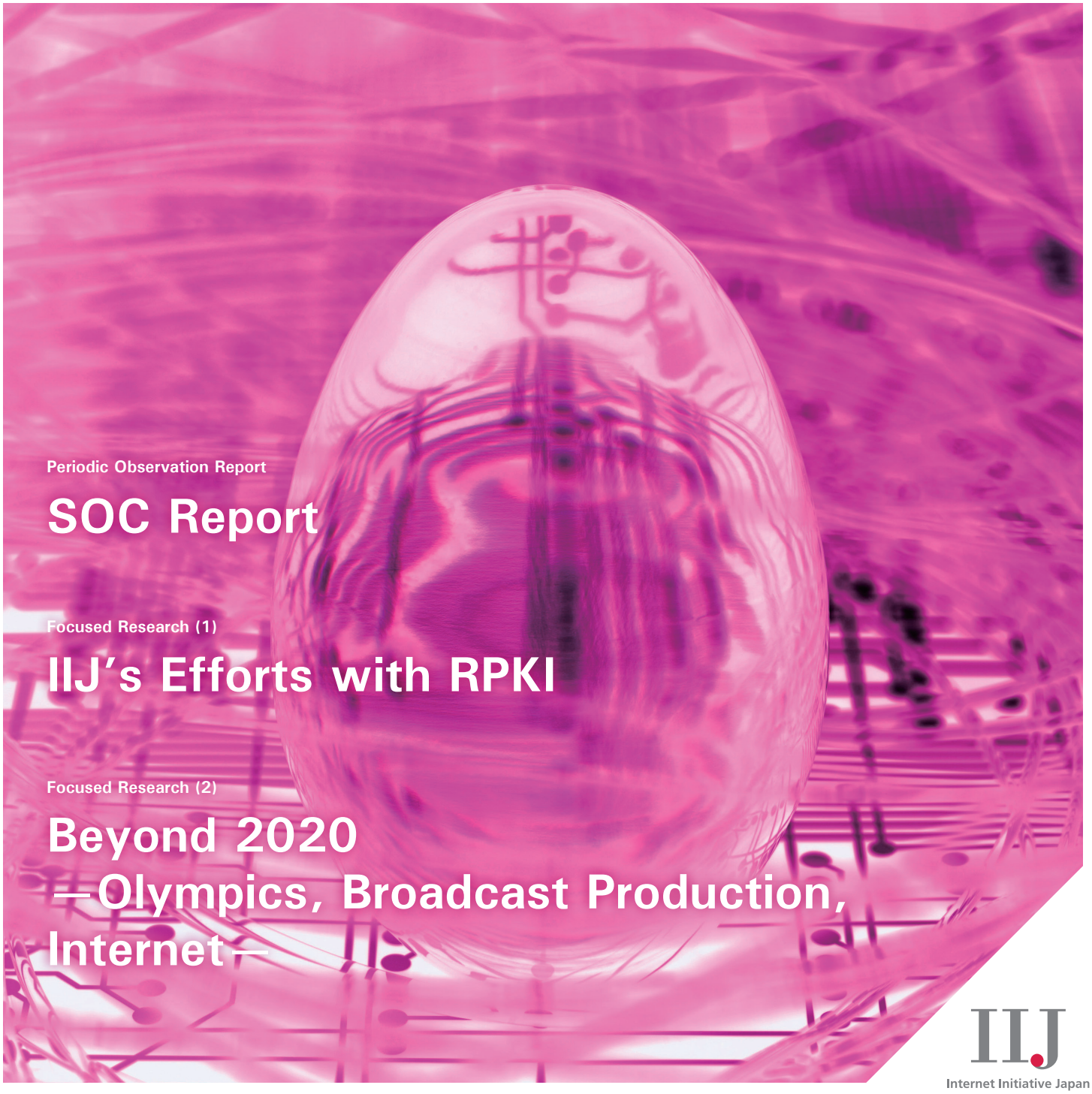
IIR

Internet
Infrastructure
Review

May 2021
Vol. 50



Periodic Observation Report

SOC Report

Focused Research (1)

IIJ's Efforts with RPKI

Focused Research (2)

Beyond 2020
—Olympics, Broadcast Production, Internet—

IIJ
Internet Initiative Japan

Internet Infrastructure Review

May 2021 Vol.50

Executive Summary ····· 3

1. Periodic Observation Report ····· 4
1.1 Introduction ····· 4
1.2 2020 Security Summary ····· 4
1.2.1 Incident Calendar ····· 4
1.2.2 Observational Data from IIJ Managed Security Services ····· 7
1.3 Security Topics ····· 9
1.3.1 SSL-VPN Product Vulnerabilities ····· 9
1.3.2 Observations on Emotet and IcedID ····· 10
1.4 Conclusion ····· 13

2. Focused Research (1) ····· 14
2.1 What is Route Hijacking? ····· 14
2.2 Overview of RPKI ····· 14
2.3 Current State of RPKI ····· 15
2.4 IIJ's Efforts ····· 18
2.5 Looking Aheadn ····· 19

3. Focused Research (2) ····· 20
3.1 Introduction ····· 20
3.2 The Olympics, Paralympics, and Broadcast Productions ····· 20
3.3 Path and Barriers to Remote Production ····· 21
3.4 The Important Relationship Between Remote Work and Networking
—A Test Using VidMeet Online ····· 22
3.5 Network Headed for the Cloud ····· 26
3.6 The Great Potential of Cloud Technology and Software ····· 27
3.7 Possibility of Providing Clocks via the Network ····· 28
3.8 What VidMeet Online Revealed...2021 and Beyond ····· 31

Executive Summary

While some countries have started vaccinating against COVID-19, variants of the virus are also now being detected, and some regions remain under heavy lockdown. The situation remains unpredictable in Japan too, with a sharp rise in case numbers seen toward the end of 2020 and a second state of emergency declared at the beginning of 2021.

While COVID-19 restricts people's activities worldwide, every day we are reminded of how information and communications technology (ICT), most prominently the Internet, supports our lives as members of society. People restricted from going out have turned to video content for entertainment, resulting in a substantial increase in Internet traffic, as previously discussed in the IIR. Companies have of course introduced remote work and people are increasingly working online. Many people have also probably noticed an increase in food delivery services—most of the orders are placed via the Internet, with payments also being made online. We also hear that online shopping transaction volumes are rising. Yet all of these services already existed, so it may also be worth asking whether they are providing any new sensations or experiences to users, or whether COVID-19 simply provided an impetus for society-wide uptake.

With vaccinations finally set to start in Japan too, we are now in a position to look toward the post-COVID world. The world faces a great many issues quite aside from COVID-19, and issues common to all have also been identified in the form of SDGs. As part of the information and communications industry, we will be looking at how these major issues for society might be solved and how ICT and the Internet can contribute in this regard.

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 presents our SOC Report, our periodic observation report for this edition. IIJ's SOC analyzes data obtained through the operation of IIJ's services, data that it collects independently, and data from external sources. Since 2017, we have published information on threats we have observed and a range of security topics through wizSafe Security Signal, and in this report we review trends in security incidents in 2020. The report looks at security incidents IIJ's SOC has been focusing on, including attacks targeting vulnerabilities in SSL-VPN products and attacks involving Emotet and IcedID.

The focused research report in Chapter 2 explains RPKI (Resource Public-Key Infrastructure). Even today, with the Internet now serving as part of our global social infrastructure, the Internet's routing system is not impervious to route hijacking and operator configuration errors. RPKI is a mechanism for bolstering this system by using digital certificates to validate routing and other information exchanged on the Internet. The report gives an overview of RPKI, discusses developments in this area, and describes IIJ's own efforts.

The focused research report in Chapter 3 discusses the use of networks in broadcast production. The year 2020 initially brought with it expectations of a huge event in the form of the Olympics, and it was also a year of advances in remote work at many places of employment. The report looks at frameworks for remote production that use IP networks suitable for broadcasting events like the Olympics, and discusses validation tests of an Internet-based remote work setup in a broadcast production setting, with some words about future prospects.

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.

SOC Report

1.1 Introduction

IIJ launched the wizSafe security brand in 2016 and works constantly to create a world in which its customers can use the Internet safely. Four years have now passed since we launched wizSafe, and at our SOC, we have been constantly reworking our systems with a view to incident response capabilities and to optimize our operations. The SOC had so far focused on creating frameworks for detecting threats using the Data Analytics Platform[*1], and we have now shifted direction toward actually using the information obtained through the Data Analytics Platform. This has enabled us to step up threat detection and the use of the information we report.

Since 2017, the SOC has reported via the wizSafe Security Signal[*2] site on threats observed via the Data Analytics Platform, which collates logs from IIJ services, and on a variety of security topics. Most events and conferences in 2020 were held remotely, and the SOC also shared its knowledge and insight by presenting remotely at IIJ Technical NIGHT and the Japan Security Analyst Conference (JSAC) 2021[*3].

IIJ Technical NIGHT is a seminar aimed at engineers, and three members of the SOC, each with different areas of expertise, presented on their activities to a large number of attendees[*4,5]. At JSAC 2021, we presented on our efforts in 2020 to proactively collect threat information on attack campaigns targeting cryptocurrency operators[*6].

In this report, we summarize our SOC's observations in the hopes they will provide useful insights to our readers. Section 1.2 looks at security topics that rose to prominence in Japan in 2020 along with security service statistics for the year. Section 1.3 discusses topics our SOC analysts focused on.

1.2 2020 Security Summary

Here, we look at prominent security incidents in 2020 along with information on attacks observed by the SOC.

1.2.1 Incident Calendar

Tables 1 and 2 summarize the major security incidents that our SOC focused on in 2020.

*1 Internet Infrastructure Review (IIR) Vol. 38 (https://www.iij.ad.jp/en/dev/iir/038.html).
*2 wizSafe Security Signal (https://wizsafe.iij.ad.jp/, in Japanese).
*3 Japan Security Analyst Conference 2021 (https://jsac.jpcert.or.jp/en/index.html).
*4 Presentation materials: IIJ Technical NIGHT Vol. 9 (https://eng-blog.iij.ad.jp/archives/6453, in Japanese).
*5 COVID-19 IT study session, 2 realizations from the switch from physical to online (https://eng-blog.iij.ad.jp/archives/7141).
*6 JPCERT/CC, "Hunting threat information on attack campaigns targeting cryptocurrency operators" (https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_302_kodera_jp.pdf).

Table 1: Incident calendar (January–June)

Month	Summary/URL(s)
January	**It was announced that a breach of personal/confidential information may have occurred because of unauthorized system access that exploited vulnerabilities in an electronics manufacturer's antivirus system for which security patches had not yet been released.** (Mitsubishi Electric) "Possible breach of personal information and corporate secrets due to unauthorized system access" https://www.mitsubishielectric.co.jp/news/2020/0120-b.pdf (in Japanese) "Possible breach of personal information and corporate secrets due to unauthorized system access (2nd report)" https://www.mitsubishielectric.co.jp/news/2020/0210-b.pdf (in Japanese) "Possible breach of personal information and corporate secrets due to unauthorized system access (3rd report)" https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf (in Japanese)
January	**A major electronics manufacturer announced that due to unauthorized access to some servers used by its defence business division, files shared between its internal departments had been accessed.** (NEC) "Unauthorized access of NEC's internal servers" https://jpn.nec.com/press/202001/20200131_01.html (in Japanese)
March	**Microsoft announced that the SMBv3 protocol contains a vulnerability that could allow an unauthenticated attacker to execute arbitrary code on an SMB server or client.** (Microsoft) "Microsoft Guidance for Disabling SMBv3 Compression" https://portal.msrc.microsoft.com/en-JP/security-guidance/advisory/adv200005 "Windows SMBv3 Client/Server Remote Code Execution Vulnerability" https://portal.msrc.microsoft.com/en-JP/security-guidance/advisory/CVE-2020-0796
March	**Trend Micro announced that several of its products had critical vulnerabilities and that it had observed attempts against at least one of these vulnerabilities in the wild.** (Trend Micro) "Security Bulletin: Multiple Critical Vulnerabilities in Trend Micro Apex One and OfficeScan" https://success.trendmicro.com/solution/000245571
April	**An education platform company announced there had been unauthorized access to a service it operates, and that around 1.22 million records, including service IDs and encrypted passwords, may have been viewed.** (Classi) "Investigation report on temporary service outage and password change request" https://corp.classi.jp/news/1926/ (in Japanese)
April	**A video game company announced that around 160,000 accounts may have been compromised due to an unauthorized third party logging into accounts on the network service the company provides.** (Nintendo) "Unauthorized logins using Nintendo Network IDs and advisory on the safe use of your Nintendo account" https://www.nintendo.co.jp/support/information/2020/0424.html (in Japanese)
April	**A vulnerability was revealed in Microsoft Teams that could allow an account to be taken over by an attacker who causes a user to view a GIF file or link on a subdomain controlled by the attacker.** (CyberArk) "Beware of the GIF: Account Takeover Vulnerability in Microsoft Teams" https://www.cyberark.com/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams/
May	**A telecommunications carrier announced that an intrusion into an overseas-based server running its services facilitated unauthorized access to one of its servers in Japan, possibly resulting in the breach of service-related construction information pertaining to 621 corporate clients.** (NTT Communications) "NTT Com confirms possible information leak due to unauthorized access" https://www.ntt.com/en/about-us/press-releases/news/article/2020/0702.html
June	**A foreign security company announced a set of 19 vulnerabilities, collectively called Ripple20, found in products with the TCP/IP stack developed by Treck for embedded devices. Ripple20 includes vulnerabilities that allow the execution of remote code.** (JSOF) "Overview- Ripple20" https://www.jsof-tech.com/ripple20

