Field Area Management Platform for Connecting Various Kinds of Things to the Digital World Easily, Stably, and Securely

● Jun Kakuta ● Yusuke Kobayashi

There is growing interest in IoT as a technology to realize business innovation and contribute to a safe and secure society. However, there are challenges concerning devices in the field area such as sensors, whose features and reliability are limited compared to PCs, and this is compounded by the fact that the wireless networks used by these devices are also unstable. As we are about to enter the era of IoT, which will involve these kinds of devices, Fujitsu Laboratories recognizes the growing importance accorded to the operation and management of diverse devices out in the field area. We thus pursue research and development of device virtualization technology, fault management technology, and secure operation technology, which respectively enable devices to be connected easily, stably, and securely. This paper describes these three types of technologies and explains the field area management platform that uses them, with examples of applications.

1. Introduction

There is growing interest in IoT as a technology that uses information obtained from various things to realize business innovation and contribute to a safe and secure society. IoT connects real-world devices to the digital world through networks, visualizes data gathered from devices, and controls other devices in the real world according to the results obtained by analysis.

For example, in a factory, information such as the operating status of equipment and the production status of production lines is collected in real time, and the production schedule of each process is optimized accordingly. Elsewhere, sensors are starting to be installed on infrastructure such as bridges and roads to detect aging or abnormalities of infrastructure based on changes in the measured data.

To easily develop such IoT applications, platforms for IoT applications are provided by many vendors. Normally, as shown in **Figure 1**, these platforms (cloud platform, gateway platform) have a device data collection function and a function for the utilization of data from applications. The data collection function acquires data from devices in the field, where operations are carried out (hereafter, field area), by various communication means such as serial communication, Wi-Fi, and Bluetooth, and transmits these data to the cloud platform. The cloud platform stores the received data, and applications acquire and use the stored data via the data utilization functions of the cloud platform. Some platform have also functions for the analysis of the stored data.

In IoT, however, it is not easy to gather data stably and securely from devices in the field area because devices often have limited functions and low reliability, and often use wireless networks that may be unstable. While it is possible to handle small-scale demonstration experiments or proof of concept (PoC) experiments manually, there are cases where it becomes impossible to cope in such manner with the increase in the number of devices and their deployment locations, and therefore enhancement of operation management functions is important. In this regard, Fujitsu Laboratories is working on the development of technologies to facilitate device installation and operation in the field area.

This paper describes operation management technology of devices and networks in the field area and the platform to utilize these technologies.

