Cybersecurity Solutions for Major International Events

● Taishu Ohta ● Masahiko Takenaka ● Masaaki Katou ● Ryusuke Masuoka
● Kousetsu Kayama ● Noriaki Fukushima ● Hosei Imai

The development of IoT has been progressing rapidly, resulting in an expanding cyberspace. However, there is a risk of an increasing number of sophisticated cyber attacks. Major international events often act as the driving force for a host country's dignity, and are exposed to large-scale attacks from all over the world. Japan is faced with the major challenge of establishing an ecosystem that enhances its cybersecurity capabilities. Fujitsu has proposed that the Japanese government improve the self-sufficiency of cybersecurity technology to build this ecosystem. Fujitsu itself has been focusing on developing technology domestically and training security engineers to counter the prospective shortage of talent. Through these efforts, we will contribute to the creation of an ecosystem to support society beyond 2020 as a social legacy. This paper describes the important perspectives of cybersecurity that will support society in 2020 and beyond. It also presents Fujitsu's initiatives in technology and personnel development.

1. Introduction

A series of major international sporting events scheduled around 2020 is expected to provide the basis for a "data-driven society" in which data gives birth to value through advanced technologies such as IoT and AI. This assumption makes cybersecurity a necessity. In Japan, we can expect a restructuring of the social infrastructure through sporting events to serve as the foundation for cybersecurity in 2020 and beyond.

Today, damage caused by cyber attacks extends beyond information leaks to critical social infrastructures such as power utilities and transportation systems. Recent years have seen a dramatic increase in ransomware, such as WannaCry that targets an indefinite number of computers, and distributed denial of service (DDoS) attacks that use the Mirai botnet to exploit vulnerabilities of IoT devices. The holding of major international events, therefore, raises the possibility of large-scale cyber attacks from anywhere in the world and an increase in cyber attacks targeting the host countries. Looking forward to 2020, cyberspace is expected to increase dramatically as the number of IoT devices reaches about 30 billion, so a further increase in highly sophisticated cyber attacks must be expected.[1)]

Under these conditions, preventing all attacks is difficult. In fact, major events for which an increase in cyber attacks can be expected must be dealt with by treating attacks or security accidents as a precondition. With this in mind, there will be a need going forward for "detection, response, and recovery," "information sharing among related organizations," and "personnel development to support the above activities." Building an ecosystem to link all of the above is therefore a challenge to be addressed. Fujitsu is putting technology development and personnel development into practice to support the above areas (**Figure 1**). Furthermore, to facilitate the creation and development of a cybersecurity infrastructure for 2020 and beyond in Japan, Fujitsu proposes that the Japanese government takes steps to improve self-sufficiency in cybersecurity technologies.

From the viewpoint of building a cybersecurity ecosystem, this paper describes the domestic development of technologies for reducing operating costs and shortening recovery times, coordinating threat information effectively, performing packet capturing that can accommodate the disruptive expansion of cyberspace, and discovering new occurrences of unauthorized communications. It also describes the personnel development for putting the development and operation of