Table 2: Incident calendar (July–December)

Month	Summary/URL(s)
July	**Our SOC confirmed that the distribution of emails designed to spread the malware Emotet had resumed after not having been observed since February. The attacks methods had become more sophisticated and included, for example, the use of emails and other information stolen from infected devices in subsequent attacks as well as password-protected ZIP files. These attacks were observed up until October.**
August	**It was reported that attackers had exploited a vulnerability in a VPN product for which an update had been released in 2019, resulting in usernames, passwords, and other information used on some 900 servers being published on a hacking forum and thus made available to third parties. It was subsequently reported in the Japanese media that the leaked information included information on several Japanese companies.** (Nikkei xTECH) "Unpatched Pulse Secure VPN exposes IP addresses of 46 Japanese companies" https://xtech.nikkei.com/atcl/nxt/news/18/08605/ (in Japanese)
September	**A provider of e-money services announced that money had been illegally withdrawn owing to unauthorized use of its e-money service by a third party at a partnering financial institution. A string of similar announcements subsequently emerged from other e-money service providers and their partnering financial institutions.** (NTT Docomo) "Unauthorized use of Docomo accounts using information on accounts at some banks" https://www.nttdocomo.co.jp/info/notice/page/200908_02_m.html (in Japanese)
September	**JPCERT/CC announced that several organizations in Japan had confirmed they had received extortionary demands for cryptocurrency under threat of DDoS attacks or that they had been impacted by DDoS attacks.** (JPCERT/CC) "Extortion attempts (DDOs threats) demanding transfer of cryptocurrency under threat of DDoS attack" https://www.jpcert.or.jp/newsflash/2020090701.html (in Japanese)
September	**A foreign security company released a report on a privilege escalation vulnerability (CVE-2020-1472) in Netlogon used in Active Directory. This vulnerability was dubbed Zerologon. It is relatively easy to exploit, and tools available to attackers also implement the ability to exploit this vulnerability. When exploited, the domain admin account password can be changed and domain admin privileges can be obtained.** (Secura) "Zerologon: Instantly Become Domain Admin by Subverting Netlogon Cryptography (CVE-2020-1472)" https://www.secura.com/blog/zero-logon
October	**The Ministry of Internal Affairs and Communications and the Council of Anti-Phishing Japan released alerts to say that emails and phishing websites purporting to offer the government's Special Cash Payments had been seen.** (Ministry of Internal Affairs and Communications) "Alert on emails purporting to offer Special Cash Payments" https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000438.html (in Japanese) (Council of Anti-Phishing Japan) "Phishing posing as notifications regarding Special Cash Payments (Oct 15, 2020)" https://www.antiphishing.jp/news/alert/kyufukin_20201015.html (in Japanese) "Update: Phishing posing as notifications regarding Special Cash Payments (Oct 19, 2020)" https://www.antiphishing.jp/news/alert/kyufukin_20201019.html (in Japanese)
November	**A video game developer announced it had been the victim of a customized ransomware attack following unauthorized access to its network by a group of attackers calling itself Ragnar Locker. As of January 2021, up to 390,000 information records had been compromised, it said, including personal information of customers, employees, and other related individuals (investigation ongoing as of this writing).** (Capcom) "Notice Regarding Network Issues due to Unauthorized Access" https://www.capcom.co.jp/ir/english/news/html/e201104.html "Update Regarding Data Security Incident Due to Unauthorized Access" https://www.capcom.co.jp/ir/english/news/html/e201116.html "3rd Update Regarding Data Security Incident Due to Unauthorized Access" https://www.capcom.co.jp/ir/english/news/html/e210112.html
November	**Our SOC observed IcedID malware infections, and these observations persisted until early December.**
November	**An operator of an event/communications management service announced that the service it operates had been the victim of unauthorized access, resulting in the theft of up to 6.77 million customer information records, including personal information. Subsequently, many organizations that had been using the service issued alerts on this incident.** (Peatix) "Apology and notification of unauthorized access of our Peatix (https://peatix.com/) service" https://announcement.peatix.com/ 20201117_ja.pdf (in Japanese) "Report of third-party investigation into unauthorized access of our Peatix (https://peatix.com/) service and our response going forward" https://announcement.peatix.com/20201216_ja.pdf (in Japanese)
December	**A power generation systems company announced it had been the victim of unauthorized access by a third party via a managed service provider (MSP), resulting in servers and PCs being infected. It also noted that the root cause was a vulnerability in software provided by the MSP but that the vulnerability was undisclosed and a patch or other countermeasures had not been made available.** (Mitsubishi Power) "Unauthorized access of our network by a third party via a managed service provider" https://power.mhi.com/jp/news/20201211.html (in Japanese)

1.2.2 Observational Data from IIJ Managed Security Services

This section looks at the SOC's observations using the Data Analytics Platform in 2020.

■ DDoS Attacks

Here, we look at DDoS attacks detected by the IIJ DDoS Protection Service.

The methods used in DDoS attacks in 2020 were largely unchanged from previous years. So existing countermeasures are likely still effective as well. Table 3 summarizes attacks detected in each month of 2020.

The largest-scale attacks in each month were all Amplification attacks using UDP as the transport protocol. Commonly used application protocols included DNS, NTP, and LDAP, and a series of attacks using multiple protocols was also observed. And aside from UDP Amplification attacks, SYN flood attacks were also observed among the longest-duration attacks in each month.

■ Attacks Detected by IPS/IDS Devices

Here, we look at attacks detected by IIJ Managed IPS/IDS Service devices.

We observed attacks that infect IoT (Internet of Things) devices with malware throughout 2020. Attackers have been specifically targeting IoT devices in recent years in a trend that is ongoing. IoT devices are increasing rapidly in number, yet some devices continue to operate with known vulnerabilities exposed because of a lack of proper patch management. Attackers exploit such vulnerabilities to infect devices with malware, allowing them to control the devices remotely. IoT devices seized by an attacker are at risk of being exploited to launch other attacks, such as DDoS attacks. Many types of malware that infects IoT devices (IoT malware) have been identified, and the range of vulnerabilities exploited to infect devices is broad. The most commonly detected attacks in 2020 were those exploiting vulnerabilities in Netis/Netcore routers. Many of these attacks were intended to infect the routers with a variant of Gafgyt, a type of IoT malware.

Table 3: Summary of Observational Data on DDoS in 2020

Month	No. of incidents (daily avg.)	Approx. max. no. of packets per sec.(x10,000)	Maximum traffic		Maximum attack duration	
			Bandwidth (Gbps)	Method	Duration (h:mm)	Method
1	14.45	~25	2.19	SNMP Amplification	0:16	NTP Amplification
2	13.07	~1114	29.02	SSDP Amplification	1:50	SYN Flood
3	16.41	~999	90.86	DNS & NTP Amplification	0:51	Amplification of DNS, NTP, LDAP, etc.
4	24.63	~184	19.17	DNS Amplification	0:19	Amplification of DNS, NTP, LDAP, etc.
5	15.06	~296	32.11	NTP & LDAP Amplification	0:22	NTP Amplification
6	23.33	~824	21.42	SSDP Amplification	1:19	SSDP Amplification
7	11.84	~93	3.34	NTP Amplification	0:29	NTP Amplification
8	11.29	~743	58.90	DNS & Apple Remote Management Service Amplification	2:43	DNS & Apple Remote Service Amplification
9	12.73	~114	11.21	DNS & LDAP Amplification	0:23	LDAP Amplification
10	18.45	~78	7.54	DNS & LDAP Amplification	0:15	DNS Amplification
11	17.00	~434	43.23	DNS Amplification	3:11	DNS Amplification
12	17.39	~532	56.56	DNS Amplification	0:32	SYN Flood

Observations showed a lot of infections for IoT malware called XTC in April and Mozi in September. The XTC infections observed in April exploited multiple vulnerabilities (CVE-2020-9054, CVE- 2020-5722, CVE-2020-8515)[*7].

Malware Detected with Accessing the Web

We now take a look at malware detected when accessing the web using the IIJ Secure Web Gateway Service.

We observed malicious JavaScript throughout the year in 2020. In many cases, legitimate websites had been modified, with malicious JavaScript being injected. Observations confirmed that visiting such websites results in cookies, device information, and the like being sent to external sites, and the browser being redirected to other sites including fake prize sites and advertisements.

We also detected a lot of traffic related to Emotet. We take a detailed look at Emotet in Section 1.3.2.

Malware Detected When Receiving Emails

Here, we look at malware detected when emails were received on the IIJ Secure MX Service. In 2020, we observed cases of attackers using emails cleverly crafted to be relevant to current events in a bid to dupe users into malware infections.

First, we look at samples of emails that use attention-grabbing words in the subject line etc. From around March, for example, we detected an increase in malware-laden English-language emails purporting to provide information on COVID-19. Similarly, we observed an increase in Japanese-language emails using terms like “work at home”, “cold & flu”, and “bonus”.

Next, we look at examples in which attackers may have deliberately timed malware emails. Figure 1 shows the hour-by-hour count of emails in which a signature indicating a suspicious Microsoft Office document was detected in September 2020. The vertical axis is normalized by setting the total number of such signatures detected over the sample period to 100%. It is evident from the graph that the emails tend to be sent during standard working hours for companies in Japan. Several factors may be behind this, one being that attackers may have deliberately selected what time to send their emails out.

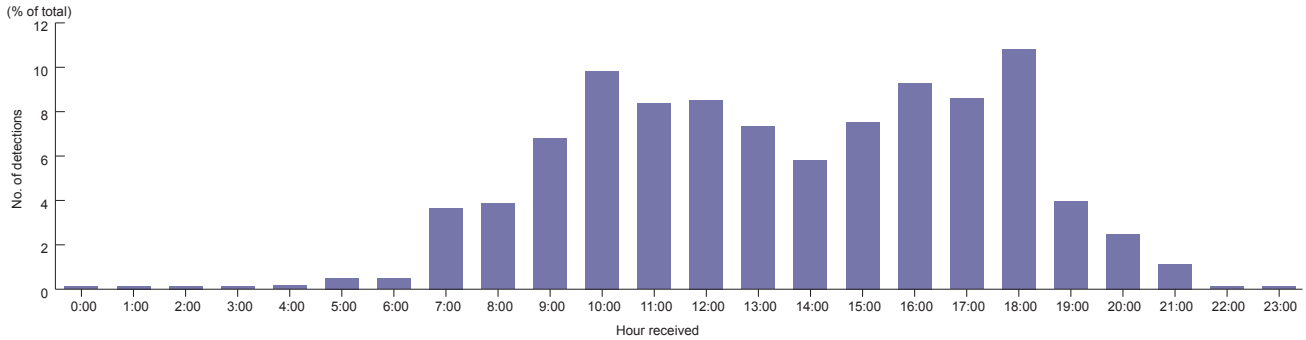


Figure 1: No. of Emails Containing Suspicious Microsoft Office Documents Received each Hour (Sep. 2020)

*7 Observations of infections with Mirai variant (https://wizsafe.iij.ad.jp/2020/05/967/, in Japanese).

1.3 Security Topics

This section looks at key topics our analysts focused on from among attacks detected by the SOC in 2020.

1.3.1 SSL-VPN Product Vulnerabilities

Virtual private networks (VPNs) are used to connect to internal systems from outside of an organization via the Internet and the like. COVID-19 sparked rapid changes in the way we work in 2020, prompting more and more companies to roll out VPNs to facilitate working from home, so it seems that a lot of VPNs are now being used in this way. Since they provide a means of accessing internal systems from outside of an organization, VPNs necessitate even greater diligence in addressing vulnerabilities. Indeed, 2020 saw cases of VPN product vulnerabilities being exploited and leading to data breaches. VPNs can use SSL/TLS to encrypt communications, and several vulnerabilities in products that use this method were revealed in 2019[*8,9]. In 2020, we observed attacks targeting these products with the 2019 vulnerabilities not properly fixed[*10,11].

Our SOC observed traffic involved in attacks targeting SSL-VPN vulnerabilities in Fortinet's FortiOS (CVE-2018-13379) and in Citrix Systems' Citrix Application Delivery Controller and Citrix Gateway (CVE-2019-19781).

■ Observations of Attacks Targeting a Vulnerability in Fortinet's FortiOS (CVE-2018-13379)

Figure 2 graphs the proportion of traffic targeting CVE-2018-13379 as detected on the IIJ Managed IPS/IDS Service. The vertical axis is normalized by setting the total number of such signatures detected over the sample period to 100%.

Exploiting this SSL-VPN vulnerability in Fortinet's FortiOS may allow an attacker to remotely read an arbitrary file on the product without authentication. We observed high levels of this traffic on November 4 and December 11 in particular, respectively accounting for 10.27% and 10.83% of the total. Traffic targeting this vulnerability tended to rise toward the end of the year, with the December detection count making up 37.93% of the total. In November, a list of hosts affected by the vulnerability was published on the Internet[*12]. Although this may have been a factor in the rise in detections in December, we did not find any clear evidence of a relationship here.

