Realizing Next-Generation Hybrid Networks for Multi-Cloud Era

● Tomoyuki Takamura ● Hideshi Sakurai ● Dai Yamamoto
● Masahiko Murakami ● Kouichi Yamasaki ● Yuki Unno

As businesses actively employ cloud technology, enterprise internal networks are reaching a major turning point. Some businesses want to migrate from a conventional closed and centralized enterprise network to a new, hybrid network that enables them to access and use software as a service (SaaS) directly on the Internet from their corporate locations. However, to realize this hybrid network, issues in terms of the operability of increasingly complex office networks with multiple sites and security measures within sites must be solved. Fujitsu and Fujitsu Laboratories approach these issues based on the concept of a software-defined wide area network (SD-WAN) and reasonable malware security measures. We also pursue R&D of security technology that achieves both greater convenience and security. This paper describes the efforts made at Fujitsu to realize a hybrid network optimized for multi-cloud environments.

1. Introduction

In recent years, many companies have been working to shift their business systems to the cloud and utilize on-demand software services (software as a service: SaaS) in order to respond to rapid changes in businesses and organizations and improve the operational environments required for work style reforms. As a result, such companies are naturally about to shift to a multi-cloud environment where different cloud services are used for different purposes according to business application and service level.

On the other hand, as the number of mobile users increases due to the promoted work style reforms, the chances of bringing malware into enterprise internal networks are also increasing. In factories, various terminal devices and sensor systems have started to connect to one another through the processes of IoT transformation. As a result, malware can be brought in from outside on PCs and USB memory devices used for maintenance work during equipment maintenance, and there have been related accidents that caused production stoppages. Thus, security measures are becoming a more important issue than ever before for companies.

Now, companies are in urgent need to think about the direction of their future network configurations, based on the trends toward multi-cloud environments and end-point diversification. This is due to the fact that the increased use of SaaS on the Internet causes congestion where each data center (hereafter, Center) is connected to the Internet, causing further bottleneck problems. More specifically, they must choose either of the following two configurations (**Figure 1**).

1) Conventional network

Enhance the network infrastructure of the data Center and migrate to a multi-cloud environment while maintaining a centralized private network between the head office and the Center.

2) Hybrid network

Unlike the conventional network, utilize the Internet as much as possible in order to migrate to a network that allows users to not only access business systems at the Center, but also directly access SaaS on the Internet from each site.

As hybrid network can reduce the costs of lines and equipment between the Center and each site and also prevent them from becoming bottlenecks, it is very attractive in terms of improving response when using SaaS. On the other hand, this type of network also has major issues, such as how to improve the operational load efficiency of network policies (hereafter, Policies), which were not required before, and how to

