Vol.74 No.2 (2022) Production Research 175

Research commentary

Utilization policy of IoT-HUB as interconnection platform

Study of challenges and solutions on IoT-HUB for practical use as an interconnection infrastructure

Hiroyuki BABA * and Tomonari YASHIRO *

Abstract

IoT is expected to create extremely diverse values by interconnecting individual systems. However, there are issues such as consistency of communication protocols, countermeasures against failures, and business concerns. These problems must be solved to realize flexible interconnection. The authors have devised these solutions and discussed their utilization policy on the basis of interconnection infrastructure called IoT-HUB which has been developed through industry-academia collaboration activities at Institute of Industrial Science, The University of Tokyo. This paper reports the contents of an idea and study.

1. Introduction

The authors focused on the Internet of Things (IoT), which is an important element of Digital Transformation (DX) and have continued various preliminary implementations at an experiment house (so-called “COMMA House”) at the Institute of Industrial Science, The University of Tokyo. As a result, this activity led to the development of an infrastructure called IoT-HUB, which interconnects various connected devices and applications (hereafter referred to as “IoT systems”). The IoT-HUB has been implemented in society by industry-academia collaboration partners. The IoT-HUB have already used used by actual users. In order to be used by actual users, it is necessary to solve not only technical issues but also business issues. Hence, this paper includes key findings related to such issues.

*Institute of Industrial Science, The University of Tokyo, Division of Human and Social Sciences

2. Issues of IoT

The IoT is the concept that everything is connected to the net (generally the internet). There is are methods of constructing closed systems consisting of the company’s products such as sensors and smartphone applications, looking at the internet as a simple communication pipe. However, if everything can be connected to the internet, it can be interconnected with the products and applications of other companies to create new value. Naturally, the interconnection strategy with other companies is expected to realize a wide variety of systems in a short time period and to create diverse values dramatically. On the other hand, there are 4 major issues as described below.

First, there is the compatibility issue between IoT systems. One of the authors has experience in the past of interconnecting systems from different manufacturers in the architecture field, where individual IoT systems are

already made in “silos” (described later). The author found the need for coordination of interests between stakeholders, in addition to technical discussions on communication protocols in order to construct a system which controls in an integrated manner. They were extremely complex problems. A general solution to this old-new problem is standardization. A standardization process is the unification of parts of different systems by the parties concerned. Hence, it should originally be a collaborative area. However, in reality, the aim is for the specifications promoted by one company to have a business advantage most likely. It often becomes a competitive area that can be a struggle for a leadership. As a result, a standardization process often takes a lot of time. In the meantime, the world’s giant IT companies, known as big techs, who have strong competitiveness, will go their own way, raising concerns that an oligopoly situation will progress.

In addition, since IoT is a concept that “everything (hereinafter referred to as “thing”) is connected to the internet”, there is a wide range in the price range of things, for example, from a 2,000-yen electric fan to a 1-million-yen entrance door. Making things connected naturally incurs some additional cost, but due to the large difference in the price of the thing, there is also a difference in the ability to bear the cost of making things connected. In other words, even if a single communication protocol is determined as a standard for Interconnection, there will be cases where this cost-bearing ability is not met. In view of this fact, we have decided to develop a system that differs from standardization, and rather interconnects different IoT systems without a great deal of effort. Interest in how to make it happen is in the background of this research.

The next issue is how to deal with the case where the whole system does not work well. This can be said to be a “fault isolation” problem of who should take the initial action when a failure occurs. In a system in which devices and applications from different manufacturers and service providers are interconnected in a complex manner, if a problem occurs as a whole, it is not efficient, of course, for the relevant companies to search for failures all at once. In particular, in the case of IoT, things are located at the end-user’s home, and so it is necessary to send field engineers to the site to deal with failures, which is a factor in increasing costs.

First of all, it is important to find out which business operator’s scope of work is likely to be the cause of the failure, and to make an initial action to the business operator responsible for that scope of work. Specifically, it is very important to adopt an architecture that can set a clear demarcation point of responsibility between interconnected IoT systems, and to isolate failures with an awareness of the demarcation point of responsibility.

Interconnection of IoT system presents additional problems. While the construction of a data utilization society is being advocated, there is a concern that “a third party may use the operation data of my system without permission”. There are both explicit and implicit cases for that, but this concern is very deep-rooted. We would like to point out this “concern about data distribution”, as the third issue, in addition to the “interoperability between systems” and “a demarcation point of scope of work and fault isolation”, as described above.