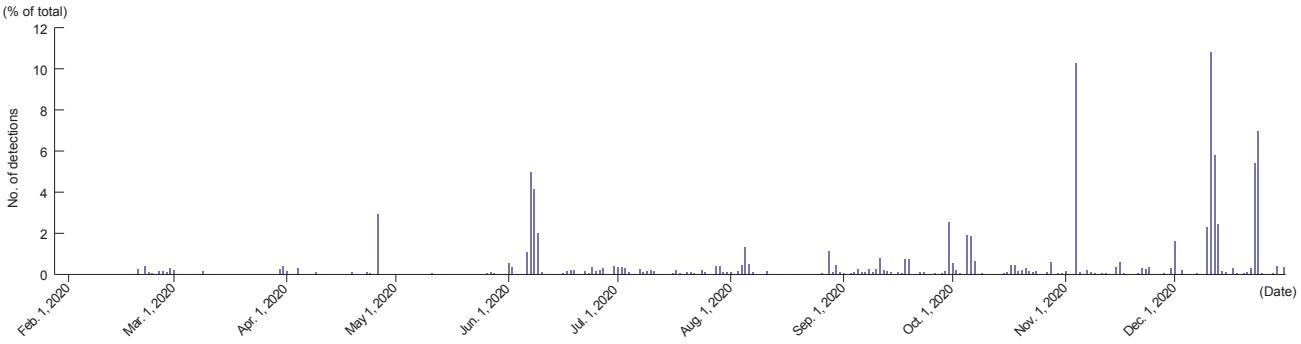


Figure 2: CVE-2018-13379 Detections (Feb.–Dec. 2020)

*8 JPCERT/CC, "Alert Regarding Vulnerabilities in Multiple SSL VPN Products" (https://www.jpcert.or.jp/at/2019/at190033.html, in Japanese).
*9 JPCERT/CC, "Alert Regarding Vulnerability (CVE-2019-19781) in Citrix Products" (https://www.jpcert.or.jp/at/2020/at200003.html, in Japanese).
*10 Bad Packets, "Over 14,500 Pulse Secure VPN Endpoints Vulnerable to CVE-2019-11510" (https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/).
*11 Bad Packets, "Over 25,000 Citrix (NetScaler) Endpoints Vulnerable to CVE-2019-19781 (https://badpackets.net/over-25000-citrix-netscaler-endpoints-vulnerable-to-cve-2019-19781/).
*12 JPCERT/CC, "About the disclosure of information regarding hosts affected by vulnerability (CVE-2018-13379) in Fortinet's FortiOS SSL VPN feature" (https://www.jpcert.or.jp/newsflash/2020112701.html, in Japanese).

■ Observations of Attacks Targeting a Vulnerability in Citrix Application Delivery Controller and Citrix Gateway (CVE-2019-19781)

Figure 3 graphs the proportion of traffic targeting CVE-2019-19781 as detected on the IIJ Managed IPS/IDS Service. The vertical axis is normalized by setting the total number of such signatures detected over the sample period to 100%.

Exploiting this vulnerability in Citrix Systems' Citrix Application Delivery Controller and Citrix Gateway may allow an attacker to remotely execute arbitrary code without authentication. We observed high levels of this traffic on February 18 and March 13 in particular, respectively accounting for 13.23% and 10.36% of the total. The number of detections tended to decline from March onward, but we observed traffic targeting this vulnerability intermittently right up until December. Given the rise in detections at points in November and December, this activity will also bear close watching ahead.

■ Countermeasures

The vulnerabilities CVE-2018-13379 and CVE-2019-19781 were disclosed in 2019, but we observed attacks on them throughout 2020. If you are using an affected version of these products, you need to address this by updating to a fixed version of the software. We also recommend staying abreast of information on vulnerabilities in products used within your organization and not just VPN products.

1.3.2 Observations on Emotet and IcedID

This section looks at the Emotet and IcedID malware, which featured prominently in 2020. First, we describe the characteristics of Emotet and summarize observations related to Emotet detections on the IIJ Security MX Service and IIJ Secure Web Gateway Service. We then look at IcedID's characteristics and summarize observations related to its detection on the IIJ Security MX Service and IIJ Secure Web Gateway Service.

■ Emotet Observations

Attacks that spread malware via emails occur every day. Most prominent among these are attacks that spread Emotet, and they were rampant in 2020. Emotot originally started out as a type of malware called a banking Trojan, designed to steal financial information and the like, but it has morphed as new functionality has been added to it. Specifically, it has gained the ability to spread itself, botnet functionality, and loader functionality that lets it distribute other malware. The self-spreading functionality steals data from infected computers such as email addresses, account information, and email text and attachments, and sends this to a C&C server. Also, based on the information it steals, Emotet sends forged emails to the original email senders, inducing them to open attachments. These characteristics make Emotet a powerful type of malware. Known methods by which Emotet spreads are emails with doc file attachments, and URLs in email text and document files that cause

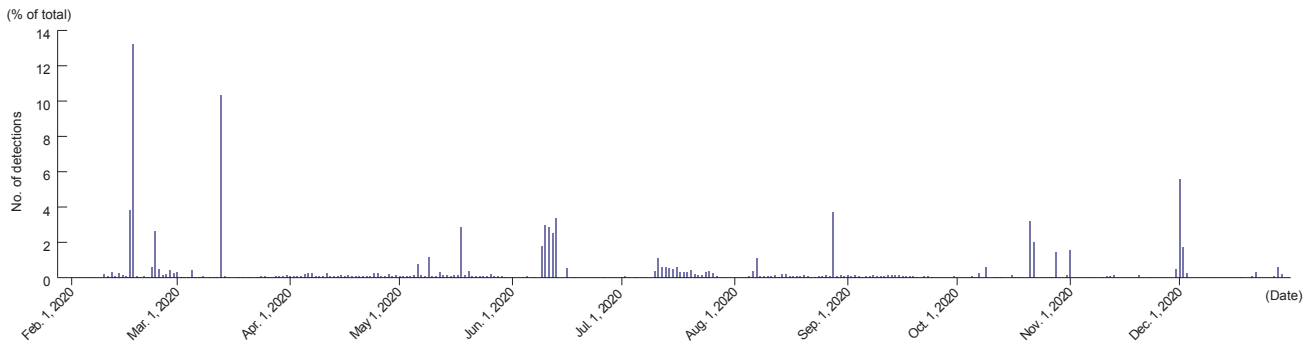


Figure 3: CVE-2019-19781 Detections (Feb.–Dec. 2020)

doc files to be downloaded. This is now joined by a new method observed in September whereby Emotet sends a doc file in a password-protected ZIP archive[*13]. Because the contents of files compressed into password-protected ZIP archives cannot be scanned, the files cannot be inspected by antivirus tools, sandboxing tools, and so forth. So password-protected ZIP files have a greater chance of reaching the user than doc files that are simply attached in the conventional way.

JPCERT/CC observations confirmed an increase in email activity related to Emotet around July[*14]. And Cisco reported[*15] that this activity continued beyond that. The activity died down from end-October, but activity related to the distribution of Emotet resumed in late December[*16].

Our SOC observed Emotet-related attacks from July through September. We saw a sharp rise in attacks spreading Emotet in September in particular.

Figure 4 shows the Emotet-related detection rates for attacks detected on the IIJ Secure MX Service between July and October. The vertical axis is normalized by setting the total number of Emotet-related detections over the sample period to 100%.

Emotet observations were increasing from late July. They then increased rapidly around September 15 and peaked on September 18.

Emotet traffic was also detected on the IIJ Secure Web Gateway Service. The service detected two types of Web access related to Emotet.

1. Downloads of files in Microsoft Word 97-2003 (doc) format that contain macros designed to cause Emotet infections
2. Emotet communications with command and control (C&C) servers post infection

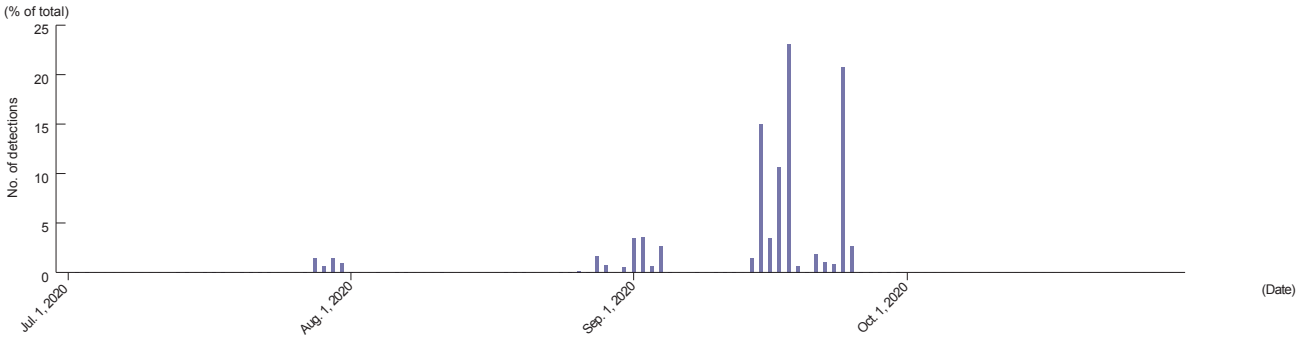


Figure 4: Detection of Emotet when Receiving Emails (Jul.–Oct. 2020)

*13 Information-technology Promotion Agency, Security Center, "Sharp increase in inquiries / Example of attack using password-protected ZIP file (added Sep. 2, 2020)" in "Emails designed to cause infections with the virus called Emotet" (https://www.ipa.go.jp/security/announce/20191202.html#L13, in Japanese).
*14 JPCERT/CC, "Resumption of distribution of emails leading to infections with the Emotet malware (update)", https://www.jpcert.or.jp/newsflash/2020072001.html, in Japanese).
*15 Cisco Japan Blog, "Activity resumes: Analysis of 2020 Emotet activity" (https://gblogs.cisco.com/jp/2020/11/talos-emotet-2020/, in Japanese).
*16 JPCERT/CC, "Stay wary of emails likely to cause Emotet and other malware infections" (https://www.jpcert.or.jp/newsflash/2020122201.html, in Japanese).

Figure 5 graphs Emotet-related traffic detected on the IIJ Secure Web Gateway Service between July and October. The vertical axis is normalized by setting the total number of Emotet-related detections over the sample period to 100%.

In our 2019 IIR periodic observation report[*17], we only had detections of HEUR:Trojan.MSOffice.SAgent, but in 2020, we also detected Trojan-Banker.Win32.Emotet. In the case of HEUR:Trojan.MSOffice.SAgent, we detected doc files that download Emotet. In the case of Trojan-Banker.Win32.Emotet, we confirmed that all files detected were Emotet. HEUR:Trojan.MSOffice.SAgent detections first appeared on July 21 and peaked on July 28. Trojan-Banker.Win32.Emotet was first detected on September 2 and peaked on September 3.

IcedID Observations

In November, when Emotet declined after showing up repeatedly since July, we observed attacks spreading malware called IcedID. Like Emotet, IcedID was originally a type of banking Trojan, but in addition to this functionality, it has now gained the ability to serve as a loader for other malware. Once it infects a computer, IcedID steals financial institution credentials and other information, and sends the data to a C&C server. Emotet and IcedID share commonalities in that they both use emails to spread malware, and they use doc files as an infection vector. And since it was first observed, IcedID has been spreading by attaching password-protected ZIP archives to emails, similar to the method Emotet has been using since September[*18]. So there are commonalities between the two, but unlike Emotet, IcedID does not build botnets.

Figure 6 graphs proportional counts for communications with C&C servers observed on the IIJ Secure Web Gateway Service between October and December. The vertical axis is normalized by setting the total number of communications with C&C servers over the sample period to 100%. The first observation came on November 3, with November 20 being the peak. As the graph shows, these communications continued up to December 2. We also determined that there were changes between the November 3 and November 20 observations in terms of the operations performed between when the doc file used in the attack was opened and when the infection occurred[*19], and these dates correspond to the day on which we first observed communications with C&C servers and the point in time in our observational window at which these communications were at their peak.

Countermeasures

Both Emotet and IcedID infect computers when a doc file is opened and a VBA macro executed. So one way of reducing the damage caused by infections is to disable the execution of macros when files are opened. See our wizSafe Security Signal article[*20] for details of how to disable macros to prevent malware infections. It is also crucial that users do not

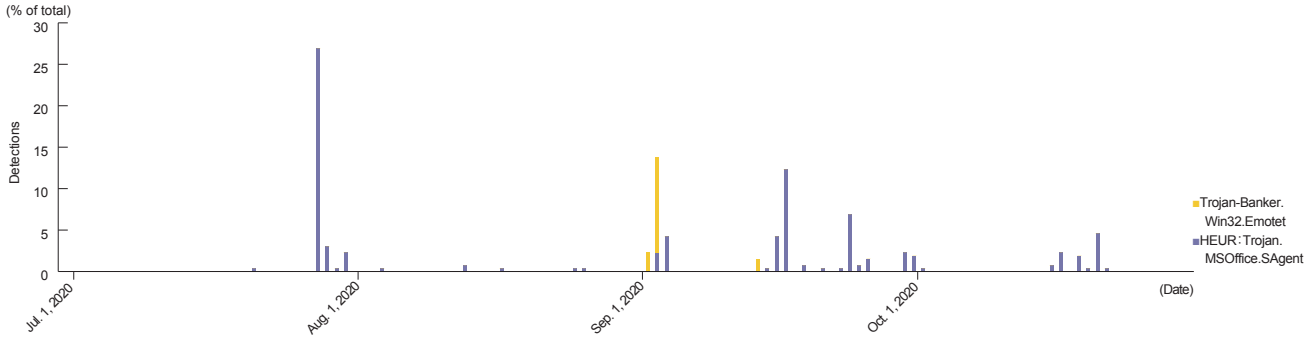


Figure 5: Detections of Emotet-related Traffic when Accessing the Web (Jul.–Oct. 2020)

*17 Internet Infrastructure Review (IIR) Vol. 46 (https://www.iij.ad.jp/en/dev/iir/046.html).
*18 JPCERT/CC Analysis Center (https://twitter.com/jpcert_ac/status/1324561915738091522/, in Japanese).
*19 Analysis of the IcedID campaign directed at Japan (https://mal-eats.net/2020/11/12/analysis_of_the-_icedid_campaign_for_japan/, in Japanese).
*20 Disabling VBA macros as a countermeasure against malware infections (https://wizsafe.iij.ad.jp/2020/09/1044/, in Japanese).

inadvertently open attached files that cannot be confirmed as safe.