2. Field area characteristics

The field area refers to the sites where operations

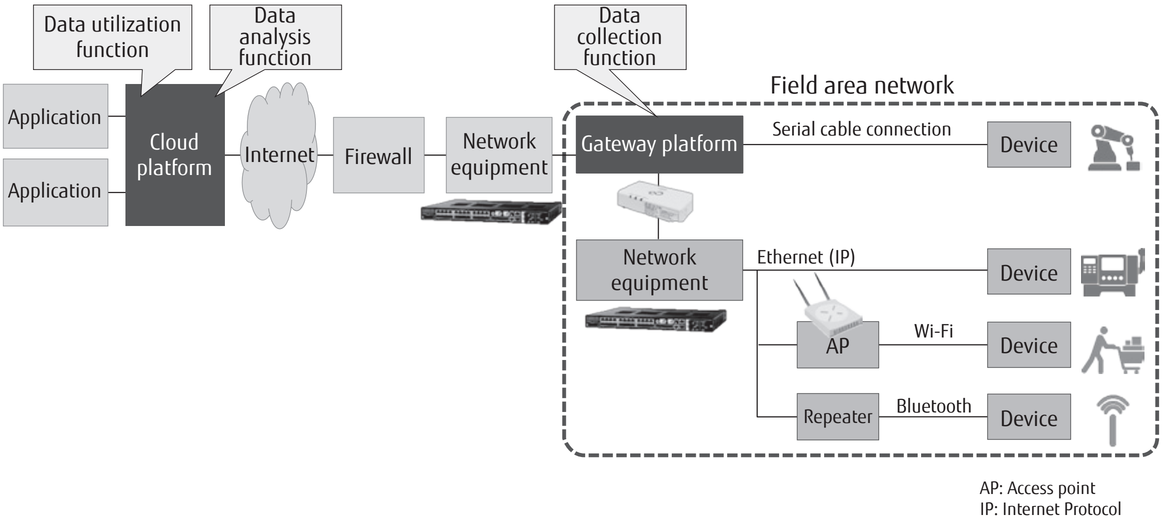


Figure 1
IoT system configuration.

are actually carried out. The field area has the following characteristics, which differ from those of the operation sites of ordinary ICT systems.

1) Diversity of devices that are used

IoT involves the use of a great diversity of devices. In addition to the diversity of types of devices, many devices support both wired and wireless connection and can be used with either types of communication. Moreover, wireless communication comprises many different standards, including wireless standards such as Wi-Fi and Bluetooth, and communication protocols such as Modbus[1] and ECHONET Lite.[2] Furthermore, device functions vary by manufacturer, and in many cases, interfaces such as application programming interfaces (APIs) and data models for using functions differ.

2) Harshness of operating environment

In the field area, it is often desirable to operate by wireless connection so as not to hinder the execution of operations and to increase flexibility in terms of device installation locations. However, in factories and the like, it may be difficult to stably carry out wireless communication, as in the case of parts shelves located in a place where radio waves are blocked, or a location where manufacturing equipment generates interference waves (noise) when in operation.

Also, as time goes by, the field area environment may change. For example, in indoor spaces, wireless communication that was operating stably at the time of introduction may become unstable due to layout changes. Also, outdoors, the construction of new structures may cause marked degradation of radio communication conditions.

3) Difficulty in system operation management

In the industrial field, where the introduction of IoT is progressing, security breaches may cause production stops and other disruptions resulting in considerable losses. However, since IoT is strongly tied to operations, the operation and management of field area systems is often left up to the work sites. As a result, there are cases where the management of devices and networks in the field area is inadequate. For example, security measures may not be appropriately implemented, or the kinds of devices that are connected to the network may not be managed.

However, since the field area is intimately tied to operations, changing that environment for the sake of IoT is not necessarily reasonable. Aware of such issues, Fujitsu Laboratories is working on the following three technological developments to ensure stable operation of systems under various constraints presented by the different operational environments (**Figure 2**).

1) Power-saving device operation technology[3), 4)]
- Battery-less sensing using solar cells and low power communications

2) Wireless network design and operation technology[5)]
- High-speed simulation of device and wireless

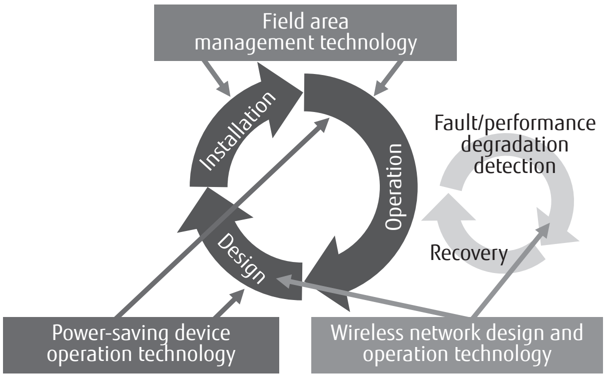


Figure 2
Technology development and operation cycle in the field area.

access point installation locations
- Visualization of wireless communication conditions

3) Field area management technology
- Easy connection of various devices to the system and use of these devices via common APIs
- Detection and response to faults and security threats in the field area for stable and secure operation

In the following sections, we introduce Fujitsu's field area management technology, which connects various IoT devices easily, stable, and securely to systems and makes them easy to use from applications.