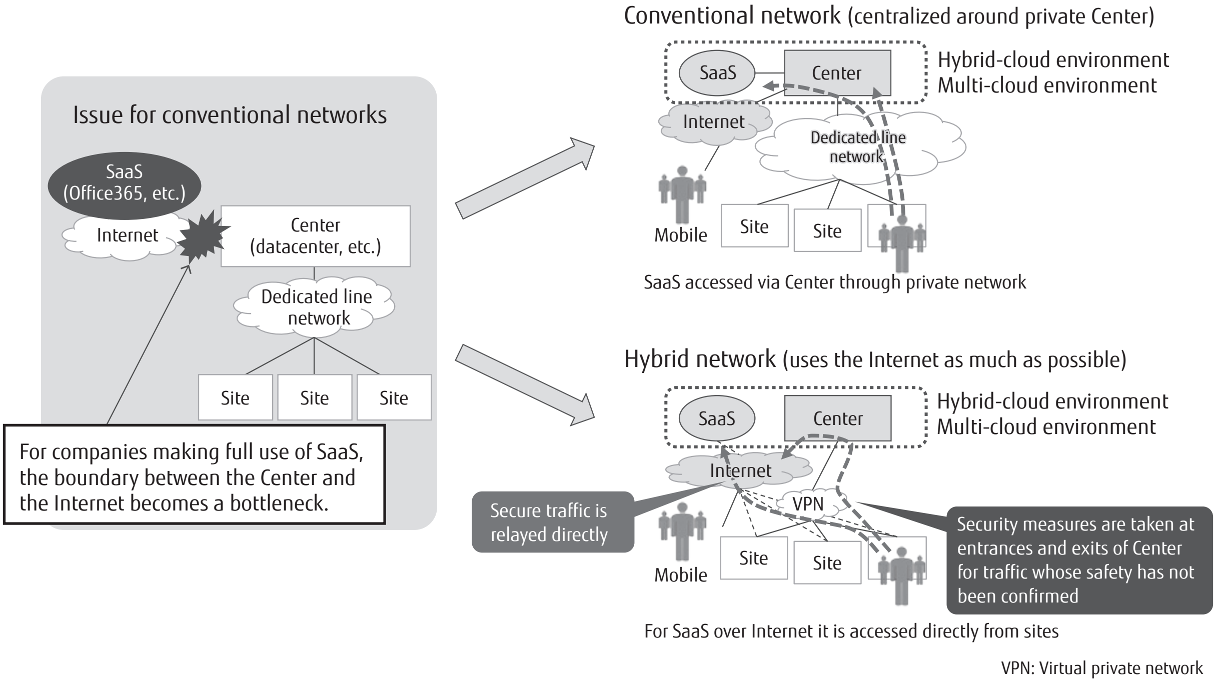

Issue for conventional networks
SaaS (Office365, etc.)
Internet
Center (datacenter, etc.)
Dedicated line network
Site
Site
Site
For companies making full use of SaaS, the boundary between the Center and the Internet becomes a bottleneck.
Conventional network (centralized around private Center)
SaaS
Center
Hybrid-cloud environment
Multi-cloud environment
Internet
Dedicated line network
Mobile
Site
Site
SaaS accessed via Center through private network
Hybrid network (uses the Internet as much as possible)
SaaS
Center
Hybrid-cloud environment
Multi-cloud environment
Internet
VPN
Secure traffic is relayed directly
Security measures are taken at entrances and exits of Center for traffic whose safety has not been confirmed
Mobile
Site
Site
For SaaS over Internet it is accessed directly from sites
VPN: Virtual private network

Figure 1
Comparison between conventional and hybrid networks.

review security measures for each site.

This paper describes the issues that a company may face when migrating to a hybrid network and the efforts that Fujitsu and Fujitsu Laboratories (hereafter, collectively “Fujitsu”) are making to solve such issues.

2. Issues in migrating to hybrid network

The following two issues lie in migrating to hybrid network.

2.1 Operation of Policies at many sites

In the hybrid network configuration, each site has direct access to SaaS on the Internet. For this reason, certain Policies are required to determine which traffic should be relayed via the Internet and which traffic should be relayed to Center via a virtual private network (VPN). In other words, it is necessary to configure settings for the Internet and settings for the intranet through VPN connection for all of the sites to which such Policies apply. As a result, many operational tasks are generated according to the number of sites.

There are two situations where operational tasks for Policies are required. The first situation is that settings must be added for all sites when a new SaaS starts to be used. The second situation is that, when a new site is established, settings must be added and Policies applied to the other sites accordingly. The latter is a key point for considering the operational load in the distribution industry where the number of stores changes dramatically in industries where require temporary offices and at companies that carry out mergers and acquisitions frequently.

Considering the above, companies want to be able to manage Policies by each site in a simple manner in order to reduce the load when carrying out Policies and also to be able to apply Policies with little burden when there is an increase in the number of network sites to which the Policies apply.

2.2 Security measures for internal network

These days, it is necessary to recognize that malware will infiltrate enterprise internal networks, which are then exposed to the constant danger of becoming targeted for a variety of attacks.

