# 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.

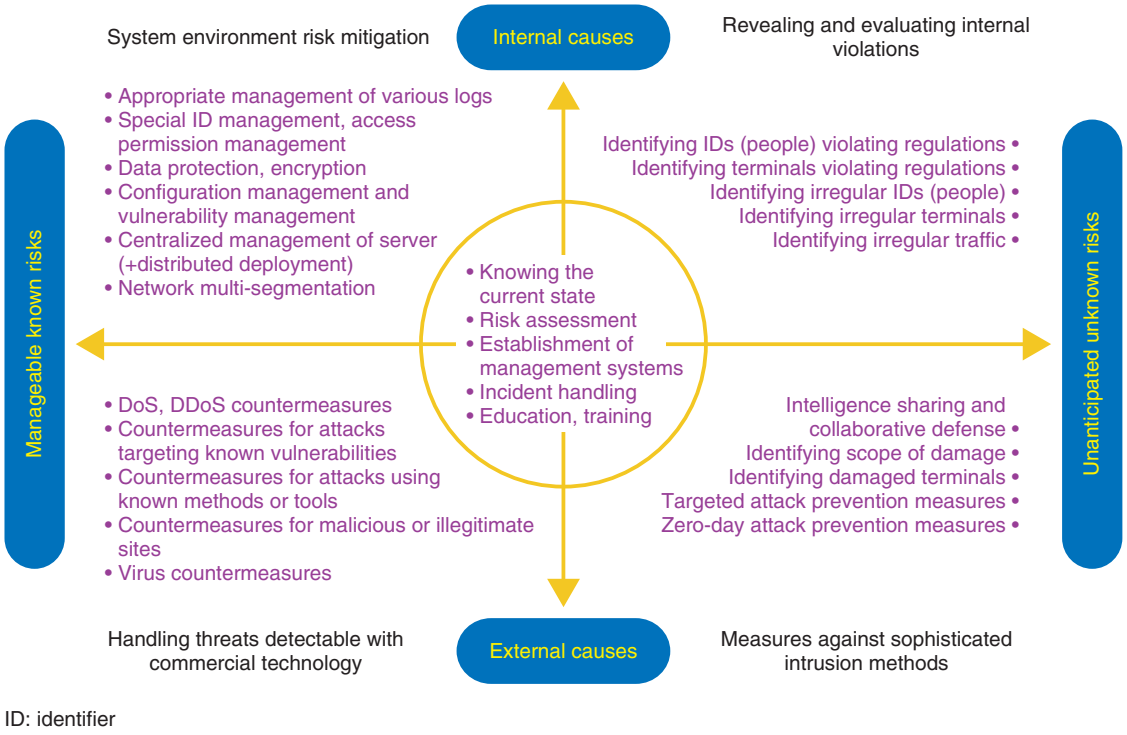
## 2. NTT Communications security measures and business development