3. Issues for connecting IoT devices

Based on the field area characteristics discussed in the preceding section, this section describes the tasks for connecting IoT devices easily, stably and securely to systems.

1) Easy connection

Devices often differ in functions and interfaces. Therefore, it is necessary to develop software for using the connection and functions of each device individually, which is time-consuming and costly. In addition, since new devices are often added after the start of operation in IoT, it is impossible to develop software individually in a timely manner. Thus, concealment of differences in function and interface among devices is a requirement.

2) Stable connection

In the field area, some devices are connected using different communication standards and protocols. IoT devices are less reliable than PCs and servers, and many are difficult to operate stably. Moreover, in the short-range wireless communication used by many devices, the connection may be dropped or the transmitted data may be lost as communication conditions change. Therefore, real-time management of the operating status of devices and the communication status of wireless networks, and quick response when faults occur, are requirements.

3) Secure connection

Many IoT devices connected to the field area cannot be installed with security software due to restrictions in terms of CPU performance, memory capacity, and so on. Moreover, even if the software that controls the manufacturing facility has security risks, patches or other software solutions may not be available, or the requirement of round-the-clock facility operation may preclude the application of patches or other software solutions. Therefore, security measures developed based on the premise that handling of security risks at the IoT device level is not possible are required.

4. Field area management technology to meet requirements

This section describes device virtualization technology, fault management technology, and secure operation technology developed to solve the three requirements mentioned in the previous section.

4.1 Device virtualization technology

To enable easy device connection, we developed device virtualization technology that treats any device as a device having a common interface (virtual device). This technology models the functions of devices as operations of properties that are defined for each device. This makes it possible to conceal differences in functions and interfaces among devices.

At the core of this technology are device adaptation technology that performs communication processing for each device and connects it to a gateway, and device management APIs that operate virtual devices from applications.

1) Device adaptation technology

The communication processing of various devices is handled by combining adapters that perform Internet Protocol (IP) and other communication processing, and adapters that perform data processing such as unit conversion in accordance with the ECHONET Lite standard.[6] The conventional way to do this was to develop all the software required for connection for each type of device, as shown in **Figure 3 (a)**. With device adaptation technology, only additional adapters need be developed, as shown in **Figure 3 (b)**, which makes it possible to reduce the number of software modules to develop, achieve savings in terms of development cost and time, and gain the ability to respond promptly to system updates.

2) Device management APIs

As device management APIs for manipulating virtual devices, we adopted Web of Things (WoT) Thing Description, and the Draft of WoT Protocol Binding Templates.[7), 8)] Fujitsu is leading WoT standardization at the World Wide Web Consortium (W3C). WoT is a standard that makes it possible to handle all devices with web technology and achieve the interconnection of various IoT systems. Providing the WoT API as a device management API allows easy use of devices in the field area. This is also expected to help accelerate the creation of new applications that integrate existing web services and devices, as well as new applications that integrate IoT services of other standards and devices.

4.2 Fault management technology

We have developed fault management technology for the stable operation of devices and networks in the field area. For stable operation of devices in the field area, three processes are required: fault occurrence detection, fault cause identification, and fault recovery. In this section, we describe the operation information collection technology and fault analysis technology required to realize fault detection and fault cause identification.

1) Operation information collection technology

The acquisition of the operation management information on devices and network equipment required for fault detection and cause analysis was realized through the extension of the aforementioned device virtualization technology.[9] Concretely, operation information with different interfaces for each device is collected by adapters. This information is managed as properties of the virtualized devices, and it can be acquired by the device management APIs.

