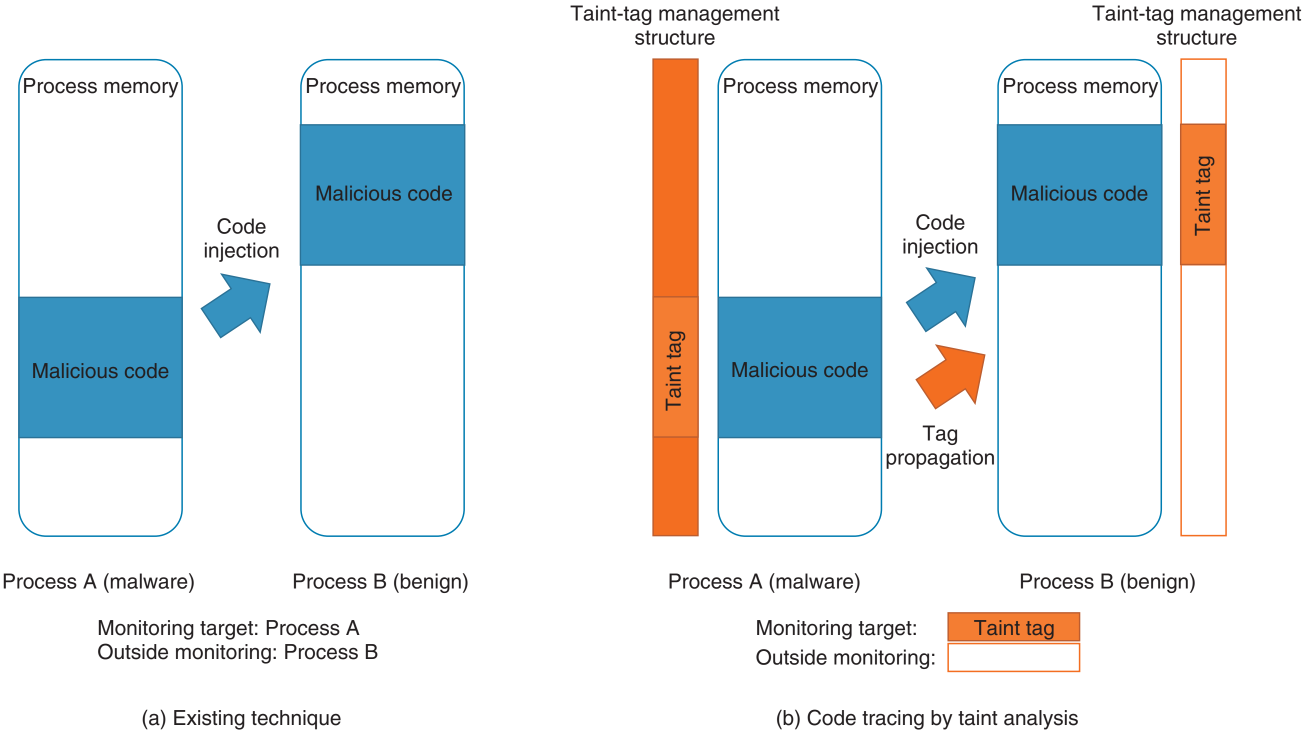


Fig. 7. Determination of analysis target by taint analysis.

enables us to detect specific attacks aimed at NTT customers that are unable to be detected by vendor-provided IOCs designed to defend against major attacks, which are widely seen in many places. In this way, we can provide MDR services that protect the networks and assets of NTT customers.

### 2.1 Problems with existing technology

Ordinary malware employs various anti-analysis techniques to avoid analysis and detection. These include code injection that injects a portion of malicious code into another process and virtual machine (VM) detection that detects whether the malware itself is running on a VM.

(1) Code injection

This technique injects code into a benign process (e.g., explorer.exe) to perform malicious actions within the process. Standard malware analysis and detection systems treat the processes of malware as monitoring targets, but benign processes are often outside the scope of monitoring, with the result that malicious behavior within benign processes may be overlooked. Additionally, even if benign processes are treated as monitoring targets, it may be difficult to distinguish between behavior driven by benign code in the process and that driven by malicious code in it (**Fig. 7(a)**).

(2) VM detection

This technique collects information on the environment in which the malware itself is running to determine whether that environment is a VM. If the malware determines that it is running on a VM, it terminates malicious activities and starts to behave in a different way (i.e., in a harmless manner) to deceive the analysis and detection system.

### 2.2 Taint analysis

We apply taint analysis to trace injected code and correctly determine the behavior of executed malware (**Fig. 7(b)**).

Taint analysis is a type of data flow analysis technology that traces the movement of specific data targeted for monitoring in a host. Specifically, it attaches an identifier called a taint tag to the targeted data. This taint tag is managed outside of the usual program execution environment (such as within a VM monitor). In the event that the data affixed with the taint tag are moved or copied, the taint tag as well will be propagated to the move or copy destination. Data flow throughout the host can be analyzed through repeated propagation of this tag.

In short, even when malware injects its own code into a benign process, using taint analysis in this way to trace data belonging to malware makes it possible to trace that injected behavior and identify malicious code copied into a benign process. This scheme can also identify the behaviors resulting from the execution of the malicious code—that is, the code affixed with the taint tag—and correctly distinguish such behaviors from those generated by the execution of benign code [4].

### 2.3 Multipath execution

We use multipath execution technology to analyze the multiple paths taken by a malware program and exhaustively extract malware behaviors.

Multipath execution is technology that follows and analyzes the multiple paths that can be taken by a program. An ordinary program can take a variety of paths (specified by *if* statements). Program processing is achieved by changing program behaviors according to such branch conditions. In multipath execution, the analysis system records the branch destination selected when program execution reaches a branch. Then, on completion of that program execution, the system executes the program again and adjusts the state of execution by selecting a branch destination different from the previously selected one. In this way, the system can execute a different path every time the program is executed.

Thus, even if malware should select an execution path that is different from usual if it detects a VM, using multipath execution in this way makes it possible to select other execution paths on reanalysis and extract behavior original to that malware. This technology can exhaustively extract malware behavior.

### 2.4 Future development

Going forward, we plan to develop technology for tuning IOCs generated using the above technology so they conform with individual endpoints. This will enable our custom IOCs to be used in diverse endpoint products provided by vendors. We also plan to conduct field trials using our custom IOCs with the aim of enhancing MDR services.

## 3. Security orchestration

In this section, we review two key efforts underway to strengthen security against and recovery from cyberattacks.

### 3.1 Countering cyberattacks using unified threat management (UTM) in small and medium-sized businesses

Cyberattacks against public organizations and companies continue to evolve as reflected by targeted attacks and ransomware. Countermeasures to cyberattacks are necessary for all enterprises regardless of size. These countermeasures generally take the form of detection and blocking based on virus definition files and signature updates using security appliances. As security consciousness grows even among customers operating small and medium-sized businesses, the introduction of low-priced UTM[*1] is increasing.

In these circumstances, as an effort to deal with cyberattacks targeting small and medium-sized businesses that make up a majority of Japanese enterprises, we introduce a security system that links UTM with a resilient security engine developed by NTT Secure Platform Laboratories and an example of actually using this system within the NTT Group.

### 3.2 Security orchestration activities

At NTT Secure Platform Laboratories, we have been carrying out R&D of security orchestration technology to achieve rapid recovery from cyberattacks. These efforts have resulted in the development of the Resilient Security Engine (RSE) for information and communication technology (ICT) businesses [5, 6]. This RSE is installed inside a datacenter or on a company network to collect log data from various types of security appliances such as a firewall or WAF (web application firewall). Analyzing this collected information enables detection of attacks, automatic execution of measures on those security appliances based on analysis results, and presentation of attack detection to operators. In addition, the RSE recommends countermeasures, which enables a quick response to cyberattacks and reduces the burden on operators.

The RSE is not limited to dealing with attacks from the outside. With the aim of blocking external access to malware that has already infiltrated an enterprise, as in targeted attacks and zero-day attacks, it includes a function for extracting high-priority blacklists from massive threat-intelligence platforms provided by security vendors at a volume that can be set in firewalls and UTM appliances. This has the same effect

[*1] UTM: An appliance that integrates multiple security functions such as firewalls, anti-virus measures, an intrusion prevention system, anti-spam measures, and web filters.

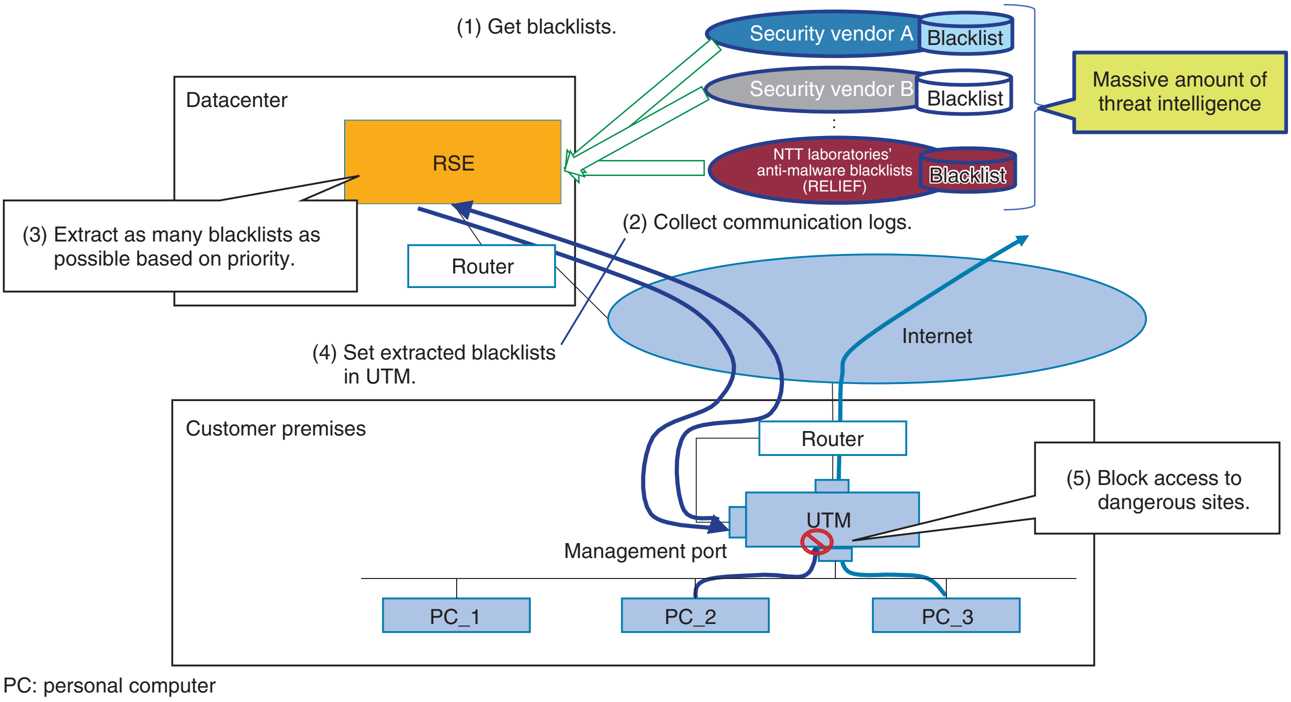

(1) Get blacklists.
Security vendor A
Blacklist
Security vendor B
Blacklist
NTT laboratories' anti-malware blacklists (RELIEF)
Blacklist
Massive amount of threat intelligence
Datacenter
RSE
Router
(3) Extract as many blacklists as possible based on priority.
(2) Collect communication logs.
Internet
(4) Set extracted blacklists in UTM.
Customer premises
Router
UTM
Management port
(5) Block access to dangerous sites.
PC_1
PC_2
PC_3
PC: personal computer

Fig. 8. Blacklist delivery to UTM by RSE.

as setting threat intelligence from multiple security vendors (**Fig. 8**).

### 3.3 UTM solutions using RSE and use by an NTT Group company

To respond to the escalating security needs of small and medium-sized businesses, NTT EAST maintains and operates UTM appliances under contract with customers. Here, the RSE delivers anti-malware blacklists (RELIEF)[*2]—the threat intelligence platform of NTT Secure Platform Laboratories—to a UTM appliance managed by NTT EAST to add those blacklists to those already possessed by the UTM. This scheme enables customers using the UTM managed by NTT EAST to enjoy even safer use of the network. In this way, the RSE helps differentiate the NTT Group from the security services of other companies and enables the provision of safe-and-secure value-added services in a rapidly growing UTM market.

## 4. Future development

Going forward, we plan to expand the application of security appliances and undertake the development of new security measures that include not only blacklists but also other types of information.

## References

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

[2] D. Chiba, T. Yagi, M. Akiyama, T. Shibahara, T. Yada, T. Mori, and S. Goto, "DomainProfiler: Discovering Domain Names Abused in Future," Proc. of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2016), pp. 491–502, Toulouse, France, June/July 2016.

[3] D. Chiba, M. Akiyama, T. Yagi, T. Yada, T. Mori, and S. Goto, "DomainChroma: Providing Optimal Countermeasures against Malicious Domain Names," Proc. of the 41st IEEE Annual Computer Software and Applications Conference (COMPSAC 2017), pp. 643–648, Turin, Italy, July 2017.

[4] Y. Kawakoya, M. Iwamura, E. Shioji, and T. Hariu, "API Chaser: Anti-analysis Resistant Malware Analyzer," RAID 2013, Lecture Notes in Computer Science, Vol. 8145, pp. 123–143, Springer, Berlin, Germany, 2013.

[5] T. Koyama, K. Hato, H. Kitazume, and M. Nagafuchi, "Resilient Security Technology for Rapid Recovery from Cyber Attacks," NTT Technical Review, Vol. 12, No. 7, 2014.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201407fa3.html

[*2] RELIEF: The proprietary threat intelligence platform developed by NTT Secure Platform Laboratories consisting of blacklists generated by honeypots and dynamic analysis that includes malicious sites not easily discovered by other companies.

[6] T. Koyama, B. Hu, Y. Nagafuchi, E. Shioji, and K. Takahashi, "Security Orchestration with a Global Threat Intelligence Platform," NTT Technical Review, Vol. 13, No. 12, 2015. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201512fa4.html

**Takeo Hariu**

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

He received an M.S. in electro-communications from the University of Electro-Communications, Tokyo, in 1991. Since joining NTT in 1991, he has been engaged in network security R&D. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and the Institute of Electrical Engineers of Japan (IEEJ).