The first security measure for migrating to a hybrid network is to separate out only the traffic that is regarded as secure according to its Policies, and relay the traffic to the Internet directly. On the other hand, the basic principle is that any traffic that has yet to be confirmed as secure should go through a VPN and security measures should be implemented at the entrances and exits of the enterprise internal network.

It must be noted that when malware infiltrates the network, its injection spreads from the originally infected terminal to other terminals, which increases information leakage routes. Therefore, it is important to separate infected terminals from the network more quickly than ever before. Considering the above, the operation manager needs to have a method to search for the location of a terminal and to separate it from the network. In addition, the network configuration of each site must allow for the detection of malware infections and minimize the spread of such malware infections.

3. Fujitsu's efforts to solve issues

This section introduces Fujitsu's efforts in solving the issues described in the previous section, when shifting to a hybrid network.

3.1 Reducing operational load when number of sites increases

The concept of the so-called software-defined wide area network (SD-WAN) is an answer to the implementation of efficient operations management, even if there is an increase in the number of network sites to which Policies apply. The operations management portal is used to visualize the statuses of routers, LAN switches, and other network devices (hereafter, devices) and manage them in an integrated manner (**Figure 2**). Template Policies are applied to a new site to be established. It is important to identify the location of a malware-infected terminal immediately and to handle the infection even in a network configuration with many sites.

Also, when a device is connected to the network, it is automatically configured by zero-touch configuration. Fujitsu has had the technology and implemented zero-touch configuration functions for over 10 years. Since zero-touch configuration functions by overseas vendors are based on Dynamic Host Configuration Protocol (DHCP), which largely dominates the global market, they are not very compatible with the next-generation network (NGN) environment in Japan; therefore, zero-touch is not actually used in many cases. Fujitsu, on the other hand, has implemented a zero-touch configuration functions that are suitable for the Japanese network environment based on Point-to-Point Protocol over Ethernet (PPPoE) and Internet Protocol over Ethernet (IPoE).

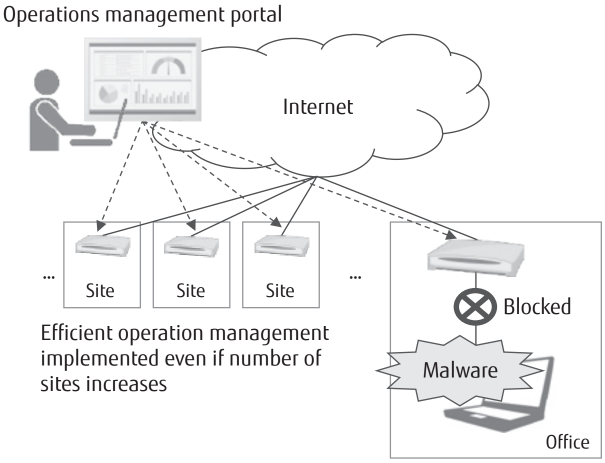

Operations management portal
Internet
...
Site
Site
Site
...
Blocked
Malware
Office
Efficient operation management implemented even if number of sites increases

Figure 2
Points for solving issues.

3.2 Security measures for internal network

This subsection describes the prevention, detection, and handling of malware infections as security measures required for the internal network.

