IIR

Internet
Infrastructure
Review

Jul.2020
Vol.47

Periodic Observation Report

Messaging Technology

Focused Research (1)

IIJ's Efforts to Promote LoRaWAN® in Agricultural IoT

Focused Research (2)

COVID-19's Impact on FLET'S Traffic

IIJ
Internet Initiative Japan

Internet Infrastructure Review

July 2020 Vol.47

Executive Summary

We touched briefly on COVID-19 at the beginning of the previous IIR issue's executive summary, and not a day has passed since that COVID-19 has not been on our minds. Many countries have gone into lockdown as the world continues working to contain the spread.

The use of information and communication technology (ICT) has come into the limelight under these circumstances. It is playing a major role underpinning our way of life amid the pandemic. ICT provides leisuretime in our homes while we are forced to stay in and stream videos, for instance; it lets people keep on working even while opportunities for interacting with others in person are diminished; it facilitates distance learning for students unable to physically attend a classroom due to school closures; and it helps to smoothly deliver assistance to people experiencing financial distress. Meanwhile, some issues have been raised, including the question of how we should approach the balance between individual privacy and the public interest when it comes to, for example, public institutions using ICT to monitor infected people via devices and surveillance cameras. And as we noted here in our previous issue, the reliability of the information coursing through the Internet is another issue. People are working to address these concerns from across many sectors, including government, healthcare, energy, transport, and distribution. The information and communications industry is a key part of the infrastructure that underpins our society, and we will continue striving to develop technology as we look to play an even greater role than ever before.

The IIR introduces the wide range of technology that IIJ researches and develops, comprising periodic observation reports that provide an outline of various data IIJ obtains through the daily operation of services, as well as focused research examining specific areas of technology.

Chapter 1 is our periodic observation report. These reports cycle through four topics over the course of each year. In this edition, it is time for messaging technology. IIJ's email services provide SPF, DKIM, and DMARC sender authentication when emails are received, and we constantly monitor the authentication results. Our observational results show that, while use of SPF and DKIM continues to spread, DMARC deployment rates are still low, which tells us that we need to continue advocating for increased use of DMARC. The report also looks at the use of sender authentication technology on phishing emails and goes over the JPAAWG 2nd General Meeting.

The focused research report in Chapter 2 discusses IIJ's use of LoRaWAN® in agricultural IoT. LoRaWAN® is a type of LPWA (low-power wide-area) wireless network for IoT devices that is gaining attention as it allows people to build and run networks without having to rely on communications carriers. The report describes the knowledge we gained and challenges we faced through our real-world efforts to install base stations and IoT devices in paddy fields, and I think you will find it an intriguing read.

The focused research report in Chapter 3 examines the role that information and communications has played amid the COVID-19 situation. At different times from February onward, people in Japan were asked to observe restrictions on their activities, which included the government requesting schools be closed, prefectural authorities urging people to stay indoors, and the government declaring a state of emergency. Analyzing changes in fixed-line broadband traffic patterns around the time each of those requests were made provides insight into how the requests affected Internet usage. These data will no doubt be a valuable impetus for reaffirming the importance of developing Internet infrastructure.

Through activities such as these, IIJ strives to improve and develop its services on a daily basis while maintaining the stability of the Internet. We will continue to provide a variety of services and solutions that our customers can take full advantage of as infrastructure for their corporate activities.

Junichi Shimagami

Mr. Shimagami is a Senior Executive Officer and the CTO of IIJ. His interest in the Internet led to him joining IIJ in September 1996. After engaging in the design and construction of the A-Bone Asia region network spearheaded by IIJ, as well as IIJ's backbone network, he was put in charge of IIJ network services. Since 2015, he has been responsible for network, cloud, and security technology across the board as CTO. In April 2017, he became chairman of the Telecom Services Association of Japan MVNO Council.

Messaging Technology

1.1 Introduction

According to the Council of Anti-Phishing Japan's reports[*1], the number of phishing cases reported to the council is rising rapidly. April 2020 saw 11,645 cases reported, an increase of 1,974 vs. the previous month (March 2020) and a hefty 9,257-case year-on-year rise (vs. April 2019). The substance of these cases shows a large volume of phishing impersonating major companies that maintain an online presence. Indeed, I have also received a number of such emails. The Subject header and the display name and local part of the From header generally look the part, but the sender domain name is often completely different. And because fraudulent emails impersonating government agencies may be on the rise, countermeasures should be taken by both email recipients as well as owners of domains likely to be spoofed.

As we have repeatedly reported, sender authentication is effective against phishing and other forms of email spoofing. Those who send phishing emails are aware of these measures, however, so using them properly is important to ensure effectiveness. Further, some posit that the rise in these emails reflects the recent social situation, so it may persist for some time yet.

In this issue, we report on the prevalence of sender authentication technologies (SPF, DKIM, DMARC) that are effective against email spoofing. We also discuss how to use the results of sender authentication against the type of phishing emails currently circulating. We also report on the JPAAWG 2nd General Meeting, held last year.

1.2 Sender Authentication Rates

It is now 14 years since the first SPF (Sender Policy Framework) specification, RFC 4408[*2], was published in April 2006. This was later followed by the DKIM specification, which uses digital signatures, and eventually DMARC, which uses SPF and DKIM authentication results. We report on the current prevalence of these sender authentication technologies.

*1 Council of Anti-Phishing Japan, monthly reports listing (https://www.antiphishing.jp/report/monthly/, in Japanese).

*2 Subsequently revised in April 2014 as RFC 7208.

1.2.1 Results Based on Emails Received

Given the practical implications, the percentage breakdown of authentication results for received emails can be considered important from the perspective of studying sender authentication deployment rates. IIJ's email services provide the ability to perform SPF, DKIM, and DMARC sender authentication upon email receipt. This feature returns a "none" result for each method if the received email cannot be authenticated. So the proportion of received emails that do not return "none" can be interpreted as the deployment rate for received emails.

Figure 1 shows the breakdown of SPF authentication results for emails received in April 2020. The "none" result accounts for 12.1%, meaning that the deployment rate was 87.9%. This is a 2.2%pt increase vs. the rate of 85.7% reported a year ago in IIR Vol. 43. The figure for "pass", meaning SPF authentication was successful, rose 9%pt from 70.1% in April 2019 to 79.1% in April 2020. So the proportion of authentication failures (hardfail, softfail, and neutral in the case of SPF) also fell by 6.4%pt, indicating a rise in emails not spoofing as far as SPF is concerned. The increase in phishing reports, however, implies that spoofed emails are not themselves in decline. That is, spoofed emails that are not spoofing as far as SPF is concerned may be on the rise.

Figure 2 breaks down DKIM authentication results for emails received in April 2020. The "none" result accounts for 51.7% (48.3% deployment rate), a 10.5%pt drop from 62.2% a year earlier, meaning that the deployment rate increased 10.5%pt. Implementing DKIM as a sender requires some effort as it requires adding a DKIM digital signature on the sending email server. The current deployment rate is by no means adequate, but 13 years since the first DKIM specification was released in RFC 4871, it has finally spread to around half of all emails received (in terms of emails received on IIJ services).

Figure 3 breaks down DMARC authentication results for emails received in April 2020. The "none" result accounts for 75.4%, indicating a deployment rate of 24.6%, a 1.5%pt increase vs. a year earlier. This is a very small increase relative to SPF, which in practical terms is now

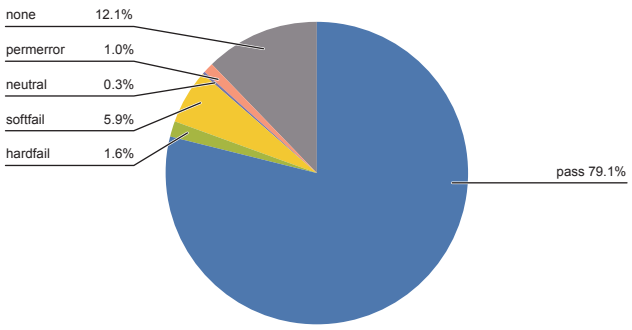

Figure 1: Breakdown of SPF Authentication Results

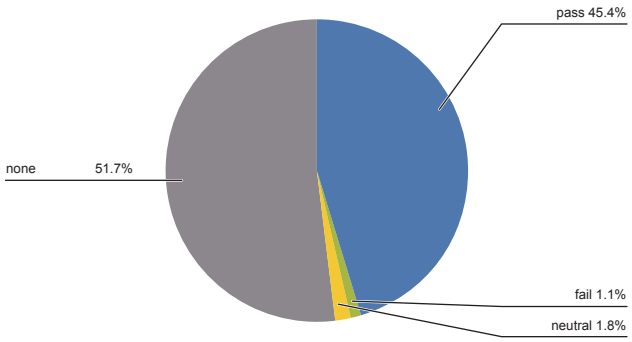

Figure 2: Breakdown of DKIM Authentication Results

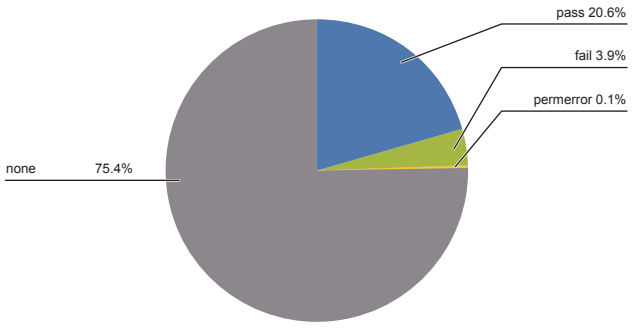

Figure 3: Breakdown of DMARC Authentication Results

almost fully deployed, and DKIM, which generally entails an implementation cost. Deploying DMARC requires either SPF or DKIM, or both, to be present, but if that requirement is satisfied, DMARC can be implemented by simply publishing a DMARC record (text resource record) on the DNS, as is done with SPF. There is no need to look at the sending email server's exit point, so DMARC records should actually be easier to configure. We still do not know whether the meagre increase in deployment relative to SPF and DKIM reflects a simple lack of recognition or administrators being unclear about the motivation for publishing a DMARC record. We intend to continue advocating for the broader deployment of DMARC ahead.