**Daiki Chiba**

Researcher, Cyber Security Project, NTT Secure Platform Laboratories.

He received a B.E., M.E., and Ph.D. in computer science from Waseda University, Tokyo, in 2011, 2013, and 2017. Since joining NTT in 2013, he has been engaged in research on cybersecurity through data analysis. He won the Research Award from the IEICE Technical Committee on Information and Communication System Security in 2016 and the Best Paper Award from the IEICE Communications Society in 2017. He is a member of the Institute of Electrical and Electronics Engineers (IEEE) and IEICE.

**Mitsuaki Akiyama**

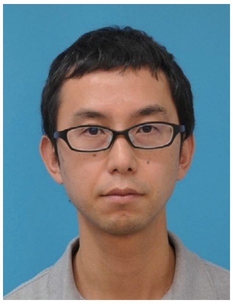
Research Engineer, Cyber Security Project, NTT Secure Platform Laboratories.

He received an M.E. and Ph.D. in information science from Nara Institute of Science and Technology in 2007 and 2013. Since joining NTT in 2007, he has been researching and developing network security techniques, focusing especially on honeypots and malware analysis.

**Takeshi Yagi**

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

He received a B.E. in electrical and electronic engineering and an M.E. in science and technology from Chiba University in 2000 and 2002. He also received a Ph.D. in information science and technology from Osaka University in 2013. Since joining NTT in 2002, he has been engaged in the research and design of network architecture and traffic engineering. His current research interests include network security, especially honeypots and security-data analysis based on machine learning. He is a member of IEICE, IEEE, and IEEJ.



**Yuhei Kawakoya**

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

He received a B.E. and M.S. in science and engineering from Waseda University, Tokyo, in 2003 and 2005. He has been involved in R&D of computer security since 2005. He is a member of the Information Processing Society of Japan (IPSJ) and IEICE.

**Yukio Nagafuchi**

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

He received a B.S. and M.S. in science and engineering from Saga University in 1996 and 1998. He joined NTT in 1998 and has been engaged in designing and developing network systems, VoIP (voice over Internet protocol) network systems, virtual network systems, and network security systems. His research interests lie in the area of security orchestration systems for ICT and Internet of Things (IoT) environments. He is a member of IEICE and IPSJ.

**Takaaki Koyama**

Senior Research Engineer, Supervisor, Secure Architecture Project, NTT Secure Platform Laboratories.

He received a B.A. and M.M.G. in media and governance from Keio University, Kanagawa, in 1994 and 1996. He joined NTT Software Laboratories in 1996 and has been studying software CALS (Continuous Acquisition and Life-cycle Support). Since 1999, he has also been studying GMN-CL (Connectionless networking technologies for Global Megamedia Networks)—a kind of IP-virtual private network technology—and developing network security equipment and operation systems. His research interests have recently extended to security orchestration systems for ICT and IoT environments. He is a member of IPSJ.

# Digital-preprocessed Analog-multiplexed Digital-to-analog Converter for Ultrahigh-speed Optical Transmitter

*Hiroshi Yamazaki, Munehiko Nagatani, Fukutaro Hamaoka, Masanori Nakamura, Toshikazu Hashimoto, Hideyuki Nosaka, and Yutaka Miyamoto*

**Abstract**

We have developed technology to extend the analog bandwidth of digital-to-analog converters (DACs), which are essential in advanced high-speed optical transmitters. We used a digital preprocessor, two sub-DACs, and an analog multiplexer to generate arbitrary signals with a bandwidth nearly twice that of each sub-DAC. This technology was used to successfully demonstrate various high-speed transmissions, including an intensity-modulated directly detected transmission at a record-high data rate of 250 Gbit/s.

*Keywords: DSP, DAC, analog multiplexer*

## 1. Introduction

The continued growth of data traffic in communications systems has resulted in the need to find ways to increase data rates of optical transmission systems [1]. Digital signal processors (DSPs) play key roles in current high-speed transmission systems [2, 3]. Functions of the DSPs include high-order modulation, pulse shaping, equalization, and dispersion compensation, which are essential for achieving high data rates with high spectral efficiency.

In a DSP-based transmitter, the analog bandwidth of digital-to-analog converters (DACs) is a key factor to determine the achievable data rate. The DACs used in commercial transmitters today are fabricated on silicon complementary metal-oxide semiconductor (CMOS) platforms and integrated with DSPs monolithically [2, 3]. Those CMOS DACs have a rather moderate analog bandwidth of ~30 GHz, which is one of the factors limiting the data rate.

DACs based on compound platforms such as indium phosphide (InP) or SiGe (silicon-germanium) provide larger bandwidth [4–6], but they consume more power. Compound DACs also pose some implementation challenges because the DSP will continue to be based on CMOS technology. This is why there is a strong need to develop technologies to extend the bandwidth using existing CMOS DACs.

We have developed a digital-preprocessed analog-multiplexed DAC (DP-AM-DAC) that is a promising potential solution in this context [7–10]. The DP-AM-DAC consists of a digital preprocessor, two sub-DACs, and an analog multiplexer (AMUX) and functions as a DAC with an analog bandwidth of almost twice that of each sub-DAC. We have generated signals with bandwidths of up to ~60 GHz with CMOS

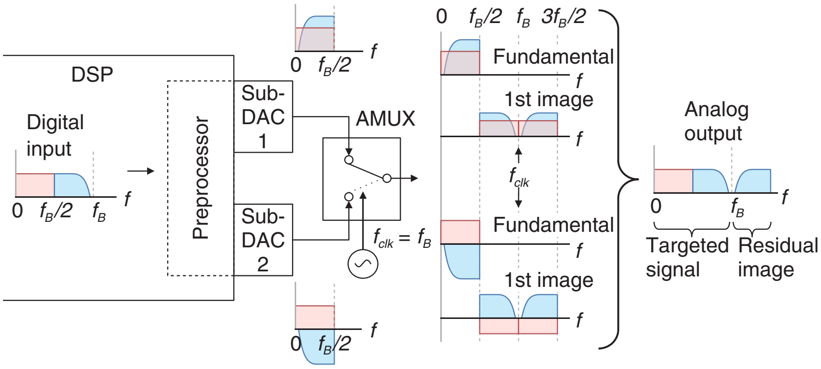


Fig. 1. Configuration and principle of DP-AM-DAC (type I).

sub-DACs and an AMUX based on an InP heterojunction bipolar transistor (HBT). Unlike other bandwidth-extension technologies that use analog mixers [3, 11], the DP-AM-DAC has a symmetric configuration with respect to the two sub-DACs and so makes it easier to balance the two branches. In this article, we review our DP-AM-DAC and the high-speed transmission experiments conducted with it.

## 2. Principle

The configuration and principle of the DP-AM-DAC is shown in **Fig. 1**. It consists of a digital preprocessor, two sub-DACs, and an AMUX [7–10]. When the bandwidth of the sub-DACs is $f_B/2$, we can obtain an arbitrary signal with a bandwidth up to around $f_B$ (twice that of the sub-DACs) as the final output from the AMUX. The schematic spectra in Fig. 1 represent the principle of the DP-AM-DAC, in which the AMUX is driven at $f_{clk} = f_B$ [7].

First, the digital representation of the target signal with a bandwidth up to $f_B$ is input to the preprocessor. The preprocessor weaves the information of the target signal into two digital sub-signals with a corresponding bandwidth of $f_B/2$ or less so that the sub-DACs can handle them without loss of information. Specifically, the preprocessor separates the input signal into low- and high-frequency components—respectively represented by red and blue—and then flips the high-frequency component around $f_B/2$ in the frequency domain. Finally, the processor adds the flipped high-frequency component to the low-frequency component with a specific amplitude ratio and complementary phases to make the two respective sub-signals.

The sub-DACs convert the digital sub-signals into the analog sub-signals, which pass alternately through the AMUX at a clock frequency of $f_{clk}$. In the frequency domain, this alternation, or multiplexing, corresponds to a superposition of the sub-signals themselves and their images (up-converted copies) generated around $f_{clk}$, where the phases of the images for the two sub-signals are complementary to each other. As seen in Fig. 1, the superposition results in the reconstruction of the target signal in the frequency region of $0 < f < f_B$. The residual image of the high-frequency component in the frequency region of $f_B < f < 3f_B/2$ can be removed by a low-pass filter. The principle explained above is what we call the type-I DP-AM-DAC. We have also developed the type-II model, which has the same hardware configuration as the type-I model but uses a different preprocessing algorithm so that we can reduce the required $f_{clk}$ by half and suppress the residual image [8].

## 3. AMUX characteristics

The key component in the DP-AM-DAC is the AMUX, which we designed and fabricated using our in-house 0.5-µm-emitter InP HBT technology [12]. As mentioned above, the AMUX is a linear high-speed selector that makes two input signals pass through it alternately at the clock frequency without any regeneration. Time-domain waveforms we measured to verify the AMUX are shown in **Fig. 2**. We input a 1-GHz sinusoidal wave to one input port while applying direct current (DC) voltage to the other and varied the clock frequency. The obtained output waveforms show that the AMUX selects the two inputs alternately at the clock frequency, as designed.

The static frequency responses of the AMUX module

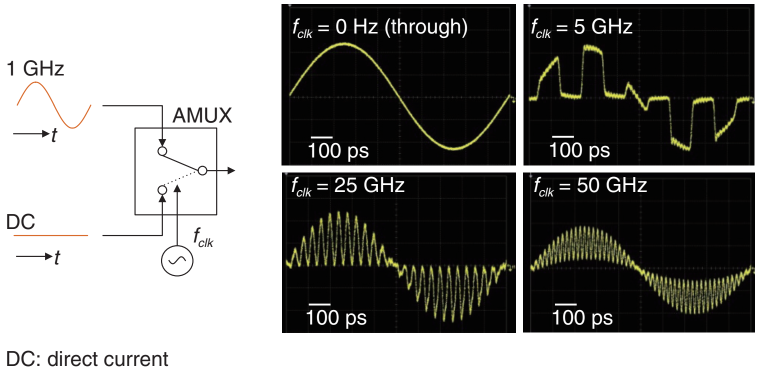


Fig. 2. Time-domain waveforms output from the AMUX multiplexing a 1-GHz sinusoidal wave and DC voltage at clock frequencies of 0, 5, 25, and 50 GHz.

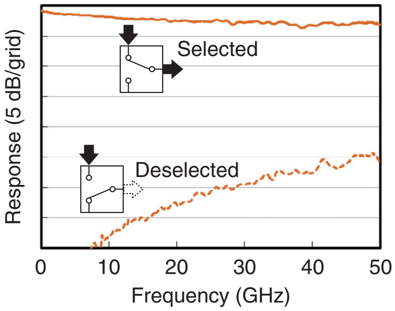


Fig. 3. Static frequency responses of AMUX when the input signal is selected and deselected.

are shown in **Fig. 3**. The response is measured by applying DC voltage to the clock port to select and deselect the input analog signal under test to measure the through and isolation characteristics, respectively. Up to the measured frequency range of 50 GHz, the through loss is less than 3 dB, while the isolation (the difference between the two curves) is more than 20 dB.

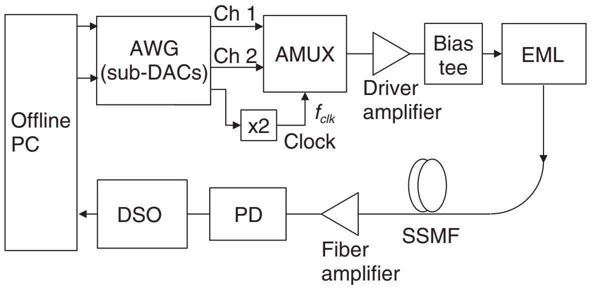
## 4. Transmission results

The DP-AM-DAC was first demonstrated in a high-speed intensity-modulated direct-detection (IMDD) transmission, in which we employed Nyquist-shaped 80-Gbaud (160-Gbit/s) four-level pulsed amplitude modulation (PAM4) [7]. The experimental setup is shown in **Fig. 4**. We used two channels of a CMOS-based arbitrary waveform generator (AWG) as the sub-DACs with an analog 3-dB bandwidth of ~20 GHz. The signal was generated using the type-I DP-AM-DAC at $f_{clk}$ = 43.3 GHz. As the optical transmitter, we used an O-band (1.3-µm) externally modulated laser with a modulation bandwidth of > 55 GHz [13]. The optical signal was transmitted over 20-km standard single-mode fiber (SSMF) and then amplified by a fiber amplifier and received by a photodiode. The DSP, including the preprocessor of the DP-AM-DAC, the receiver-side filter, and an adaptive equalizer (AEQ) was emulated by an offline personal computer.

The electrical spectra of the output signals from the two sub-DACs and the AMUX are shown in **Fig. 5(a)–(c)**. Although the signals from the sub-DACs have a bandwidth of only ~22 GHz, that from the AMUX includes a rectangular waveform with a bandwidth of ~40 GHz, which corresponds to the target 80-Gbaud Nyquist PAM4 signal. The residual image at > 46 GHz observed in the AMUX output was removed by the receiver-side matched filter in this experiment.

The eye diagram of the 80-Gbaud (160-Gbit/s) PAM4 signal after transmission over 20-km SSMF and through the digital matched filter and the AEQ is shown in **Fig. 6**. The bit error rate (BER) was 6.2 x $10^{-3}$. This result corresponds to the net data rate of 142.9 Gbit/s, assuming the use of 12%-overhead (OH) hard-decision forward error correction (FEC) code [14].

We also demonstrated a higher net data rate of 250 Gbit/s with the type-II DP-AM-DAC [8]. The setup was similar to the one shown in Fig. 4, but the sub-DACs (AWG) were upgraded to those with an analog 3-dB bandwidth of ~32 GHz, and the $f_{clk}$ was changed to 37.5 GHz. With the type-II principle, we can generate signals with the analog bandwidth up to



AWG: arbitrary waveform generator
DSO: digital storage oscilloscope
EML: externally modulated laser

PC: personal computer
PD: photodiode
SSMF: standard single-mode fiber

Fig. 4. Experimental setup for high-speed IMDD transmission experiments using the DP-AM-DAC.