There are more business issues. Paradoxically

with the first problem, the difficulty of an interconnection (generally referred to as “siloed”) is the result of a kind of a differentiation policy, which is also the source of competitiveness in the market. As already mentioned, it is possible to create a new value by combining the devices and applications of other companies with those of your own company. This means that the competing third party may obtain the environment providing the free interoperability. It is also true that there is an awareness of the problem of whether or not we should welcome this situation from a competitiveness point of view. The authors regard this as the fourth issue and call it “the problem of maintaining a fair competitive environment in the cooperative domain”. Table 1 summarizes the 4 major issues as described above.

3. Solutions to Individual Issues

3.1 Solutions for Compatibility Between Systems

As a method that does not rely on a standardization process, the authors focused on the relationship between personal computers and printers. We use a variety of personal computers and printers at home and at work, but the communication protocol between Company A’ printer and Company B’s printer is not unified. However, we, the users, actually use them without any inconvenience. Taking this example as a hint, the authors thought that interconnection problems could be greatly alleviated by constructing a similar structure on the Internet for interconnection between IoT systems on a large scale.

As a result of various examinations and demonstrations with industry-academia collaboration partners, the authors developed an infrastructure named the IoT-HUB [1),2),3)]. Any IoT system, such as an application or an IoT device, can be interconnected by preparing a small piece of software called a “driver” that supports the communication protocol and by connecting them back-to-back in principle.

The principle is simple, but there is an issue that requires some ingenuity. Devices with connected functions (thereafter referred to as “IoT devices”) are usually categorized into 2 types. Either devices accommodated in the private cloud operated by the manufacturer of the devices or devices having a function that can correspond to the communication protocol. The authors commonly refer to the former as “the cloud accommodation type” and the latter as “the local connection type”. To build a usable interconnection infrastructure, we need to be able to apply the “drivers back-to-back” principle to both styles. For this reason, for the local connection type IoT devices, we have prepared a function similar to the IoT-HUB extension device that can be installed at the site such as the end user’s house and supports the driver. Specific devices to be used include general-purpose devices such as PCs and tablet PCs are suitable from the viewpoint of cost.

Authors developed an architecture called the R-Edge so that the driver can handle main body and the extension device in the same way. R-Edge works like a driver’s socket either on the main body of the IoT-HUB on the internet or on the extension device named the IoT Router. By doing this, both the cloud accommodation type and the local connection type can be connected in the same way by the driver. The IoT-HUB itself is socially implemented as a virtual infrastructure constructed by a public cloud service called the “Function as a Service”. This makes it possible to convert infrastructure construction costs into variable costs.

The IoT Router is an extension device that provides the

access point of the IoT-HUB on the local site, and it is a part of the IoT-HUB. In a home automation, etc., we see an architecture in which a local controller-like terminal called a Home Gateway (HGW) is placed, but the position of the IoT Router is totally different from this HGW.

Applications generally deal with an interface called the Web API (Application Program Interface), and there are few cases where a special driver is required. However, in cases where there are a wide variety of interconnection destinations and a large number of command formats delivered to each destination, a method of absorbing these differences with a driver named “Application Driver” may also be implemented.[4] This way of thinking ensures a sort of an ideal state in which “you are free to take responsibility for yourself”, from applications and devices to drivers. Figure 2 shows an overview of the infrastructure that integrates the explanations as described above.

A driver is a small piece of software sending and receiving commands that match the communication protocol of the IoT system. It can be developed in about one week by one software engineer. The interface with IoT devices varies, depending on the device: type (1) published on a website, etc., type (2) prepared to be provided under an Non-Disclosure Agreement (NDA), and type (3) discussed individually. Based on our experimental experience, it seems that connected devices take type (1) and (2) mainly.

3.2 Implementing the Fault Isolation function

By bringing the concept of interconnection by drivers, it became relatively easy to construct the fault isolation function. It is a common sense for all PC users in a daily life to recognize that the printer and its printer driver are provided as a package by their manufacturer, and that the printer driver and the printer are within the responsibility of the manufacturer. Of course, it is also a common understanding that the USB cable connecting the PC and the printer is out of scope of the manufacturer of the PC and the printer.

Likewise, the IoT device and the driver is within the responsibility of the manufacturer, and this is consistent with the common sense of life described above. In the demonstration experiments conducted by the authors, many people understood that it was rational to set the back of the driver (the interface with the R-Edge) as the point of separation of responsibility. For this reason, IoT-HUB defines the back of the driver as the demarcation point.