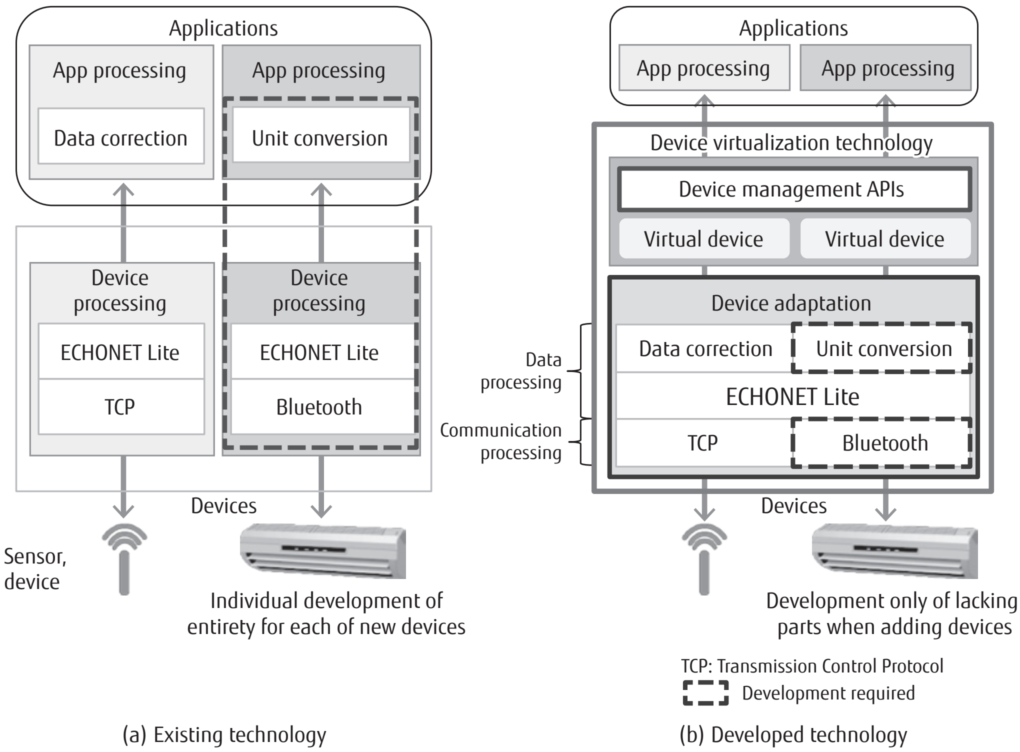


Figure 3
Comparison of existing technology and device virtualization technology.

For collecting operation information from devices, an extension of the Home Network Topology Identifying Protocol (HTIP), which is a protocol for managing the connection configuration of home networks, is used. This extension[10] of the existing HTIP data format was designed to collect information on devices and network equipment, quality information on wireless networks, and the like, and was established as a standard by The Telecommunication Technology Committee (TTC) (**Figure 4**). At the same time, in cooperation with device vendors, we are conducting interoperability tests with devices and network equipment compatible with HTIP, with a view to improving operation management.

2) Fault analysis technology

This technology makes it possible to manage the connection configuration information (topology), from gateways to devices, by using the connection information included in the operation management information collected from the devices and network equipment in the field area. Further, through the use of information such as whether or not operation management information can be acquired, it is possible to grasp the operating state of devices and the state of the network. This allows the topology and the operating status in the topology to be managed in real time.

In addition, by applying machine learning to indicators for radio quality included in the operation management information, radio interference and shielding, which are frequent occurrences in the field area, can be detected. The indicators include received radio signal strength, communication link quality, and communication response time. Moreover, by applying machine learning to these real-time measurement values of radio quality information and feature values such as standard deviation within a fixed time, offsite radio wave patterns can be identified as the cause of radio interference.[11] By indexing radio wave patterns with the situations when they occur in advance, it becomes possible to identify the causes of degradation of radio quality.

In this way, detection of device faults in the field area and determination of the cause of degradation of radio quality can be done in real time, making it possible to respond quickly to faults and improve device connection stability.