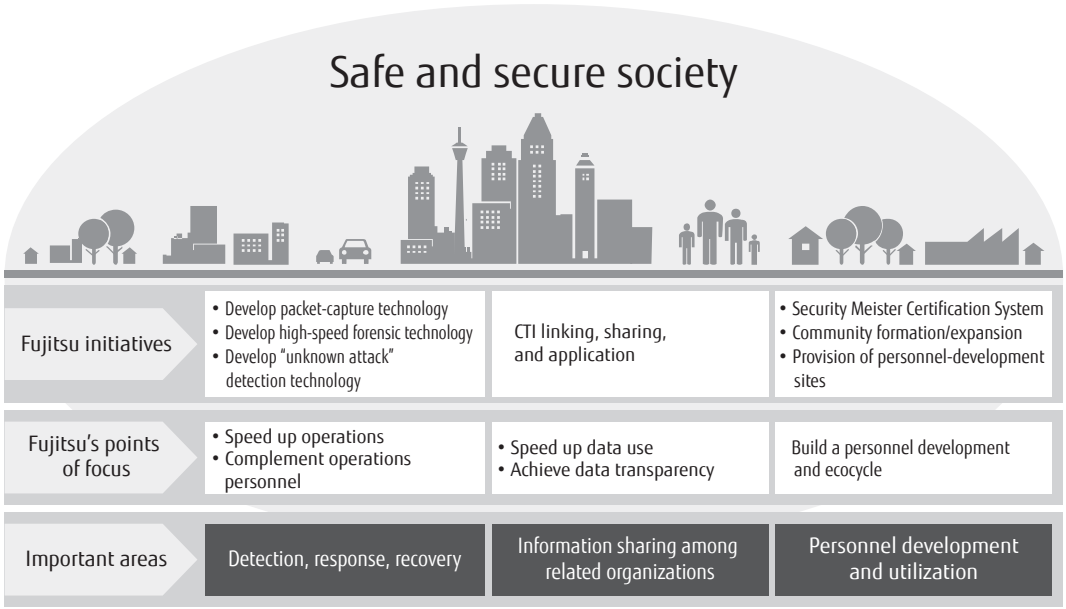


Figure 1
Important areas supporting major events.

these technologies into practice.

2. Ecosystem via major international sporting events

Today, in an era in which attackers use cyberspace freely to meet their objectives, it is important to improve the technical competence of individual users and reinforce the connections between them. Moreover, to promote digital innovation that uses cyberspace to the maximum, an ecosystem must be built in which many individuals can cooperate with each other in making cyberspace safe. Fujitsu seeks to contribute to the further evolution of domestically developed technology, to personnel development, and to the creation of a safe and secure society for 2020 and beyond through the formation of social rules.

To build such an ecosystem, we need to have an accurate understanding of the objectives of cyber attacks mounted against major international sporting events. In this regard, an event held as a matter of national prestige requires that countermeasures be formulated at the national level to prevent any attempt at obstructing the event. In addition, the objectives of attacks mounted by criminal organizations or politically/ideologically motivated attackers may extend beyond financial gain or harassment to terrorist activities, blackmail, etc.

With this in mind, we consider that DDoS attacks will become the most common type of attack for obstructing events. The successful mounting of such an attack generally requires repetitive espionage activities conducted through various types of advanced persistent threat (APT) attacks mounted against related institutions or enterprises. Such activities will likely be repeated until a sufficient number of computers and IoT devices have been hijacked to participate in the DDoS attack.

To counter such an attack, devices converted to bots by such activities must be removed and an ecosystem that contributes to Internet safety must be built. This requires that the following three requirements be satisfied and coordinated.

1) Mechanism for becoming aware of attacks and responding quickly based on new technological approaches
2) Mechanism for quickly sharing information on threats made against society
3) Training of advanced security engineers having high moral standards in step with the formation of an appropriate community

3. Fujitsu initiatives in domestic technology development

The following describes technology development initiatives at Fujitsu to satisfy the three requirements described above.

3.1 Strategic Innovation Promotion Program (SIP)

With a view to 2020, the "Cybersecurity for Critical Infrastructure" program under the management of the New Energy and Industrial Technology Development Organization (NEDO) was added to the Cross-ministerial Strategic Innovation Promotion Program (SIP) led by the Cabinet Office, Government of Japan. Coordinated among government, industry, and academic entities, SIP features an all-encompassing approach from research to social implementation.[2)]

In this program, Fujitsu is conducting research and development with a focus on the information-communications infrastructure as head of "soundness determination technology through traffic analysis of information/control network devices." Given the recent manifestation of diverse cyber attacks on critical infrastructures, the aim of this R&D is to detect active threats within organizations and to recommend countermeasures against intrusions that cannot be completely prevented. In this regard, an information-communications platform serving as a critical infrastructure has traditionally been made up of all types of old and new devices.

Today, however, such infrastructures are rapidly being converted to virtual systems and networks through the adoption of widely used technologies. With this being the case, Fujitsu aims to adopt a technique for monitoring and analyzing communication packets that can be easily introduced by adding only a minimal amount of equipment and that can operate without interfering with devices in operation.

To this end, Fujitsu is researching and developing the following three topics:

1) Visualization of virtual space through the high-performance packet collection technology supporting a virtualized system and network
2) Low-cost and high-scalability systems through the high-speed packet storage and retrieval technology that uses general-purpose servers in parallel
3) Extraction of a small number of devices performing suspicious communications from a massive volume of communication data through the collective-behavior analysis technology focusing on regularity and relation in communications.