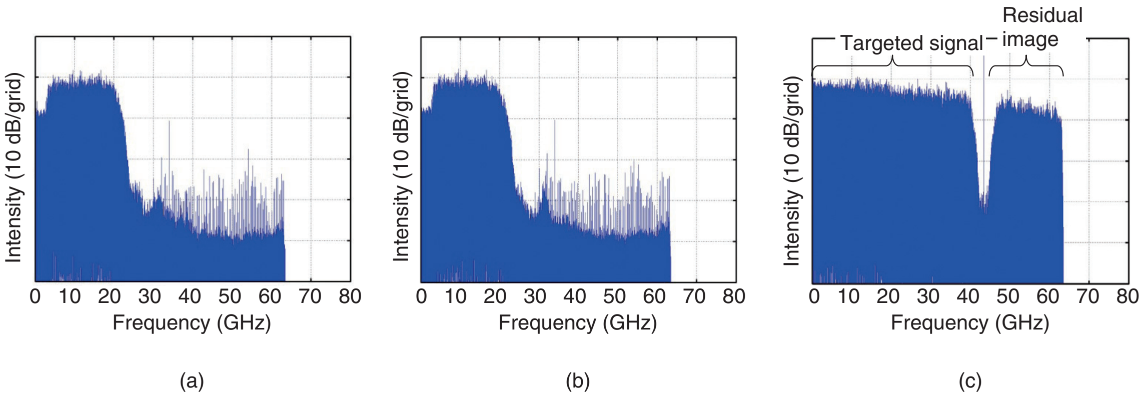


Fig. 5. Electronic spectra of output signals from (a) sub-DAC channel 1, (b) sub-DAC channel 2, and (c) AMUX measured in the 80-Gbaud PAM4 transmission experiment.

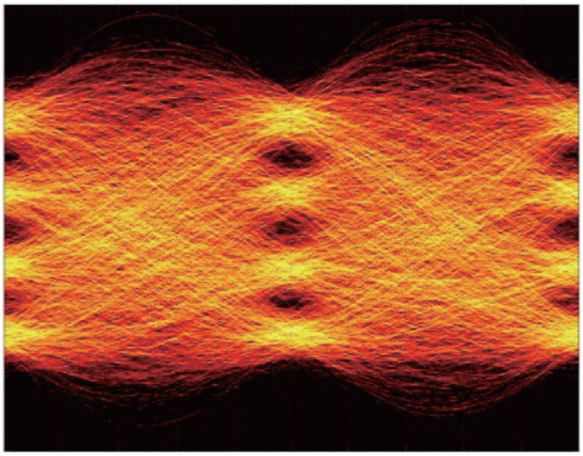


Fig. 6. Eye diagram of 80-Gbaud PAM4 signal after 20-km SSMF transmission and digital AEQ.

$2f_{clk}$ = 75 GHz, although the bandwidth used in the experiment was limited to 62 GHz by the bandwidth of the DSO (digital storage oscilloscope). We employed discrete multitone (DMT) modulation [15] to efficiently utilize the available bandwidth. The electronic spectrum and constellations of the received DMT signal at the total bit rate of 300.12 Gbit/s after transmission over 10-km SSMF are shown in **Fig. 7**. The total BER was 2.63 x $10^{-2}$, which is lower than the threshold of the 20%-OH soft-decision FEC code [16], and it corresponds to the transmission at a net data rate of 250 Gbit/s.

In addition to the results described above, we have reported various high-speed transmission experiments utilizing DP-AM-DACs, including long-haul digital coherent transmission [17–20].

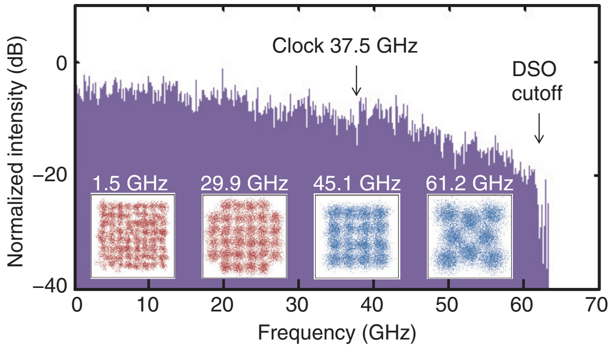


Fig. 7. Electronic spectrum and constellations of the 300.12-Gbit/s DMT signal after 10-km SSMF transmission.

## 5. Conclusion

With the DP-AM-DAC, we can overcome the bandwidth limitation imposed by the analog bandwidths of CMOS DACs. The combination of the digital preprocessor, two CMOS sub-DACs, and the high-speed AMUX enables us to generate arbitrary signals with a bandwidth nearly twice that of each sub-DAC. This technology is promising for use in future ultrahigh-speed optical transmitters for various application fields, including short-reach IMDD and long-haul digital coherent systems.

## References

[1] Y. Miyamoto, "Over 400 Gbit/s Digital Coherent Channels for Optical Transport Network," Proc. of the 21st OptoElectronics and Communications Conference/International Conference on Photonics in Switching 2016 (OECC/PS 2016), ThB3-1, Niigata, Japan, July 2016.

[2] O. Ishida, K. Takei, and E. Yamazaki, "Power Efficient DSP Implementation for 100 G-and-beyond Multi-haul Coherent Fiber-optic Communications," Proc. of the 39th Optical Fiber Communication Conference and Exhibition (OFC 2016), W3G.3, Anaheim, CA, USA, Mar. 2016.

[3] C. Laperle and M. O'Sullivan, "Advances in High-speed DACs, ADCs, and DSP for Optical Coherent Transceivers," J. Lightw. Technol., Vol. 32, No. 4, pp. 629–643, 2014.

[4] M. Nagatani, H. Wakita, H. Nosaka, K. Kurishima, M. Ida, A. Sano, and Y. Miyamoto, "75 GBd InP-HBT MUX-DAC Module for High-symbol-rate Optical Transmission," Electron. Lett., Vol. 51, No. 9, pp. 710–712, 2015.

[5] A. Konczykowska, F. Jorge, J.-Y. Dupuy, M. Riet, V. Nodjiadjim, H. Aubry, and A. Adamiecki, "84 GBd (168 Gbit/s) PAM-4 3.7 $V_{pp}$ Power DAC in InP DHBT for Short Reach and Long Haul Optical Networks," Electron. Lett., Vol. 51, No. 20, pp. 1591–1593, 2015.

[6] K. Schuh, F. Buchali, W. Idler, Q. Hu, W. Templ, A. Bielik, L. Altenhain, H. Langenhagen, J. Rupeter, U. Dümler, T. Ellermeyer, R. Schmid, and M. Möller, "100 GSa/s BiCMOS DAC Supporting 400 Gb/s Dual Channel Transmission," Proc. of the 42nd European Conference on Optical Communication (ECOC 2016), M.1.C.4., Dusseldorf, Germany, Sept. 2016.

[7] H. Yamazaki, M. Nagatani, S. Kanazawa, H. Nosaka, T. Hashimoto, A. Sano, and Y. Miyamoto, "Digital-preprocessed Analog-multiplexed DAC for Ultra-wide-band Multilevel Transmitter," J. Lightw. Technol., Vol. 34, No. 7, pp. 1579–1584, 2016.

[8] H. Yamazaki, M. Nagatani, F. Hamaoka, S. Kanazawa, H. Nosaka, T. Hashimoto, and Y. Miyamoto, "Discrete Multitone Transmission at Net Data Rate of 250 Gb/s Using Digital-preprocessed Analog-multiplexed DAC with Halved Clock Frequency and Suppressed Image," J. Lightw. Technol., Vol. 35, No. 7, pp. 1300–1306, 2017.

[9] H. Yamazaki, M. Nagatani, S. Kanazawa, H. Nosaka, T. Hashimoto, F. Hamaoka, and Y. Miyamoto, "Discrete Multi-tone Transmitter at Net Data Rate of 200 Gbps Using a Digital-preprocessed Analog-multiplexed DAC," Proc. of ECOC 2016, Tu.3.C.2, Dusseldorf, Germany, Sept. 2016.

[10] H. Yamazaki, M. Nagatani, F. Hamaoka, K. Horikoshi, M. Nakamura, A. Matsushita, S. Kanazawa, T. Hashimoto, H. Nosaka, and Y. Miyamoto, "Ultra-high-speed Optical Transmission Using Digital-preprocessed Analog-multiplexed DAC," Opt. Commun., Vol. 409, No. 15, pp. 66–71, 2018.

[11] X. Chen, S. Chandrasekhar, S. Randel, G. Raybon, A. Adamiecki, P. Pupalaikis, and P. Winzer, "All-electronic 100-GHz Bandwidth Digital-to-analog Converter Generating PAM Signals up to 190-GBaud," J. Lightw. Technol., Vo. 35, No. 3, pp. 411–417, 2017.

[12] M. Nagatani, H. Yamazaki, H. Wakita, H. Nosaka, K. Kurishima, M. Ida, A. Sano, and Y. Miyamoto, "A 50-GHz-bandwidth InP-HBT Analog-MUX Module for High-symbol-rate Optical Communications Systems," Proc. of 2016 IEEE MTT-S International Microwave Symposium (IMS), TU1C-3, San Francisco, CA, USA, May 2016.

[13] S. Kanazawa, H. Yamazaki, Y. Nakanishi, Y. Ueda, W. Kobayashi, Y. Muramoto, H. Ishii, and H. Sanjoh, "214-Gb/s 4-PAM Operation of Flip-chip Interconnection EADFB Laser Module," J. Lightw. Technol., Vol. 35, No. 3, pp. 418–422, 2017.

[14] M. Scholten, T. Coe, J. Dillard, and F. Chang, "Enhanced FEC for 40G/100G," Proc. of the 35th European Conference on Optical Communication (ECOC 2009), WS1, Vienna, Austria, Sept. 2009.

[15] W. Yan, T. Tanaka, B. Liu, M. Nishihara, L. Li, T. Takahara, Z. Tao, J. Rasmussen, and T. Drenski, "100 Gb/s Optical IM-DD Transmission with 10G-class Devices Enabled by 65GSamples/s CMOS DAC Core," Proc. of the 36th Optical Fiber Communication Conference and Exhibition (OFC 2013), OM3H.1, Anaheim, CA, USA, Mar. 2013.

[16] D. Chang, F. Yu, Z. Xiao, N. Stojanovic, F. N. Hauske, Y. Cai, C. Xie, L. Li, X. Xu, and Q. Xiong, "LDPC Convolutional Codes Using Layered Decoding Algorithm for High Speed Coherent Optical Transmission," Proc. of the 35th Optical Fiber Communication Conference and Exhibition (OFC 2012), OW1H.4, Los Angeles, CA, USA, Mar. 2012.

[17] K. Horikoshi, F. Hamaoka, A. Matsushita, M. Nagatani, H. Yamazaki, A. Sano, T. Hashimoto, H. Nosaka, K. Yonenaga, A. Hirano, and Y. Miyamoto, "96Gbaud Nyquist-PDM-QPSK Signal Transmission over 12,120 km Using DP-AM-DAC and Decision-feedback Equalizer," Proc. of OECC/PS 2016, ThD2-3, Niigata, Japan, July 2016.

[18] A. Matsushita, F. Hamaoka, M. Nakamura, K. Horikoshi, H. Yamazaki, M. Nagatani, A. Sano, A. Hirano, and Y. Miyamoto, "Super-Nyquist 9-WDM 126 GBaud PDM-QPSK Transmission over 7878 km Using Digital-preprocessed Analog-multiplexed DAC for Long-haul Applications," Proc. of ECOC 2016, W.3.D.2, Dusseldorf, Germany, Sept. 2016.

[19] M. Nakamura, F. Hamaoka, A. Matsushita, H. Yamazaki, M. Nagatani, A. Sano, A. Hirano, and Y. Miyamoto, "120 GBaud Coded 8 Dimensional 16QAM WDM Transmission Using Low-complexity Iterative Decoding Based on Bit-wise Log Likelihood Ratio," Proc. of the 40th Optical Fiber Communication Conference and Exhibition (OFC 2017), W4A.3, Los Angeles, CA, USA, Mar. 2017.

[20] F. Hamaoka, S. Okamoto, M. Nakamura, A. Matsushita, T. Kobayashi, H. Yamazaki, M. Nagatani, Y. Kisaka, A. Hirano, and Y. Miyamoto, "Experimental Demonstration of Simplified Adaptive Equalizer for Fractionally Sampled 120-GBaud Signal," Proc. of the 43rd European Conference on Optical Communication (ECOC 2017), P1.SC3.34, Gothenburg, Sweden, Sept. 2017.

**Hiroshi Yamazaki**

Distinguished Researcher, NTT Device Technology Laboratories and NTT Network Innovation Laboratories.

He received a B.S. in integrated human studies in 2003 and an M.S. in human and environmental studies in 2005, both from Kyoto University, and a Dr.Eng. in electronics and applied physics from Tokyo Institute of Technology in 2015. He joined NTT Photonics Laboratories in 2005, where he has been researching optical waveguide devices for communication systems. He is concurrently with NTT Network Innovation Laboratories and NTT Device Technology Laboratories, where he is involved in research on devices and systems for optical transmission using advanced multilevel modulation formats. Dr. Yamazaki is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

**Munehiko Nagatani**

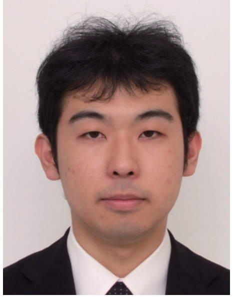
Distinguished Researcher, NTT Device Technology Laboratories and NTT Network Innovation Laboratories.

He received an M.S. in electrical and electronics engineering from Sophia University, Tokyo, in 2007. He joined NTT Photonics Laboratories in 2007, where he has been engaged in research and development (R&D) of ultrahigh-speed mixed signal integrated circuits (ICs) for optical communications systems. He is concurrently with NTT Network Innovation Laboratories and NTT Device Technology Laboratories. Mr. Nagatani is a member of IEICE.

**Fukutaro Hamaoka**

Senior research engineer, NTT Network Innovation Laboratories.

