IIR

Internet
Infrastructure
Review

Feb.2024
Vol. 61

Periodic Observation Report

Internet Trends as Seen from IIJ Infrastructure—2023

Focused Research (1)

The Latest SIM Developments—Evolving from Hardware to Software Profiles

Focused Research (2)

IIJ and the Evolution of Security —Commemorating 30 Years

IIJ
Internet Initiative Japan

Internet Infrastructure Review

February 2024 Vol.61

Executive Summary

In this final IIR issue for 2023 (Vol. 61), I would like to reflect on the year that has been.

Generative AI was, without a doubt, a massive topic for the Internet and for IT in general in 2023. The rate at which generative AI is evolving and percolating through society is startling. At the same time as it inspires hope for the huge promise it offers, it also evokes a certain fear. Ethics and governance as they relate to the correct and proper use of this technology that we call AI will no doubt become increasingly important ahead.

On the governance front, the 18th annual meeting of the IGF was held in Japan in 2023. The issue of AI certainly did come up, but the 10,000-odd stakeholders from 178 countries also discussed such broad-ranging issues as Internet fragmentation and cybersecurity.

The Internet is now part of our social infrastructure, and as such it cannot be divorced from the issue of economic security. In Japan, preparations are underway for the Economic Security Promotion Act to take effect in 2024. As a provider of core infrastructure, the telecommunications sector has a key role to play in ensuring this security.

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.

Our periodic observation report in Chapter 1 presents our look at Internet trends as seen from IIJ's infrastructure. Every year, we present trend analyses based on data related to BGP and routes, DNS query analysis, and IPv6 traffic obtained from IIJ's servers and other equipment. The figures all indicate that the broad-based rollout of IPv6 is progressing well. IPv6 support on smart devices is one of the driving forces behind IPv6 uptake, and the high IPv6-enabled rates of US manufacturers leave quite an impression.

In our focused research report in Chapter 2, titled "The Latest SIM Developments—Evolving from Hardware to Software Profiles", we take another look at the SIM (Subscriber Identity Module) technology used in mobile phones. The report gives some background to the development of GSM standards and the birth of SIM cards, covers the history of SIM card miniaturization, and looks at developments that took us from physical SIM cards to virtual SIM technologies like eSIM. Against that backdrop, the report also describes solutions developed by IIJ and the future outlook for standards in this area.

The focused research report in Chapter 3 continues our series commemorating IIJ's 30-year history, this time with a look at security. IIJ regards attack safeguards as vital for anyone using the Internet and began providing firewall-based protection as a service immediately after launching its own Internet connectivity services. IIJ's security business differs considerably from that of other security providers in that IIJ runs it as a company that is also involved in Internet operations and not just as a narrowly focused security specialist. The article looks at how IIJ has thought about and dealt with the issue of Internet security over the past 30 years.

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's MVNO Council, stepping down from that post in May 2023. In June 2021, he also became a vice-chairman of the association.

1. Periodic Observation Report

Internet Trends as Seen from IIJ Infrastructure —2023

Internet services provider IIJ operates some of the largest network and server infrastructure in Japan. Here, we report on Internet trends over the past year based on information obtained through the operation of this infrastructure. In particular, we analyze changes in trends from the perspective of BGP routes, DNS query analysis, IPv6, and mobile.

Topic 1

BGP and Routes

We start by looking at IPv4 full-route information advertised by our network to other organizations (Table 1) and the number of unique IPv4 addresses contained in the IPv4 full-route information (Table 3).

The number of routes increased by only 14,000 over the year, the smallest increase since we started this periodic observation report. That growth has remained in a downtrend since peaking in 2018 (see Figure 1), and it looks like the total might not reach the one-million milestone. We observed declines in the number of /20 and /21 routes for the first time this year. The number of routes with /13 – /18 prefixes is falling, and the increase in /22 – /24 routes was only a third of last year's figure, as a result of which the number of unique IPv4 addresses fell by close to 13 million (0.4%).