It will take some time before IoT device manufacturers deliver their device drivers attached together. Until then, drivers will inevitably be made available from third parties. However, it is possible to make the back of the driver the demarcation point of operation by recognizing mutually the awareness of the parties concerned, based on the IT common sense in a daily life, as mentioned above.

By making the back of the driver the demarcation point of responsibility in this way, the problem of who should take the initial action in the event of a failure becomes much easier to deal with. Furthermore, we have confirmed that the function that enables this can also be implemented in the IoT-HUB. Figure 3 shows the principle. By switching the information transmission route and testing, it is possible to estimate the section where the failure occurs.

Specifically, the service provider that received the failure report from the user switches the information route of the failure occurred from the normal route B to the route A by the IoT-HUB operation command that is permitted to the service provider itself. A “virtual device” that emulates the response from the IoT device is placed at the end of the route A. Since the “virtual device” only emulates responses, it is practically a piece of software that is not much different from a driver. Based on the difference in the responses of the route B and the route A, the fault section is estimated as shown in the table in Figure 3. If this is compared with the demarcation point of responsibility defined as the back of the driver, the operator that should make the first move is determined. Operators responsible for the initial action include the following 3 candidates: “the Service Provider”, “the IoT-HUB operator” and “the IoT device manufacturer”. In practice, the former two parties will take care of the first move as one team. If the failure is within the scope of responsibility of the IoT device manufacturer, it is expected that the manufacturer will first use its own troubleshooting tool and search for the failure within the scope of responsibility of the company.

The IoT-HUB implemented in society already has more advanced functions. If the driver is developed using the SDK (Software Development Kit) provided, the mechanism for the driver etc., to return a response to the command is incorporated. Therefore, the fault location can be estimated without relying on the theoretical switching method as described above.

3.3 Measures to resolve concerns about data distribution

In interconnecting IoT systems, there are concerns in a user operator side which cannot be wiped away that the operating data of own devices, etc., may be peeped, stored, and used improperly by the IoT-HUB operators. This concern is so strong that it may cancel out the functional merits of interconnection nodes such as the IoT HUBs, and we need a convincing and reasonable solution.

The authors studied the use of laws and regulations. Telecommunications business is stipulated as the one that “intermediates other people’s communications” [5], and the IoT-HUB is also included in this category. Article 4 of the Telecommunications Business Law stipulates (Protection of Confidentiality) that the secrecy of communication pertaining to the handling of telecommunications carriers shall not be violated.

If the operator of the IoT-HUB becomes a telecommunications carrier, the act of worrying about the data distribution that IoT-HUB users have will be prohibited by law, and, therefore, this measure will be a clear solution message.

3.4 Measures to maintain a fair competitive environment in cooperative areas

The IoT-HUB can be called a function that enables a mutual interconnection with other systems on an equal footing (hereafter, “flat interconnection”) after clarifying the scope of responsibility of various IoT systems. In this environment, competitors also can obtain the same benefits, and there is a view that the company's competitiveness may be reduced in the end accordingly. The IoT-HUB operators can solve this problem by adopting the following business scheme.

It is explained in Figure 4, taking the cloud storage

style as an example. The IoT devices are operated by sending signals to the API. In general, multiple APIs are prepared for one type of the IoT device, and each API corresponds to the individual operation of the device or is dedicated to troubleshooting by the manufacturer.

To make it simple, it is assumed that 2 service providers, Company A and Company B, would like to interconnect with the same model of the IoT devices of Company Z. Company Z determines a scope of API to grant access to Company A and Company B differently, depending on the business profit-and-loss account and the technical level of each of Company A and of B. Even if a connection is made in the same way via the IoT-HUB, the system by Company Z-A and the system by Company Z-B can be differentiated.

This should be called a business scheme rather than a technical matter, and the authors call it a measure to maintain a fair competitive environment in the cooperative area. If the IoT-HUB operator mediates these discussions using the Web, etc., an one-stop service for a mutual connection will be realized. Social implementation of this measure is to be made available in the future.

4. Use cases

4.1 As a measure to ensure the flexibility of the core system

This infrastructure was implemented in society in 2019 by industry-academia collaboration partners. It is currently used by actual customers. Figure 5 illustrates an example of a use case by a so-called general contractor. General contractors actively promote the integrated management and operation of incidental facilities such as energy management and information communication systems for the buildings they have constructed by using a core system called a “Building OS”. Incidental facilities include basic facilities that can be used by any tenants, as well as a wide variety of facilities that can be selected according to tenant preferences. It is clear that modifying the “Building OS”, which is the core system, each time they deal with these highly variable projects would result in long response times and increased costs. In this application example, it can be realized without modifying the core system by passing some of the auxiliary system support parts, that should be flexibly handled, via the IoT-HUB,.