Figure 4 shows the breakdown of DMARC certification results over time, from January 2016. Rather than April 2020 being an extremely low point for DMARC, the graph instead shows that while there is a gradual increase in sender domains supporting DMARC, that growth is very slow.

Figure 5 breaks down the TLDs (top level domains) of domain names that passed DMARC authentication. The percentages are not relative to the volume of emails received; they indicate TLD counts as a proportion of the total number of separate DMARC domain names (unique domain names). The .com TLD had the largest pie piece at 53.2%. Second was .net with 9.5%, and Japan's .jp domain name was third with 6.7%. Among domain names that passed SPF authentication, .com was again the most common TLD, so there was no major difference in the rankings.

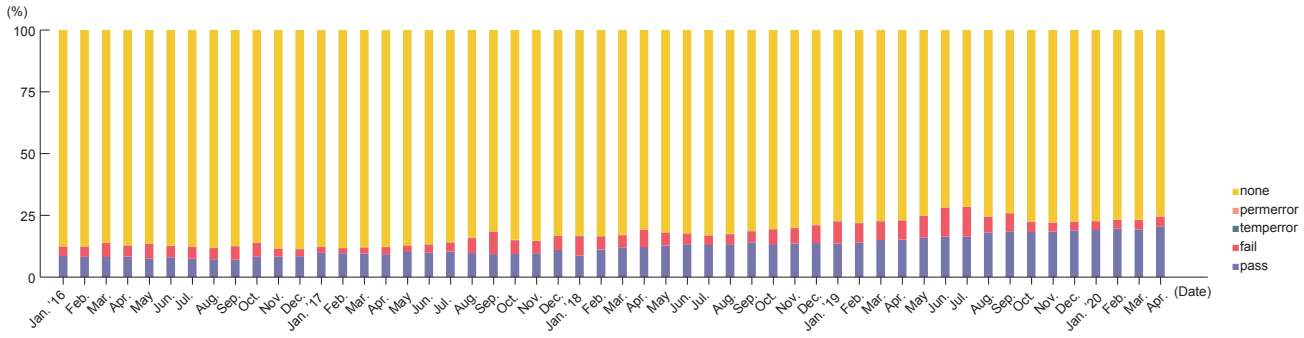

Figure 4: Breakdown of DMARC Authentication Results Over Time

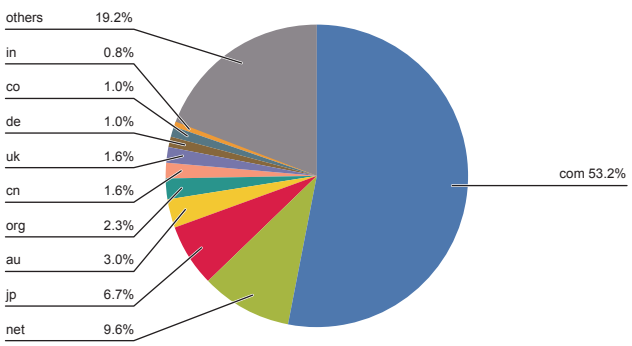

Figure 5: TLD Breakdown for DMARC Domain Names

1.2.2 Results Based on Domain Names

Another view on sender authentication technology is provided by looking at how many records for each sender authentication technology are registered for registered domain names. To do this, we have to set a scope and obtain all domain names within that scope.

As reported in IIR Vol. 39, we are studying jp domain names in collaboration with Japan Registry Services (JPRS), and we currently have a joint research agreement with Internet Association Japan (IAjapan). I am taking part in the studies as a member of IAJapan.

DKIM needs the DKIM selector name to acquire the digital signature information (DKIM record), but since the selector is specified in the email header, the domain name alone is insufficient to determine the DKIM record's location. It is sometimes possible to guess whether a DKIM record has been created[*3], but this is not always accurate. This is why only study results on the prevalence of SPF and DMARC, and not DKIM, are published[*4]. In each case, the proportions are based on domain names that have MX resource records, enabling us to determine that the domain name is used for email. There are, of course, ways of configuring SPF and DMARC records (and, recently, MX resource records too) for non-email domain names, but we'll cover the details of that another time.

Here, we report on the latest study results for SPF and DMARC. In March 2018, when our study began, SPF was on an average of 57.3% of all jp domain names. Our latest results, for May 2020, show a 7.8%pt increase to 65.1%.

Figure 6 plots DMARC deployment on jp domain names. From 0.57% in March 2018, it rose 0.62%pt to 1.19% in May 2020. So the rate doubled over roughly two years, but it was low to begin with and the increase itself was very small relative to that for SPF, so both readings were very low. By domain type, DMARC is currently most prevalent on go.jp domains, but only with a 5.4% reading. SPF has 92.4% prevalence on go.jp, so we hope to see similar efforts to drive increasing use of DMARC records on all jp domains.

1.2.3 Sender Authentication as a Measure Against Email Spoofing

Government agencies and so forth are implementing a range of measures under the current societal situation, and email communications are set to increase as part of that process. Online purchasing and the like is also on the rise as people avoid going out. As a reflection of this, fraud via phishing and email spoofing may be on the rise.

For example, emails impersonating Amazon are frequent and adopt a number of patterns, but emails from the actual Amazon support SPF, DKIM, and DMARC, so sender authentication will tell you if an email is spoofed or not. And the Amazon SPF record ends with "-all", so an SPF authentication failure always returns the strongest result of "fail". The DMARC policy is also set to the relatively strong "p=quarantine". So Amazon seems to have actively adopted sender

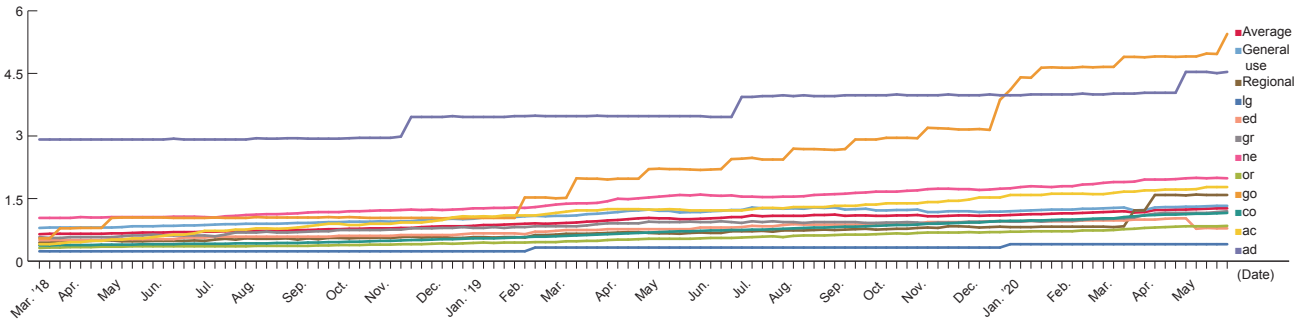

Figure 6: DMARC Deployment on jp Domain Names[*5] Over Time

*3 How to Measure Deployment Ratio of Domain Authentications (http://member.wide.ad.jp/wg/antispam/stats/measure.html.en).
*4 Anti-spam Measures | Statistical Data (https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei, in Japanese).
*5 Regional (newly registered) includes prefectural domain names.

authentication technology and bolstered defences against email spoofing. A point to note about detecting Amazon spoofing emails is the need to check that the authenticated domain name is correct. In Japan, Amazon uses the amazon.co.jp domain name. Many of the spoofed emails use completely unrelated domain names and are set up so as to pass SPF and DMARC. The Subject header and the display name in the From header contain the string "Amazon". So ensuring that the authenticated domain name is also checked is key to avoid being defrauded.

Of the jp domain name types shown in Figure 6, lg.jp, which is used by local governments and such, has consistently had the lowest DMARC deployment rate since our study began. Of course, local governments do not only use lg.jp, but the deployment rates shown indicate what proportion of domains with MX records have a DMARC record configured, and the proportion of those with an SPF record was a high 80.7%, coming in behind go.jp. So here again, to protect against spoofed emails, administrators first of all need to configure a DMARC record to protect the sender domain in the header. And to determine just how many emails are spoofing the domain, they also need to get set up to receive DMARC reports so they can constantly monitor what is happening.