He received a B.E., M.E., and Ph.D. in electrical engineering from Keio University, Kanagawa, in 2005, 2006, and 2009. He joined NTT Network Service Systems Laboratories in 2009, where he was involved in R&D of high-speed optical communications systems, including a digital coherent optical transmission system. His research interests include high-capacity optical transport systems with digital signal processing, and space-division multiplexing. He is a member of IEICE.



**Masanori Nakamura**

Researcher, NTT Network Innovation Laboratories.

He received a B.S. and M.S. in applied physics from Waseda University, Tokyo, in 2011 and 2013. He joined NTT Network Innovation Laboratories in 2013, where he conducted research on high capacity optical transport networks. He was the recipient of the 2016 IEICE Communications Society Optical Communication Systems Young Researchers Award. He is a member of IEICE.

**Toshikazu Hashimoto**

Senior Research Engineer, Group Leader of Optoelectronics Integration Research Group, NTT Device Technology Laboratories.

He received a B.S. and M.S. in physics from Hokkaido University in 1991 and 1993. Since joining NTT in 1993, he has been researching hybrid integration of semiconductor lasers and photodiodes on silica-based planar lightwave circuits and carrying out theoretical research on the wavefront matching method. He is a member of IEICE, the Physical Society of Japan, and the Optical Society.

**Hideyuki Nosaka**

Senior Research Engineer, Group Leader of High-Speed Analog Circuit Research Group, NTT Device Technology Laboratories.

He received a B.S. and M.S. in physics from Keio University, Kanagawa, in 1993 and 1995, and a Dr.Eng. in electronics and electrical engineering from Tokyo Institute of Technology in 2003. He joined NTT Wireless System Laboratories in 1995, where he was engaged in R&D of monolithic microwave ICs and frequency synthesizers. Since 1999, he has been involved in R&D of ultrahigh-speed mixed-signal ICs for optical communications systems. He was the recipient of the 2001 Young Engineer Award and the 2012 Best Paper Award presented by IEICE. Dr. Nosaka is a member of IEICE.

**Yutaka Miyamoto**

Senior Distinguished Researcher, Director, Innovative Photonic Network Research Center, NTT Network Innovation Laboratories.

He received a B.E. and M.E. in electrical engineering from Waseda University, Tokyo, in 1986 and 1988. He later completed a Dr.Eng. in electrical engineering from the University of Tokyo. He joined NTT Transmission Systems Laboratories in 1988, where he engaged in R&D of high-speed optical communications systems including FA-10G (the first 10-Gbit/s terrestrial optical transmission system) using erbium-doped optical fiber amplifier inline repeaters. He was with NTT Electronics Technology Corporation between 1995 and 1997, where he was involved in the planning and product development of high-speed optical modules at data rates of 10 Gbit/s and beyond. He has been with NTT Network Innovation Labs since 1997, where he has been involved in R&D of optical transport technologies based on 40/100/400-Gbit/s channels and beyond. He currently serves as Chair of the IEICE technical committee of Extremely Advanced Optical Transmission (EXAT). He is a member of the Institute of Electrical and Electronics Engineers (IEEE) and a Fellow of IEICE.

# Satellite Communications Modem Unit *COM-U*—Enhanced Maintenance, Operations, and Spectrum Utilization Efficiency of Satellite Transponders for Remote Island Satellite Communications and Disaster Relief Satellite Communications

*Hiroki Shibayama, Keishin Yano, Izumi Urata, Jun-ichi Abe, Akira Matsushita, and Fumihiro Yamashita*

## Abstract

A major advantage of satellite communications is the ability to implement communication networks virtually anywhere in Japan very simply. The NTT Group has been utilizing satellite communications to provide services in situations where optical fiber, mobile telephony, and other terrestrial facilities are impractical: remote islands, offshore areas, and stricken regions where people have been forced to temporarily flee in the face of earthquakes and other natural disasters. The Group continues to pursue research and development on satellite systems to make them more efficient and advanced. Here we present an overview of NTT's new satellite communications modem unit called COM-U (satellite circuit-terminating common unit), that markedly improves the spectrum utilization efficiency of satellite transponders and the maintenance and operations of satellite communications used for remote island and disaster relief satellite communications.

*Keywords: satellite communications, remote island satellite communications, disaster relief satellite communications*

## 1. Highly Efficient Satellite Communications System

Capitalizing on the inherent advantages of satellite communications—the ability to quickly and easily set up communications networks that provide services over an extensive area—the NTT Group is currently working to extend communications services to places that are inaccessible to optical fiber, mobile telephony, and other terrestrial infrastructure. These areas include remote islands, offshore areas, and stricken regions where people have been forced to

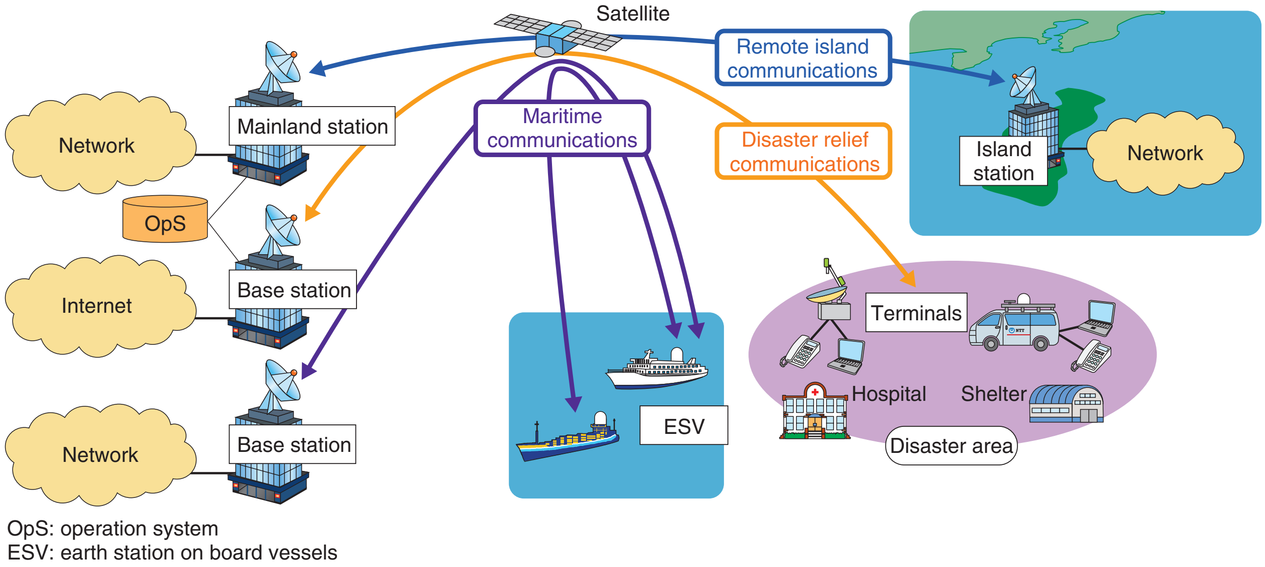


Fig. 1. Schematic overview of HESCS.

evacuate due to natural disasters. The NTT laboratories recognize the necessity and key importance of satellite communications and are therefore pursuing research and development of the Highly Efficient Satellite Communications System (HESCS) that will dramatically improve the efficiency and operability of satellite communications equipment. A schematic overview of HESCS is shown in **Fig. 1**. HESCS will support three critically important services provided by the NTT Group: disaster relief communications, maritime broadband communications, and remote island communications.

Disaster relief satellite communications can be used to provide a range of essential services in disaster-stricken areas and evacuation centers that have been hit by an earthquake or other natural disaster. Such services include special public telephones and Internet connectivity by rapid deployment of temporary radio links. Maritime broadband satellite communications can provide reliable communications services to ships and seagoing vessels, and finally, remote island satellite communications can provide communications services to residents on remote islands that are not served by submarine optical cable or to provide backup communications in the event that a submarine cable is disrupted.

A schematic illustrating HESCS that would be deployed to support remote island satellite communications is shown in **Fig. 2**. The system consists of a satellite communications modem unit called COM-U (satellite circuit-terminating common unit) featuring a highly efficient group modem module (HEGMM), a satellite circuit-terminating system unit (SYS-U) that connects transmission equipment with the COM-U, and a satellite-element management system (SAT-EMS) with monitoring and control capabilities.

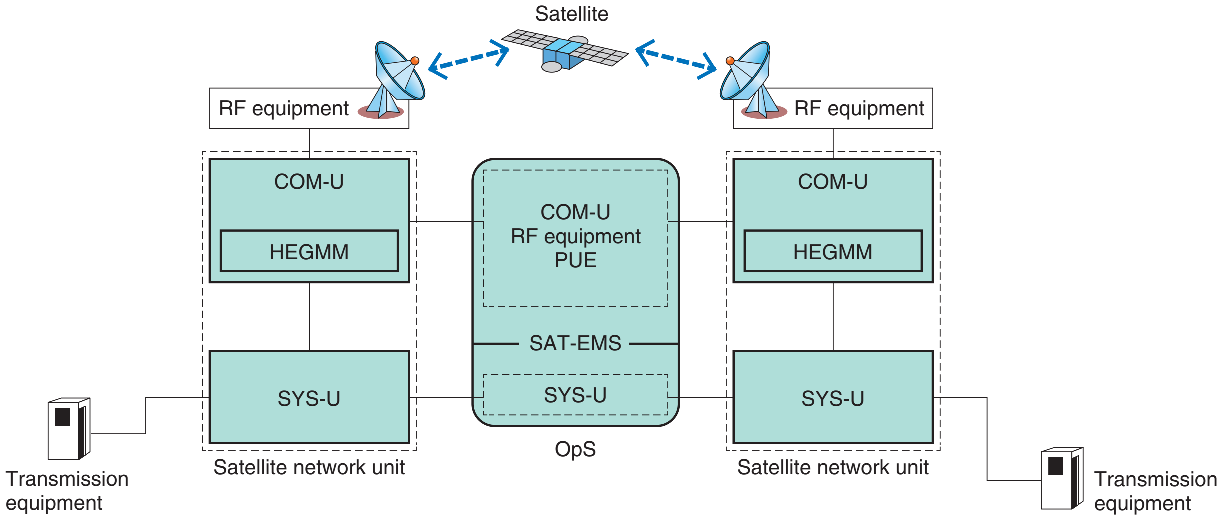
The HEGMM is essentially a key modem module with the ability to send and receive multiple satellite channels at the same time [1]. The COM-U described in this article is a satellite communications modem unit equipped with a HEGMM. In the remote island satellite communications system, the SYS-U connects terrestrial transmission equipment to the COM-U. The SAT-EMS monitors and controls the various elements of the satellite communications system including the SYS-U, COM-U, radio frequency (RF) equipment such as antennas and amplifiers, and the portable unit earth station (PUE).

## 2. COM-U development concept

In this section, we explain the concept of COM-U and the improvements achieved with it in maintenance and operations.

### 2.1 Enhanced utilization efficiency of satellite transponders

The NTT Group is currently providing services using satellite transponder bandwidth leased from satellite operators. Transponder bandwidth is costly,



COM-U: satellite circuit-terminating common unit
HEGMM: highly efficient group modem module
PUE: portable unit earth station
RF: radio frequency
SAT-EMS: satellite-element management system
SYS-U: satellite circuit-terminating system unit

Fig. 2. HESCS for remote island satellite communications.

so it is critical to utilize this bandwidth as efficiently as possible. Guard band settings between adjacent carriers can be greatly reduced by adopting a HEGMM in the COM-U that is capable of allocating carriers at arbitrary speed over arbitrary frequencies. This makes it possible to allocate carriers much closer together than with the prevailing system, which means that transponder bandwidth is significantly reduced assuming the same number of carriers. To put it another way, this markedly increases the number of carriers able to use the same frequency bandwidth.

### 2.2 Improved maintenance and operations

The components of the current system are separated function by function, and several devices interwork to terminate satellite lines. This involves a lot of wiring between devices, which requires a lot of extra effort to assemble, install, and replace the wiring. Likewise, increased wiring increases the likelihood that more wiring-related mistakes will occur.

The COM-U is compactly integrated in a single housing by packaging functionally similar components together. When the equipment malfunctions, recovery time can be minimized since the technicians only have to replace the malfunctioned package. This single housing configuration means that the number of system components to be maintained is also greatly reduced, which further improves the maintenance and operability. In addition, the various packages for the disaster relief satellite communications system and the remote island satellite communications system are commonly integrated in the same housing.

## 3. Overview of development

A functional block diagram of the COM-U is shown in **Fig. 3**. The COM-U has a disaster relief mode for disaster relief satellite communications and a remote island communications mode for remote island satellite communications, but the functional block is identical. One can see from the figure that the circuit interface connects to the network; the input data from the network are modulated by the HEGMM in the modem, and the modulated signals are then passed to the frequency converter. The signals output from the frequency converter are sent to the RF equipment, which then transmits the signals to the communication satellite transponder.

For the reception function, the RF equipment receives the signals from the satellite transponder and sends them to the COM-U frequency converter. After demodulation by the HEGMM in the modem, the data are output from the circuit interface to the network. The clock subsystem receives a clock from the clock supply module (CSM), generates the required clock in the COM-U from that clock, and distributes it to each component. The operation module is

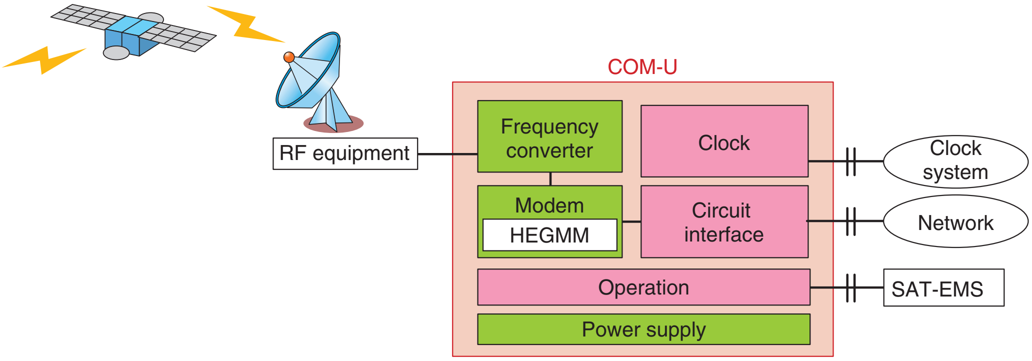


Fig. 3. Functional block diagram of COM-U.