1.4 Conclusion

This report presented a 2020 incident calendar, annual data for IIJ security services, and observational information that our SOC analysts were focused on in 2020. We expect to continue to see attacks targeting the SSL-VPN vulnerabilities we discussed in Section 1.3.1 and attacks using Emotet and IcedID, which we covered in Section 1.3.2, even as the targets, methods, and names involved change over time. We also observe a range of other security threats, beyond the examples discussed here, every day. And to go beyond the discussion in Sections 1.2 and 1.3, properly understanding and dealing with such threats is crucial. IIJ's SOC will continue to publish a range of information such as updates on threats observed on the Data Analytics Platform and key security topics, and we hope this information will prove useful in your security countermeasures and operations.

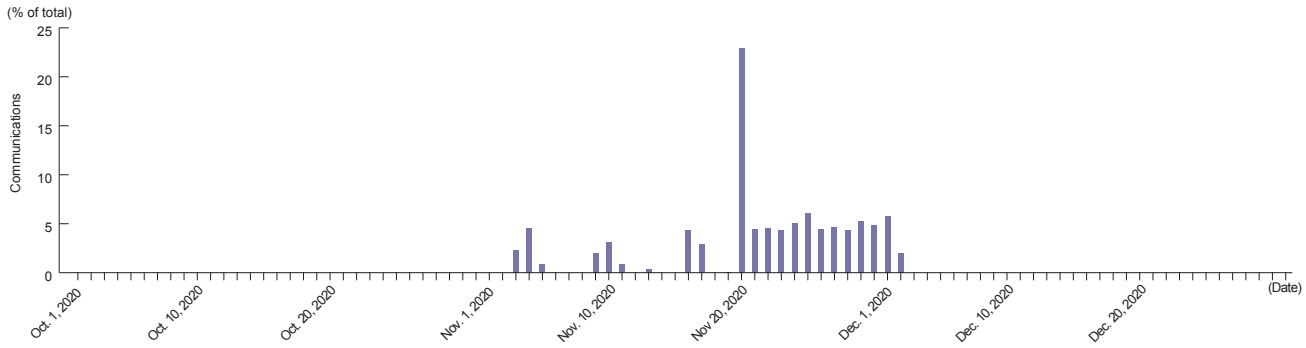
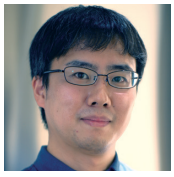
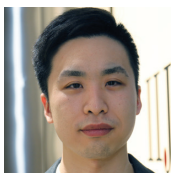


Figure 6: Communications with C&C Servers by IcedID (Oct.–Dec. 2020)



Hiroyuki Kamogawa
Security Operations Center, Security Business Department, Advanced Security Division, IIJ

Satoshi Kobayashi
Security Operations Center, Security Business Department, Advanced Security Division, IIJ



Shun Morishita
Security Operations Center, Security Business Department, Advanced Security Division, IIJ

Shimpei Miyaoka
Security Operations Center, Security Business Department, Advanced Security Division, IIJ

IIJ's Efforts with RPKI

2.1 What is Route Hijacking?

The Internet is formed by the interconnection of organizations (networks) identified by 2-byte or 4-byte AS (Autonomous System) numbers (e.g., IIJ's AS is 2497). The ASes are connected by a routing protocol called BGP (Border Gateway Protocol), and each AS advertises its own IP address to one another in the form of route information. This information propagates around the world and thus provides a mechanism by which packets can arrive at a destination from the other side of the globe.

The IP addresses each AS uses are strictly controlled by the RIRs (Regional Internet Registries; in Asia this is APNIC (Asia-Pacific Network Information Center)) delegated for each region by IANA (Internet Assigned Numbers Authority) and by the NIRs (National Internet Registries; in Japan, this is JPNIC (Japan Network Information Center)) for each country. Each AS receives IP address allocations from these authorities. As long as each AS accurately advertises BGP routes only for the addresses it has been allocated, no problems occur, but what happens if an AS, for whatever reason, ends up advertising IP addresses it has not been allocated? For example, naturally only IIJ should be advertising the route 202.232.0.0/16, which includes 202.232.2.164, the IPv4 address of the IIJ website (www.iij.ad.jp). But if an AS somewhere that is not IIJ were to advertise 202.232.2.0/24, which is part of the above route, packets intended for the IIJ homepage will reach this AS (a principle of routing is that routes with longer lengths take priority). There is not really much of an impact in the case of the IIJ website, but it is easy to imagine what the impacts could be in the case of DNS servers or banking sites.

This phenomenon is generally called route hijacking, and these sorts of issues do actually happen on the Internet on a daily basis. Examples include prominent video site YouTube's service being suspended because an AS that is not Google advertised a certain route, and incidents in which BitCoin is said to have been misappropriated when routes encompassing BitCoin-related site addresses were advertised by a separate AS. So how do problems like this arise? Each AS essentially self-declares the aforementioned BGP route advertisements. Confirming that the routes advertised by the AS of the system you are connected to are legitimate is utterly infeasible as it would require routers to reflect the innumerable IP allocations that are updated daily, so there is no choice but to almost unconditionally accept the advertised routes. So in some sense, the Internet as it currently stands is on quite precarious footing.

2.2 Overview of RPKI

With the Internet having now become an indispensable part of our social infrastructure, leaving the situation unaddressed would expose society as a whole to considerable risk, so RPKI (Resource Public-Key Infrastructure) has been devised to rectify this. The idea of RPKI appeared circa 1998, around the time the Internet finally became widespread in Japan, and it represents amazing foresight on the part of researchers.

In a nutshell, RPKI provides a mechanism for verifying/validating the legitimacy of resources (Internet number resources such as IP addresses and AS numbers) using digital certificates (X.509). As mentioned, IP address allocations are managed by IANA, RIRs, and NIRs, so these operating organizations form a tree structure (to be precise, a tree with five RIRs at the top), and digital certificates guarantee that the resources are correct. Users of the information use these digital certificates to determine that the resources are correct. RPKI itself is a general-purpose mechanism that is also applicable to scenarios beyond BGP routing, but we limit our discussion here to BGP routing.

An AS, having received an IP address allocation, registers the IP addresses for which it intends to advertise BGP routes, along with the maximum prefix length and the origin AS number, with the RPKI system managed by its NIR. The RPKI system issues a digital certificate in response[*1]. This digital certificate is called a ROA (Route Origination Authorization).

Users of these ROAs rely on information called TALs (Trust Anchor Locators), which correspond to the vertices of a tree structure, to traverse the tree up through the NIR and RIR and acquire the ROA, which they then verify and save as validated data (VRP, Validated ROA Payload). It is the role of a cache server to provide this VRP to the router. The information is supplied to the BGP router via a protocol called RPKI-RTR (RPKI to Router Protocol). Based on this information, the BGP router verifies whether route advertisements it receives are correct by matching their content up against the VRP data. Consider, for instance, a VRP with IP address 202.232.0/16, maximum length /17, and ASN 2497. A route advertisement with IP address 202.232.2.0/24 and ASN 64494 would be invalid, and refusing to accept this route can prevent route hijacking. Validating the origin AS on received routes using RPKI information (ROA) like this is called ROV (Route Origin Validation). How the validation results are handled is left up to the operating policies of each AS, but common practice at present is to discard only those routes that are clearly invalid (for reasons explained below).

2.3 Current State of RPKI

As of January 2021, BGP route information for around 930,00 routes (IPv4 830,000, IPv6 100,000) is being exchanged on the Internet, but the number of valid ROAs stands at about 210,000. The ROA count as of October last year was roughly 190,000, so it has increased by 20,000 in four months and is thus right in the middle of its expansion. Figure 1 shows routes that can and routes that cannot be validated using ROA as a proportion of all BGP routes (930,000). Although the number is steadily increasing, over 70% of BGP routes do not yet have a ROA, so it is not possible to validate the originating AS using ROA. Above, I explained that with current ROV, routes are generally only discarded when they are clearly invalid, and this is why. When it is unclear whether a route is proper or not because it cannot be validated, there is no option but to accept it. The hope is that RPKI will continue to spread to that point that all IP addresses can be validated, but that will likely take a decent amount of time.

Of the roughly 71,000 ASes for which BGP routes exist, around 20,000 have ROAs with the AS listed as the origin AS. In the case of the AS with the most routes, ROAs exist for around 4,000 of the roughly 9,600 BGP routes originated by that AS, but this AS has a prefix length / maximum prefix length of /20, and it also has ROAs for this range broken into the prefix lengths /21, /22, /23, and /24. Normally in this case, a single ROA would do with a prefix length of

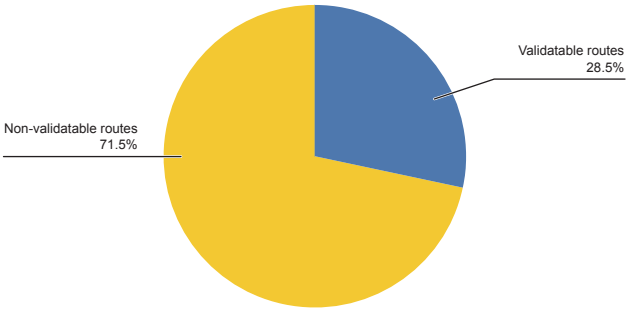


Figure 1: Validatable and Non-validatable Routes

*1 The IP address user can also issue a digital certificate. In this case, the user is the CA (Certification Authority) and will be incorporated into the trust tree as the authority for the IP address assigned by the NRI.

/20 and a maximum prefix length of /24, so it is unclear what is being achieved here, but we can say that creating unnecessary ROAs is not the proper thing to do as it results in the unnecessary consumption of router resources.

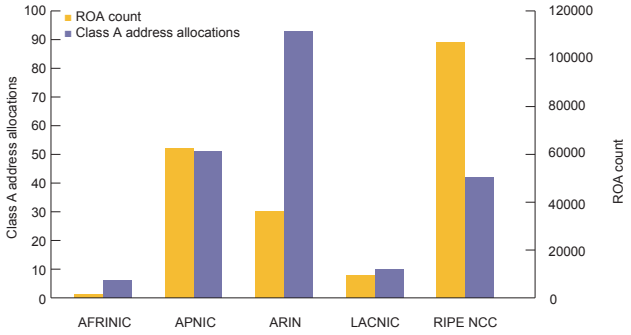


Figure 2: Address Allocations and ROAs by RIR

Next, we look at the state of ROAs by region. Figure 2 shows the number of class A address allocations and ROAs for each RIR*2.

As you can see, APNIC, which oversees the Asian region including Japan, RIPE, which oversees Europe, and LACNIC, which oversees Latin America, create a large number of ROAs relative to the number of allocated addresses. And on a country-by-country basis, it looks like some countries have reached 100%*3. Unfortunately, the adoption rate is not high in Japan, so hopefully we will see greater efforts in this regard ahead.

Let's look at the ROA prefix lengths. Figures 3 and 4 show the distribution of, respectively, IPv4 and IPv6 ROA prefix lengths and maximum prefix lengths. Generally, the usual practice on the Internet is to exchange IPv4 prefix lengths of up to /24 and IPv6 prefix lengths of up to /48, and so routes with prefix lengths longer than those are not exchanged. Yet

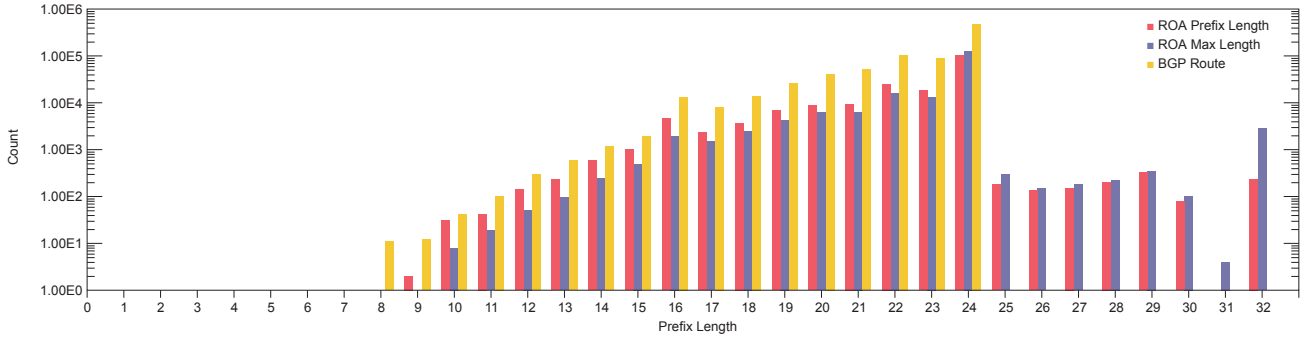


Figure 3: ROA Prefix Lengths and BGP Prefix Lengths (IPv4)

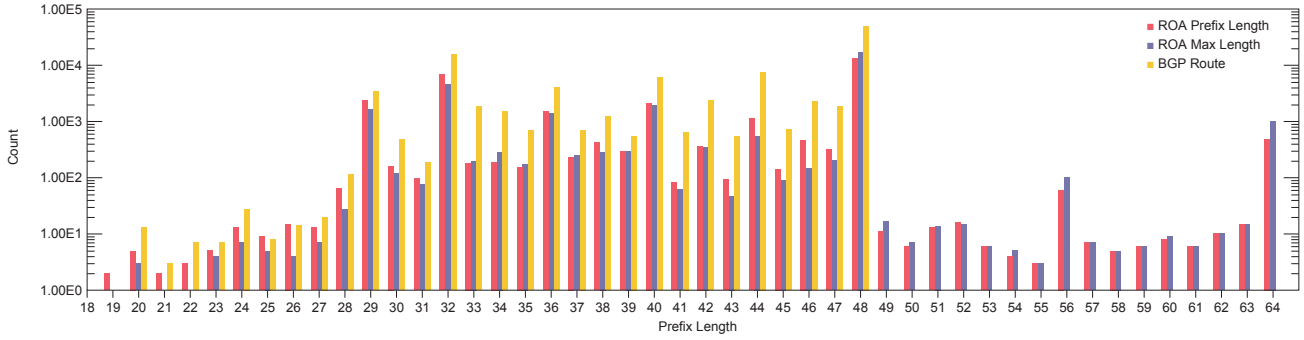


Figure 4: ROA Prefix Lengths and BGP Prefix Lengths (IPv6)

*2 Allocations to each RIR are based on IANA data (https://www.iana.org/numbers). Because international address transfers are made to ensure IPv4 works effectively, differences arise between RIR allocations and the actual region of use, so the figures do not necessarily show the correct region of use.