1.3 JPAAWG 2nd General Meeting

The JPAAWG 2nd General Meeting (GM) took place at Bellesalle Iidabashi First on November 14–15, 2019 (Figure 7). As in 2018, it was held in conjunction with IAJapan's Anti-Spam Conference. And as with the 1st GM, IIJ was again a platinum sponsor.

In light of the 1st GM's outcomes, the following new ideas were tried at the 2nd GM.

1. Hold meeting over two days
2. Welcome many speakers and attendees from abroad, including M³AAWG members
3. Hold training sessions (paid)
4. Conduct Open Round Table discussions

Open Round Table (ORT) sessions are held at every M³AAWG General Meeting[*6], allowing participants to gather and discuss topics of interest to them. ORTs can even be the point of inception for documents like new technical specifications and Best Practices, making them one of the driving forces behind M³AAWG's activities. JPAAWG set five themes for the sessions, and JPAAWG members served as moderators to facilitate balanced discussion involving all participants. JPAAWG hopes to continue hosting activities like ORTs to provide a forum for discussing issues and thinking about solutions.

We wanted to hold the JPAAWG 3rd General Meeting in a similar format in 2020. Under present circumstances, however, a large gathering does not look all that viable. We are in the process of considering what sort of format would work, so we will provide notice on the website[*7] once a decision is made.

*6 Messaging, Mobile and Malware Anti-Abuse Working Group (https://www.m3aawg.org).
*7 Japan Anti-Abuse Working Group (JPAAWG) (https://www.jpaawg.org/).

1.4 Conclusion

I attended the JANOG45 meeting held in Sapporo over January 22–24, 2020, and made a presentation in the "Current State of Phishing and Countermeasures" session. I went because I felt it was important for a large number of people in the field to be aware that adoption of sender authentication technologies, DMARC in particular, is low, as discussed in this report. At the M³AAWG 48th General Meeting in San Francisco over February 17–20, 2020, we again held a JPAAWG BoF group meeting, and in a session titled "State of Messaging Anti-Abuse in Japan", I presented on JPAAWG's activities along with other JPAAWG/M³AAWG members.

So in 2020, we had opportunities to present both in Japan and abroad, and we were all set to continue communicating our key insights with increased vigor. But the situation took a turn, as you know, and forced a rethink of the format in which meetings are held. Yet our work is aimed at promoting the proper use of the various tools available on the Internet, so even under circumstances such as these, I think we should continue working to make communication happen and ensure that those tools are not misused.

Figure 7: Photo taken at the JPAAWG 2nd General Meeting

Shuji Sakuraba

Senior Manager, Application Service Department, Network & Cloud Division, IIJ. Mr. Sakuraba is engaged in the research and development of communication systems. He is also involved in various activities in collaboration with related external organizations aimed at bringing about safe and secure messaging environments. He has been a member of M³AAWG since its establishment. He is the chair of the Japan Anti-Abuse Working Group (JPAAWG). He is acting chairperson of the Anti-Spam mail Promotion Council (ASPC) and a member of its administrative group, as well as chief examiner for the Technology Workgroup. He is a visiting researcher at Internet Association Japan and chairman of its Anti-Spam Measures Committee. He is a visiting researcher at JIPDEC.

IIJ's Efforts to Promote LoRaWAN® in Agricultural IoT

2.1 Introductions

IoT initiatives are expanding rapidly across a whole range of fields. As the use cases multiply in manufacturing, healthcare, automobiles, and other areas, IIJ has turned its eye to agriculture. Agriculture is a core industry and backbone of the nation, yet it is plagued by issues including serious workforce aging and a lack of successors as well as poor profitability. To address these issues, Japan's Ministry of Agriculture, Forestry and Fisheries has made "smart agriculture" a keyword and is actively engaged in demonstration testing nationwide.

Against this backdrop, IIJ is looking at whether it can lend a hand to ease the burden on Japanese agriculture and help make it more economically viable. Our track record so far includes developing paddy field sensors that use LoRaWAN®, a new wireless communications technology that IIJ is focused on.

The biggest issue facing IoT for agriculture is enabling data communications. Here, we take a deep dive into the know-how we have amassed through experience and trial-and-error in the field, which has involved installing base stations, evaluating data link performance, and the like.

2.2 Testing IoT-based Paddy Field Water Management

With support from the National Agriculture and Food Research Organization's special scheme project on vitalizing management entities of agriculture, forestry and fisheries, IIJ has been developing and testing a low-cost ICT water-management system that facilitates labor saving in the area of paddy field water management. This year, we launched Mizukanri Pack S [Water Management Pack S], which packages together the results of these efforts as a set of paddy field sensors that measure water levels and temperature, a wireless base station, a smartphone water management app, and cloud services (Figure 1). The paddy field sensors and wireless base station use LoRaWAN® to communicate. A package that automates water management is also available, comprising the Mizukanri Pack S paddy field sensors and base station as well as a valve that automatically controls water volume based on water levels measured by the sensors.

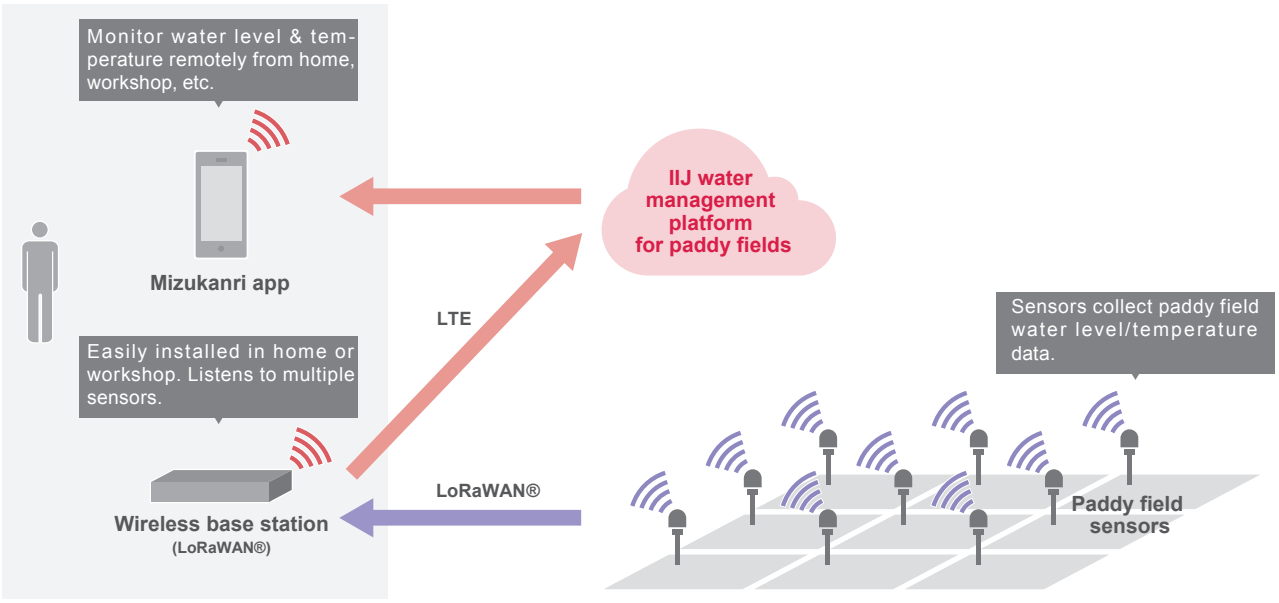

Figure 1: Mizukanri Pack S Saves Labor in Paddy Field Water Management

IIJ is a communications carrier, so working in an unfamiliar area like agricultural IoT and venturing outside of our area of expertise to develop new devices like paddy field sensors was challenging and a constant struggle. We detail these efforts in "The IIJ Stories"[*1].

In this report, we focus on the wireless base stations, part of IIJ's business domain, and describe efforts to promote use of LoRaWAN® in agricultural IoT. Although it is part of our business domain, we were inexperienced in many respects and faced a range of challenges. In particular, we travelled frequently to measure data link status, from Hokkaido in the north down to Kyushu in the south. Before delving into the knowhow those efforts produced, we first provide some background knowledge on LoRaWAN® and how it is distinct from other LPWA standards.

2.3 A Single Base Station Can Cover Several km with LoRaWAN®

2.3.1 About LoRaWAN®

LoRaWAN® is a wireless networking specification that uses a spread spectrum modulation technique called LoRa®, developed by Semtech. Although LoRa® communication speeds are slower than Wi-Fi and BLE, it can cover an even wider range than LTE, as illustrated in Figure 2. It also makes it possible to create low-power devices that can communicate for several years on battery power alone. Mizukanri Pack S paddy field sensors take advantage of these characteristics to cover an area of several kilometers with a single base station and operate throughout an entire growing season on two AA batteries, with no need for the batteries to be replaced.