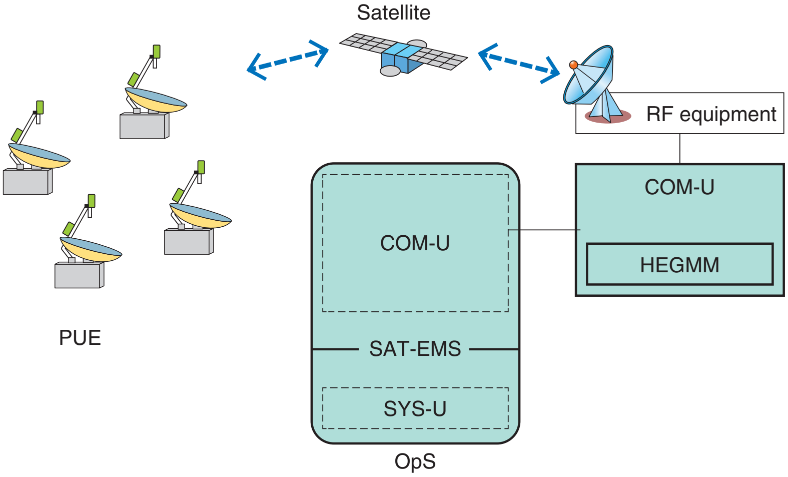


Fig. 4. HESCS for disaster relief satellite communications system.

connected to the SAT-EMS by the monitor control network; it monitors and controls the COM-U, PUE, and the RF equipment. All component modules of the COM-U act on control commands from the SAT-EMS. The modules are set, and alarms are collected from each component module. These consist of device alarms warning of equipment failures and communication alarms indicating deterioration of communication quality. These alarms are sent to the SAT-EMS.

### 3.1 Disaster relief satellite communications system

A schematic of the disaster relief satellite communications system is shown in **Fig. 4**. In this system, the COM-U connects to the Internet protocol (IP) network via the circuit interface, which interconnects via satellite channels to the PUE set up at the disaster site. The circuit interface of the COM-U for disaster relief communications is equipped with an Ethernet port for connecting to the IP network. In the outbound direction from the COM-U to the PUE, the COM-U unit supports up to thirteen 1536-kbit/s communication channels (with each channel shared by four earth stations), and in the inbound direction from the PUE to the COM-U, the COM-U supports a maximum of fifty-two 384-kbit/s communication channels. Since the current system in service uses the same frequency width and a maximum of 32 channels, the new system greatly expands the channel capacity. In addition to the channels already described, there are also control channels (CSC channels). The SAT-EMS sends control commands to the COM-U to start/stop communication and to set up channels, which are then sent on to the PUE over a CSC channel. Moreover, the COM-U can monitor the operations of up to 52 PUEs via CSC channels, and send an alarm to the SAT-EMS if a malfunction is detected.

In terms of specific services, the PUE can simultaneously provide voice (voice over IP) and IP data communications. To prioritize voice communication from the COM-U to the PUEs, the COM-U has a priority control capability it can impose on IP packets. Priority control is implemented by referring to the PCP (Priority Code Point) value in the VLAN (virtual local area network) tag of the IEEE* 802.1Q frame input from the network.

### 3.2 Remote island satellite communications system

In the remote island satellite communications system, the COM-U is connected to the SYS-U at the circuit interface. An RS-422 port is implemented at the circuit interface for remote island communication to connect to the SYS-U. Setting up COM-Us and SYS-Us on both the mainland and island means that the COM-Us are connected via satellite channels, while the transmission switching equipment is also connected by satellite links. The COM-U can simultaneously transmit and receive up to fifteen 1544-kbit/s channels.

Telephony, leased-line, and other existing services are delivered over networks using time-division multiplexing, and thus, the operation clocks of devices on the network must be precisely aligned and the entire network synchronized. To achieve network synchronization, the clocks of subordinate or slave devices must be synchronized to the clock supplied from the master clock. In terrestrial systems, clocks from the master clock are typically allocated to each building, where the CSM generates a clock based on the master clock, which the CSM distributes to all equipment in the building.

Similarly, network synchronization is required in the remote island satellite communications system in order to provide telephony and leased-line services. Network synchronization is achieved on the mainland side by the CSM, which is supplied over the terrestrial transport network, which then supplies clocks to the various COM-U and SYS-U devices.

The island side COM-Us and SYS-Us must also be synchronized to the mainland equipment, which means that the island side CSM must somehow receive a synchronized clock from the mainland CSM. In the remote island satellite communications system, the clock is transmitted to the island over a satellite channel. This is done by first generating a modulated signal in the mainland COM-U using the synchronized clock symbol rate of the mainland CSM. The modulated signal is then transmitted to the island over a satellite channel. The island COM-U then extracts the symbol rate clock from the received modulated signal. A 6.312-MHz signal is generated from the extracted clock, which is then supplied to the island CSM from the island COM-U clock transmitter. As a result of this procedure, the island CSM becomes network synchronized, and the clock is then supplied to all buildings with COM-U and SYS-U equipment on the island.

The clock is transmitted to the island over a satellite channel as we have described, but this raises the possibility that the quality of the clock sent from the COM-U to the island CSM could be degraded as a result of radio interference or another problem on the satellite channel. If a poor quality clock is sent to the island CSM, it could adversely affect all of the equipment that relies on the clock.

One solution would be to monitor the clock quality at the COM-U clock transmitter and stop the clock from being delivered if it is degraded. For example, if the satellite channel used to send the clock is out of sync, or if the reception level has fallen below a certain level, or the component in the COM-U that handles delivery of the clock has malfunctioned, clock output from the clock transmitter to the island CSM would be suspended. If any of these contingencies occur, services continue based on clock quality that is sufficient at least for the time being by having the island CSM switch over to a free-running clock.

A prototype of the new COM-U is shown in **Fig. 5**. To enhance maintenance and operations of the new system, functional capabilities are implemented as discrete packages, so problems can be quickly and easily resolved by simply swapping out the defective package. The packages are also hot pluggable, so they can be replaced with the power left on without affecting other packages or the main signal transmission. In addition, settings information for each package is backed up in the COM-U and is automatically written to any new package that is installed in the system. This permits fault handling and recovery without bringing in a technician to reset the new package when a failure occurs. The unit also includes remote lamp control, which sets off a blinking alarm on the defective package so the technician can spot the problem package immediately upon arriving at the site.

* IEEE: The Institute of Electrical and Electronics Engineers

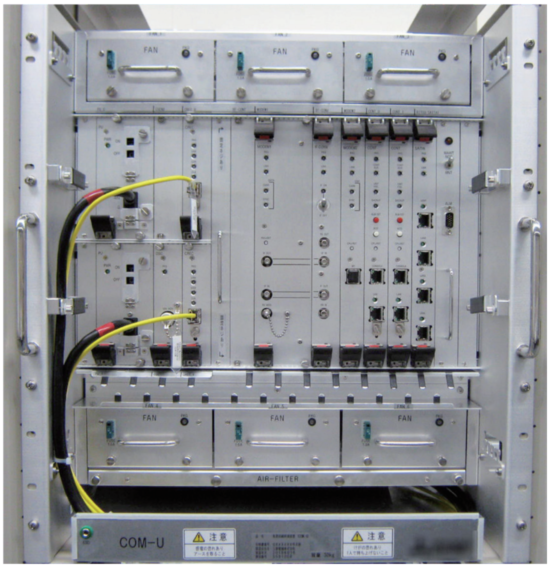


Fig. 5. Prototype of COM-U.

## 4. Future development

We described here the recent development of the COM-U module—a key component of NTT's HESCS—that is optimized to improve spectrum utilization efficiency of satellite transponders as well as maintenance and operations. Building on the progress made so far, we will continue to develop and deploy component systems including RF equipment for satellite communications systems that achieve greater cost savings and convenience.

## Acknowledgment

Part of this work (HEGMM) is being supported by the Ministry of Internal Affairs and Communications of Japan through the funds "Research and Development of Highly Efficient Frequency Use Technique for the Communication Satellite Transponder" and "Research and Development of Capacity Enhancing Technology for Satellite Communications by Employing Dynamic Polarization and Frequency Control."

## Reference

[1] F. Yamashita, K. Yamanaka, and K. Kobayashi, "Development of Highly Efficient Group Modem Module and Turbo Codec Module for Next Generation Satellite Communication Systems," NTT Technical Review, Vol. 14, No. 3, 2016.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201603ra1.html

**Hiroki Shibayama**

Senior Research Engineer, Satellite Communications Group, NTT Access Network Service Systems Laboratories.

He received a B.E. and M.E. in electrical engineering from Tokyo University of Science in 1996 and 1998. He joined NTT Radio Communication Systems Laboratories in 1998. He has been engaged in research and development of wireless LAN systems, next-generation Ethernet systems, and satellite communications systems. He is currently working on the development of a future satellite communications system. He received the Young Researcher's Award from the Institute of Electronics, Information and Communication Engineers (IEICE) in 2004. He is a member of IEICE.

**Keishin Yano**

Research Engineer, Satellite Communications Group, NTT Access Network Service Systems Laboratories.

He joined NTT in 1986 and was transferred to NTT Access Network Service Systems Laboratories in 2014. He is currently working on the development of a new satellite communications system.

**Izumi Urata**

Senior Research Engineer, Satellite Communications Group, NTT Access Network Service Systems Laboratories.

He received a B.E. in statistics analysis from the University of Tokyo in 1992 and joined NTT the same year. He worked on systems development and architecture of a graphics database server system, high-speed academic network, and a satellite communications system for marine vessels. He was transferred to NTT Access Network Service Systems Laboratories in 2012, where he contributed to developing the satellite circuit-terminating equipment known as SYS-U and the new satellite communications modem called COM-U. He is currently working on the development of a future satellite communications system for remote islands.

**Jun-ichi Abe**

Research Engineer, Satellite Communications Group, NTT Access Network Service Systems Laboratories.

He received a B.E. in computer science and an M.E. in international development engineering from Tokyo Institute of Technology in 2004 and 2006. He joined NTT Access Network Service Systems Laboratories in 2006. He is currently working on modulation and demodulation schemes for next-generation satellite communications systems. He received the Young Engineers Award from IEICE in 2013. He is a member of IEICE and IEEE.

**Akira Matsushita**

Senior Research Engineer, Satellite Communications Group, Wireless Entrance Systems Project, NTT Access Network Service Systems Laboratories.

He received a B.S. and M.S. in communication engineering from Waseda University, Tokyo, in 1993 and 1995. He joined NTT in 1995. He has mainly been engaged in research and development and commercial introduction of satellite communications systems and wireless access systems. He is currently involved in developing satellite communications systems.

**Fumihiro Yamashita**

Senior Research Engineer, Supervisor and Group Leader, Satellite Communications Group, NTT Access Network Service Systems Laboratories.

He received a B.E., M.E., and Ph.D. in electrical engineering from Kyoto University in 1996, 1998, and 2006. He joined NTT Radio Communication Systems Laboratories in 1998, where he worked on modulation and demodulation schemes for broadband mobile satellite communications systems. From 2010–2013, he was the Assistant General Manager of the NTT Research and Development Planning Department. He was transferred to NTT Access Network Service Systems Laboratories in 2013. He is currently working on the development of a new satellite communications system. He received the Excellent Paper Award of the 14th IEEE International Symposium on Personal Indoor Mobile Radio Communications (PIMRC) in 2003 and the Young Researcher's Award from IEICE in 2004. He is a member of IEICE.

# Trends in Standardization of Blockchain Technology by ISO/TC 307

*Hideyuki Iwata, Takashi Tominaga, and Takeshi Morikawa*

## Abstract

The second meeting of ISO/TC 307 (International Organization for Standardization Technical Committee 307: blockchain and electronic distributed ledger technologies) was held in Tokyo in November 2017. This TC is working to develop international standards for blockchain technology. This article introduces the concept of blockchain technology—the fundamental technology used for bitcoin—as well as trends in the international standardization of electronic distributed ledger technologies and some applications of blockchain technology beyond cryptocurrency.

*Keywords: blockchain, distributed ledger, traceability*

## 1. Introduction

In April 2016, Australia proposed to the International Organization for Standardization (ISO) to set up a technical committee (TC) on standardization of blockchain technology, which was in the spotlight as the fundamental technology of cryptocurrency, as represented by bitcoin. In September 2016, a TC on blockchain and electronic distributed ledger technologies was established (TC 307), and international standardization efforts began in the areas of *blockchain and electronic distributed ledger systems* and *application, interoperability, and data exchange between users*. The second meeting* was held in Tokyo in November 2017, following the first meeting held in Sydney in April 2017.

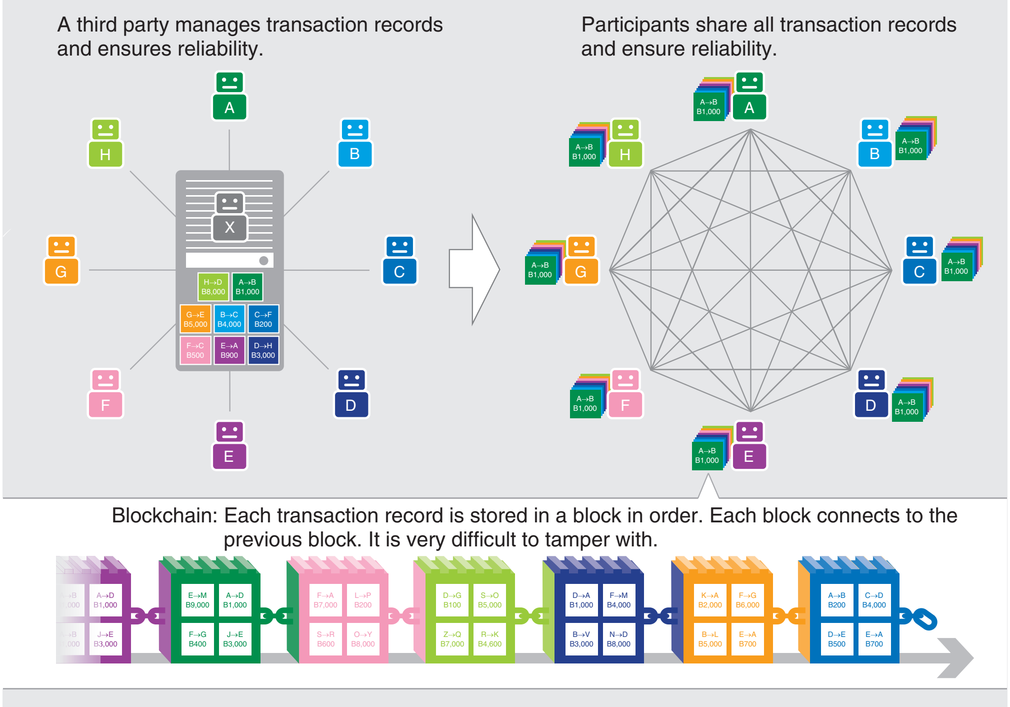
In line with international standardization efforts on blockchain technology, a domestic committee for making proposals to ISO/TC 307 was established, and JIPDEC (Japan Institute for Promotion of Digital Economy and Community) [1] took on the role of secretariat of the committee. Many Japanese organizations and companies involved with blockchain technology participated and began making recommendations. NTT and NTT DATA are the NTT Group companies participating in the domestic committee.