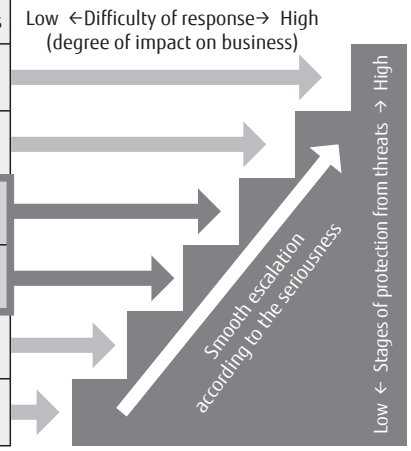
Furthermore, believing that stability and continuity of critical infrastructures and services are of prime importance on implementing security measures, Fujitsu is also working to support such measures and escalation processes based on technology for recommending countermeasures commensurate with urgency and business importance. Among the levels shown in **Figure 2**, levels 2 and 3, which correspond to the activities of a security operations center (SOC) operator and responders of a computer security incident response team (CSIRT), are considered to be especially important. These operators and responders suffer from staffing shortages and task overload, so the plan is to provide support by presenting recommended countermeasures.

As part of this R&D, Fujitsu has developed key technologies. First, as a high-performance packet collection technology, we have developed a lossless packet capture technology operating at a rate of 10 Gbps, approximately seven times faster than that of any existing technology, which is a world first. Next, as a high-speed packet storage and retrieval technology, we have developed a technology for storing collected communication data in real time at a rate of 100 Gbps by sorting the data among different storage destinations in accordance with data type.[3)] From here on, Fujitsu aims to promote the real-world implementation of these technologies together with infrastructure operators and contribute to the stable operation of information-communications infrastructures during event periods.

3.2 High-speed forensic technology

At present, the most common approach to dealing with a cyber attack after detecting an intrusion is manual malware analysis. Such analysis requires advanced knowledge, but there has been a constant shortage of personnel with such skills. Even at a general level, this deficiency in information-security personnel is becoming quite serious. A study conducted by the Ministry of Economy, Trade and Industry has found that this shortfall in human resources will increase to about 190,000 people by 2020.[4)]

Threat detection level (definition)		Person who determines countermeasures	Viewpoint of countermeasures
Level 5	Detecting abnormal operations on business and/or service	Top management	To continue business in accordance with BCP
Level 4	Detecting abnormal system behavior	Chief information security officer (CISO)	To keep system in good condition
Level 3	Detecting chain of abnormal states (spreading infection) in internal network	Computer security incident response team (CSIRT)	To improve system stability
Level 2	Detecting malicious communication (C&C communication) with external network	Security operator (SOC)	To identify substantial impact
Level 1	Detecting impact on internal network	Network operator at NOC	To identify and eliminate the victims
Level 0	Detecting attack from external network	Tools installed in equipment	To identify and eliminate the victims



BCP: Business continuity planning
NOC: Network operations center
SOC: Security operations center
C&C: Command and control

Figure 2
Threat detection level and countermeasure escalation.

In response to this problem, Fujitsu developed "high-speed forensic technology" that even general-level information-security personnel can use to deal with a sophisticated attack after intrusion.[5,6] It is known that malware that has infiltrated an organization through a cyber attack can repeatedly log in illicitly and spread viruses using the Windows remote-operation command. This technology can reconfigure a remote-operation command in real time from actual communications and can record it together with information on the user performing that operation. Consequently, if a sensor equipped with this technology were to be installed within an organization to monitor internal communications, it would be possible to comprehend in detail the progress status of an attack that has infiltrated the organization. Additionally, this data could be used to present an overall picture of the attack's range of impact (**Figure 3**).