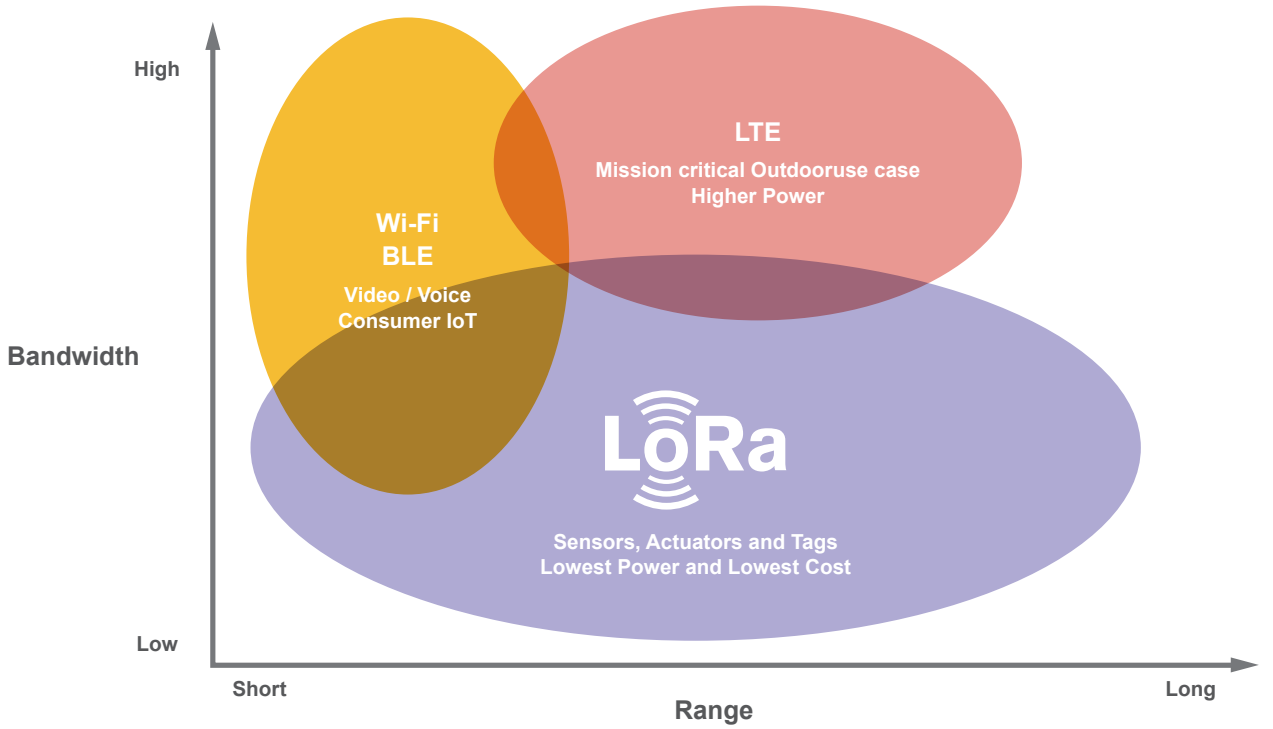

Figure 2: LoRa® Relative to Other Standards

*1 The IIJ Stories | IoT is changing the future of Japanese agriculture by supporting rice farmer work-style reforms (https://www.iij.ad.jp/interview/03.html, in Japanese).

Some LoRa® wireless networks use proprietary protocols, but the standard is LoRaWAN®, specified by the LoRa Alliance®, comprising over 400 member companies including IIJ. LoRaWAN® certificated devices are interconnectable, opening up a wide range of choice with respect to sensors and other connected devices from different manufacturers.

Figure 3 shows the structure of a LoRaWAN® system. The devices communicate via gateways and LoRaWAN®. The gateways connect to a network management server, called a network server, via LTE, Wi-Fi, or wired Ethernet. The network server provides management capabilities, including device activation, elimination of duplicate data received from the same device via multiple gateways, control of communication routes to the application server for each data payload, and variable data rate control. The application server communicates with the network server via a REST API or the like, and stores data received from end-devices, provides application-based visualizations, and controls devices according to user command or automatically according to preset criteria.

2.3.2 Features Compared with Other LPWA Standards

LoRaWAN® is a type of LPWA (low-power wide-area) network. These networks are characterized by low power consumption, low bit rates, and wide area coverage. Many other LPWA wireless networks exist, including Sigfox and LTE-M. Communications carriers operate base stations nationwide for Sigfox and LTE-M, and the networks can be used within the coverage areas without the need to install your own base station.

Sigfox is very inexpensive, with usage fees as low as 100 yen per device per year (depending on the number of devices under contract), and covers 95% of the population as of January 2020. In basic terms, it allows for uplink only with payloads limited to 12 bytes and the number of messages per day limited to 14. Yet it is the leader in Japan in terms of number of devices deployed, with, for example, 850,000 compatible devices that use these features for taking gas meter readings already slated for installation.

The LTE-M standard is developed by 3GPP, and three mobile carriers provide LTE-M services in Japan: NTT Docomo, KDDI, and SoftBank. Using a bandwidth of 1.4MHz allows bidirectional communication of up to 1Mbps, and it also supports FOTA (Firmware Over-The-Air) remote device firmware updates. It also supports handover switching of base stations when on the move, so it can be used in much the same way as regular LTE. However, if used only on carrier networks, the data charges are 100–150 yen per device up to 10,000 devices, which is far more expensive than Sigfox.

Some carriers provide their own LoRaWAN® base stations and base stations shared among users, but generally you need to install your own base station. Low-price LoRaWAN® gateways are available that are similar to mass-market LTE-capable IoT gateways, like the Kiwi Technology TLG3901BLV2 included in Mizukanri Pack S.

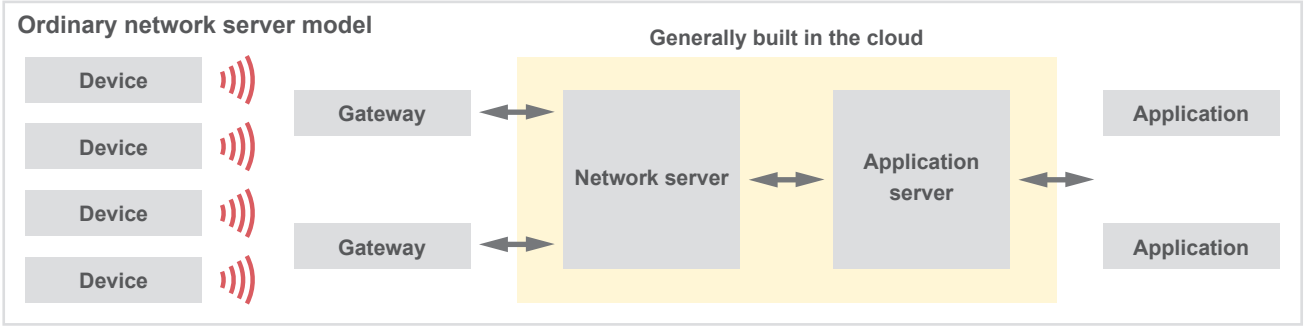

Figure 3: Overview of a LoRaWAN®-based System

2.3.3 Applications Suited to LoRaWAN®

Having to install your own base station puts LoRaWAN® at a disadvantage to Sigfox and LTE-M in terms of equipment and installation costs. But an advantage is the ability to add base stations to reach areas not covered by outdoor base stations, such as basements and inside buildings. And because there are no data charges for communications between devices and the gateway, the cost benefits are considerable if only a few base stations are used to serve a large number of devices. LoRaWAN® is particularly suitable for low-cost applications that involve multiple battery-powered devices installed in large buildings, such as factories, shopping centers, and offices.

With no downlink restrictions, LoRaWAN® is also effective in agricultural IoT, including paddy field water management, when there is a need to control devices like water supply valves. Ensuring profitability in agricultural IoT can be difficult if expensive devices and services are used, so the advantages of LoRaWAN® and inexpensive equipment come into play here to enable low-cost services even when using multiple devices of different types. A range of LoRaWAN®-compatible devices from different manufacturers are already available for agricultural IoT, including paddy field sensors and water supply valves for paddy field water management, weather sensors for measuring rainfall and temperature, and soil sensors for measuring soil temperature and moisture. These can all be accommodated by a single LoRaWAN® base station. Another advantage is the ability to set up your own base stations to provide coverage in areas where carrier-operated base stations can struggle, such as mountainous terrain.

Figure 4: Kiwi Technology's TLG3901BLV2

2.4 Challenges in Promoting LoRaWAN® for Agricultural IoT

So far we have discussed:

- Features of LoRaWAN® and suitable applications
- Advantages of LoRaWAN® in agricultural IoT

So what challenges do we face in popularizing LoRaWAN® for agricultural IoT?

2.4.1 Installing Inexpensive Outdoor Base Stations

I was involved mainly in base station design as part of the three-year paddy field water management IoT demonstration testing project, and based on my experience, the biggest issues are finding places to install base stations and obtaining a power supply.

The TLG7921M is a waterproof outdoor LoRaWAN® gateway with strong wireless performance, so a single unit can cover a wide area if installed in an elevated spot, such as a rooftop or mountain. But it is more expensive than indoor LoRaWAN® gateways, and the cost of installation, including wiring, is also high, so it is an expensive option unless installed on a decent scale (e.g., rolled out across an entire region).