4.2 As a tool for utilizing existing management resources

Figure 6 shows a use case by one of the big leasing companies. Leasing companies often use mobile communication terminals to find out the leased equipment used by client companies. With the emergence of low-cost communication systems using latest technological advances such as the LPWA (Low Power Wide Area Network), there is an opportunity to reduce the communication costs described above. However, in order to use this, system vendors often propose that it would be necessary to rebuild the entire existing management system. It results in a high cost, which the leasing company has concerns about.

As a result, this leasing company left the existing management system as it is and introduced the IoT-HUB in the connection part from the mobile phone system (4G) to the LPWA system to convert the protocol, thereby minimizing the system modification cost and reducing the communication cost. This is a successful example of the BPR (Business Process Reengineering) in enterprise.

(Accepted on February 14, 2022)

5. Conclusion

There are no particular restrictions on the interconnection targets of this infrastructure. Distributed energy resources that can contribute to carbon neutrality are also considered as an important IoT system that should be targeted. If micro-carbon credit transactions are added to this[7], it will be possible to realize complex services that go beyond the energy domain.

This research was made available with the help of the member companies of the IoT Special Study Group established in 2015, as well as with the help of organization that concluded a collaborative agreement with the Special Study Group and conducted various demonstration tests. We would like to express our gratitude once again. Furthermore, we would like to thank Yoshihiro OBATA and Jun MATSUMURA, representative directors of IoT-EX Inc., who have implemented the research results in society, for their great support. We would like to express our deepest gratitude again.

Figure 1. COMMA House

Table.1 Issues related to an interconnection of IoT systems

#	Issues	Concerns	Solutions
1	Compatibility of communication protocols etc.	①In the IoT field with a wide price range, the ability to bear the incremental cost for connection varies widely. ②It often takes time to standardize.	Needs to study measures, not relying on a standardization activity
2	Fault isolation function	①In order to reduce costs, we would like to minimize an on-site support for the IoT device installed. ②In case of services consisting of applications and equipment by providers, we would like to know which provider will take the first action.	Needs to implement a separation function utilizing the demarcation point of responsibility
3	Concern about data theft	There is a concern about data on the IoT-HUB is peeped and stored to be used without permission	Needs a measure clarifying that anyone does not take a wrong action
4	Maintaining a fair competitive environment	Connecting equally and freely will lead to reduce competitiveness of the individual business	Needs a mechanism to maintain a fair competitiveness even in the collaboration area of the IoT-HUB