In short, using Fujitsu's high-speed forensic technology in this way makes it possible to visualize the state of progress and range of impact of an attack that has infiltrated an organization. This enables even general-level information-security personnel to initiate advanced countermeasures, which helps in resolving the shortage of qualified personnel while greatly shortening the time required to restore the soundness of the network.[7]

3.3 Utilization of cyber threat intelligence: S-TIP

One of the keys to building an ecosystem to make cyberspace safer is cyber threat intelligence (CTI), which essentially describes the who, when, why, where, what, and how (5W1H) of a cyber attack. That is, it would describe who was behind the attack, its timeframe (when), why and where it was mounted, what were the attack indicators, and how it was carried out. The use of CTI enables proactive responses such as deploying defensive resources effectively on the basis of the inferred attacker' intentions and trend analysis of cyber attacks.

CTI can be broadly divided into human CTI and system CTI. Human CTI consists of knowledge related to cyber attacks that is consumed by people through security-dedicated social media, e-mail and other media. System CTI, on the other hand, consists of attack-related knowledge that is consumed by systems in a format that can be understood by computers, namely, Structured Threat Information eXpression (STIX).[8)-10)] Human CTI contains much contextual information that can be effective in obtaining an overall picture of a cyber attack. System CTI, meanwhile, being knowledge exchanged between computers, can be shared at extremely high speeds. System CTI is also amenable to automation. For example, malicious IP addresses

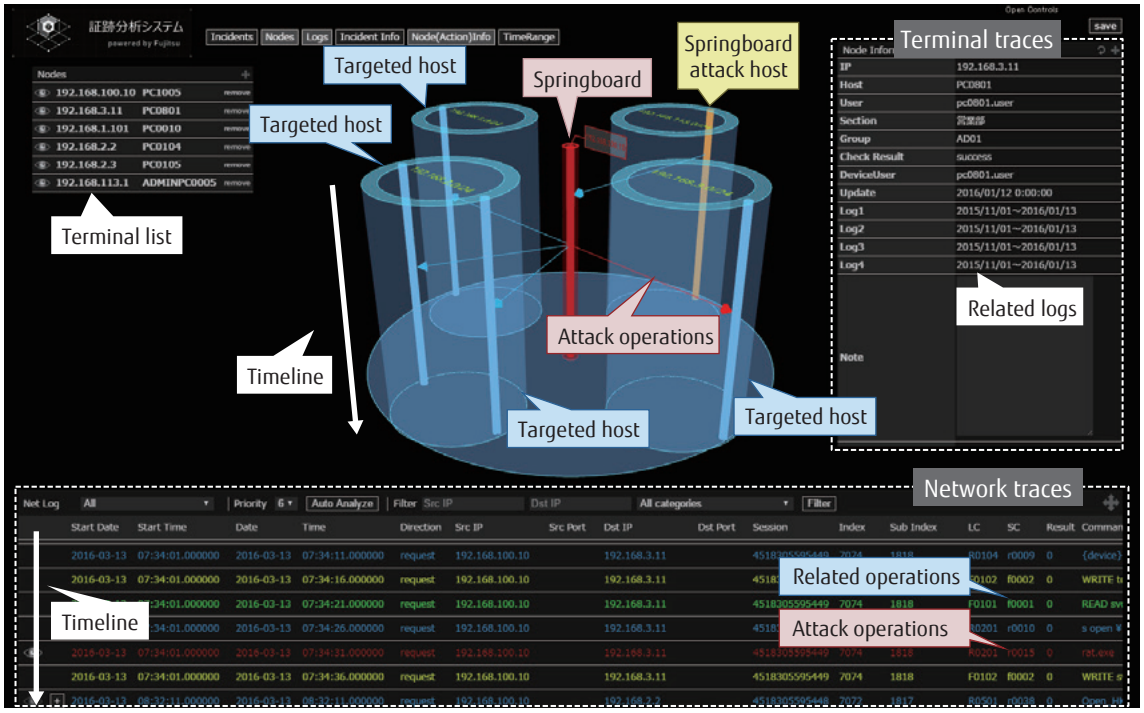


Figure 3
Visualization of a targeted attack's progress.

contained in system CTI can be automatically set in security equipment such as proxy servers.

The sharing and use of both human CTI and system CTI is important, but the fact that these two types of CTI are essentially decoupled presents a problem. For example, human CTI stored in security-dedicated social media needs to be converted to the STIX format before it can be used by systems, which requires labor and time. System CTI, meanwhile, being knowledge unseen by humans, does not lead to human actions nor get evaluated by people.