## 2. Standardizing the concept of blockchain

Blockchain technology is often mentioned, but it is not easy to explain it clearly in a short and simple phrase. The reason for this is that it simply is an unconventional concept. It is most commonly explained as a noncentralized ledger in a network system. The Ministry of Economy, Trade and Industry and the Financial Services Agency of Japan use the expression *distributed electronic ledger* to explain blockchain technology.

A blockchain collects a certain amount of data as a block and has a data structure connected like a chain

* Participating countries and regions: France, United States of America, Australia, United Kingdom, Germany, Denmark, Malaysia, Russia, Croatia, Japan, Korea, the Netherlands, Ireland, Austria, China, Canada, Finland, Spain, Italy, Indonesia, Luxembourg, Argentina, Iran, Hong Kong, Belgium, New Zealand, South Africa, Israel, Sweden, Norway, Switzerland, Slovakia, Singapore, Thailand, Czech Republic.



Source: Ministry of Economy, Trade and Industry, "Development of platform on digitization and service of economy and society (Research on domestic and overseas trends in services using blockchain technology)."

Fig. 1. Concept of blockchain.

(**Fig. 1**). The context of blocks forming the chain is defined using cryptographic technology. A blockchain is equivalent to a data store that takes the role of a ledger in a network system consisting of several nodes. There are many different ways for a data store to take on the role of a ledger in a network system, but the blockchain has a unique feature in terms of structure. It may be imagined that each node in a network possesses part of the ledger, and the nodes together form a ledger as an entire system (hence the idea of a distributed ledger).

In fact, though, the parts of the blockchain (ledger) that each node possesses are all the same, and thus, each node possesses a complete ledger where all transactions are recorded. The word *distributed* is used because even though there are no nodes with a centralized role in the network, the network that uses a blockchain is designed to autonomously maintain the blockchain. The point is, what is distributed is not data, but authority. Moreover, the mechanism for forming and maintaining the blockchain is typically called blockchain technology [2]. The international standardization efforts for blockchain technology in ISO/TC307 are being carried out in order to standardize the blockchain concept and the mechanism to support it.

## 3. Blockchain technology spread by standardization

A representative theme of blockchain is its use in cryptocurrency. A mechanism applying bitcoin and altocoin is being studied. Meanwhile, other uses of blockchain technology outside the area of cryptocurrency are now being studied, notably traceability and digital identity. These uses have the following characteristics:

- Many participants (including different business sectors) can use the same platform.
- Conventionally, most of the interactions have not used an information system.

Various obstacles arise when an information system used by a specific organization needs to connect to another organization's information system. Examples of such obstacles include the connection method and the emergency response method. Therefore, in some cases, paper-based work is done when connecting to another organization. Also, there may be cases in

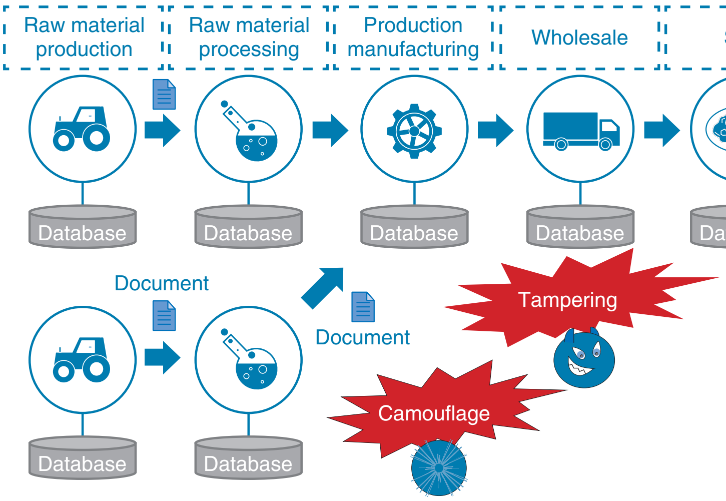


Fig. 2.   Conventional traceability system.

which documents are acquired from another organization in paper form and then have to be input to the acquiring organization's information system. These are things to consider when looking at possibilities for using the blockchain to perform tasks currently being handled using the existing system.

## 4.   Effects of blockchain when applied to traceability

Here, we explain the expected effects of applying blockchain to traceability. The example described here involves the case of a problem occurring in a product component. An investigation of such a problem would typically require a lot of time and effort to find when the component was made, which organization provided it, what type of product the component was used in, and other details. Moreover, the possibility of data tampering and/or data disappearance may need to be considered (**Fig. 2**).

A distributed ledger—the key blockchain feature—is premised on sharing information between platform participants, recording transaction information in chronological order, and easily implementing the technologies for performing these functions. New participants can easily join and leave the blockchain because it is based on the premise that information is shared between participants. When problems occur, an investigation can easily be done by tracing the data structure because the data are managed in chronological order. Also, many different types of blockchain technologies can be easily used because mechanisms to access them via smartphones as well as via a web browser are provided (**Fig. 3**).

Prompt transactions can be carried out, even with transactions that would conventionally be paper based, as information can be shared with the other organization through the blockchain by operating on a conventional computer screen. The possibility of shortening the operating time in international trade transactions has been reported [3].

## 5.   Future perspectives

This article explored the application of blockchain technology to traceability. Although positive effects can be expected in such applications, such effects may be limited because blockchain technology is still in a growth stage. Research and development of higher uses of blockchain is necessary in order to advance the technology.

For instance, the following points require further research:

- Concealment of data on blockchain [4]
- Mechanism to easily manipulate data on blockchain
- Improvement of consensus algorithm (agreement method of distributed ledger)
- Mechanism to easily connect between conventional information system and blockchain

A research network for blockchain technology called BSafe.network [5] and an industry-academia cooperation organization called BASE Alliance [6] have been established. The focus on blockchain has

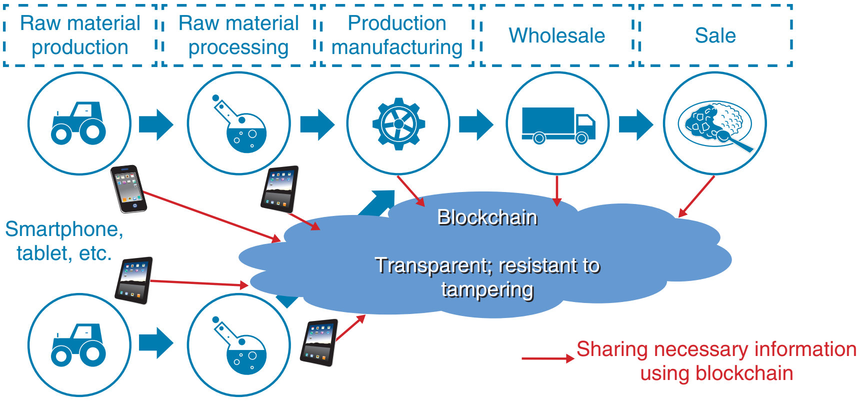


Fig. 3. Traceability system using blockchain.

thus spread to the academic sector as well.

In addition to technological development, efforts to establish legal systems and rules on system procurement by the government are also important. At the keynote speech in the opening ceremony of the Tokyo meeting, a representative from the Ministry of Economy, Trade and Industry reported on some government-leading projects as advanced use cases, including a demonstration project involving a land registry in Sweden, and a policy to create venture companies related to blockchain that was triggered by electronic governmentization (e-governmentization) efforts in Estonia.

Blockchain is certainly spreading from the elemental technology of cryptocurrency to other technology applications that use the distributed ledger. A world where the blockchain is used in an invisible part of the services that we use is not that far away.

## References

[1] Website of JIPDEC, https://english.jipdec.or.jp/

[2] J. Kishigami, S. Fujimura, H. Watanabe, S. Ohashi, and A. Nakadaira, “Introduction to Blockchain Technology,” Morikita Publishing, Tokyo, Japan, 2017 (in Japanese).

[3] Appendix to the press release issued by NTT DATA on April 24, 2017 (in Japanese). http://www.nttdata.com/jp/ja/news/release/2017/pdf/042401-01.pdf

[4] H. Watanabe, S. Ohashi, S. Fujimura, A. Nakadaira, and S. Sakuma, “Technology and Challenges of Blockchain Platforms,” IEICE Tech. Rep., Vol. 117, No. 114, ICM2017-8, pp. 21–26, 2017 (in Japanese).

[5] BSafe.network, http://bsafe.network/

[6] Keio Research Institute at SFC; Keio University Center for Socio-Global Informatics; and Institute of Industrial Science, the University of Tokyo, “Announcement of BASE Alliance Establishment,” 2017. https://www.kri.sfc.keio.ac.jp/ja/press_file/20170724_base_en.pdf

**Hideyuki Iwata**

Senior Research Engineer, Supervisor, 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 International Electrotechnical Commission (IEC) Subcommittee 86A (optical fiber and cable) since 1998 and of the International Telecommunication Union - Telecommunication Standardization Sector Telecommunication Standardization Advisory Group since 2003. He is a vice-chair of the Expert Group on Bridging the Standardization Gap in the Asia-Pacific Telecommunity Standardization Program Forum. In 2004, he received an award from the IEC Activities Promotion Committee of Japan for his contributions to standardization work in IEC.

**Takashi Tominaga**

Senior Manager, Strategic Business Creation Team, Research and Development Planning Department, NTT.

He received a B.S. in physics from Ehime University in 1995. He joined NTT in 1995 and worked at a corporate sales and service creation department of NTT WEST. Since 2017, he has been responsible for research and service creation in the area of financial technology.

**Takeshi Morikawa**

Producer/Manager, Produce Group, Research and Development Planning Department, NTT.

He Joined NTT in 1995 and was in charge of developing Internet networking systems that connected universities and elementary/secondary schools. In 2004, he was seconded to the Ministry of Economy, Trade and Industry of Japan, where he took part in establishing policies to promote home electric appliance networks. In 2007, he began overseeing the development of set-top boxes for digital broadcasting via the Internet. In 2011, he initiated the establishment of NTT SMILE ENERGY Corporation to provide maintenance services for solar power generation. He has been in his current position since 2015.

# Report on NTT R&D Forum 2018

*Yojiro Nishiyama, Hiroto Ishii, Yuji Uekusa, Haruhisa Nozue, Norio Sakaida, and Masaki Hisada*

## Abstract

NTT held NTT R&D Forum 2018 at the NTT Musashino Research and Development Center for five days from February 19 to 23, 2018, with February 19 and 21 set aside solely for the press and NTT Group employees. This article reports on the lectures and exhibits presented in the forum.

*Keywords: R&D Forum, corevo, latest technology*

## 1. Forum overview

The NTT Group is fully committed to being a value partner that continues to be sought after by customers. NTT R&D Forum 2018 presented lectures and exhibits displaying the latest research and development (R&D) results and their role in this effort. The main concept of this year's forum was Digital Technologies for a Brighter Future. Technologies related to artificial intelligence (AI), Internet of Things (IoT), media, user interfaces (UIs), networks, and security were introduced. To facilitate visitors' understanding of the latest R&D in these areas, presentations featured business cases in which research results have been commercially applied. Attendance was high and included NTT Group customers in Japan and around the world, business partners, IR (investor relation) stakeholders, and people from government agencies and universities.

## 2. Lectures and workshops

On February 20, Hiroo Unoura, NTT President and CEO, gave a keynote address entitled "Co-creating a Virtuous Cycle of New Value," in which he talked about the B2B2X (business-to-business-to-X) model, an initiative NTT is pursuing together with partners to create new value by supporting digital transformation in a variety of fields. This initiative is aimed at implementing *Society 5.0*, which is a Japanese government strategy to accelerate the penetration of digital technologies into government, industry, and society by developing innovative technologies and utilizing a diverse range of data.

For this initiative, the NTT Group is collaborating with players in various fields, including entertainment, sports, automotive, transport, manufacturing, and environmental protection. To promote digitization of industry and society and accelerate the realization of Society 5.0, NTT is proposing to build a Japanese-model ecosystem, in which a consortium of industry, academia, and government participants formed in each regional block collects and utilizes data.

As the first step, NTT concluded the Sapporo Town Planning Partner Agreement with Sapporo City. According to this agreement, three companies—namely, a department store, supermarket, and drugstore—have brought together their information about purchases made by inbound tourists so that they can analyze the data to a greater extent possible than when using only the information owned by individual companies. These analyses have enabled them to revise their marketing strategies, resulting in the creation of new earning opportunities.