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




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

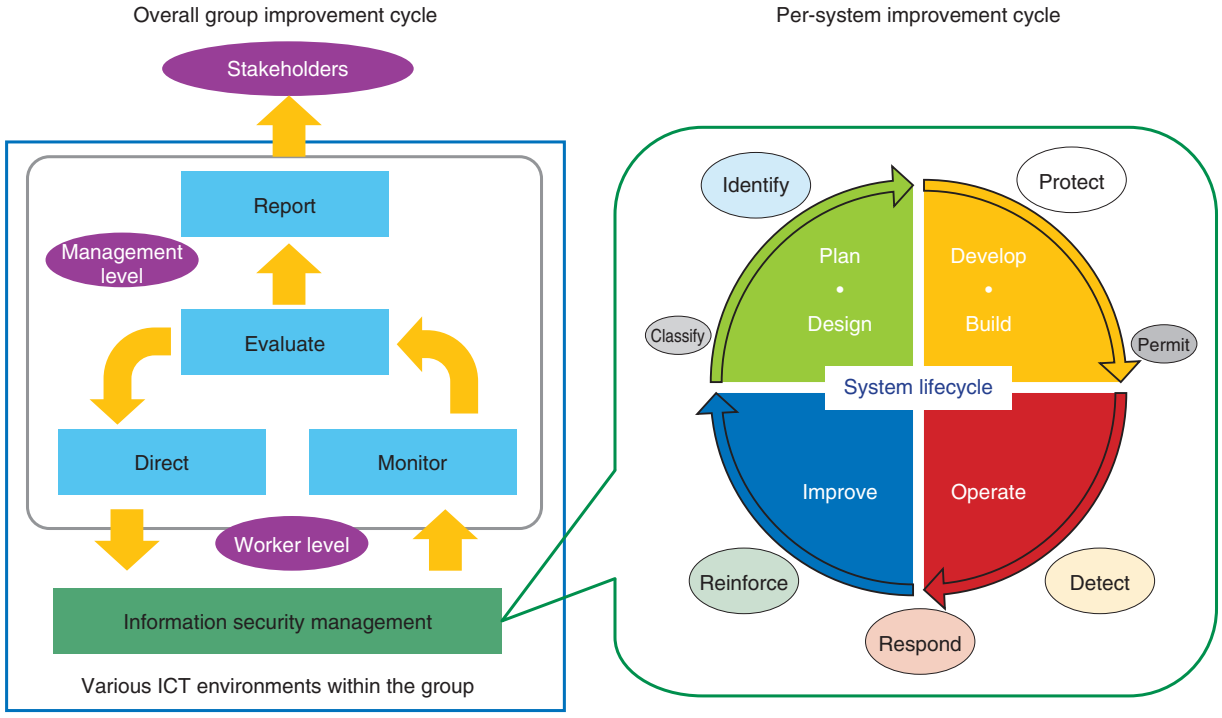



Fig. 2. Establishment of improvement cycle anticipating unknown risks (plan, do, check, act cycle).

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

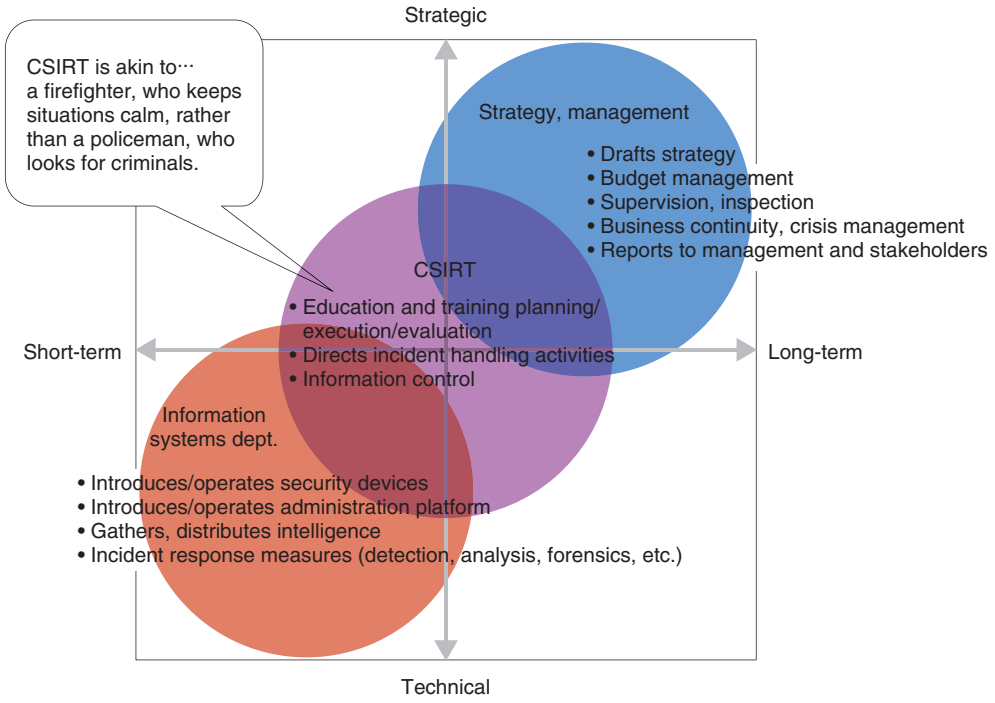



Fig. 3. Overall image of risk management system.