As the next stage in CTI utilization, Fujitsu has developed the Seamless Threat Intelligence Platform (S-TIP) that enables the seamless sharing and use of human CTI and system CTI. With S-TIP, people can exchange CTI via security-dedicated social media or e-mail as usual, which will then be automatically converted to the STIX format for sharing and use as system CTI. In addition, system CTI will be mixed in with human CTI on the security-dedicated social media timeline and displayed in an easy-to-understand format. Therefore, people reviewing the security-dedicated social media can share, use, and evaluate system CTI too. In this way, S-TIP seamlessly incorporates not just people but also systems like computers and security equipment into an ecosystem using CTI thereby achieving a new dimension in responding to cyber attacks.

3.4 New technology for detecting targeted cyber attacks: Malicious Intrusion Process Scan

Existing technology for detecting targeted cyber attacks primarily focuses on the malware used in such attacks. This technology detects malware by comparing the unique values, or "signatures," of suspected malware against a database of known signatures, checking the operation of that malware in a virtual environment, etc. Regardless of the method used, the idea here is to discover a targeted cyber attack by detecting malware. With these methods, however, there are cases in which detection fails due to malware evolving faster than signature updates and cases in which the malware itself detects a virtual environment and halts operation enabling it to go undetected.

Furthermore, in addition to signature and virtual environment, there are detection methods that collect

logs for various types of devices installed in the network and apply correlation analysis rules to those log data. This type of operation, though, requires advanced knowledge and technologies such as the setting of criteria for judging danger with respect to alerts issued by network devices, but personnel who are capable of such tasks are in short supply.

In light of the above, Fujitsu developed Malicious Intrusion Process Scan, a new technology for detecting targeted cyber attacks. This technology can detect a threat in real time by performing correlation analysis of attacker behavior on the network without observing malware.[11),12)] Two key features of this technology are:

1) Detection technology "discovering unseen attacks"

This detection technology makes use of an "attacker behavior-transition model" as a new approach. The model describes the transitions made in the behavior of malware launched by an attacker, which makes it possible to discover attack activities by applying actual network communications (**Figure 4**). As a result, this technology enables real-time detection of targeted cyber attacks that can slip by conventional security measures, which helps to reduce the risk of information leaks.

2) Sophisticated automation feature to visualize attack process after discovery

This sophisticated feature makes it easy to visualize an attack process by automating the tasks required for prioritizing countermeasures to an attack after its discovery, conducting surveys such as collecting and analyzing logs, etc. In this way, information needed to deal with the attack can be accurately grasped and SOC operations can be made significantly more efficient.

4. Security personnel development at Fujitsu

This section introduces the meaning of and approach to personnel development from a Fujitsu perspective and the ecocycle of an existing "connected secure society" that Fujitsu wishes to achieve through personnel development.

Encouraged by the incessant need for personnel development in the security field, Fujitsu has been active in personnel development since 2014 with the launch of its Security Meister Certification System. Originally designed with a target of 700 trainees, this system has trained more than 2,700 persons as security meisters as of December 2017, three and a half years after its launch.

On the other hand, it is sometimes said that attention is focused only on training while neglecting the use and employment of trained personnel and ongoing skill improvement and support. What then does "personnel development" really mean? After three and a half years of putting security training into practice, Fujitsu's answer to this question is "connecting people." With this type of personnel development, people can talk about security using a common language and can form a network having a common awareness of problems and an overall image of security.