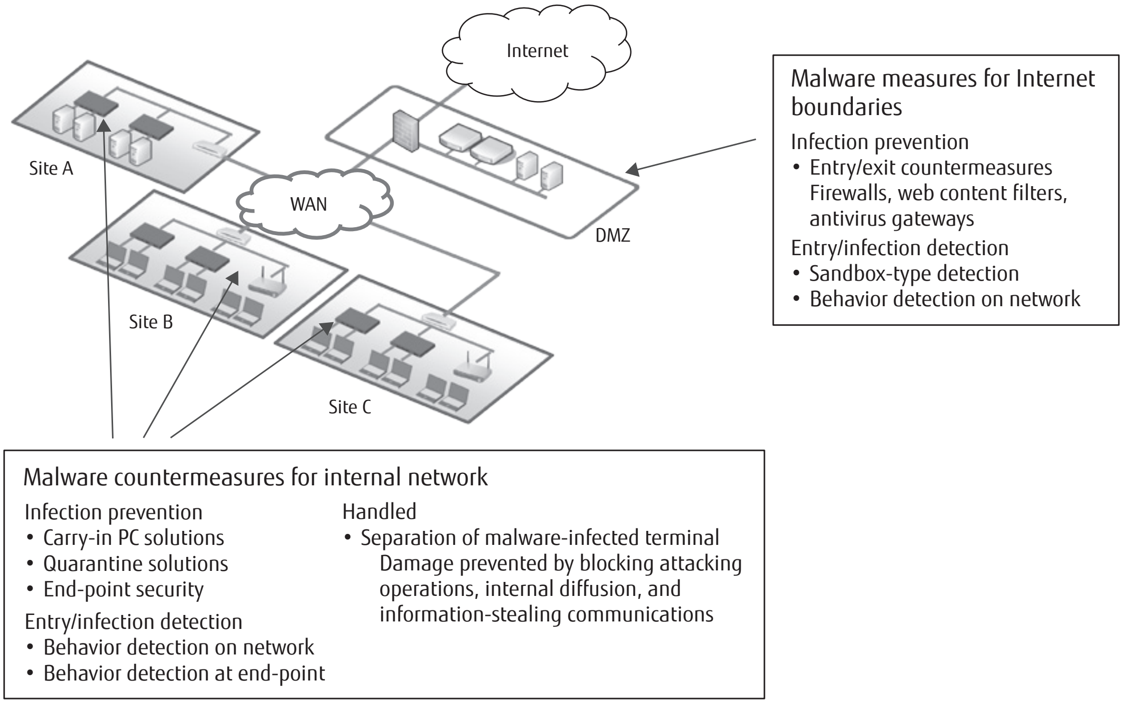
Measures and technologies against malware must cover the entire hybrid network (**Figure 3**). The above-mentioned entrance/exit measures should be perfected in the demilitarized zone (DMZ), which represents the boundary between the Internet and the internal network. In addition, advanced malware detection measures that use the latest technology should be applied. On the other hand, the following measures should be taken for the internal network:

- Either, prohibit connection of vulnerable terminals, or isolate them to reduce the infection risk.
- Detect malware-infected terminals based on their behaviors on the network.
- Separate a malware-infected terminal from the network immediately after detecting it.

Each of the measures are detailed below.

1) Prevention of malware infections

Limit the connection of terminals that are not under the management of the information system



Malware measures for Internet boundaries

Infection prevention
- Entry/exit countermeasures
  Firewalls, web content filters, antivirus gateways

Entry/infection detection
- Sandbox-type detection
- Behavior detection on network

Malware countermeasures for internal network

Infection prevention
- Carry-in PC solutions
- Quarantine solutions
- End-point security

Entry/infection detection
- Behavior detection on network
- Behavior detection at end-point

Handled
- Separation of malware-infected terminal
  Damage prevented by blocking attacking operations, internal diffusion, and information-stealing communications

Figure 3
Security measures covering entire hybrid network.

department and limit the connection of vulnerable terminals. Fujitsu offers a carry-in terminal solution and a network quarantine solution for handling such connections. In addition, appropriate segmentation (i.e. logical separation of the network) and limits on communication with external networks should be implemented in order to prevent the spread of malware infections. While segmentation is needed to increase the level of security, it also has the disadvantage of increasing the operational load. For this reason, Fujitsu is committed to the development of a segmentation technology that can achieve both convenience and security.