*3 NLnet Labs, RPKI Tools (https://nlnetlabs.nl/projects/rpki/rpki-analytics/).

there appear to be quite a number of ROAs with long prefix lengths. Further, Figure 5 shows the distribution of the difference between ROA prefix length and maximum length, and while there is no difference in the overwhelming number of cases, there are also substantial differences in quite a few cases. RPKI-based ROV only verifies that the combination of IP address and origin AS is correct; it does not deal with cases in which information, including the origin AS itself, is spoofed. In general, routes become hijacked when an operator originates a route with a prefix that is longer than that of the normal BGP route, and setting a maximum length in a ROA that is longer than the BGP actually being advertised contributes to this risk. So it is best to do everything possible to ensure that advertised BGP routes and ROAs have the same maximum length. But if you do accidentally advertise a prefix longer than the ROA's maximum length, the route will be discarded under ROV, causing a routing failure, so considerable care must be taken.

So far we have looked at the state of ROA. Now let's look at how many invalid routes are detected via ROV using ROAs. As I will explain, IIJ adopted ROV at end-2020, so in principle there are no invalid routes within the IIJ network. We thus use slightly older data and look at the situation around August 2020, before IIJ began using ROV. Figure 6 shows the results of ROV on BGP routes received by IIJ. Along with "valid" and "invalid" results, we also have "not found", which means there was no ROA, so validation is not possible. As indicated, around 3,000 routes, or 0.3% of the total, were invalid as of end-August 2020.

These roughly 3,000 invalid routes are broken down in Figure 7. Around half have the correct origin AS but the wrong prefix length (mismatch length); around 30% have the wrong origin AS (mismatch origin); and the remaining 20% have the wrong origin AS and prefix length (mismatch origin and length). Many of the length mismatches are probably cases in which routes internal to the AS that have long prefix lengths are accidentally advertised externally when they shouldn't be (leaked). The mismatches of both origin AS and length are possibly malicious route hijacking attempts, but there are also likely many cases in which part of an address range allocated to one AS is being advertised by another AS (commonly called hole punching). Where hole

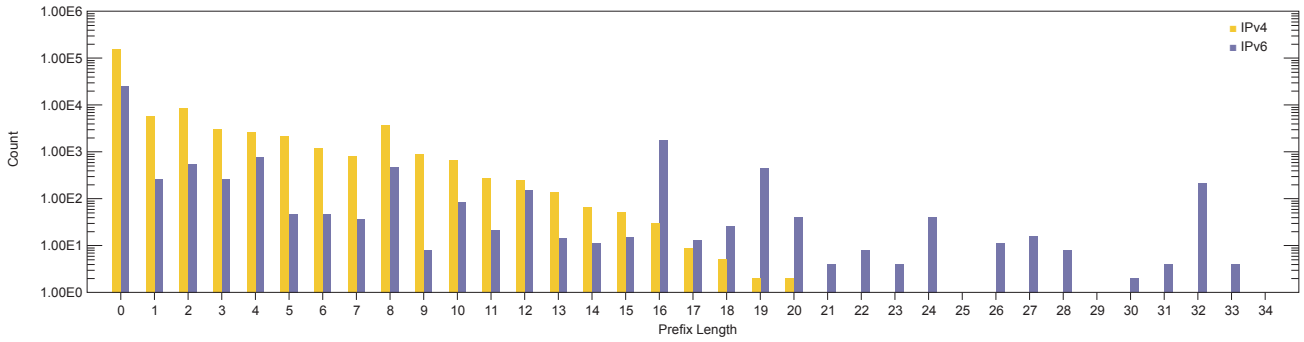


Figure 5: Difference between ROA Prefix Length and Max Length

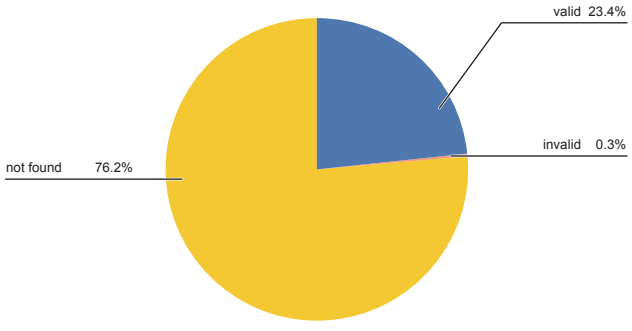


Figure 6: Breakdown of ROV Results

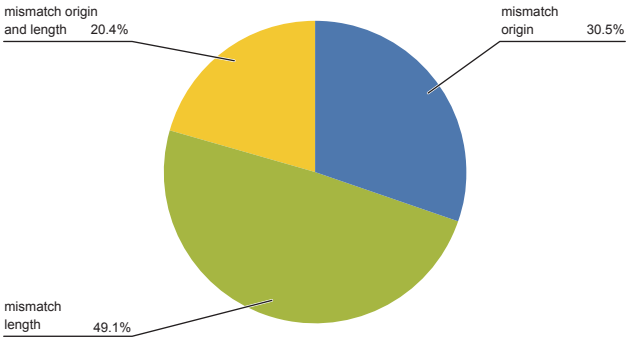


Figure 7: Breakdown of Invalid Routes

punching is occurring, separate ROAs should be created for the different origin ASes and prefix lengths based on the allocated address range and the more specific range, but it is conceivable that someone has neglected to create a ROA for the more specific range. But either way, only the people creating the routes actually know what their real intentions are. From the outside looking in, it's impossible to tell if it's simply an oversight, route hijacking due to a configuration error, or malicious route hijacking. So routes deemed invalid by ROV are uniformly discarded, resulting in a non-zero chance of dropping some routes that should not be dropped. Proper management of ROAs and advertised routes is the responsibility of the AS that receives the IP address range, so there is no fault on the part of ASes that discard routes according to ROV.

This means that roughly 3,000 routes ROV deems invalid are all discarded, but this does not necessarily mean that they all become unreachable. For example, even if 192.0.2.0/25 is discarded, reachability is retained if there is a route for 192.0.2.0/24, which encompasses this. But there are actually many cases in which the origin ASes for, in this example, 192.0.2.0/25 and 192.0.2.0/24 differ, and in such cases, even if 192.0.2.0/24 does exist, it is difficult to objectively determine whether packets reach the proper destination. If cases where the origin ASes differ are permitted, there are alternative routes for around 2,500 of these roughly 3,000 routes, and if only cases in which the origin AS is the same are permitted, there are alternative routes for around 1,500 of them. So taking a strict view, ROV results in reachability being lost for around 500 routes (roughly 0.04% of all BGP routes); and taking a looser view, it results in around 1,500 routes (0.15%) becoming unreachable.

Table 1: Test Routes Retained

Route	RPKI	route views	RIS
93.175.146.0/24	Valid	28 AS	287 AS
93.175.147.0/24	Invalid	13 AS	207 AS
2001:7fb:fd02::/48	Valid	N/A	290 AS
2001:7fb:fd03::/48	Invalid	N/A	205 AS

Naturally, reducing route hijacking itself is the objective of ROV, so discarding invalid routes is the right course of action, but the introduction of ROV does bring with it the possibility of blocking traffic that was previously being routed, even if perhaps improperly. So it would be good to have an idea of what the impact of that would be beforehand.

So how many ASes around the world have adopted ROV? Unlike with ROA, it is difficult to tell for sure from an external perspective whether each AS has adopted AS. Although it depends on self-reporting by ASes, according to the website https://isbgpsafeyet.com/, created to increase awareness of RPKI, around 100 ASes have implemented ROV. More objective information can be gleaned from routes advertised by RIPE NCC, the RIR for Europe, for the purpose of measuring certification technology uptake[*4]. The routes intentionally include both routes designed to be valid and invalid according to ROV, so the degree to which ASes retain these routes can be used to measure ROV implementation status, as in Table 1. Two projects, route views[*5] and RIS[*6], connect to ASes and collect routes to facilitate various measurements. In both cases, the data show that around half to two thirds of ASes have invalid routes when compared with valid routes. However, just because a particular AS does not have invalid routes does not mean that it has implemented ROV. If an upstream AS has implemented ROV, the downstream AS that obtains the routes thus propagated will also no longer have invalid routes. So these results do not indicate that an AS has implemented ROV, but they do demonstrate the effect of ROV in terms of the objective of not propagating invalid routes. These numbers can be expected to change ahead as ROV is increasingly deployed.

2.4 IIJ's Efforts

IIJ is also working on RPKI. FIrstly, at end-2020 IIJ created ROAs for most of the IP addresses it has been allocated by JPNIC (IPv4 82%, IPv6 100%). This allows us to mitigate the risk of IIJ's IP addresses being subject to route hijacking via ASes that have implemented ROV. This effect will increase as more ASes implement ROV. In cases where we have not created ROAs, there are either special circumstances that result in incompatibilities with the JPNIC

*4 RIPE NCC, "Routing Certification Beacons" (https://labs.ripe.net/Members/markd/routing-certification-beacons/).
*5 Routeviews, "University of Oregon Route Views Project" (http://www.routeviews.org/routeviews/).
*6 RIPE NCC, "RRC00 -- RIPE-NCC Multihop, Amsterdam, Netherlands -- Peer List" (http://www.ris.ripe.net/peerlist/all.shtml).

system, which issues the ROAs, or some or all of the addresses are advertised by a customer's AS, so we will need to coordinate with them. We intend to resolve these issues in all cases ahead.

The creation of ROAs for IIJ's allocated IP addresses is going well, but looking at all routes for which AS2497 (IIJ) is the origin AS, only around 30% have ROAs. This is due to customers who use IIJ's services receiving address allocations directly from JPNIC (provider-independent addresses) and using AS2497 as the origin AS. ROAs must be created by the organization that was allocated the addresses, not the AS advertising the BGP routes, so in these cases, the customers should be creating the ROAs themselves. And in these cases, IIJ is indeed encouraging its customers to create ROAs.

IIJ continues to implement ROV on its connections with other ASes and had done this on over 50% of such connections as of end-2020. Connections between ASes can generally be put into three categories: peer connections, upstream (or transit) connections to upstream ISPs, and customer connections whereby the AS provides connectivity to its customers. ROV is implemented on all of IIJ's peer and upstream connections. We have not yet implemented it for customers who purchase connectivity services from IIJ, but we use strict route filtering on points of connection with our customers and thus almost no invalid routes enter the mix. As a result, there are almost no invalid routes within IIJ's network, but even so, implementing ROV for customer connections as well will allow us to more reliably exclude invalid routes, and we thus plan to implement ROV for our customers possibly as early as FY2021.

Customer understanding and cooperation is essential to implementing RPKI for service users as well, but awareness of the importance and need for RPKI remains inadequate. We believe RPKI will be essential to improving not only the stability of customers' data communications but the stability of the Internet of a whole as well, so we are working to raise awareness about RPKI through a range of channels.

2.5 Looking Aheadn

We have discussed origin AS validation using RPKI, but this is not a panacea for all the various sorts of routing failures that occur on the Internet daily. As explained, origin AS validation only involves validating the combination of IP address and origin AS. It cannot detect route hijacking when the origin AS itself is spoofed.

Alongside route hijacking, another problem that frequently occurs is route leaking. This phenomenon, which tends to be due to configuration errors, occurs when routes received from a given AS are propagated by being advertised to other ASes when they shouldn't be. When this happens, traffic passes through ASes that it normally shouldn't, resulting in problems such as substantial traffic delays and packet losses. These incidents actually do occur several times a year on the Internet, affecting prominent online services and ISPs and causing disruptions with a large enough impact to make the mainstream news. Origin AS validation is ineffective against route leaks.

Various technologies and mechanisms for dealing with such events are being studied and discussed, and some are moving toward being standardized and implemented, but they will likely take quite some time to gain full traction given that the idea for RPKI appeared before 2000 and is only now finally beginning to take hold. Even so, now that the Internet has become a key part of our social infrastructure, major failures could have an immeasurable impact. So every AS that makes up part of the Internet should be working hard and consistently to address this, and as a member of the Internet community, IIJ is also doing its utmost in this area.

Takafusa Hori
Manager, Network Technology Section, Network Technology Department, Infrastructure Engineering Division, IIJ
Mr. Hori is engaged in running the IIJ backbone network.