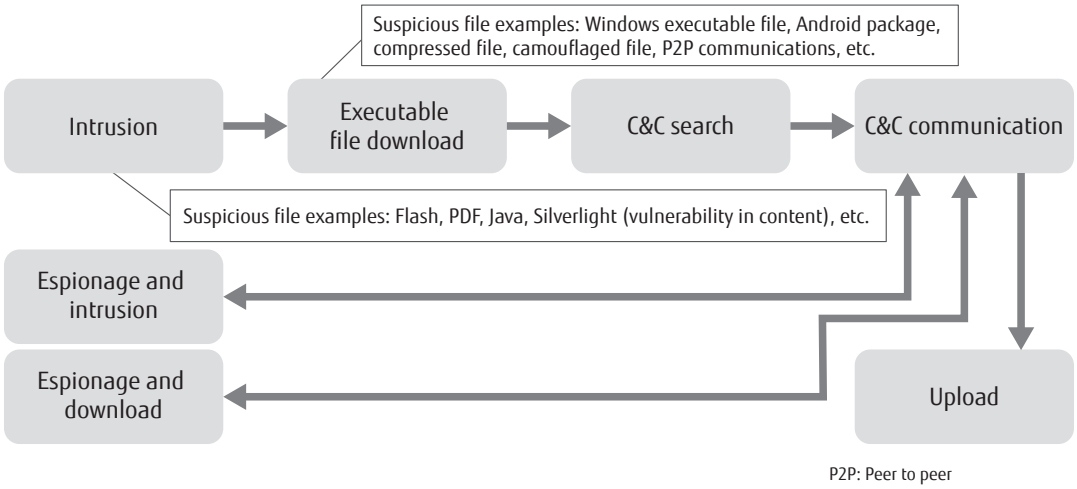


Figure 4
Attacker behavior-transition model.

If people are connected, the organization is connected. In general, an organization that tends to be vertically divided by mission will circulate information through connections between people. The circulation of information, meanwhile, gives birth to mutual understanding. If sites that use digital data have an understanding of security and if the security department has an understanding of how digital data is used, security takes on added value making the organization all the more competitive.

Taking such a "connection" into consideration, Fujitsu developed CYBERIUM as a domestically produced "cyber range" (virtual practice field) that takes personnel development beyond Fujitsu to include customers, regions, and young people such as students. This is a forum where participants can learn about security, experience it, and think about it while sharing the failures and successes of their predecessors. It is also a place where participants can communicate with new colleagues and improve their skills together with trained security meisters (**Figure 5**).

Looking to the future, trained security meisters will continue to put the safe and secure use of data into practice. They will aim to create a society in which people can lead secure lives with 2020 as one step to this end.

5. Conclusion

From the viewpoint of dealing with rising operation costs and a lack of qualified security personnel, this paper described Fujitsu's points of focus, the development of supporting technologies, and personnel development. Going forward, the holding of major events will require a transition to a society with enhanced cybersecurity measures and resilience (ability to recover).

The solutions described in this paper are already in a state capable of social implementation. In addition to introducing them into organizations and facilities directly targeted by attackers at the time of a major event, we can also expect them to be proactively introduced into many enterprises, groups, and organizations that use cyberspace. Furthermore, as a cross-sectional theme in the promotion of digital innovation (Society 5.0), we expect cybersecurity to be synchronized with the building of an ecosystem for 2020 and beyond and to be implemented rapidly in society by industry, government, and academia.

Part of the research described in this paper was supported by the Council for Science, Technology and

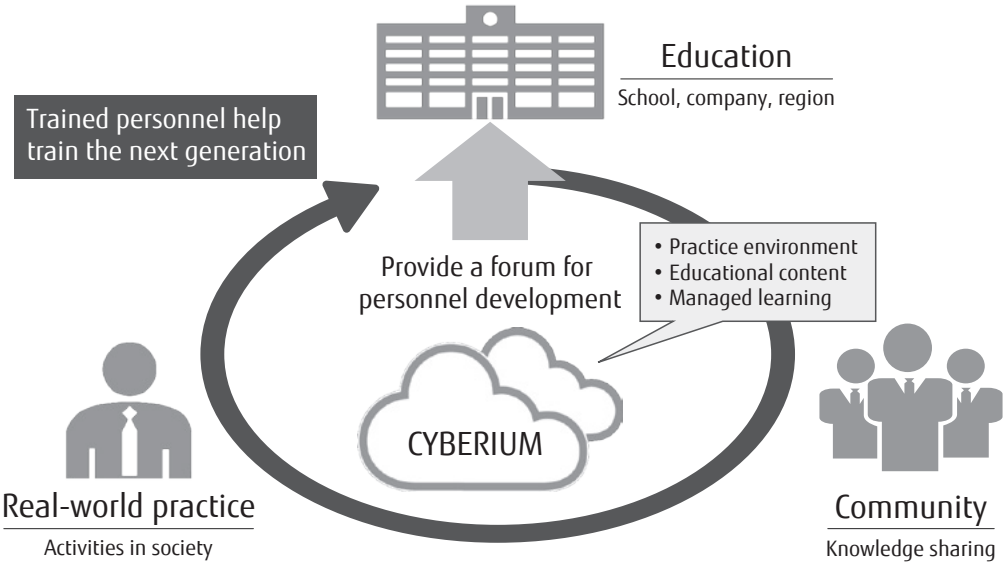


Figure 5
Personnel utilization cycle centered about CYBERIUM.

Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), and "Cyber-Security for Critical Infrastructure" (funding agency: NEDO).

References

1) Ministry of Internal Affairs and Communications: 2017 White Paper on Information and Communications in Japan (Outline), July 2017.
http://www.soumu.go.jp/main_content/000504683.pdf
2) Cabinet Office, Government of Japan: Cross-ministerial Strategic Innovation Promotion Program (SIP).
http://www8.cao.go.jp/cstp/panhu/sip_english/4-6.pdf
3) New Energy and Industrial Technology Development Organization (NEDO), Fujitsu Ltd.: New Lossless Data Acquisition and Storage Technology for Communication Data in Networks Developed.
http://www.nedo.go.jp/english/news/AA5en_100349.html
4) Ministry of Economy, Trade and Industry: Study of Recent Trends and Future Estimates Concerning IT Human Resources. June 10, 2016.
http://www.meti.go.jp/english/press/2016/0610_01.html
5) Y. Unno et al.: High-Speed Forensic Technology for Promptly Analyzing Damage After Targeted Attacks, FUJITSU Sci. Tech. J., Vol. 53, No. 5 (2017).
http://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol53-5/paper10.pdf
6) Fujitsu Laboratories Ltd.: Fujitsu Develops High-Speed Forensic Technology to Grasp at a Glance the Entirety of a Cyber Attack. May 13, 2016.
http://www.fujitsu.com/global/about/resources/news/press-releases/2016/0513-02.html
7) Fujitsu Ltd.: Fujitsu Enhances Intranet and Endpoint Security by Expanding its Global Managed Security Service. May 12, 2017.
http://www.fujitsu.com/global/about/resources/news/press-releases/2017/0512-01.html
8) OASIS: OASIS Cyber Threat Intelligence (CTI) Technical Committee.
https://www.oasis-open.org/committees/cti/
9) IPA: Outline of Structured Threat Information eXpression (STIX). (in Japanese)
https://www.ipa.go.jp/security/vuln/STIX.html
10) IPA: Outline of Trusted Automated eXchange of Indicator Information TAXII. (in Japanese)
https://www.ipa.go.jp/security/vuln/TAXII.html
11) S. Terada et al.: Technology Detecting Advanced Targeted Cyber Attacks– Malicious Intrusion Process Scan–. PFU Tech. Rev., Vol. 27, No. 1, pp. 33–40 (2016). (in Japanese)
https://www.pfu.fujitsu.com/about/technology/no49/images/49-5.pdf
12) PFU: Development of New Technology for Detecting Targeted Cyber Attacks from Attacker's Behavior. October 28, 2015. (in Japanese)
https://www.pfu.fujitsu.com/news/2015/new151028.html

Taishu Ohta
Fujitsu Ltd.
Mr. Ohta is currently engaged in fostering and spread of domestically produced technology and activities supporting personnel development.

Masahiko Takenaka
Fujitsu Laboratories Ltd.
Dr. Takenaka is currently engaged in research and development of information security, cryptography implementation, and cybersecurity.

Masaaki Katou
Fujitsu Ltd.
Mr. Katou is currently engaged in large-scale-network security business.

Ryusuke Masuoka
Fujitsu System Integration Laboratories Ltd.
Dr. Masuoka is currently engaged in research and development on the use of cybersecurity technology and cyber threat intelligence (CTI) in particular.

Kousetsu Kayama
Fujitsu Ltd.
Mr. Kayama is currently engaged in cooperative activities with outside organizations and personnel development in collaboration with Fujitsu Group companies.

Noriaki Fukushima
PFU Ltd.
Mr. Fukushima is currently engaged in security products planning.

Hosei Imai
Fujitsu Ltd.
Mr. Imai is currently engaged in surveying of international trends in cybersecurity.