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

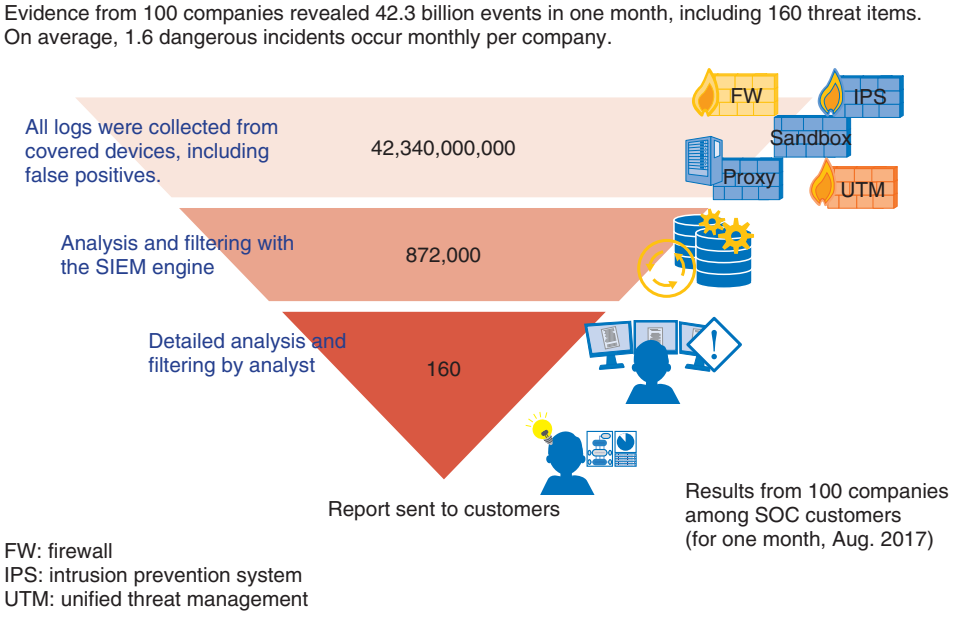



Fig. 4. SIEM effectiveness (August 2017 results).

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

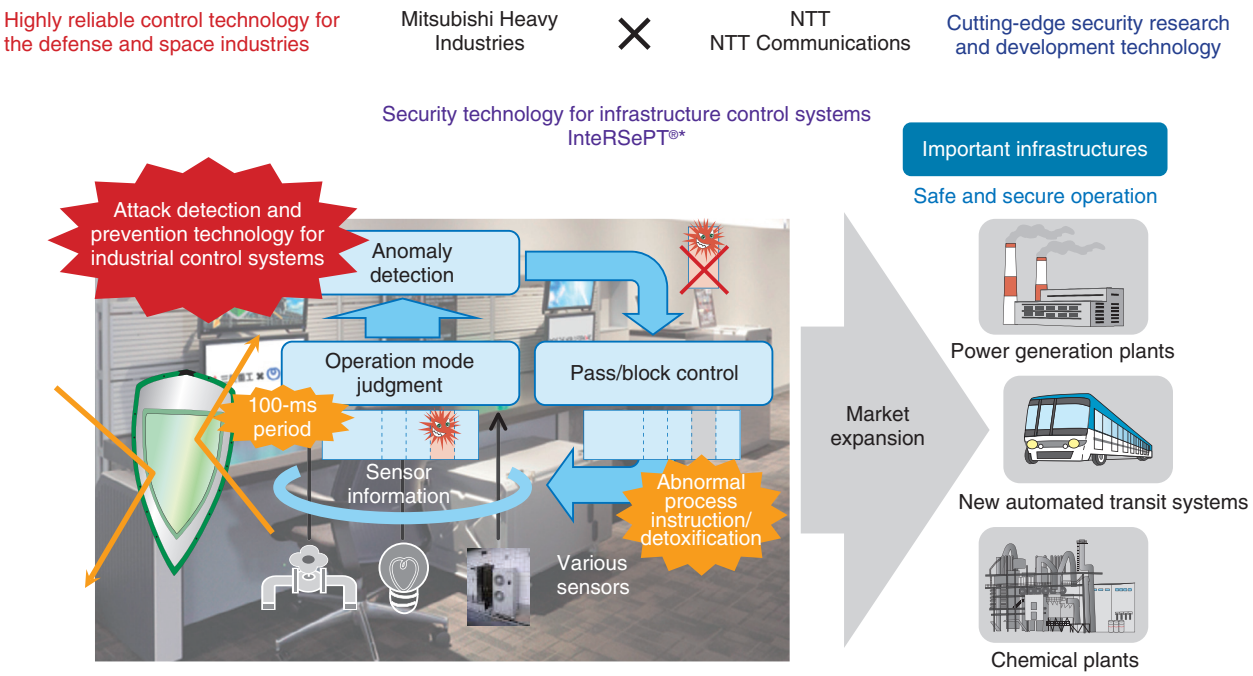
A critical infrastructure system consists of the ICT domain (information systems) and the OT domain (industrial control systems). Industrial control systems are operated (and have been for decades) 24 hours a day, 7 days a week, and they require high availability. In contrast, information systems are 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.




* "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

**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.