Kiwi Technology's TLG3901BLV2 is a very cheap LoRaWAN® gateway included in the Mizukanri Pack S. It is an indoor device intended for installation in homes or offices of agricultural businesses, but offices and homes are often far from the paddy fields where the sensors are installed, and the data links can be unstable. Installing them in private homes with a power source near the fields would work, but

this is not all that realistic since users themselves would have to negotiate with property owners about how much to pay for the electricity used by the LoRaWAN® gateway and so forth.

2.4.2 Simple Pre-installation Data Link Tests

Even if you are able to install inexpensive base stations outdoors, you may need to relocate them or add additional units if you are unable to easily determine beforehand that they can link to devices without any issues.

Several companies offer commercial wireless simulators that let you enter base station latitude, longitude, and installation height to simulate data links with peripheral devices. We actually tried one of these, but while the simulator included topographical data, it did not include data on buildings and trees, so we were unable to determine the effect of such objects on data links. When we compared the results of the wireless simulator with real-world measurements taken in the vicinity of the paddy field water management IoT test site, the simulation tended to match the real world in places with few buildings, but even then, when testing close to a building, we found that small changes in device position can greatly affect data transfer success rates. Even if data on buildings and trees is incorporated into the simulator in the future, covering all buildings and trees is likely to be difficult, as is keeping the data up to date, so disparities between simulation and real-world testing seem inevitable. In the real-world tests, the data links were also sometimes unstable near busy roads. Assessing such time-based changes in data link status is also likely to be difficult in wireless simulators, even in the future.

So simulation-based pre-installation checks of connectivity do have their limitations, and you need to do real-world tests to say anything with certainty. However, there are limits to the extent to which we, or a contractor, can measure connectivity every time a base station or device is installed, and this would also be costly.

2.5 Solutions to the Issues

So far, we have explained that promoting the use of LoRaWAN® for agricultural IoT will be difficult unless we can achieve either of the following:

- Install inexpensive base stations outdoors
- Easily assess data link performance before installation

To solve these issues, our aim was to make the system as DIY-friendly as possible for agricultural businesses. I describe our solutions below.

2.5.1 DIY Solar-powered Base Stations to Expand Installation Options and Cut Installation Costs

If the TLG3901BLV2 indoor LoRaWAN® gateway included in Mizukanri Pack S could be waterproofed and made to run on a cheap solar panel and battery, obviating the need for a power supply, then it could be installed on the edge of paddy fields where it was previously not possible to do so and thereby provide stable data links. So we decided to make available a DIY solar-powered base station package that agricultural businesses can easily set up themselves, consisting of a cheap solar panel and battery and materials readily available online or at home centers. Agricultural business owners are used to DIY, with many building their own greenhouses for instance, and they often have a decent set of tools, so we believe they will be able to install the DIY solution themselves as long as we provide a clear set of instructions. Finding an installation spot along the side of a field should also be easy, and the cheap price means that the system can easily be restored if it is, say, damaged by natural events or stolen.

We expect the package we are putting together to provide a solar-powered base station that runs year round at an additional cost of about 70,000 yen on top of the TLG3901BLV2. To evaluate the package, we have already obtained materials and built a DIY solar-powered base station ourselves (Figure 5), and I blogged about the process. See my posts for more details[*2].

*2 IIJ Engineers Blog, "We set up a solar-powered LoRaWAN® base station for smart agriculture (Parts 1 & 2)" (https://eng-blog.iij.ad.jp/ archives/5567, in Japanese) (https://eng-blog.iij.ad.jp/archives/5599, in Japanese).

Four of us installed the first solar-powered base station, but we believe we need to make improvements as we develop the package so that two people or fewer can install it in a shorter amount of time. So we recently arranged to use a location relatively close to our workplace for a day, and undeterred by rain, ten of us tested out a number of installation patterns using various tools and materials. I hope to write the experience up in a blog post soon. And we look forward to launching a package that embodies what we learned.

2.5.2 Simple Data Link Tests via a Wireless Survey Tool

To enable agricultural businesses to easily measure data link performance themselves, we decided to develop a wireless survey tool, a device that measures data link performance. We started out with the following development requirements.

1. We will not create a smartphone testing app. The system will consist of only the TLG3901BLV2 and a wireless survey tool. Both will run on a mobile battery or dry-cell battery.
2. The measurement process will take 5 minutes and consist of 30 individual measurements taken at 10-second intervals.
3. The wireless survey tool will have an LCD screen to display measurements in real time.
4. The TLG3901BLV2 will be usable without a SIM.

We decided on Requirement 1 to make it easy to conduct testing anywhere. If we created a smartphone app, users would need to learn how to operate it, but some agricultural businesses are not all that familiar with smartphones. Mizukanri Pack S includes a smartphone app, so users need to acquaint themselves with its use once they decide to install the system, but we wanted to make the bar as low as possible in the initial pre-installation survey stage. Making the devices battery powered not only eliminated the need to be near a power source, it also made it possible to eschew a power button and have tests start automatically when the battery is connected.

Figure 5: DIY Solar-powered Base Station

Requirement 2 is in line with devices we have used for testing so far. Although the LoRaWAN® specification allows for shorter intervals, we selected our interval in light of potential interference in the case of multiple devices using the same 920MHz band being nearby as well as the potentially strong effect of environmental noise from, for example, moving vehicles.

We decided on 3 instead of a smartphone app. The wireless survey tool sends an ACK request via uplink to the Kiwi Technology LoRaWAN® gateway. If an ACK is returned, it is counted as a success; if no ACK is returned, this is a failure. Successes and failures are displayed as 0 and X on screen. Once the data link test is complete, the screen shows the number of successes over the total number of tries (Figure 6). Displaying the test results in real time was also a good idea because the user can disconnect the battery and stop the test if no data is being received at all.

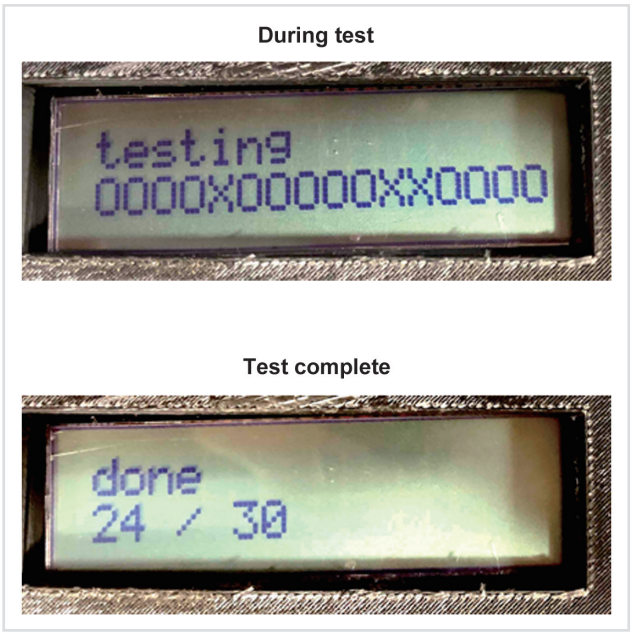

Figure 6: The Wireless Survey Tool's LCD Screen

Requirement 4 is there because otherwise, if we were to create several sets of the TLG3901BLV2 and wireless survey tool to lend out to people, we would need the same number of SIMs. As Figure 3 shows, LoRaWAN® systems normally need to connect to a network server in the cloud and thus need a mobile line accessed via a SIM or the like. Fortunately, Kiwi Technology LoRaWAN® gateways feature their own built-in network server. Figure 7 illustrates a LoRaWAN® system using the built-in network server.

The built-in network server enables the gateway alone to provide almost the same level of functionality as network servers usually available in the cloud. The gateway can store data received from devices in internal storage for a period, allowing for its retrieval externally at any time via a REST API. You can also request control of devices via the REST API. When an ACK is received from a device, you can return an ACK from the unit. This allows for bidirectional communication with devices even if the application server cannot be reached. The built-in server was originally intended to facilitate PoC in the absence of a network server contract, but we were also able to make effective use of this feature in the wireless survey tool.

Figure 8 shows the prototype wireless survey tool that we developed. We have actually already lent it to a number of people to use, and in addition to the expected outcome of users being able to perform a preliminary survey of wireless performance, some also expressed surprise at the system's range: "It picks it up from this far away?!" So the tool also

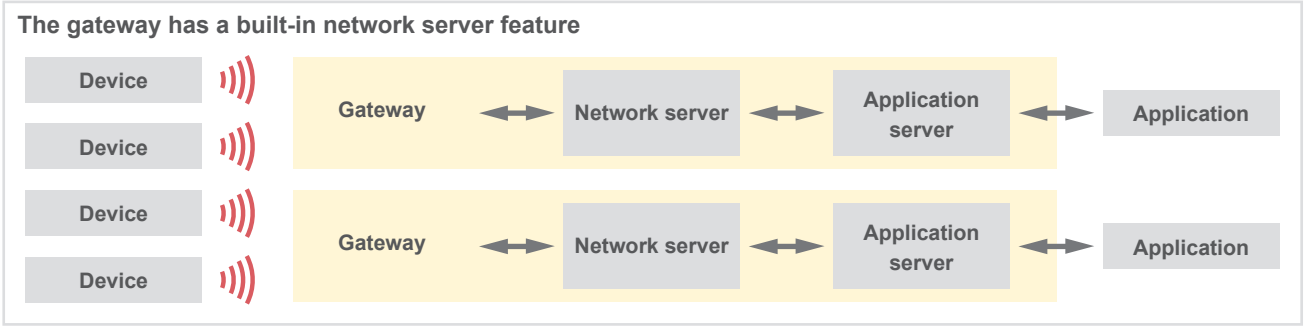

Figure 7: Overview of a LoRaWAN® System Using the Built-in Network Server

turns out to be an effective way for people to experience the long range LoRaWAN® offers before installing a system. It is also an effective way of collecting real-world test data from a whole range of locations, something we could not do alone, so we hope to continue utilizing the wireless survey tool while making additional improvements going forward.