Beyond 2020 —Olympics, Broadcast Production, Internet—

3.1 Introduction

How will people remember 2020? Life is different for everyone, but no doubt many will share the memory of 2020 being the year the COVID-19 pandemic began. COVID-19 had a major, widespread impact on our lives as it raged around the world. One effect was the postponement of the Tokyo Olympic and Paralympic Games. People may have a range of views on what its significance really is, but 2020 was supposed to be remembered as the year the Olympics and Paralympics came to Tokyo.

3.2 The Olympics, Paralympics, and Broadcast Productions

Broadcasting, particularly television broadcasting, has become inseparably linked with big events in recent years, especially major sporting events such as the Olympics and the World Cup. The media wants large-scale events to attract an audience, and event organizers rely on the mass media to more effectively use their influence. Wide-bandwidth broadcasting can provide a rich media experience (visual, auditory) and thus occupies a dominant position when it comes to covering big events that attract the interest of people all over the world. Broadcasting is the only mechanism that allows people in every country around the world to receive rich media virtually simultaneously. The Internet is still outmatched when it comes to this sort of content distribution on a massive scale.

Even in this context, the Olympics and Paralympics broadcasts are quite special. A huge number of events take place in a short period of time, with programs produced and broadcast around the world. Since 2008, Olympic Broadcasting Services (OBS), established by the IOC, produces international coverage on all Olympic and Paralympic events, and this coverage is supplied under contract to broadcasters around the world. In Japan's case, a consortium of broadcasters called the Japan Consortium has a contract with the IOC. The coverage supplied does not contain announcer/analyst commentary in every language, nor any individualized coverage, so the broadcasters have to do the work of adding these elements into the production. Sudden demands often arise with these sorts of large events. An athlete may win an event unexpectedly (surprise contender), sparking a sudden need for live coverage, or two high-profile events may end up being held at overlapping times. Such uncertainties inevitably lead to a shortage of production resources.

Production of this sort of event coverage is generally handled on-site. This can mean, for example, sending a large truck converted into a broadcast vehicle (called an outside broadcasting van or OB van) to set up in a stadium parking lot, tasked with collecting feeds from cameras and microphones deployed inside the stadium, and with staff stationed in the vehicle to edit the audiovisual content. A prime example of this editing work would be video switching, but there is a whole lot of production work involved besides, including video camera aperture control and microphone audio mixing & adjusting. So a lot of broadcast engineers are needed on deck.

OB vans are fully equipped with all the production equipment they need so they can function independently. The onboard equipment has equivalent functionality to that back at the station but with slightly fewer inputs and outputs. But when the vehicles are not in use, that onboard equipment remains completely idle. This is because it is not realistic to install and remove the equipment every time the vehicles are put into use given the onboard space limitations. But in some cases, such as when the equipment is quite expensive, broadcasters need to make as much use of it as they can, so it is transported into the field on occasion. In any case, this is not an efficient way of doing things.

Ensuring enough broadcast engineers are on deck can also be difficult when covering separate events taking place at the same time. Broadcast engineers have to travel to the

location to operate the equipment, which creates a travel time overhead. This makes it impossible for them to cover multiple events at the same time, so multiple broadcast engineers must be assigned separately to each location. And when covering events too far away for a day trip, the broadcast engineers often have to stay in faraway hotels.

3.3 Path and Barriers to Remote Production

I began to wonder if we might use IP to address the situation by using it to facilitate the remote production of broadcast programs (Figure 1). In simple terms, this means equipping cameras and microphones with an IP gateway so that video and audio recorded on location can be ferried over long distances in high quality via IP, allowing the production work to be performed at the station. This opens the door to the idea of gathering the necessary resources for producing programs in a single place. Only a bare minimum of equipment need be taken out on location, and engineers need not travel to perform their jobs. No doubt this would not only reduce overheads but also increase efficiency and quality of work (although it may be sad news for engineers fond of going on the road).

The desire to improve efficiency by consolidating equipment as well as the engineers/operators who use it is a common one for the ICT industry. Amid the ongoing trend of shifting from on-premise systems to the cloud, from solutions to services in the past dozen or more years, companies have constantly sought to save on labor and streamline investment outlays by adopting ICT. All sorts of media has come to be distributed via IP over the last 20 or 30 years, with the last remaining area of any considerable size being that of broadcast production technology.

More and more broadcast equipment is supporting IP, partly urged on by the roll out of 10GbE and 100GbE high-speed Internet. Support for IP has ramped up rapidly in the last five or six years, and it is now commonplace for broadcast equipment to feature an Internet interface (mainly SFP+, SFP28 or QSFP). In response to this technological innovation, IP technology is increasingly being implemented in large-scale broadcast station equipment, particularly in the US and Europe. Within the broadcast equipment space, IP technology has now spread to the point that it can no longer be left out of the conversation on future prospects.

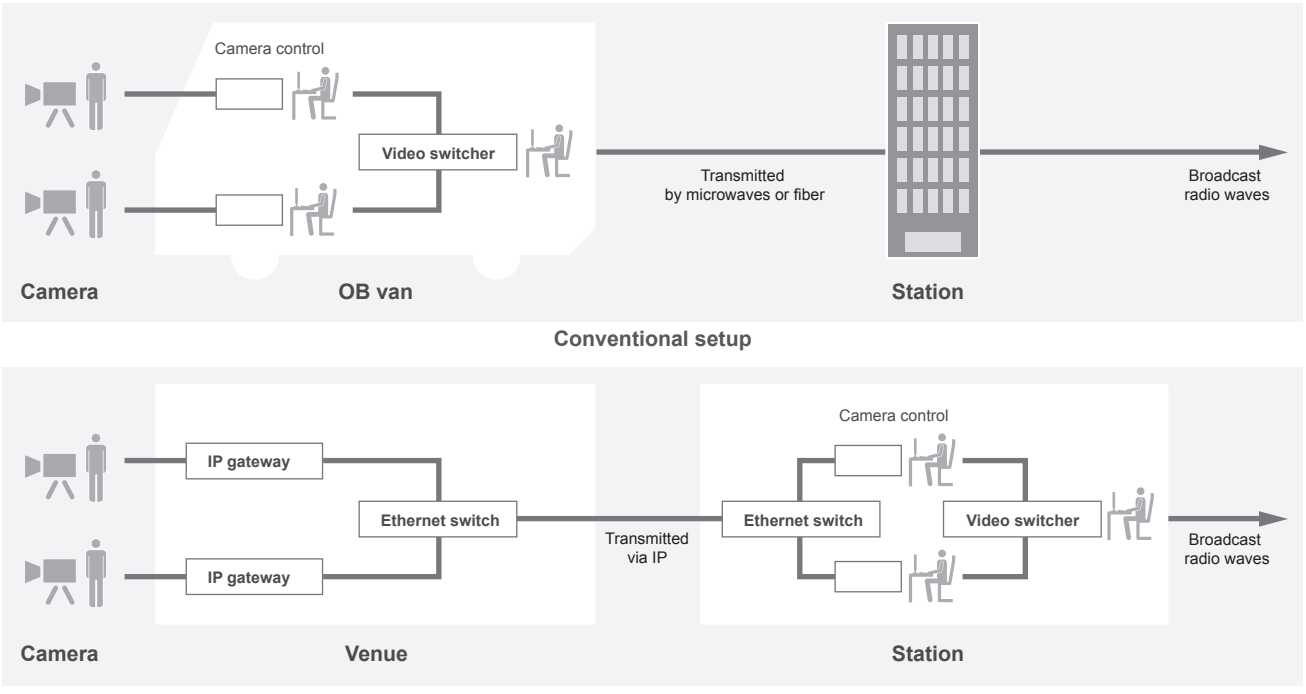


Figure 1: Conceptual Diagram of Remote Production

As with IP support at the station building, high-capacity data lines are also essential to making remote production work. Covering large sporting events typically involves setting up over 10 cameras and dozens of microphones to record events. If these sources are to be transmitted without compromising current production quality levels, then several data lines in the 10GbE or 100GbE class are needed (transmitting full high-definition video without compression requires around 1.5Gbps, and 4K requires around 13Gbps). These are far greater quality requirements than those for online broadcasts created for OTT (over-the-top) services. Telecommunications carriers do provide these sorts of high-capacity data line services, but in almost all cases they involve annual contracts with high monthly charges. This is above and beyond what broadcasters need given that they budget outlays on a program-by-program basis. It also takes considerable time to sort out the necessary arrangements for setting up these data lines, so the reality is that these services are not amenable to "casual" use cases such as setting a line up for three days only to cover a weekend event.

Remote production can be seen as one type of work-style reform, and from a big-picture perspective, it can be viewed in terms of the digitalization trend. Digitalization can not only facilitate workflows, it can also alter them from the ground up. Put differently, unless you ultimately seek to overhaul the workflow itself, you cannot maximize the effect of your efforts with digitalization. However, one opinion voiced by some involved in production following a remote production proof of concept we conducted can be summed up as follows: "This sinks a scalpel into our practice of centralizing production on-site by gathering people together." The problem, it seems, is that IP divides the flow of communication that close proximity had made possible. This is no longer a technical issue; it falls into the realm of organizational theory for digitalization. It is also in some sense a test case for how the industrial and business world should prepare in the face of a declining birthrate.

Evidently, issues remain to be addressed if we are to implement remote production on a daily basis. To liken it to climbing a mountain, we have climbed 50%, or perhaps 80%, of the way up the summit trail, so the truly hard yards still lie ahead of us. While we are gradually acquiring the skills, gear, budget, and timing we need to make the summit, there is a sense among those involved in the process that bringing these together all at once will be difficult. Some, perhaps, may even give up and turn back from the summit.

However, IP networks surely have other contributions to make. Instead of aiming for the world's highest peaks right out of the gate, another approach is to start by tackling the mountains that are currently more within your capacity to summit. Just as I was thinking this, the COVID-19 pandemic threw the world into disarray. And an issue of concern to everyone and of much greater urgency than the implementation of remote production came to the fore. Namely, measures to prevent the spread of COVID-19 in the workplace. In Japan, for example, we urged people to avoid the 3 Cs (closed spaces, crowded places, and close-contact settings).

3.4 The Important Relationship Between Remote Work and Networking—A Test Using VidMeet Online

Remote work is these days seen as a key part of companies' response to the COVID-19 situation. Until the present moment, remote work usually came up in the context of work-style reforms, but it is now held up as an effective strategy for combating viral infections. Broadcasters are no exception here, and workshops on remote work were even being held at European broadcasters as of March 2020. Limits placed on the number of people allowed in workplaces made it impossible to assemble the teams needed to produce programs in the usual way. To get around this, employees log into their workplace via a VPN to control resources at the station remotely. Among the announcements and discussion in this area was a story about one

stout-hearted individual who controlled the switcher that is essential to live broadcasts from a remote location, which really seems like quite an astonishing feat.

So, what form should networking that facilitates remote work take? To me, this seemed like an issue worth pursuing in 2020, and I sought an answer from the real world in the form of a demonstration. That demonstration was VidMeet Online, which was run online by a number of interested individuals from October to December 2020.

VidMeet is an event that began in 2017 as a Video over IP study group. I have organized nine such meetings at IIJ so far, but COVID-19 forced us to suspend these activities. So in the early summer of 2020, an online meeting for interested individuals from manufacturers and providers of broadcast and IP equipment took place. With all sorts of events shifting online or being cancelled, the attendees discussed the prospects of themselves organizing online events. As we settled on a direction, a decision was made to use the VidMeet name in the event title. VidMeet provides an opportunity to contribute to the community, and I think it was well received as an appropriate name for the event.

The theme of VidMeet Online is “New operational styles created by broadcast equipment combined with the Internet, datacenters, and the cloud”. We were interested in what would happen if broadcast equipment were centralized in datacenters and the cloud and linked via the Internet. The appeal of this event is in figuring out how remote networking, which is a readily available resource, can contribute in a broadcast production setting. We looked at what we can do right now with even less footwork than is required with remote production (Figure 2).

The concept for the event was to use the datacenter as the broadcast station and participating companies’ offices as the broadcast locations. The Flet’s Hikari service was

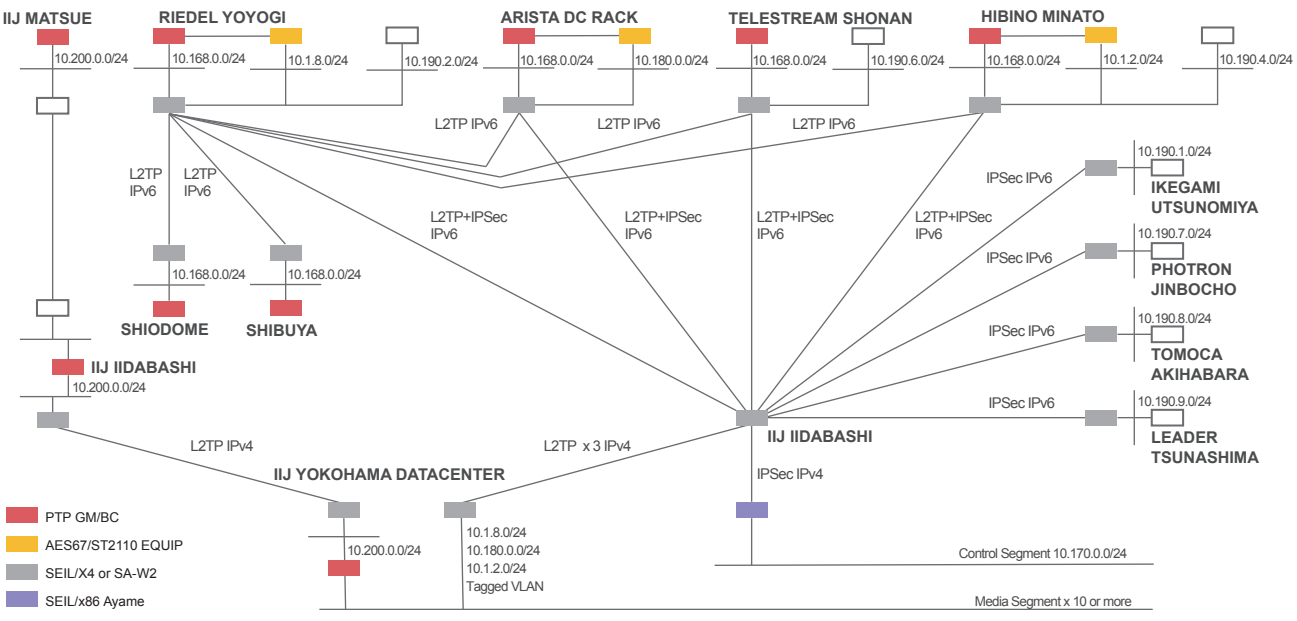


Figure 2: VidMeet Online Network Structure

used to connect the companies and the datacenter, with the connections made via an Internet VPN (Figure 3).