2) Detection of malware infiltration and infection

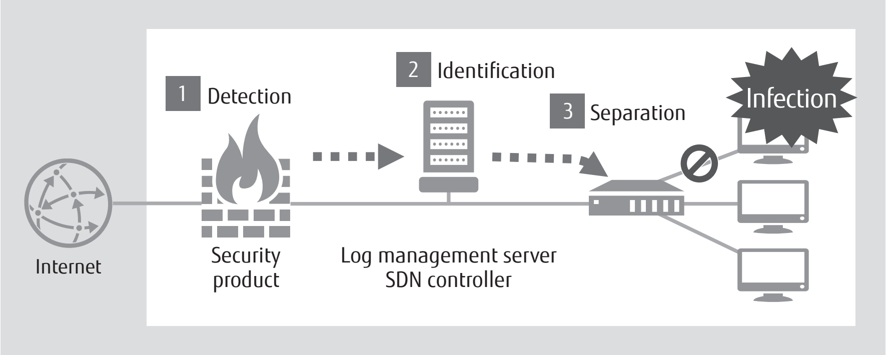
Detect malware, based on its behaviors on the internal network. Malware must be detected in various places such as the boundary between the Internet and the internal network, inside the cloud, at end points, and on the network within each site by making full use of technology that is suitable for each site. Fujitsu is also committed to R&D of new detection technologies as well as offering new solutions according to malware evolution.

3) Handling of malware infections

In the case of a malware infection, it is important to identify the infected terminal and separate it from the network, regardless of where it is detected. The procedure for detecting and handling a malware infection is shown in **Figure 4**. When a malware infection is detected, first identify where the infected terminal is located within the network. Then, the infection activity and information leakage should be prevented by separating the infected terminal from the device closest to the terminal to isolate it. In this case, the infection must be handled so as to limit its impact on operations only locally.

When a malware-infected terminal is found in an ordinary company, it is difficult to identify where the terminal is located, as the connection status of the terminal is not visualized sufficiently. Also, since separating the terminal requires a special network engineer, the situation cannot be dealt with promptly. To solve these problems, Fujitsu offers a solution to identify where an infected terminal is located and perform simplified operations or separate the terminal from the network automatically.

As mentioned above, Fujitsu can implement a safe and secure network environment, while reducing the operational load of the operation manager in order to



SDN: Software-defined networking

Figure 4
Separation of malware-infected terminal.

address the two issues in migrating to a hybrid network.

4. Elemental technologies toward implementation

This section outlines Fujitsu's three proprietary technologies as elemental technologies for security that can achieve both the convenience and security of a safe and secure hybrid network.

4.1 Secure provisioning technology

The concept of an SD-WAN is required to enable efficient and secure operation of a hybrid network. When establishing each site, zero-touch configuration is employed to configure its devices automatically.

However, there used to be some issues in the conventional techniques used to validate the devices to be configured. With zero-touch configuration, a remote server needs to be informed of "device association information," which indicates which site each device is installed at and what serial number the device has. Such device configuration also includes security-related settings such as the VPN connection between the Center and the site. If there is an error in the association information, the desired configuration cannot be correctly arranged in the device at the site, which may lead to security risks during operation. For this reason, up until now, the association information had to be generated carefully by engineers with specialist knowledge.

In response, Fujitsu has developed a secure provisioning technology to reduce the risk of mixing up devices and installing them at incorrect sites, regardless of who installs the devices or links them (**Figure 5**). This technology uses a management terminal (e.g. tablet) that can communicate with the remote server to install and associate devices. Mix-up of devices are prevented, as the remote server authenticates each device via the management terminal. Furthermore, as the management terminal reads a one-time password based on a QR code sent to the site beforehand, the device can be associated to the site with certainty. This technology can reduce the security risks and achieve highly reliable zero-touch configuration.