2.6 Conclusion

We have discussed the features and suitable applications of LoRaWAN® compared with other LPWA wireless networks and the advantages of LoRaWAN® in agricultural IoT. We also looked at challenges to promoting the use of LoRaWAN® in agricultural IoT along with solutions.

However, solving the issues we discussed merely means we have done the minimum groundwork necessary to put Mizukanri Pack S on the market. If sales volumes rise, we will have to address issues including simplifying pre-shipment kitting and making it easy to diagnose the situation when problems arise after a product is shipped. To that end, IIJ is working with Kiwi Technology to extend the features of the LoRaWAN® gateway by adding SACM zero-config support, for instance.

SACM is a next-generation management system service for routers and IoT gateways, developed by IIJ based on SMF technology, which enables the automatic connection and centralized management of devices, and offered on an OEM basis. With zero-config support, a device will automatically connect to SACM when powered on, acquire its settings, and start running. This eliminates any need to operate a device directly. The user interface allows SACM administrators to centrally configure, monitor, and manage a large number of devices. See our Focused Research report in IIR Vol. 36 for details of SACM[*3].

The features we have developed for agricultural IoT and the sales and operating knowhow we have built will also be effective in deploying LoRaWAN® solutions for other applications. By continuing to develop this technology and build a knowledge base, IIJ aims to lower the bar to implementing LoRaWAN® and see it deployed in a range of different fields.

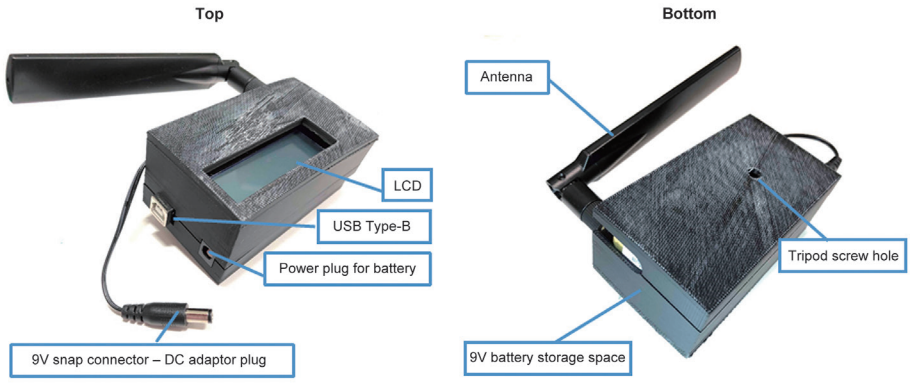

Figure 8: Wireless Survey Tool Prototype

Moto Onishi
Product Manager, New Business Promotion, IoT Business Division, IIJ
Mr. Onishi joined IIJ in June 2016. He handles project planning for IoT and camera solutions.

*3 Internet Infrastructure Review (IIR) Vol.36 (https://www.iij.ad.jp/en/dev/iir/036.html).

COVID-19's Impact on FLET'S Traffic

3.1 Introduction

The COVID-19 situation prompted the closure of Japan's schools nationwide from March, resulting in a sharp rise in people working remotely from home. The changes in many people's Internet usage patterns put a strain on individual services and communication links, and social media was filled with people observing this phenomenon and expressing dissatisfaction. Yet there is not much information out there on the macro situation. As such, we report on the impact on traffic on IIJ's FLET'S-based services as a bellwether of broadband services used mainly in the home.

COVID-19 began spreading in Japan in mid-February. Remote work was still experimental at that point, but in late February, companies like Dentsu and Shiseido embarked on large-scale remote work programs. Schools closed nationwide on March 2, and that same week, many companies initiated remote work, and as more and more people began staying in, there was a sudden paucity of faces on the streets. Trends in FLET'S traffic underwent a clear change from March 2. Later, on March 25, the Tokyo government began urging people to stay indoors. Japan declared a state of emergency covering seven prefectures on April 7, and this was expanded nationwide on April 16. These events greatly altered the societal landscape. Although the number of people staying at home has undoubtedly increased, we have not seen that large a change in FLET'S traffic volume.

3.2 About the Data

The traffic volume data is collected from the interface counters on routers that accommodate the fiber-optic and ADSL customers on IIJ's personal and enterprise broadband services. We use data collected via Sampled NetFlow to study the origin of traffic (sender organizations). Further details about the data are available in last year's Broadband Traffic Report[*1].

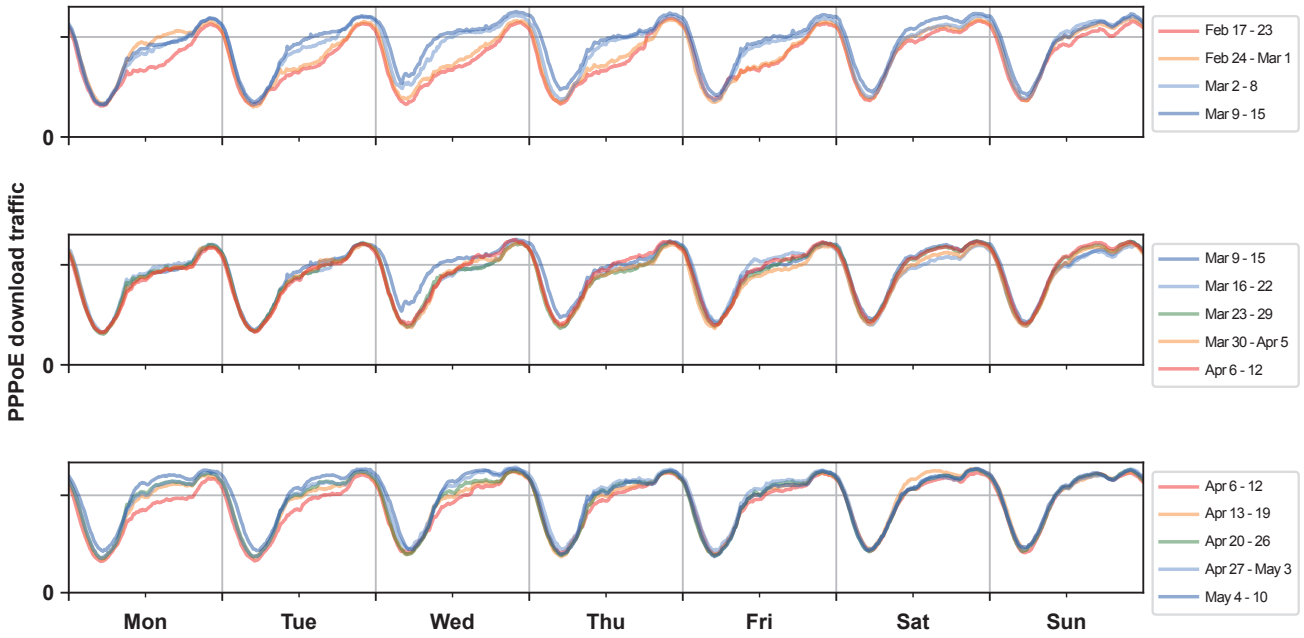

Figure 1: FLET's Traffic
Download: Feb 17 – Mar 15 (top), Mar 16 – Apr 12 (middle), Apr 13 – May 10 (bottom)

*1 Kenjiro Cho, Broadband Traffic Report: Moderate Growth in Traffic Volume Ongoing, Internet Infrastructure Review, Vol.44. pp4-9, November 2019.

3.3 Traffic Condition

IIJ's FLET'S services include IPv6 IPoE in addition to conventional PPPoE. IIJ's IPv6 IPoE service uses Internet Multifeed Co.'s transix service, and the traffic does not pass directly through IIJ's network. The volume of traffic here is currently around 20% of that on PPPoE. Congestion on network termination equipment has become a problem with PPPoE in the past few years, and an increasing number of ISPs are recently recommending the use of IPoE.

3.3.1 FLET'S Traffic (PPPoE)

Figures 1 and 2 overlay IIJ's total FLET'S traffic week by week. This is PPPoE traffic and does not include IPv6 IPoE. Figure 1 shows download and Figure 2 upload traffic.

The chart covers 12 weeks from the week of February 17, broken into three four-week subplots. The middle and bottom subplots contain five weeks of data as they include the final week from the previous subplot for comparison. The holidays in this period are February 24 (Mon), March 20 (Fri), April 29 (Wed), May 4 (Mon), May 5 (Tue), and May 6 (Wed), and the traffic patterns on these days do differ from other weekdays.