4.3 Secure operation technology

To securely connect the devices installed in the field area to the system, we developed technology to securely operate IoT devices, for which it is difficult to

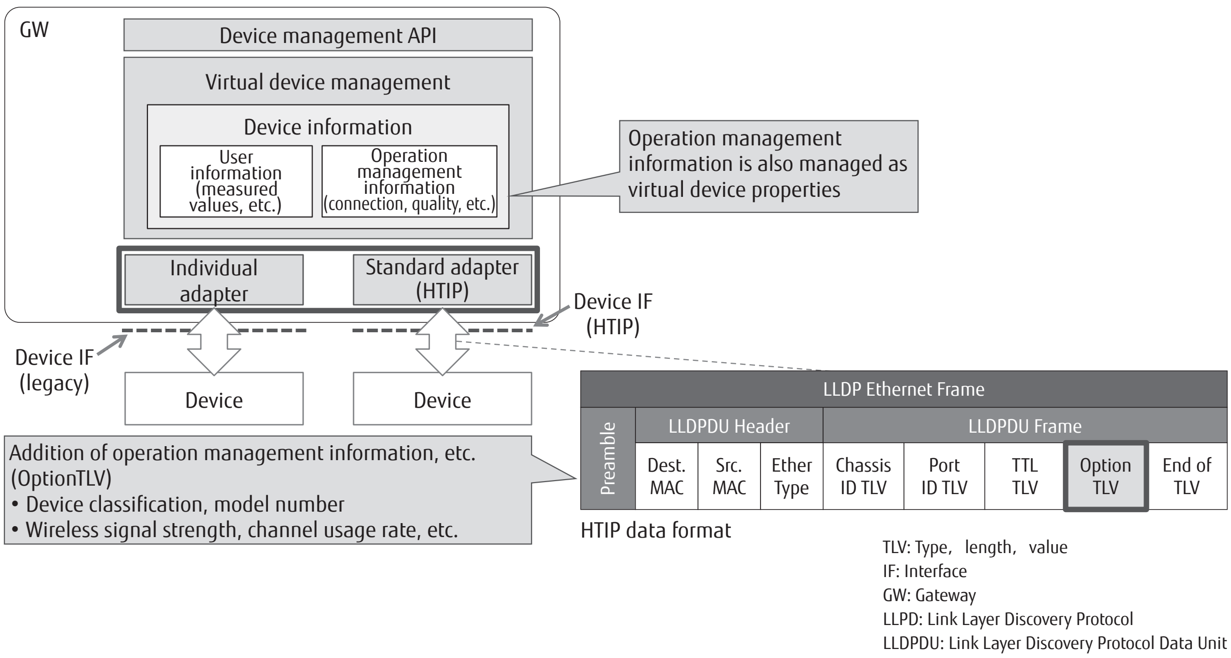


Figure 4
Outline of operation information collection technology.

implement security measures, by utilizing device virtualization technology and fault management technology.

The network in the field area is separated from the external network by gateways. Since gateways can provide security measures equivalent to those of a PC, external attacks via networks can be prevented. Meanwhile, cases of infection with viruses have occurred by connecting maintenance terminals or USB flash drive brought in from outside to the network. Therefore, the implementation of countermeasures to prevent this problem is a key point for the networks in the field area.

The developed device virtualization technology is designed so that the gateway performs the communication processing for each device, so that devices communicate only with the gateway. We decided to utilize the feature of operation management technology that topology can be managed by fault management technology, along with the fact that the communication destination of devices is limited to the gateway by the device virtualization technology. In other words, we developed control technology that disconnects from the network any devices that show unusual communication with terminals other than the gateway and are therefore considered to be suspicious devices.[12]

Unusual communication can be detected based on the information of the Intrusion Detection System (IDS) connected to the network equipment in the field area or the communication log of the network equipment. Device disconnection is done in a manner that reduces as much as possible the impact of disconnection on the communications of other devices. This is realized by deciding the network equipment to be controlled by referring to the topology, closing the communication port of that network equipment, and setting an access restriction (**Figure 5**).