The success in this unprecedented value creation prompted more than 20 companies to participate in this joint effort. This is expected to give rise to the development of new applications such as using the collected data to implement electronic payment

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

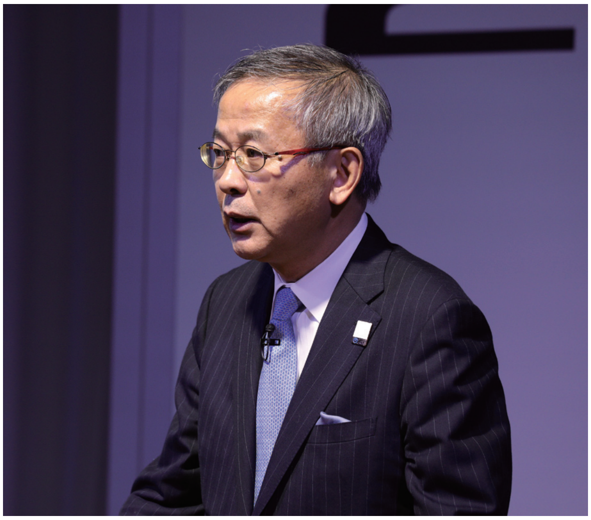


Photo 2. Keynote address by Hiromichi Shinohara, Senior Executive Vice President and Head of the Research and Development Planning Department, NTT.

systems or to share information about the operation of snow plow trucks.

NTT is pushing nationwide deployment of this Japanese-model ecosystem by expanding it from Sapporo City to the entire Hokkaido region and to other parts of the country. President Unoura expressed his commitment to bringing about Society 5.0 and to promoting value creation by supporting digital transformation in a variety of fields in collaboration with partners (**Photo 1**).

This address was followed by another keynote by Hiromichi Shinohara, NTT Senior Executive Vice President and Head of the Research and Development Planning Department, entitled “Creating a Prosperous Future through the Fruits of R&D.” He introduced NTT’s R&D activities for strengthening industrial competitiveness such as improving productivity and empowering individuals, and NTT’s efforts to overcome social problems such as by promoting safety, preventing disasters, revitalizing local economies, and ensuring a sustainable global environment.

Advances in information and communication technology make it possible to understand the intent of consumers and to provide services and information in a natural manner without requiring consumers’ conscious action. Thus, future technologies will be such that they enter our daily lives more naturally than before. Enterprises will be able to provide products that detect changes in customers’ behavior and use collected data to remain more closely connected with their needs. NTT considers AI, IoT, media, UI, networks, and security as key technical fields in which further R&D will help address social issues. Mr. Shinohara introduced the latest technologies in these fields (**Photo 2**).

In a workshop held on February 22, Hiroshi Nakamura, Executive Vice President, Chief Technology Officer, and Executive General Manager of the R&D Innovation Division of NTT DOCOMO, talked about the company’s R&D activities under the title “Co-creation Generates Smart Innovation – DOCOMO’s Strategy Toward 5G.” He introduced the fifth-generation mobile communications network (5G), which enables high-speed, high-capacity, and low-delay transmission and connections with numerous terminals, and presented cases of co-creation with partner enterprises with a focus on corevo®, the NTT Group’s initiative to utilize its AI-related technologies.

This workshop was followed by a special lecture entitled “The Future of the AI Era” by Yoshiharu Habu, professional *shogi* (Japanese chess) player. He acknowledged that shogi is a field susceptible to AI technology and talked about how AI is affecting humans. He first looked back at the history of using AI in games. He stated that the dramatic improvement in performance in recent years is enabling AI to analyze a large number of possible moves of pieces, which is in contrast to humans, who are good at developing a big-picture strategy to determine the next moves to make.

Photo 3. Special lecture by Yoshiharu Habu, professional shogi player.

It has become routine for younger members in the shogi world to use AI to study strategies. This has resulted in the revival of once-abandoned strategies and the discovery of bold moves that only AI can conceive, since unlike humans, it is fearless. He said that in this new environment, it has become even more important for shogi players to bring to bear aesthetics, originality, and identity in countering moves made by AI (**Photo 3**).

Two workshops took place on February 23. First, Ryutaro Kawamura, Vice President of NTT Network Innovation Laboratories, introduced cases in which value is created using IoT together with partners, in a workshop under the title of "IoT Activities in NTT and Its Future." Next, Hiroki Takesue, Senior Distinguished Scientist, NTT Basic Research Laboratories, gave a lecture entitled "Quantum Neural Network: a New Computer Using Light" that featured a computer system that uses various networked light emitters (lasers) to rapidly solve optimization problems that arise in various contexts in modern society.

These lectures introducing NTT's R&D activities were well received by the audience.

## 3. Exhibits of research results and sessions dedicated to specific themes

Under the concept of Digital Technologies for a Brighter Future, the forum presented 123 exhibits (about 30% more than last year's event) on the latest R&D results, which were classified into five selected exhibit themes: media & UI, corevo, IoT, network & security, and basic research. In addition, NTT Group companies, including NTT DOCOMO, NTT DATA, NTT Communications, NTT WEST, NTT EAST, and NTT i3, contributed exhibits covering a wide range of technologies, from those in the basic research stage to those that have been introduced commercially.

To enhance visitors' appreciation of the latest R&D results, exhibits were grouped in five main sites, and depending on the nature of the research, some were presented outdoors or in individual rooms, and some involved unique demonstrations.

### 3.1 Media & UI

Media processing technologies that provide user experiences with a high sense of reality and UI technologies that allow services to be tailored to individual users were introduced.

(1) Media technologies that create new value

This year, the immersive telepresence technology "Kirari!" was introduced in several usage situations together with its element technologies. In a theater-type exhibit, NTT collaborated with a stage director to produce a new sense of excitement with Kirari!. In addition, two new forms of Kirari! were exhibited: "Kirari! For Arena," which makes a new spectator experience possible by transmitting data representing the entire arena's interior, thereby enabling the user to view the arena environment from four different angles, and "Kirari! For Mobile," which works with a smartphone to enable the user to easily view a three-dimensional (3D) video.

In addition, a wide range of media technologies were introduced. "HenGenTou (Deformation Lamp)" uses some characteristics of human visual processing to create the illusion that parts of a photo or a picture are moving. "Hidden Stereo" is a stereoscopic video generation technology that provides a video that appears as a clear 2D video to the naked eye, but as a 3D video when the viewer puts on dedicated glasses (**Photo 4**).

(2) UI technologies for 202X

Technologies for diversity navigation were also exhibited. These technologies are aimed at making mobility in everyday life safer and easier. Specifically, 2.5D map position search technology provides easy-to-understand navigation with simple spoken words so that the user does not need to look up a map. Walking guide technology is aimed at enabling visually impaired persons to walk to their destinations without anxiety. There were also exhibits that

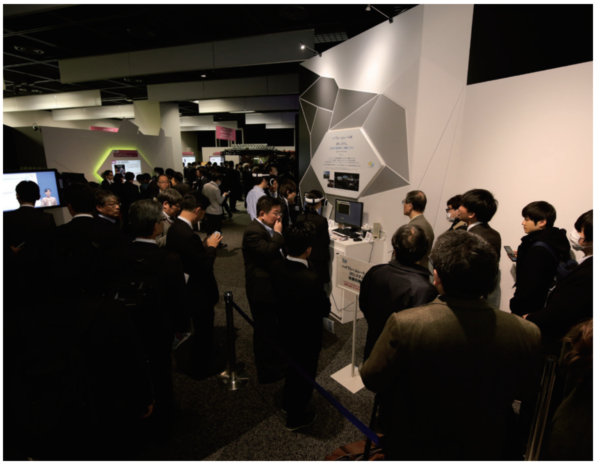


Photo 4. Media technologies that create new value.

Photo 5. AI that supports people.

introduced a wide range of UI technologies. For example, communication facilitating technology enables a natural dialog between a human and an agent played by a robot.

### 3.2 corevo

Several exhibits introduced “corevo,” an initiative that embraces the NTT Group’s-AI related technologies and services. This initiative is being accelerated so that new value will be created using AI, which is attracting interest in a wide variety of fields.

(1) AI that supports people

Agent-AI technologies were introduced that analyze speech to understand the speaker’s intention and emotion, and to provide responses in a manner as natural as those of humans. corevo@Home enables an agent to understand speech correctly and to carry out a natural dialog, while corevo@ServiceDesk understands the intention of a customer’s questions and provides service desk operators with the most appropriate information. Cross-lingual speech synthesis technology synthesizes speech in different languages using the user’s voice (**Photo 5**).

(2) AI that supports society

Ambient-AI technologies are aimed at analyzing information about humans, things, and events, and making instantaneous prediction or control possible. For example, learning-based guidance technology to estimate the flow of people from observed data on the number of people in a certain area was introduced. This technology also uses simulation to help develop an optimal guiding policy. It consists of multidimensional composite data analysis technology and spatio-temporal variables-based online-prediction technology that together predict upcoming changes from various kinds of data collected across time and space. It also uses machine learning technology.

(3) Core technologies that support corevo

Technologies that support the implementation of corevo technologies and services were introduced. Learning acceleration technology improves the stability and speed of deep learning. Encoding technology represents a huge volume of spatial information data with a small number of feature values.

### 3.3 IoT

(1) Sense, Connect & Drive

Technologies were introduced that digitize and transmit information about events that are detected by interpreting data about things. The technology of the biosensing fabric “hitoe” was introduced, together with its use in a growing variety of fields, including healthcare. Also exhibited was technology for extending the distance covered by LoRa, which collects data from sensor terminals in places that are hard for radio waves to reach (**Photo 6**).

(2) Data & Software Logistics

IoT data exchange technology enables high-speed data exchange between devices and lends itself to applications in manufacturing, as well as in automobile and ship control. Edge computing technology makes real-time distributed processing possible so that a large volume of data can be processed with low delay.

(3) Analysis & Prediction

Research results that combine big data analysis and

Photo 6. Sense, Connect & Drive.

Photo 7. Smart network operation.

deep reinforcement learning in the IoT field were introduced under the category of corevo. For example, device control technology analyzes people flows and the energy consumption of building equipment in order to optimize the control of air-conditioning and other active structural accessories.

### 3.4 Network & security

Network and security technologies aimed at enriching future society were introduced in four categories.

(1) Smart network operation

Technologies for operations that are smart and yet do not demand high skill will be required for network construction and management in the future. Technologies that use AI to support network operators or to predict imminent failures were introduced (**Photo 7**).

(2) Technologies that enhance network speed

The age of 5G is near, and 5G-related technologies that enable high-speed transmission and the construction of high-capacity optical networks were exhibited.

(3) Flexible and efficient networks

A wide range of technologies and activities were introduced that are aimed at building flexible and efficient networks with general-purpose devices or based on new architecture, such as SDx (software-defined anything) control.

(4) Security in the era of IoT/AI

Security technologies that can be applied in a wide variety of fields were exhibited. They included multi-party key exchange, secret-sharing, and anonymization technology.

### 3.5 Basic research

Basic research that will open up new horizons, and leading-edge research that will transform society by developing eco- and human-friendly technologies were introduced. The field of basic research was divided into four subthemes: communication science, quantum applications, energy manipulation, and devices. A total of 15 research results were exhibited and viewed by many visitors. Four technologies attracted special interest: tactile technology that gives a person a false sense of irregularity on a flat magnetic sheet; a biodegradable battery that decomposes into soil to minimize its impact on nature and living things; LASOLV—a quantum neural network that solves complex optimization problems at high speed; and new display device technology derived from optical circuit technologies that have been developed for optical communication.

In addition, some exhibits were more popular than had been expected. The basic research exhibit site was livelier than in previous forums (**Photo 8**).

On February 22, a live *niconico* interview took place at the forum site and was broadcast on the niconico website. The topic of the interview was the biodegradable battery. Young researchers involved in this project introduced their research results, intermixed with talks about their aspirations and private lives. The interview made the research easy to understand and was also entertaining.

## 4. Conclusion

This year, the forum was attended by about 16,000 people, a dramatic increase over last year. We believe

Photo 8. Exhibits of basic research.

that rising expectations for NTT's R&D were the reason for the growth in the number of participants. This was substantiated by voices heard at the forum site and in responses to our questionnaire survey. To meet these ardent expectations for our R&D, we will make even greater efforts to develop and deploy new technologies.

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

# Japan-Taiwan Joint Experiment Successfully Demonstrates White-box Based Carrier-grade Networking—International Service Provider Collaboration in Software-defined Networking Pushes Forward IP Packet Transport to Employ Commodity Products

## 1. Introduction

NTT and Chunghwa Telecom succeeded in carrying out joint experiments in collaboration with ITOCHU Corporation and ITOCHU Techno-Solutions Corporation (CTC) to verify the service continuity and reliability required by telecommunications carriers for virtual network control. These experiments were made possible by the combination of NTT's Multi-Service Fabric (MSF) and Chunghwa Telecom's orchestrator called NAPA (Network Adapter with Programmability and Automation). MSF is technology for organizing white-box switches to work as an Internet protocol (IP) transport network. NAPA controls various products in response to user requirements.

In 2015, the four companies began jointly studying software-defined networking and network functions virtualization (SDN/NFV) technologies with the aim of establishing network technologies to quickly respond to a wide range of needs with architecture that maximizes the use of commodity network products.

The results of these experiments confirmed that highly reliable networks with high resistance to failure are possible by maximizing the functionality of white-box switches, which has led to further advances in studies on future application of white-box switches to commercial networks.

## 2. Background to joint experiments and history of cooperation

In recent years, carriers have not only been required to reduce costs but also to provide networks that can respond quickly and flexibly to the dramatic increase in traffic and to the growing diversification of network uses. In order to achieve this, it is becoming more important to utilize globally used common, generic technologies and products, rather than simply relying on traditional carrier network products. This has led NTT and Chunghwa Telecom to work on solving issues across wide areas of telecommunications carrier networks.