Downloads usually peak in the evening and fall off sharply after midnight, with the lowest point coming in the early morning. Daytime traffic is high on weekends/holidays. Upload traffic is almost an order of magnitude smaller than download traffic, and there are no clear peaks.

First, we look at download traffic in Figure 1. Comparing the two weeks represented by the red and orange series with those represented by the aqua and blue series (i.e., before and after March 2) in the top subplot shows that weekday download traffic increased after March 2. Volumes were still a bit lower than on ordinary weekends. The peak values

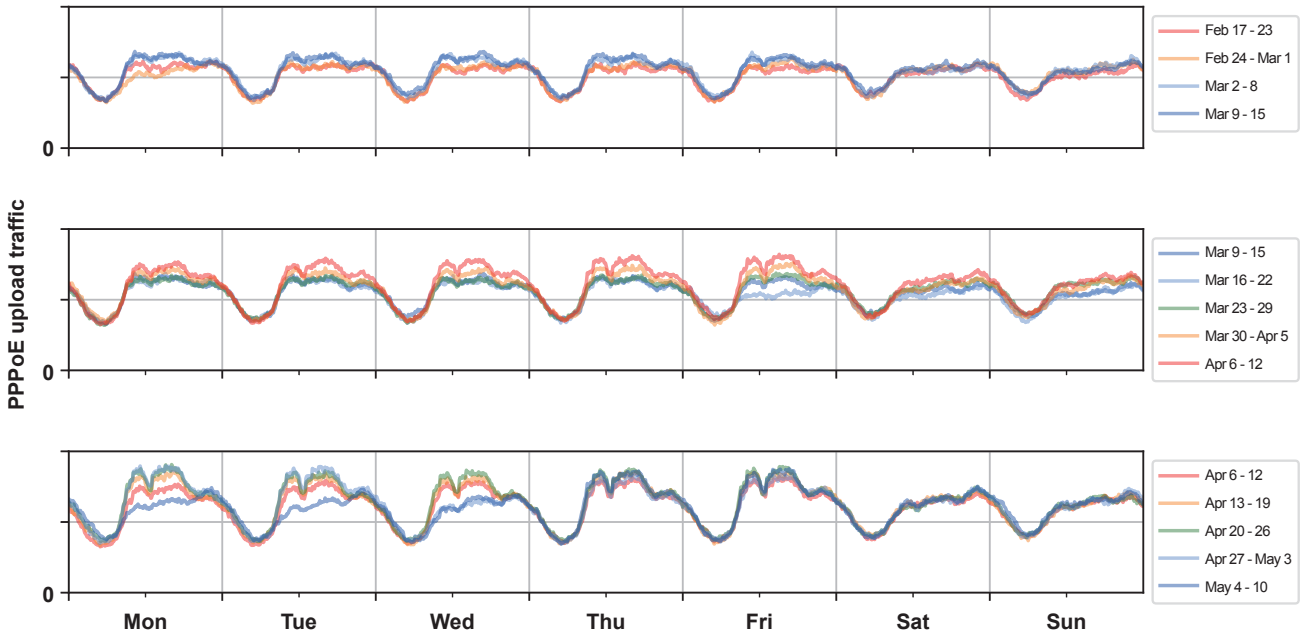

Figure 2: FLET's Traffic
Upload: Feb 17 – Mar 15 (top), Mar 16 – Apr 12 (middle), Apr 13 – May 10 (bottom)

also increased just slightly. Not much changes in the middle subplot, but the bottom subplot shows that weekday daytime traffic began increasing again in April. The increase in traffic from early in the morning on March 11 (Wed) is likely due to the release of the popular video game Call of Duty: Warzone. Microsoft released a monthly update on the same day, and this also probably contributed.

Next, we look at upload traffic in Figure 2. The top subplot shows that daytime traffic on weekdays rose slightly through mid-March, but the increase eased off in the evenings, so it is probably related to video conferencing and other remote work applications. The middle and bottom subplots show a progressive rise in weekday daytimes from April, likely a reflection of remote work arrangements gradually coming together. The dip around lunchtime is probably due to a lull in video conferencing. Through mid-March, upload traffic only increased on weekdays, but thereafter evening and weekend/holiday traffic also rose. We think this is probably due to an increase in video conferencing for private gatherings, like afterwork drinks, as people became accustomed to the tools. The upload peak value, however, is only about 1/7th the download peak value, so upload traffic certainly did not rise as much as download traffic.

To determine whether the increase in weekday daytime traffic was due to specific services, we also looked at Sampled NetFlow data. A comparison of the Tokyo area data for February 26 (Wed) and March 4 (Wed) shows an overall 1.19-fold increase in download volume. By sender

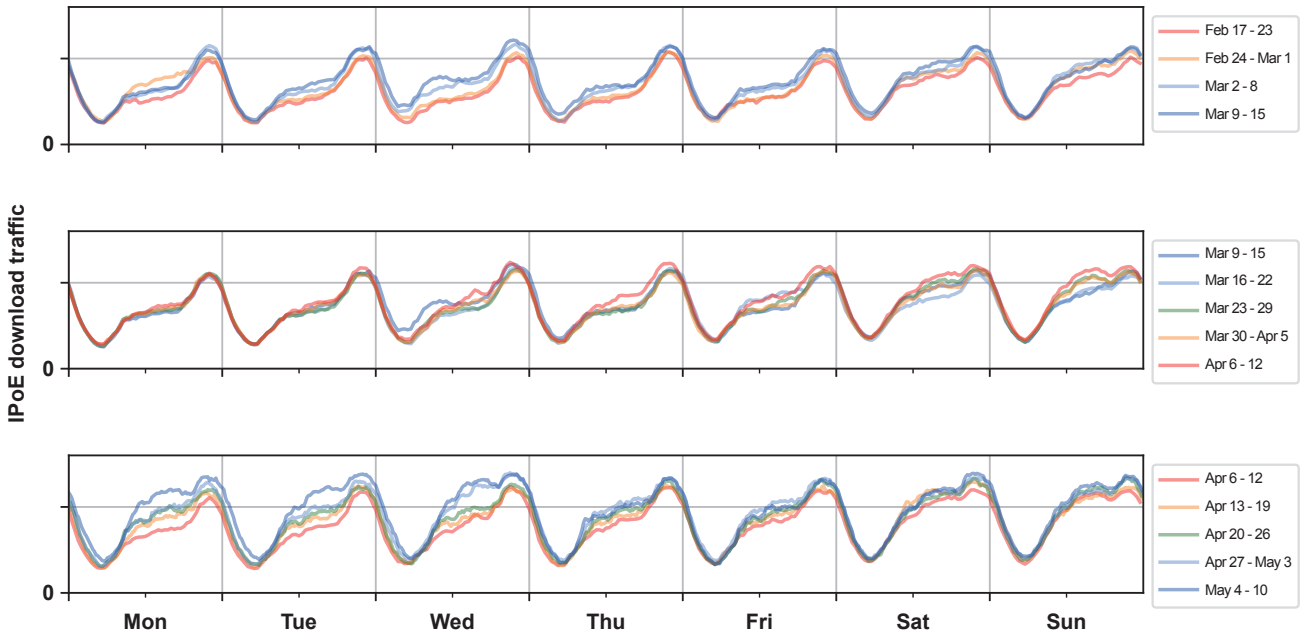

Figure 3: IPv6 IPoE traffic
Download: Feb 17 – Mar 15 (top), Mar 16 – Apr 12 (middle), Apr 13 – May 10 (bottom)

organization (AS), the data show a decent increase in the proportion of traffic from CDN operators, with the breakdown among major content providers remaining largely the same. Specifically, the figures were Google 1.16x, Amazon 1.16x, Netflix 1.17x, Facebook 1.10x, and Microsoft 1.23x. So this was overall growth that was roughly equivalent across different sources of popular content, with no particular service being a clear standout.

To examine the changes that followed, we now compare February 26 (Wed) and April 22 (Wed). Overall download volume was up 1.20 fold, only a slight increase over March 4, but the breakdown among major content providers shifted a little. Specifically, Google was unchanged at 1.16x, while Amazon had 1.63x, Apple 1.00x, Netflix 1.36x, Facebook 1.32x, and Microsoft 2.40x. This points to growth in full-length video content, such as movies, and content tied to business applications.

3.3.2 IPv6 IPoE Traffic

The reason PPPoE peak traffic is not rising could be that the FLET'S network is congested, so here we look at IPv6 IPoE, which should have ample capacity. Figures 3 and 4 plot IPv6 IPoE traffic volume. The download chart certainly shows the peaks rising, by a few percent in the top subplot, barely at all in the middle subplot, and then again by a few percent in the bottom subplot. And compared with PPPoE, weekday daytime traffic is lower relative to its peak. The increase in weekday daytime upload traffic is also smaller than for PPPoE.