5. Outline of field area management platform and its use case

To realize a platform for IoT applications with enhanced operation management functions, we developed a field area management platform that integrates the field area management technologies described so far. The developed platform operates on the gateways installed in the field area.

The field area management platform connects devices and network equipment to the gateways by device adaptation technology, and it manages them as virtual devices. In addition to user information such as the measured values of the device, virtual devices also store operation management information. The topology management function and the fault management function perform topology generation and fault detection and fault cause identification analysis in the field area based on this operation management information, and the results are saved as data of the virtual device.

Furthermore, the secure operation function uses topology information to disconnect suspicious devices

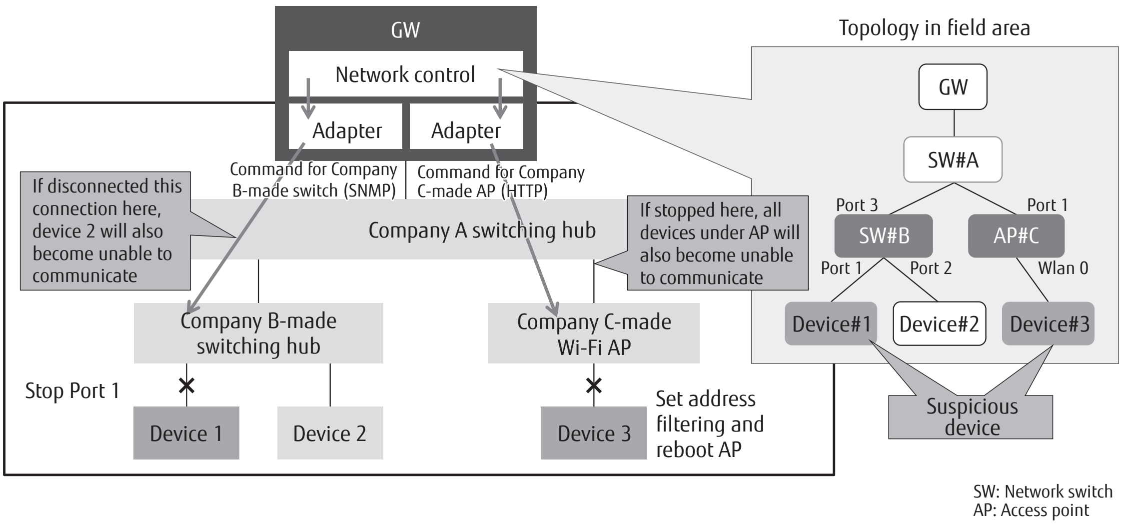
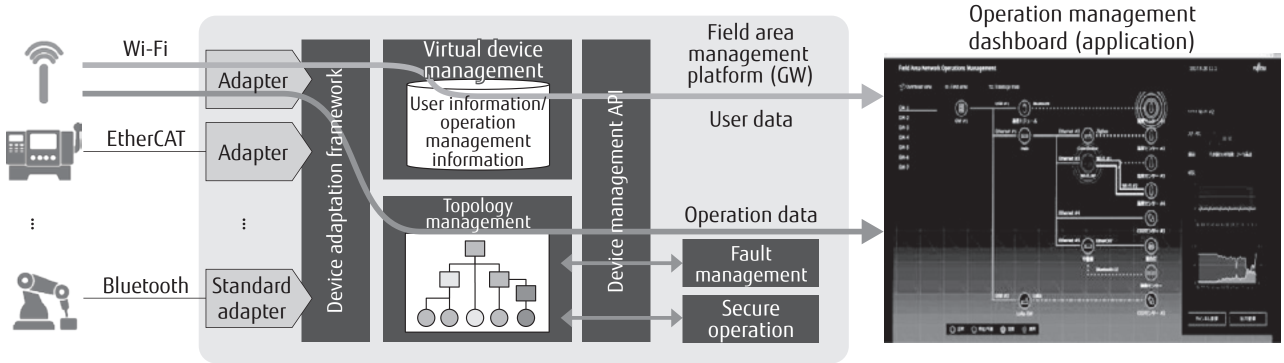


Figure 5
Secure operation technology.