We had two reasons for locating the broadcast equipment in a datacenter. One is that datacenters would have to be a candidate destination when looking to outsource and relocate station systems. While it's probably not possible to relocate all broadcast equipment, we wanted to explore the possibilities. For resources that can be moved to a datacenter, the option of ultimately moving into the cloud also comes into view. The other reason is that we wanted to connect the broadcast equipment to a high-capacity Internet line and control it remotely. If we could successfully perform a demonstration of broadcast equipment located in a datacenter over the Internet, this would mean that the technology could also be used for remote networking. The users taking part in the demo would be unexpectedly verifying the practicality of this technology.

The following tests were run during the VidMeet Online demonstration.

- Place the hardware control panel in the office and control the video processor installed in the datacenter via VPN.
- Feed voice packets generated in the office via a VPN to the voice processor at the datacenter for mixing.
- Operate the video packet analyzer installed in the datacenter from the office via a Web browser.
- Control the broadcast camera robot arms installed in the office via an Internet VPN.
- Configure and operate the network switch via a VPN.
- Remotely control the video server set up in the datacenter.
- Send PTP packets over VPN to synchronously drive broadcasting equipment at multiple remote points.

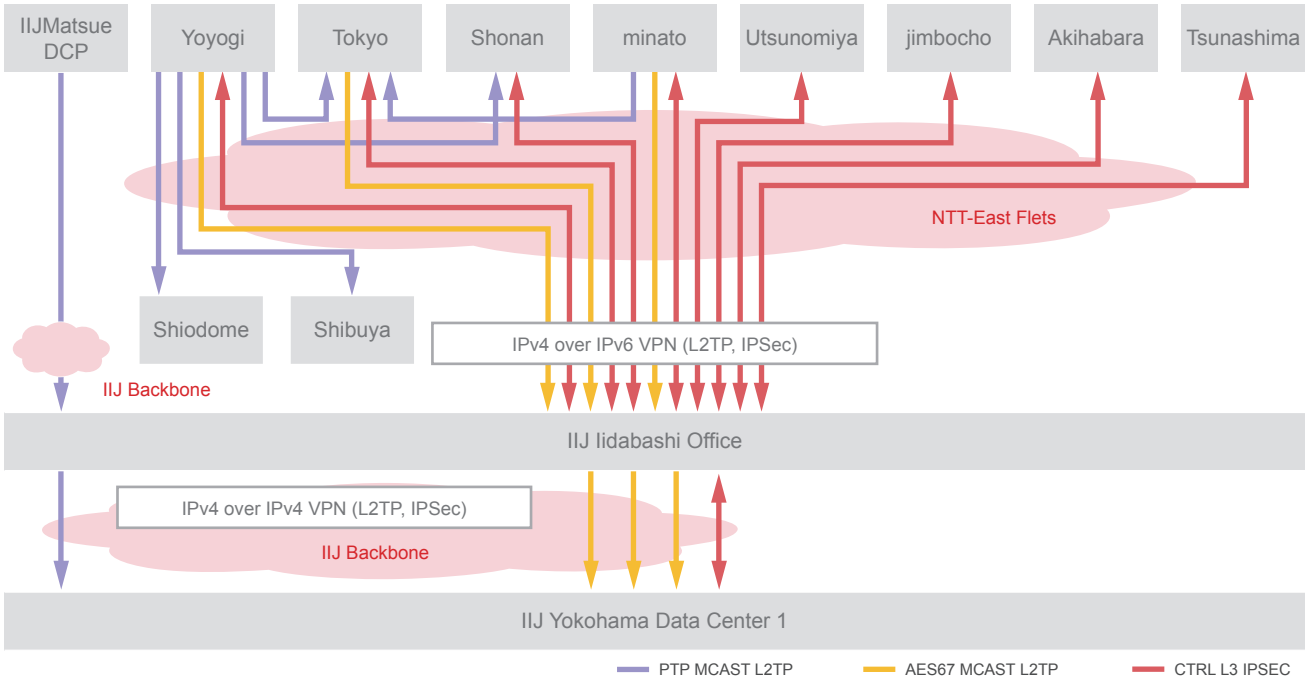


Figure 3: VidMeet Online Flow of Traffic over VPN

We also set up VMware ESXi servers in the datacenter on virtual infrastructure, installed applications on the virtual servers, and mainly operated control servers.

- The control servers installed on the virtual servers control the video server equipment set up in the datacenter and at the remote locations.
- We installed a monitoring application on the virtual servers to monitor the various devices.
- Interoperability between devices is checked on a metadata control server on the virtual servers.

Figure 4: Rack-mounted Broadcast Equipment

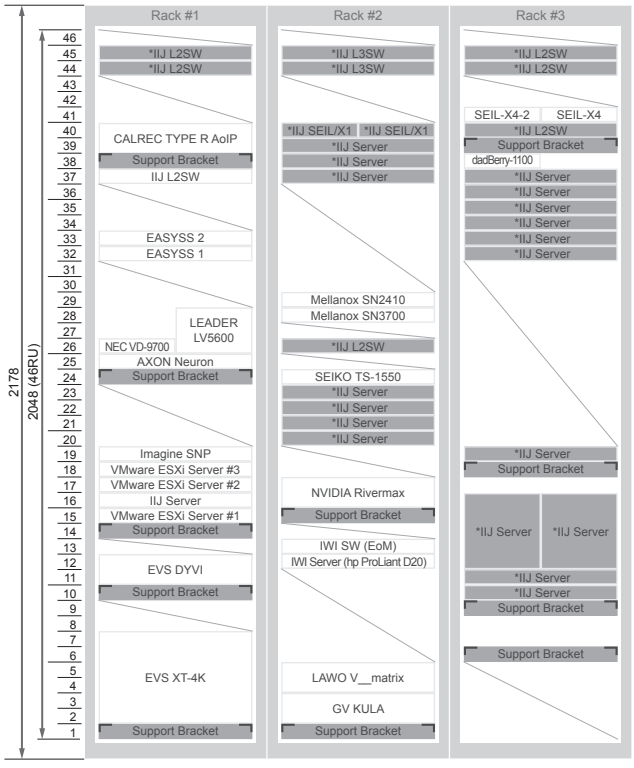


Figure 5: Rack Mounting Schematic

Datacenter racks usually have routers, switches, and servers installed in them, but for VidMeet Online the racks contained the sort of equipment seen in broadcast stations and vehicles. Since this is a rare sight for a telecommunications carrier's rack, I obtained permission to show you some details (Figures 4 and 5, Table 1).

When we actually built the VidMeet Online network, my thought was, "This could, surprisingly, be quite sufficient for practical purposes." We only used general-purpose protocols—L2TP, IPsec, and OSPF—to build the VPN, so it was

Table 1: VidMeet Online Participants

Arista Networks, Inc.
IKEGAMI TSUSHINKI CO.,LTD.
ITOCHU Cable Systems Corp.
Internet Initiative Japan Inc.
Intelligent Wave Inc.
NVIDIA Corporation
OTARITEC Corp.
Servants International Corporation
Seiko Solutions Inc.
Telestream Japan GK
NEC Corporation
TECHNO HOUSE INC.
TOMOCA Electronics Co., Ltd.
Network Additions Co., Ltd.
Hibino Corporation
PHOTRON LIMITED
Macnica, Inc.
Media Links Co., Ltd.
Leader Electronics Corporation
Riedel Communications Japan KK
One Diversified Japan GK

a fairly basic setup. Yet the tests we ran using the network were extremely wide-ranging, as listed above, and I think in terms of testing aspects of remote control and remote work, there have not been many examples of events like this around the world.

We ran these tests continually in the form of demonstrations from October 6 to December 11, 2020, announcing the results through webinars as well as seminars run by participating companies. We held a total of 16 webinars with over 300 cumulative attendees. The webinar presentations and announcements from each company have been archived, so I encourage you to visit the website at https://vidmeet.tv/.

It's worth noting that we even ran the project itself via remote networking. Although we did bring the equipment into and later remove it from the datacenter, and although physical work was performed by the participating companies, we controlled all the installed equipment via the network. Meetings and webinars took place via Zoom, with no physical gatherings held among project members. Networks can be highly useful from the perspective of project management too. Looking forward, I think this will prompt us to take a fresh look at how to best divide up things in terms of the importance of being on-site and what tasks can be done online.

3.5 Network Headed for the Cloud

VidMeet Online demonstrated the technical feasibility of remotely controlling broadcast equipment. The key going forward will be how we are to apply this knowledge to production environments and actual project proposals. We have opened the door to the possibility of connecting systems in broadcast vehicles and so forth via mobile VPNs for centralized monitoring in the cloud. Naturally, we cannot say that using mobile connections in the field is 100% safe and stable. Congestion can occur at crowded event venues, for instance. Data line selection becomes all the more important if the idea is to use cloud technology. A range of scenarios remains to be considered, such as the use of Flet's services in addition to mobile and the use of network services directly connected to the cloud.

Use cases for cloud technology in broadcast production and broadcast station systems are unquestionably on the rise. This has been happening in other industries for several years now, and broadcast stations have already started working on Web servers and video streaming. Cloud technology is one of the most impressive fruits of the Internet and the ICT domain in general, and there is very little choice but to use it at this point. One example is the centralized control and monitoring of cloud-based network devices.

The combination of devices used in broadcast production systems differs depending on program content, specifically program scale and direction. Until now, the equipment was simply set up on location, but things are not so simple when using IP. IP addresses must be assigned first of all, and we also need to configure network switches, implement PTP, and check and configure monitoring of connections between devices. Setting up complex systems like this without IP engineers would be quite problematic. The training and development of IP engineers at broadcast stations is still in its infancy, and the reality at present is that broadcast engineers are simply doing what they can to pick up IP technology in between performing their main work duties.

Adopting tools used in the ICT field is likely to be effective in this environment. Typical examples are applications for the centralized management of network switches and tools for monitoring broadcast equipment. For example, installing, operating, and managing network switches manually is not scalable for large-scale systems; tool-based centralized

management is efficient in such cases. And these sorts of tools are adaptable to dynamically changing situations. The existence of tools that can set up and run equipment without being physically present on site is also a huge help in terms of reducing engineer workloads. Indeed, not having to travel to the location and the ability to set things up in advance is synonymous with avoiding the 3 Cs.

Perhaps the real benefits of networking are something best experienced through not-so-glamorous aspects such as remote monitoring and the operation of equipment. Networking technology allows you to perform work right at your fingertips or anywhere around the world with essentially no distinction between the two, and connecting devices together may serve to reduce some of the effort that was until now unavoidable. Looking at it from another angle, we could say that networking is an indispensable technology for enhancing the quality of work performed. So it offers exactly the same potential benefits as remote production.

So evidently considerable scope remains for services and solutions that employ networking to contribute to better broadcast production environments. There remain many pockets still to be tapped.

One point that bears mentioning here is that these sorts of networking applications were certainly not born out of the COVID-19 situation. What has happened is that COVID-19 has brought methods that were already around into focus for pretty much everyone. Indeed, many engineers in ICT have been working this way for some time. Working remotely from home is naturally an application of networking technology, and so too is the operation of servers located in datacenters and the cloud from an office. In short, these technologies gained renewed attention in 2020 as their effectiveness in helping us respond to COVID-19 became recognized.

3.6 The Great Potential of Cloud Technology and Software

One other key trend is unfolding: the move toward software implementations. Broadcast equipment has a very narrow focus and is only really marketable to broadcast stations. The number of broadcast stations is limited, and it is not an easy market to break into, and this inevitably means higher equipment costs. As such, there is now a trend toward implementing equipment in software using commodity IA servers. Of course, LSI and FPGA are often selected for the processors used in devices that process video and audio in real time, and these sorts of products will no doubt continue to come in the form of specialized hardware ahead. Control servers, on the other hand, do not require as much processing power, so a CPU is often sufficient. This means the products can be implemented solely in software, obviating the need for in-house development and maintenance of specialized hardware, so there are advantages in terms of maintainability and expandability.

The trend toward software implementations has accelerated over the last decade. Appliances based on IA servers were quite common in the past, but sales of software by itself have ramped up more recently. Support for virtualization technology has increased, and taking a further step forward, cases of manufacturers starting to provide their own SaaS are also on the rise. And, needless to say, the underlying foundation of SaaS is cloud technology.

In the future, it will become commonplace for software-based control servers to be run in the cloud, controlling broadcast equipment located in station buildings and broadcast vehicles over the network. An advantage of running control servers in the cloud is that it allows centralized control of many systems at once. And when combined with existing networks and VPNs, this setup allows for control server access from any location. So someone could monitor and control broadcast

equipment from their PC. No doubt this form of operational support will be needed in the remote-work paradigm.