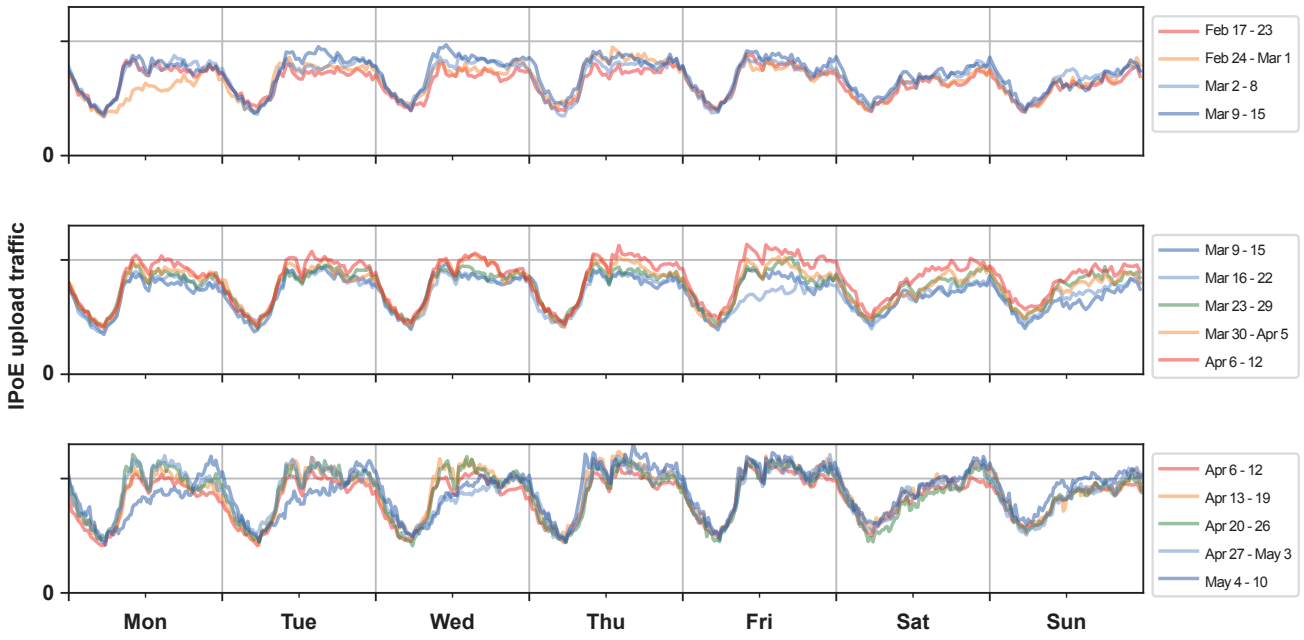

Figure 4: IPv6 IPoE traffic
Upload: Feb 17 – Mar 15 (top), Mar 16 – Apr 12 (middle), Apr 13 – May 10 (bottom)

3.4 Discussion

We were only able to take observations from IIJ services on this occasion, which tells us nothing about trends at other companies. In mid-April, however, NTT East[*2], NTT West[*3], and NTT Communications[*4] released data on FLET'S traffic volumes. Figure 5 plots the changes in weekday traffic based on IIJ's PPPoE data in the same manner as the graphs published by the NTT companies. The plot shows average download (DL) and upload (UL) traffic for the weeks of February 25 and April 20. It almost matches the observations of the NTT companies, so we think the same trends basically held for FLET'S-based broadband services. We also think the situation on non-FLET'S networks with sufficient available bandwidth is close to what we observe for our IPoE traffic.

From a macro view, weekday daytime traffic clearly increased after March 2. On weekdays, daily upload traffic was up about 6% and download traffic about 15%. A 15% increase in daily downloads is about the same as the difference between weekdays and weekends, but another way to look at it is that an increase that would normally take six months happened in a single day. But the peak values did not rise much, so from an ISP perspective, the former interpretation makes sense. The reason the peaks did not rise much may be due to capacity shortages on the FLET'S network's PPPoE network termination equipment. There may also be congestion at FLET'S network optical splitters or on consumer devices and wiring in apartment buildings. But such problems arise at the individual device level, so the peaks should be rising where there is ample capacity, but we did not observe any such differences over our observational range.

IPoE peak traffic is increasing, but IPoE traffic depends on the availability of content over IPv6, so the content breakdown differs from that for PPPoE and is not directly comparable. Also, the number of PPPoE contracts has hit a ceiling, whereas the ongoing shift to IPoE to avoid the congestion on PPPoE means that IPoE contract numbers are also growing. In overall terms, while the growth in IPoE download peak levels seems to indicate that PPPoE is running out of capacity, the potential room for an increase in PPPoE peaks is probably smaller than the amount by which IPoE has increased.

Some changes are apparent in March and April too. In March, it looks like overall Internet usage increased as the number of people at home during the daytime on weekdays increased. Then in April, it looks like traffic related to movie streaming and remote work increased as users got their systems set up properly and became accustomed to the tools. As a characteristic effect of remote work, the increase in weekday daytime upload traffic is probably due mainly to video conferencing. But the volume is not all that large through the latter half of March, likely because the number of people video conferencing from home was still limited. Working efficiently when remoting in requires not only a decent home network setup and equipment, including a PC, but also some level of experience. Companies

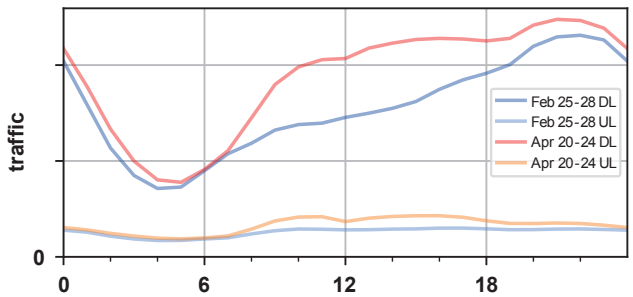

Figure 5: Average Weekday Traffic by Time of Day: February vs. April

*2 NTT East, "NTT East's efforts in response to COVID-19" (https://www.ntt-east.co.jp/aboutus/COVID-19.html#traffic, in Japanese).
*3 NTT West, "NTT West: Download traffic across all areas" (https://www.ntt.co.jp/topics/important/covid19_west.html, in Japanese).
*4 NTT Communications, "Internet traffic time series data" (https://www.ntt.com/about-us/covid-19/traffic/, in Japanese).

were apparently experiencing problems on their end, including a shortage of VPN licenses and bandwidth. And many people were probably not fully set up for video conferencing when initially trying it out. The breakdown in growth by operator shows a uniform rise in traffic from the major content providers in March, followed by growth for movie content providers and providers of remote work-related services in April.

It is also clear that traffic falls when the weather is good and rises when it is bad. People are thought to have relaxed and thus ventured out more amid favorable weather over the March 20–22 (Fri–Sun) long weekend, and as if to back this up, traffic was low over that period. Eastern Japan and the Tohoku region had stormy weather on April 18 (Sat), and traffic increased on this day. Traffic was also on the high side in Kanto on April 13 and 20, perhaps because these consecutive Mondays were both rainy.

Growth in broadband traffic was actually accelerating even before COVID-19 spread. Factors potentially behind this include households becoming better equipped to stream video as people replaced old PCs ahead of the Windows 7 end-of-life and Japan's consumption tax hike, the progressive introduction of remote work arrangements as part of work-style reforms and efforts to cope with the Olympics, and increasing interest in video streaming fueled by expectations for online streaming of the Olympics and TV broadcasts, 5G mobile services, and the like.

Video overwhelms other types of content in terms of sheer volume, however, so usage trends for non-video content are not really evident from the traffic observations because video streaming dominates download traffic and video conferencing dominates upload traffic. There are limits to what traffic alone can tell us about trends in Internet usage.

3.5 Conclusion

The spread of COVID-19 has fueled a rapid shift toward remote work. This has revealed problems with individual communication links and services, yet on a macro level, although weekday daytime traffic has increased, it has recently settled at levels within the bounds of existing capacity.

Remote work and remote education were rolled out on a huge scale from March. Until now, remote work had been an experimental affair carried out by a select few, but we are now finding out whether everyone can do it at once. And although the quality of Internet-based video conferencing, remote classes, video streaming, and the like is currently sufficient when only some people are engaged, it will take years to build systems that can cope with large numbers of people all at once. Present circumstances have made clear that society as a whole depends on online systems when push comes to shove. Our hope is that this will provide a strong impetus for reaffirming the importance of developing Internet infrastructure.

Kenjiro Cho
Research Director, Research Laboratory, IIJ Innovation Institute Inc.

July 2020 Vol.47

IIJ
Internet Initiative Japan

About Internet Initiative Japan Inc. (IIJ)

IIJ was established in 1992, mainly by a group of engineers who had been involved in research and development activities related to the Internet, under the concept of promoting the widespread use of the Internet in Japan.
IIJ currently operates one of the largest Internet backbones in Japan, manages Internet infrastructures, and provides comprehensive high-quality system environments (including Internet access, systems integration, and outsourcing services, etc.) to high-end business users including the government and other public offices and financial institutions.
In addition, IIJ actively shares knowledge accumulated through service development and Internet backbone operation, and is making efforts to expand the Internet used as a social infrastructure.

IIJ-MKTG020-0045

Internet Initiative Japan Inc.

Address: Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku,
Tokyo 102-0071, Japan
Email: info@iij.ad.jp URL: https://www.iij.ad.jp/en/