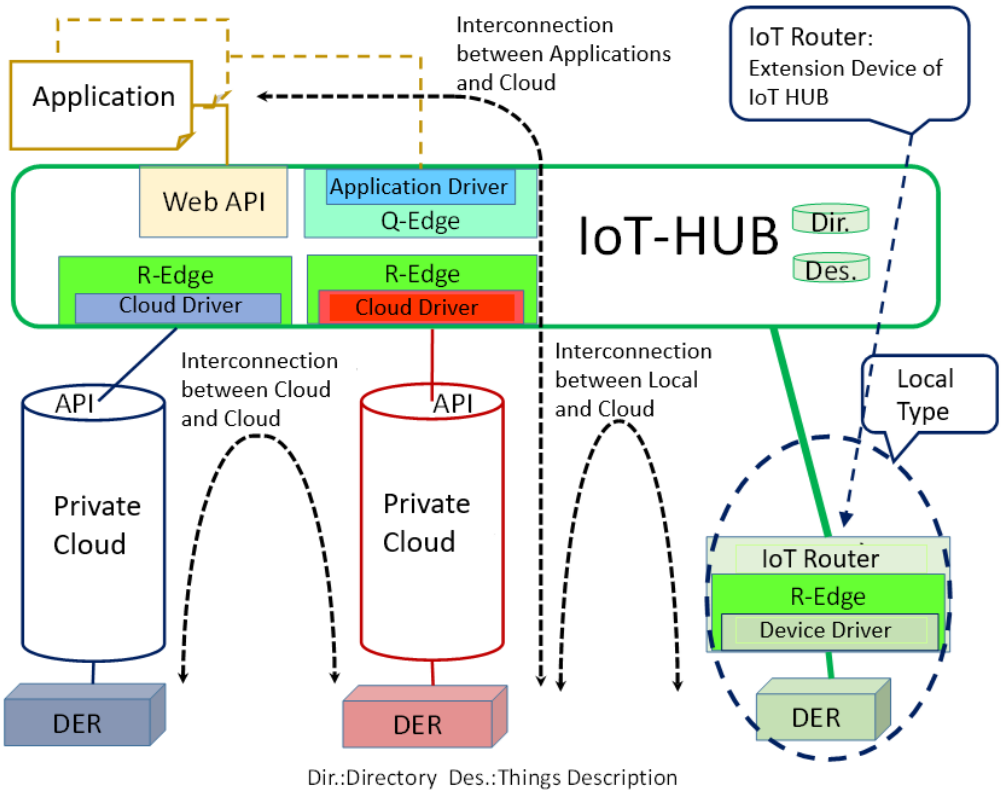

Figure 2. Overview of IoT-HUB infrastructure

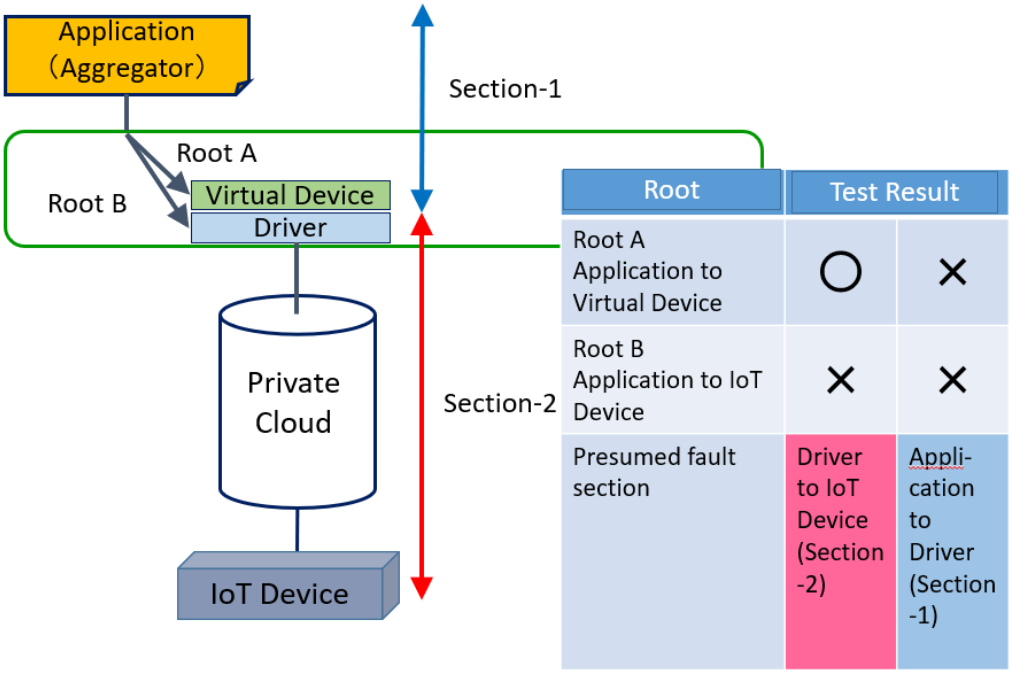

Figure 3. Implementation of a Fault Isolation function

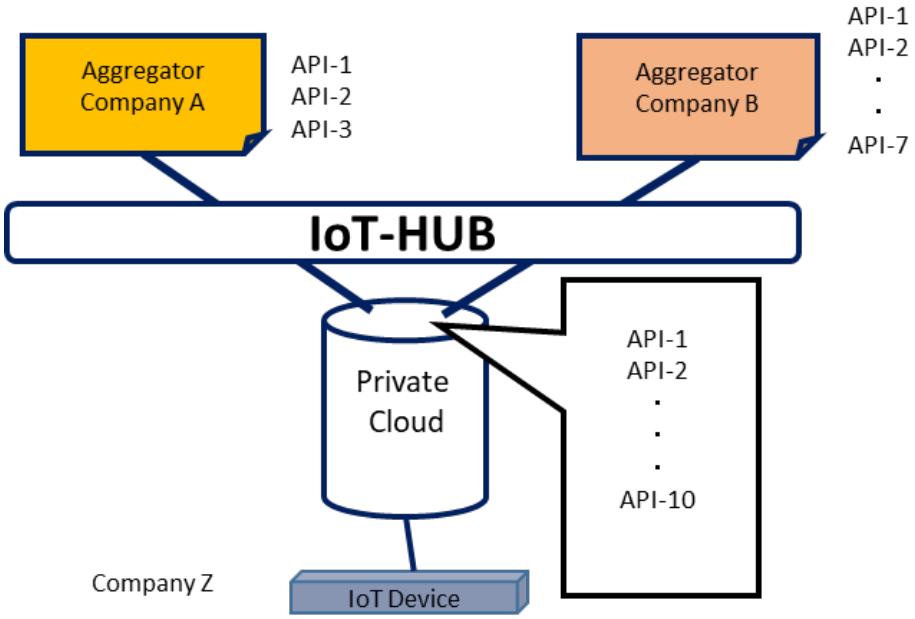

Figure 4. Measures to maintain a fair competitive environment in cooperative areas

Figure 5 Use cases by a general contractor [6)]

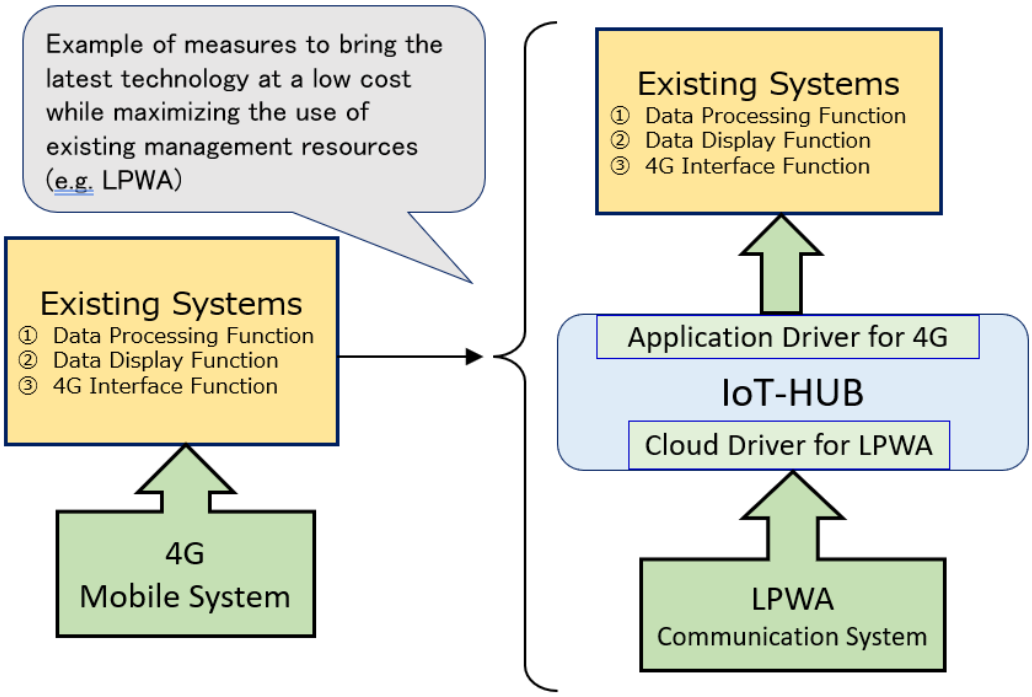

Figure 6 Examples of application by a leasing company [6)]

References

1) Hiroyuki BABA et al., Trial implementation of Surplus Electricity Utilization Scheme for Individuals between Remote Points using Electricity Trading System,
Transactions of the Institute of Electrical Engineers of Japan C, Vol.141, No.3 (2021), pp383-393

2) Hiroyuki BABA et al., Development of Interconnection Infrastructure for Various Systems for IoT,
2021 Institute of Electronics, Information and Communication Engineers General Conference, D-23-11

3) Hiroyuki BABA et al., Addition of Other Network Connection Functions to Interconnection Infrastructure for IoT,
2022 Institute of Electronics, Information and Communication Engineers General Conference, D-23-3

4) Hiroyuki BABA et al., Study of Countermeasure against Request for Information Diversity of DER,
2022 Institute of Electrical Engineers of Japan National Convention 4-164

5) Article 2 of the Telecommunications Business Law

6) Industrial Technology Research Promotion Committee IoT Special Study Group (RC-88) leaflet (2021)

7) Tomonari YASHIRO, Path and Significance of Introducing Carbon Trading in the Construction Field, Production Research, 73, 4 (2021), pp247-251