Of course, control servers do not necessarily have to be located in the cloud. If there are severe communication latency requirements for the controlled devices, a network topology that meets those requirements will be needed. The pros and cons of running control servers in the cloud should be evaluated in view of the specific characteristics of the application. Perhaps, instead of taking the cloud route, it will become common to have a server cluster within the station building. What's important here is that control servers are set up on virtual infrastructure. This makes migration between devices easy, and looking ahead, it will help lower the barrier to going back and forth between the cloud. In other words, we should be putting preparations in place to maximize the benefits of software implementations.

3.7 Possibility of Providing Clocks via the Network

Now, let's look at a technology by which networking could make substantial contributions in a broadcast production setting. That technology is PTP over WAN.

Across broadcast systems in general, video and audio are sampled, quantized, encoded, and treated as time-separated digital data. A measure of time, or a clock in other words, is essential if the original video and audio are to be recreated from this data. This is not an absolute time clock—one that reads 9:00am on January 1, 1970, for instance—but a relative time clock that is used to synchronize timing. Digital devices are always equipped with a clock. In the case of broadcast equipment, separate equipment is set up to generate the synchronization signal that coordinates the entire system, and this signal is provided to the individual devices. Audio and video can get out of sync during recording and playback unless all devices handle the data at the same time.

The clock signal for video equipment, referred to as the black burst signal, has traditionally been supplied via coaxial cable. This method has long been in widespread use. But with the shift toward using IP in broadcast equipment, IP is also now used to transmit this clock signal. PTP (Precision Time Protocol) was developed to synchronize clocks via a network. PTP uses Ethernet or IP to transmit information and provides a high level of time accuracy on the order of nanoseconds. It uses GNSS as the source and generates more accurate time information than signals provided by satellites. Because this information is extremely accurate, it is usable as a synchronization clock signal (it also includes absolute time information). The device that sends this high-precision time information out over the network is called the PTP grandmaster (or the GM for short). The protocol has been standardized by the IEEE, but it has such a wide range of applications that several standards organizations have published profiles tailored to the usage patterns of each industry.

Some barriers to the implementation of this technology do exist, however. All network devices on the routes through which PTP packets pass must support PTP. This is the case not only for the PTP GM and the broadcast equipment that receives the signal but also for the network switches that connect them. PTP-enabled devices perform special processing on just the PTP packets. To maintain accuracy, PTP-compatible devices continuously receive and correct time information from upstream, with the GM being the highest level source. When sending a PTP packet further downstream, this corrected time information is stamped on the packet. PTP-enabled devices must process packets in this manner for each separate Ethernet port. An awareness of this flow of PTP information is crucial when designing the network.

The network switches that currently support PTP are generally middle-class models or higher (probably with price tags of a million yen or more). Not all models from all manufacturers support it, so devices must be chosen carefully when installing a system. Plus, incorporating PTP technology into existing LANs and WANs is likely to be quite difficult. This is because it can lead to equipment being replaced and the question of whether certain services support PTP (there are probably not any WAN services that support PTP). If devices without PTP support exist on a route, the PTP packets will be forwarded with the original timestamp information preserved. The protocol cannot guarantee accuracy in this case, and fluctuations in packet arrival times will occur beyond the range for which it is possible to correct.

When broadcasting on location, there is also the problem of not being able to tell if a signal from a GNSS satellite will be available without testing for reception. Broadcast vehicles cannot always be set up under open skies. In generally good locations, signals may be available from 10 or so GNSS satellites, but clock accuracy is affected as the number of available satellites decreases. When a broadcast vehicle is set up between buildings, for example, sky visibility will be limited, so it may not be possible to obtain a sufficient signal from GNSS satellites. So it is argued that providing PTP over a network would be better in such cases, since a network will definitely be available if the system is being set up in the first place to enable remote production and remote control.

PTP over WAN is a technology to solve these problems. Its purpose is to supply PTP signals to remote locations even over networks without PTP support.

Several manufacturers are trying out approaches to PTP over WAN. IIJ is a member of the RPTP Alliance, through which it is promoting the development of this technology.

The RPTP Alliance is a project launched in 2019 with the aim of forming a proposal for the next generation of PTP. Its objective is to verify and popularize a technology called RPTP (Resilient PTP). Transmitting PTP signals over wide areas has until now required an expensive, dedicated network. In response, RPTP will enable high-accuracy synchronization over long distances, be compatible with PTP, and enable synchronization even on networks that cannot handle PTP signals. The companies currently driving in the RPTP Alliance's activities are Media Links Japan, Network Additions, Seiko Solutions, and IIJ.

RPTP does not modify PTP in any way. So existing PTP GMs do not need to support it. What RPTP does is add modifications to the synchronization algorithm on the signal receiving side so that the protocol can handle the time fluctuations on non-supporting networks. This provides a mechanism for resending rectified PTP packets. The conventional PTP synchronization algorithm assumes a clean LAN environment, and thus the development of RPTP is challenging from a technical perspective. But it is hoped that, because there will no longer be a need for all devices to support PTP, RPTP will ease the strict network design requirements and be easier to use.

The RPTP Alliance also participated in VidMeet Online to test PTP over WAN on the IIJ backbone. An L2 network was constructed between IIJ Matsue Data Center Park (DCP) and IIJ Yokohama Data Center 1 to facilitate PTP traffic. A GM was set up at IIJ Matsue DCP to transmit PTP packets to IIJ Yokohama Data Center 1. And the synchronization signal was converted from PTP to Black Burst (BB) so as to provide PTP and BB synchronization signal sources at the same time to the broadcast equipment. This was the RPTP Alliance's first experience distributing PTP and BB to broadcast equipment from multiple manufacturers. In each

case, we were able to establish synchronization without any problems and confirm the broadcast equipment was operating normally (Figure 6).

We have also succeeded in supplying PTP signals to remote locations in tests using wide area Ethernet services outside of the IIJ backbone. Further, we have confirmed that when we generate a BB synchronization signal from PTP and supply it to a broadcast production camera via a coaxial cable, the camera operates normally and the video captured can be transmitted without any problems (Figure 7).

We believe these results prove that RPTP can be effective. The RPTP Alliance plans to continue its efforts toward establishing RPTP as a real-world-ready technology and seeing it deployed in business.

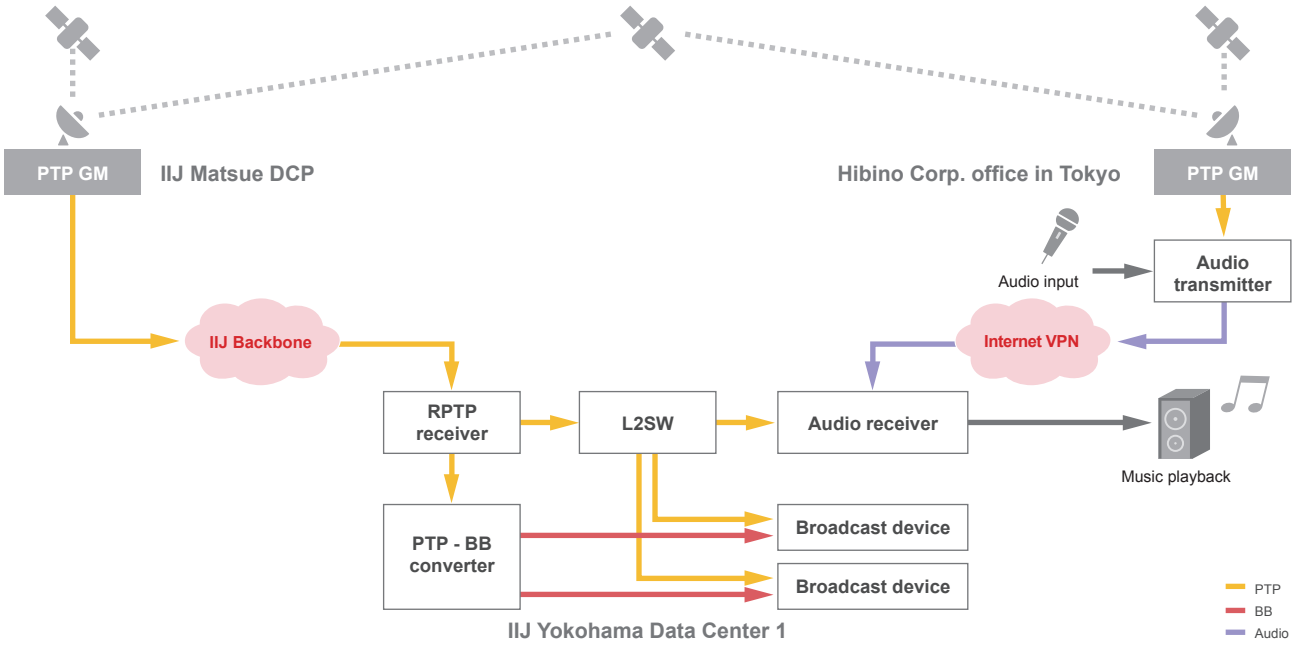


Figure 6: VidMeet Online Tests

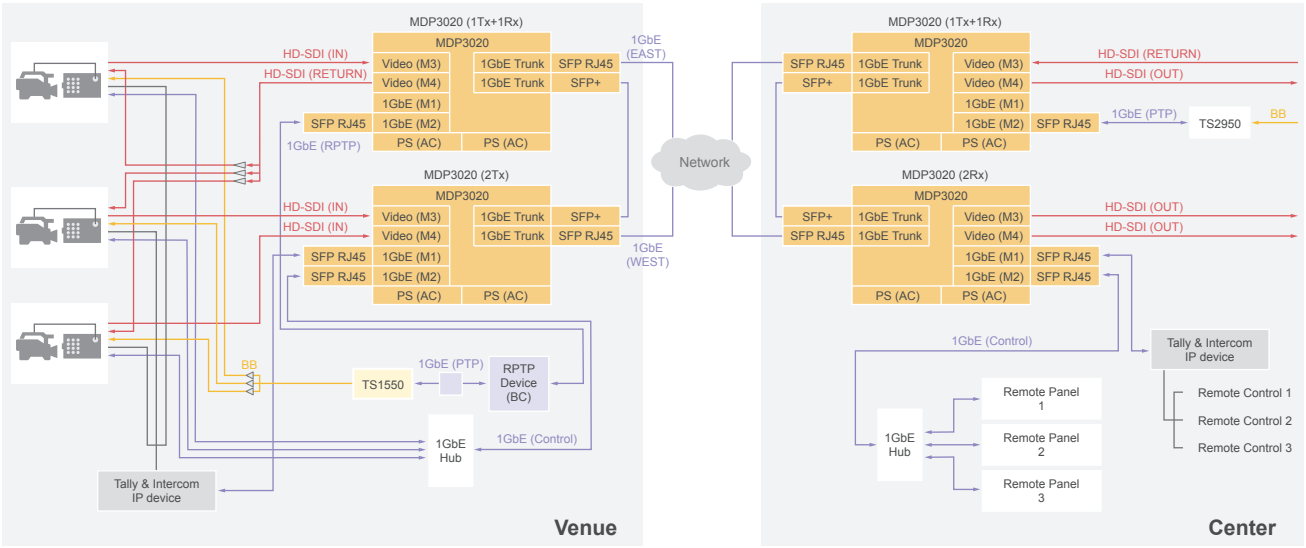


Figure 7: Successful PTP-BB Conversion

3.8 What VidMeet Online Revealed…2021 and Beyond

Eventually, high-capacity data lines will be set up at live broadcast locations. For the 2019 Rugby World Cup, an IP line was laid at International Stadium Yokohama, where the final was held, and coverage of the final was edited and produced in Australia. So while a backup crew and equipment were stationed in Shin-Yokohama, the basic operations were handled in Australia. And thus remote production is actually already a real option in a global context. Remote production achieves efficiency in response to increasing demands, and it will no doubt become commonplace and continue to increase in importance.

Yet the Olympics and Paralympics are held every two years, in the summer and in the winter, so there is a wait between games, and the host country is of course different each time. This is not an easy field to tackle. As discussed, IP has contributions to make to broadcast production in more everyday scenarios. The first step is to connect, at least in part, systems that are not yet IP-networked. We should determine the scope of application for technologies that are already widespread, inexpensive, and easy to deploy. Incorporating these sorts of endeavors into everyday operations and systems will allow us to build up technologies and experience.

I have also been searching for potential business deployments of IP-capable broadcast equipment. In fact, I have a real sense that our customers recognize connection services, which occupy the most basic position among IIJ's services, as a key technology and select them on that basis. Among IIJ's many services, connection services have the deepest history, with a wealth of both technical and sales experience, and with a wide variety of services on offer, making them one of the best services our customers can rely on. And cloud services are essentially rendered meaningless unless the connections are stable. The availability of a range of coverage including Flet's and mobile services in addition to dedicated lines is also a point of appeal. I believe that renewed recognition of the importance of connection services represents the fruits of mutual understanding.

Broadcast equipment and IP networks are set to become more deeply entwined ahead. Networking has an integral part to play in unleashing the true value of the cloud as well as in remote production and remote work. I hope to continue helping drive the evolution of networking as we seek to make it as easy as possible to use in a way that satisfies the many requirements in settings where mobility and responsiveness are crucial, such as broadcast production.

Bunjji Yamamoto
Digital Content Delivery Department, Network Cloud Division, IIJ
Mr. Yamamoto joined IIJ Media Communications in 1995 and has worked at IIJ since 2005. He is mainly involved with the development of streaming technology and efforts to popularize Video over IP. He has presided over VidMeet since 2017.

May 2021 Vol.50

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-MKTG020-0048

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/