Collaborative studies in the SDN/NFV fields began in September 2015 on IP packet transport SDN technologies and in April 2016 on NFV technologies. In February 2017, NTT, Chunghwa Telecom, ITOCHU, and CTC signed a memorandum of understanding (MoU) on joint research and experiments. The four companies agreed to focus on achieving commonization of SDN technologies to develop networks that

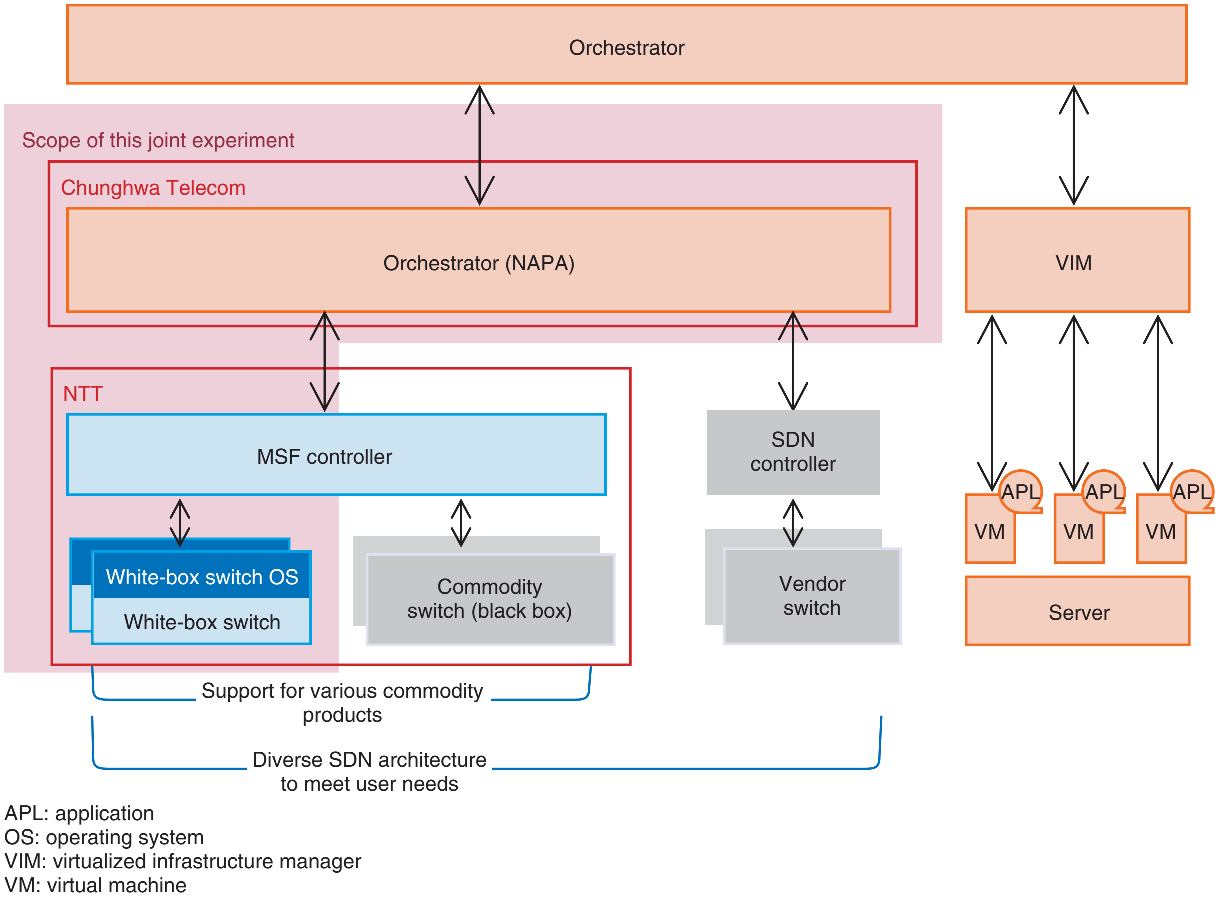


Fig. 1. Structure of the datacenter network service and scope of the joint experiments.

will satisfy various needs and to proactively use generic network products (switches etc.) under this MoU.

As part of the IP packet transport SDN technology studies that have been ongoing since the outset of this partnership, studies on white-box switch applicability for telecommunications carrier networks have been continuing, and the results of the joint experiments have successfully confirmed the applicability of these switches in the area of datacenter networks. Specifically, virtual network configuration and control technologies using white-box switches and white-box switch operating systems were verified by controlling MSF from NAPA (**Fig. 1**).

Simulations were carried out to confirm failures that were assumed to occur in telecommunications carrier network operations such as redundancy with controller failures and automatic communication route switching with white-box switch failures, and the simulation results indicated that the technology was reliable, which will enable service continuity.

These experiments ran for two weeks in the Chunghwa Telecom Laboratories in Taoyuan City, Taiwan, and finished on December 1, 2017. ITOCHU supported the technical coordination and collaboration with Chunghwa Telecom and Taiwan manufacturers, while CTC provided white-box switch (hardware and software) integration support.

**For Inquiries**

Public Relations, Planning Department,
NTT Information Network Laboratory Group
http://www.ntt.co.jp/news2017/1712e/171212a.html

# External Awards

### Spotlight on Optics

**Winner:** Toru Kawakami, Tohoku University; Munekazu Date, NTT Media Intelligence Laboratories; Mutsumi Sasai, Tohoku University; Hideaki Takada, NTT Media Intelligence Laboratories
**Date:** October 5, 2017
**Organization:** The Optical Society (OSA)

For "360-degree Screen-free Floating 3D Image in a Crystal Ball Using a Spatially Imaged Iris and Rotational Multiview DFD Technologies."

A rotational multiview depth-fused 3D (DFD) display and 360-deg displaying optics using a spatially imaged iris method are proposed to realize a 360-deg 3D image. This method enables displaying clear floating images in a crystal ball. Its symmetric optics provide clear and natural 360-deg images with smooth motion parallax in horizontal and vertical directions using the directional selectivity of a spatially imaged iris method and natural 3D images of a rotational multiview DFD display.
**Published as:** T. Kawakami, M. Date, M. Sasai, and H. Takada, "360-degree Screen-free Floating 3D Image in a Crystal Ball Using a Spatially Imaged Iris and Rotational Multiview DFD Technologies," Appl. Opt., Vol. 56, No. 22, pp. 6156–6167, 2017.

### ISUILS Best Poster Presenter Award

**Winner:** Katsuya Oguri, NTT Basic Research Laboratories
**Date:** November 2, 2017
**Organization:** International Symposium on Ultrafast Intense Laser Science XVI (ISUILS2017)

For "Development of Time-resolved ARPES and Absorption Spectroscopy System Based on Quasi-monocycle-pulse Driven High-order Harmonic Source."

We have developed a time-resolved ARPES (angle-resolved photoemission spectroscopy) and absorption spectroscopy system based on a quasi-monocycle-pulse driven high-order harmonic source driven by 20-5 fs NIR (near infrared) pulses. This system can be expected to measure electron dynamics in the whole Brillouin zone at less than 5 fs temporal resolution.
**Published as:** K. Toume, K. Oguri, H. Mashiko, K. Kato, A. Suda, and H. Gotoh, "Development of Time-resolved ARPES and Absorption Spectroscopy System Based on Quasi-monocycle-pulse Driven High-order Harmonic Source," ISUILS2017, Lijiang, China, Oct./Nov. 2017.

### Major results of 2016 from Nanotechnology Platform Japan program

**Winner:** Masayuki Hashisaka and Koji Muraki, NTT Basic Research Laboratories; Toshimasa Fujisawa, Tokyo Institute of Technology
**Date:** February 14, 2018
**Organization:** Nanotechnology Platform Japan program by the Ministry of Education, Culture, Sports, Science and Technology

For research on charge dynamics in quantum Hall edge channels.

This award is given for fine results obtained with the help of Nanotechnology Platform Japan. The research topics are one-dimensional electron dynamics in a quantum Hall Tomonaga-Luttinger liquid and time-domain observation of spin-charge separation in quantum Hall edge channels.

### Excellent Interactive Award

**Winner:** Atsushi Otsuka, Kyosuke Nishida, Itsumi Saito, Hisako Asano, and Junji Tomita, NTT Media Intelligence Laboratories
**Date:** March 6, 2018
**Organization:** The 10th Forum on Data Engineering and Information Management (DEIM2018)

For "Neural Network Based Question Generation Model for Identifying Question Intention" (in Japanese).
**Published as:** A. Otsuka, K. Nishida, I. Saito, H. Asano, and J. Tomita, "Neural Network Based Question Generation Model for Identifying Question Intention," DEIM2018, Fukui, Japan, Mar. 2018.

### NLP2018 Best Paper Award

**Winner:** Kyosuke Nishida, Itsumi Saito, Atsushi Otsuka, Hisako Asano, and Junji Tomita, NTT Media Intelligence Laboratories
**Date:** March 12, 2018
**Organization:** The Association for Natural Language Processing

For "Large-scale Machine Reading Comprehension with Multi-task Learning of Information Retrieval" (in Japanese).
**Published as:** K. Nishida, I. Saito, A. Otsuka, H. Asano, and J. Tomita, "Large-scale Machine Reading Comprehension with Multi-task Learning of Information Retrieval," The 24th Annual Meeting of the Association for Natural Language Processing (NLP2018), D5-2, Okayama, Japan, Mar. 2018.

### Awaya Prize Young Researcher Award

**Winner:** Yusuke Ijima, NTT Media Intelligence Laboratories
**Date:** March 14, 2018
**Organization:** The Acoustical Society of Japan (ASJ)

For "Performance Evaluation of Prosody Aware Word-level Encoder for DNN-based Speech Synthesis."
**Published as:** Y. Ijima, N. Hojo, R. Masumura, and T. Asami, "Performance Evaluation of Prosody Aware Word-level Encoder for DNN-based Speech Synthesis," Proc. of ASJ Autumn Meeting, 1-R-43, pp. 261–262, Ehime, Japan, Sept. 2017.

### Young Researcher's Award

**Winner:** Takuto Kimura, NTT Network Technology Laboratories
**Date:** March 22, 2018
**Organization:** The Institute of Electronics, Information and Communication Engineers (IEICE)

For "A Study of Throughphut Estimation Method for Mobile Video Streaming."
**Published as:** T. Kimura, T. Okuyama, A. Matsumoto, and T. Hayashi, "A Study of Throughput Estimation Method for Mobile Video Streaming," Proc. of the 2017 IEICE General Conference, B-11-10, Nagoya, Aichi, Japan, Mar. 2017.

### Young Researcher's Award

**Winner:** Go Itami, NTT Network Technology Laboratories
**Date:** March 22, 2018
**Organization:** IEICE

For "A Study on Filtering Characteristics of FSS for Advanced EM Shielding."

**Published as:** Go Itami, Y. Toriumi, and K. Takaya, "A Study on Filtering Characteristics of FSS for the Advanced EM Shielding," Proc. of the 2017 IEICE General Conference, B-4-17, Nagoya, Aichi, Japan, Mar. 2017.

### EMCJ Young Engineer Award in 2017

**Winner:** Go Itami, NTT Network Technology Laboratories
**Date:** March 22, 2018
**Organization:** IEICE Technical Committee on Electromagnetic Compatibility (EMCJ)

For "An Analytical Study on the Advanced EM Shielding for Mobile Devices to Provide Sufficient Transparency in Frequency Bands Used for Wireless Communications and Attenuation in Other Frequencies."

This paper describes a proposal of an advanced electromagnetic shield, which realizes both the suppression of electromagnetic radiation, and wireless communications, by applying electromagnetic-controllable materials on the shield, which is called a frequency selective surface (FSS). We have studied resonator structures of the FSS by electromagnetic field analysis, focusing on the number and center values of resonant frequencies of the FSS while considering size limitations. As a result, we have found the multi-band resonance of the FSS by applying self-similarity structures on it and found a downward shift of the resonant frequency of the FSS by extending its electrical pathways.

**Published as:** Go Itami, Y. Toriumi, and K. Takaya, "An Analytical Study on the Advanced EM Shielding for Mobile Devices to Provide Sufficient Transparency in Frequency Bands Used for Wireless Communications and Attenuation in Other Frequencies," IEICE Tech. Rep., Vol. 116, No. 399, EMCJ2016-117, pp. 45–50, 2017.

# Papers Published in Technical Journals and Conference Proceedings

### Speech Rhythm in Adults with Autism Spectrum Disorders

I. Lin, S. Hiroya, K. Asada, S. Ayaya, S. Kumagaya, and M. Kato

Acoustical Science and Technology, Vol. 39, No. 2, pp. 154–157, March 2018.

This paper examined speech in well-controlled speech materials of adults with and without autism spectrum disorders (ASD). The results show that ASD participants had longer phoneme duration for unvoiced consonants /t/ and /k/ and shorter phoneme duration for voiced consonants /d/, /g/, and /r,l/. Otherwise, there was no significant between-group difference in speech fluency, pause durations, voice onset times (for /d/, /g/, /t/, and /k/), phoneme errors, fundamental frequency, or formants. This indicates that ASD adults might have some residual errors due to audio-vocal control.

---

### Ultrafast Terahertz Nonlinear Optics of Landau Level Transitions in a Monolayer Graphene

G. Yumoto, R. Matsunaga, H. Hibino, and R. Shimano

Physical Review Letters, Vol. 120, No. 10, 107401, March 2018.

We investigated the ultrafast terahertz (THz) nonlinearity in a monolayer graphene under a strong magnetic field using THz pump-THz probe spectroscopy. An ultrafast suppression of the Faraday rotation associated with inter-Landau level (LL) transitions is observed, reflecting the Dirac electron character of nonequidistant LLs with large transition dipole moments. A drastic modulation of electron distribution in LLs is induced by far off-resonant THz pulse excitation in the transparent region. Numerical simulation based on the density matrix formalism without rotating-wave approximation reproduces the experimental results. Our results indicate that the strong light-matter coupling regime is realized in graphene, with the Rabi frequency exceeding the carrier wave frequency and even the relevant energy scale of the inter-LL transition.

---

### Correlation Analysis between Code Clone Metrics and Project Data on the Same Specification Projects

Y. Higo, S. Matsumoto, S. Kusumoto, T. Fujinami, and T. Hoshino

Proc. of the 12th International Workshop on Software Clones (IWSC 2018), pp. 37–43, Campobasso, Italy, March 2018.

The presence of code clones is pointed out as a factor that makes software maintenance more difficult. On the other hand, some research studies reported that only a small part of code clones requires simultaneous changes, and their negative influences on software maintenance are limited. Some other studies reported that code clones often have positive effects on software development. Currently, the authors are researching exploring the effect of clones on software development and maintenance. In this paper, the authors report their exploratory results on the relationship between clone metrics and project data such as the number of test cases and the number of found bugs. The targets of this exploration are nine web-based software systems. Interestingly, all of them were developed based on the same specifications. In other words, they are functionally the same software systems. By targeting such projects, we can explore how implementation differences affect software development. As a result, unit/integration/system testing become more difficult in cases where many clones exist in a project.

---