EtherCAT: Etnernet control automation technology

Figure 6
Field area management platform.

from the network by controlling the network equipment in the field area. These operation management information and security related events can be visualized and notified to applications such as the operation management dashboard via the device management APIs (**Figure 6**).

This platform, which allows easy, stable, and secure use of devices, can be applied to various fields such as the management of facilities such as factories, offices, and tenant buildings, environmental monitoring of bridges, river water levels, and so on. We believe that the proposed platform can be used to good effect in factories in particular. This is because factories are environments where various devices are connected for people flow line management, environmental monitoring, and so on, and where devices are added for the purpose of site operation improvement, and it is often difficult to implement security measures for existing production equipment.

6. Conclusion

This paper described the operation management technology of devices and networks in the field area and the platform to utilize these technologies. It is not easy to collect data stably and securely in the field area owing to its characteristics, and the importance of operation management will further increase in the future.

Fujitsu is promoting the commercialization of FUJITSU Network Virtuora MX a network solution based on IoT services that incorporate some of the operation management technologies described in this paper, for the full IoT era. With this solution, we are leading the creation of new services utilizing various devices in the real world, as well as the realization of a prosperous society.

Some of the technologies described herein include results from “Achievement of energy management communication technology in smart community” and “Establishment and demonstration of common infrastructure technology for IoT,” which are national projects of the Ministry of Internal Affairs and Communications.

References

1) The Modbus Organization: Modbus.
http://www.modbus.org/
2) ECHONET Lite Specification (Open Specs).
https://echonet.jp/spec_en/
3) Fujitsu Laboratories: Fujitsu Develops Industry’s First Flexible IoT-Supporting Beacon That Needs No Battery Replacement.
http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0325-02.html
4) Fujitsu Laboratories: Fujitsu Develops World’s Smallest Sensor Device Supporting LPWA Communication, Eliminates Need for Battery Replacement.
http://www.fujitsu.com/global/about/resources/news/press-releases/2017/1204-02.html
5) Fujitsu Laboratories: Fujitsu Develops Field Engineering Technology to Rapidly Provide IoT Services.
http://www.fujitsu.com/global/about/resources/news/press-releases/2016/0525-01.html
6) T. Sano et al.: Device accommodation cost reduction method for the popularization of IoT. Institute of Electronics, Information and Communication Engineers, March 2017 (In Japanese).
7) W3C: Web of Things (WoT) Thing Description.
https://www.w3.org/TR/wot-thing-description/

8) W3C: Web of Things (WoT) Protocol Binding Templates. *https://www.w3.org/TR/wot-binding-templates/*
9) S. Fukuta et al.: Development of operation management technology for IoT area networks. Institute of Electronics, Information and Communication Engineers, March 2018 (in Japanese).
10) Telecommunication Technology Committee: Home-network Topology Identifying Protocol (HTIP). *https://www.ttc.or.jp/application/files/1115/5443/0461/JJ-300.00Ev3.pdf*
11) Y. Nishiguchi et al.: IoT fault management platform with device virtualization. World Forum on Internet of Things, Feb, 2018.
12) Fujitsu Laboratories: Fujitsu Develops Network Control Technology to Minimize Impact of Cyberattacks on IoT Devices. *http://www.fujitsu.com/global/about/resources/news/press-releases/2018/0528-01.html*

Jun Kakuta
Fujitsu Laboratories Ltd.
Mr. Kakuta is currently engaged in research and development on operation management technology for field area networks.

Yusuke Kobayashi
Fujitsu Ltd.
Mr. Kobayashi is currently engaged in development of network solutions to promote the use of IoT.