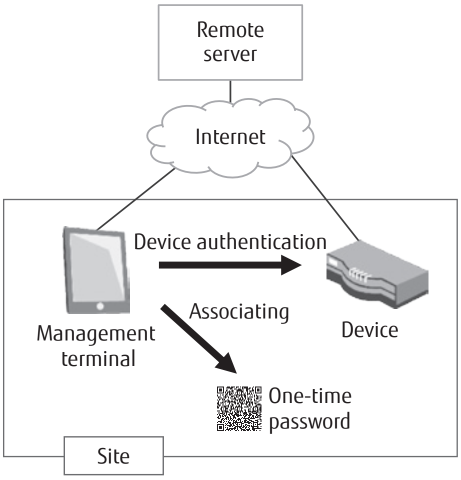


Figure 5
Secure provisioning technology.

4.2 Smart segmentation technology

Appropriate network segmentation is effective for preventing the spread of malware infections. More specifically, the internal networks are divided into small logical networks according to organizational or operational details for segmentation. Even if malware infiltrates the network, this can localize damage within a small segment, compared to having no segmentation.

However, such segmentation may decrease the flexibility of network connectivity and increase the operational load. With a segmented network, therefore, its divided segments must be rejoined securely within a short time, according to operational details, etc.

Fujitsu has developed a smart segmentation technology to allow the network manager to simply set easy Policies to rejoin segments securely within a short time (**Figure 6**). This technology changes the device setting information so that only the information required for operation can be sent and received between segments based on Policies. This minimizes the burden of the operation manager and enables the construction and operation of a secure network.

4.3 Targeted attack detection technology

Fujitsu is committed to the development of technology that detects malware based on its behaviors on the network. While there are already several known technologies of the kind, such detection technologies must continue to be improved as malware evolves.

The malware that infiltrates the internal network is called a remote access trojan or remote administration tool (RAT). When a RAT connects to the command & control (C&C) server of the attacker, which is placed in an external network, the attacker can access an infected host remotely. The attacker infiltrates the next target from the first host that was infiltrated and repeats espionage this activities to steal information. As such espionage activities use the Server Message Block (SMB) protocol, which is used in normal operation, it is difficult to distinguish attacks from the normal operation, even by checking communication logs. In response, Fujitsu has developed a technology to distinguish such communications and detect RAT-based espionage activities in the early stages.[1)]

This technology collects and analyzes communications performed by the internal network, first. Then, it extracts both, (1) the remote communications used for sending commands to the RAT-infected terminal, and (2) the internal attack communications used to infiltrate and execute commands and programs on another terminal (attack target) from the infected terminal, based on their respective characteristics. Next, it associates these two types of communications in order to detect espionage activities by the attacker (**Figure 7**).

Analysis by associating communications with different parties and the time-series analysis of such communications can find discrepancies and abnormalities across the system, even if individual communications seem normal as single behaviors. Also, when combined with a coordinating technology for collecting and integrating information from multiple monitoring points,

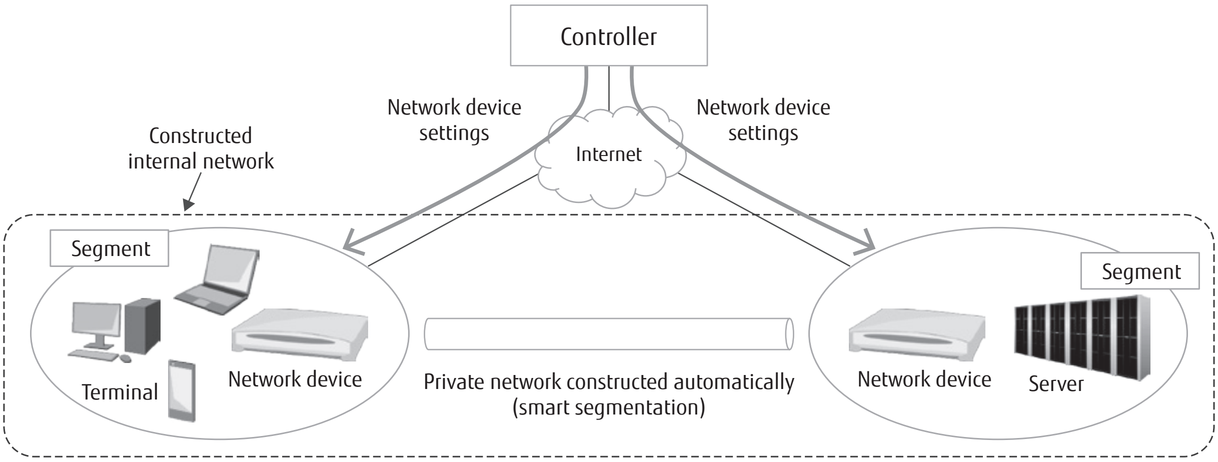


Figure 6
Smart segmentation technology.

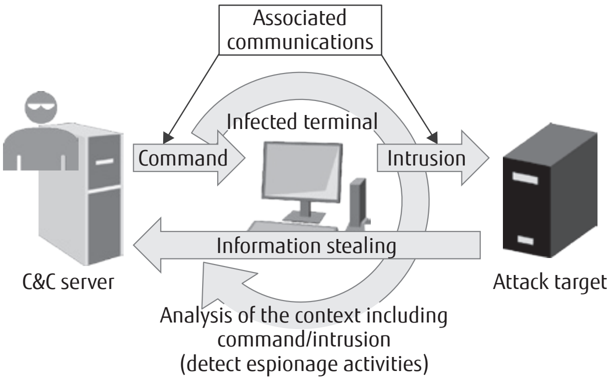

Associated communications
Infected terminal
Command
Intrusion
Information stealing
C&C server
Attack target
Analysis of the context including command/intrusion (detect espionage activities)

Figure 7
Detect espionage activities based on analysis of communications on internal network.

this technology can even detect espionage activities in which remote communications and internal attack communications are observed at different monitoring points.[2)]

This technology can be expected to promptly detect RAT-based espionage activities without depending on the malware signature (i.e. characteristic data pattern held by malware) or operation definition, and also to prevent the attacker from stealing information.

5. Conclusion

This paper described next-generation hybrid network solutions that target enterprise internal networks and Fujitsu's efforts in implementing them.

Enterprise internal networks will continue to be optimized according to the reuse of cloud services, business patterns, and end users' work styles, etc. In addition, network technologies will also continue to change according to future environmental changes and the advancement of related technologies, including the proliferation of the IoT, responses to new security threats, the proliferation of fifth generation mobile communications system (5G), the development of high technologies using AI, etc. Fujitsu is committed to developing and offering customer-oriented solutions to respond to such changes.

This research is partly conducted by commission for the R&D for analysis and detection of cyber attacks of the Ministry of Internal Affairs and Communications.

References

1) S. Torii et al.: Multi-layered Defense against Advanced Persistent Threats (APT). FUJITSU Sci. Tech. J., Vol. 50, No. 1, pp. 52–59 (2014). *http://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol50-1/paper09.pdf*

2) M. Yamada et al.: Cooperating Multi Sensors for Behavior Detection of Targeted Attack in Intranet. Symposium on Cryptography and Information Security (SCIS), 2015.

Tomoyuki Takamura
Fujitsu Ltd.
Mr. Takamura is currently engaged in the planning and strategy development of network businesses for enterprises.

Hideshi Sakurai
Fujitsu Ltd.
Mr. Sakurai is currently engaged in technical support of network solutions and integration for enterprises.

Dai Yamamoto
Fujitsu Laboratories Ltd.
Dr. Yamamoto is currently engaged in the research and development of cyber-security and cryptography implementation.

Masahiko Murakami
Fujitsu Laboratories Ltd.
Mr. Murakami is currently engaged in the research and development of network service technologies.

Kouichi Yamasaki
Fujitsu Laboratories Ltd.
Mr. Yamasaki is currently engaged in the research and development of smart segmentation technologies.

Yuki Unno
Fujitsu Laboratories Ltd.
Ms. Unno is currently engaged in the research and development of network security and cyber-security.