Next, we look at IPv6 full-route information (Table 2) and the number of unique IPv6 /64 blocks in the IPv6 full-route information (Table 3).

The total number of routes grew by about the same as last year, reaching roughly 180,000. While growth in the number of short-prefix routes was small, 60% of the growth (including other routes) was accounted for by routes without any information on shorter prefixes, which adds to the number of unique address blocks, and as such

Table 1: Number of Routes by Prefix Length for Full IPv4 Routes

Date	/8	/9	/10	/11	/12	/13	/14	/15	/16	/17	/18	/19	/20	/21	/22	/23	/24	total
Sep. 2014	16	12	30	90	261	500	983	1702	13009	7013	11659	24527	35175	37560	54065	47372	268660	502634
Sep. 2015	18	13	36	96	261	500	999	1731	12863	7190	12317	25485	35904	38572	60900	52904	301381	551170
Sep. 2016	16	13	36	101	267	515	1050	1767	13106	7782	12917	25229	38459	40066	67270	58965	335884	603443
Sep. 2017	15	13	36	104	284	552	1047	1861	13391	7619	13385	24672	38704	41630	78779	64549	367474	654115
Sep. 2018	14	11	36	99	292	567	1094	1891	13325	7906	13771	25307	39408	45578	88476	72030	400488	710293
Sep. 2019	10	11	37	98	288	573	1142	1914	13243	7999	13730	25531	40128	47248	95983	77581	438926	764442
Sep. 2020	9	11	39	100	286	576	1172	1932	13438	8251	14003	25800	40821	49108	101799	84773	473899	816017
Sep. 2021	16	13	41	101	303	589	1191	2007	13408	8231	13934	25276	41915	50664	106763	91436	497703	853591
Sep. 2022	16	13	39	101	298	592	1208	2064	13502	8292	13909	25051	43972	52203	109071	96909	536520	903760
Sep. 2023	16	14	39	102	298	577	1196	2064	13490	8245	13809	25059	43863	51012	109514	98178	550621	918097

Table 2: Number of Routes by Prefix Length for Full IPv6 Routes

Date	/16-/28	/29	/30-/31	/32	/33-/39	/40	/41-/43	/44	/45-/47	/48	total
Sep. 2014	134	481	133	6025	1447	825	248	709	592	7949	18543
Sep. 2015	142	771	168	6846	1808	1150	386	990	648	10570	23479
Sep. 2016	153	1294	216	8110	3092	1445	371	1492	1006	14291	31470
Sep. 2017	158	1757	256	9089	3588	2117	580	1999	1983	18347	39874
Sep. 2018	168	2279	328	10897	4828	2940	906	4015	2270	24616	53247
Sep. 2019	192	2671	606	12664	6914	3870	1566	4590	4165	34224	71462
Sep. 2020	205	3164	641	14520	9063	4815	2663	5501	4562	45160	90294
Sep. 2021	223	3628	705	20650	13050	10233	4170	11545	5204	61024	130432
Sep. 2022	298	4247	895	21926	15147	12509	4108	13840	6994	73244	153208
Sep. 2023	316	4357	923	23228	17427	14828	5518	16453	9579	86881	179510

the number of unique /64 blocks increased sharply, rising another 30% over the previous year. The IPv6 rollout and expansion of IPv6 networks is evidently progressing nicely.

Lastly, let's also look at IPv4/IPv6 full-route Origin AS figures (Table 4). In the past year, an additional 2048 32-bit only ASNs were allocated to APNIC, and 3072 to RIPE NCC.

The decrease in 16-bit Origin ASNs was again smaller than in the previous year. The number of 32-bit-only Origin ASNs also fell heavily, but this reflects many of the IPv6-only ASes, which saw a huge increase in the APNIC region last year, no longer appearing in the route information. Routes that were advertised by those ASes are now generally being advertised by different ASes thought to be the same organization, so we surmise that these organizations have consolidated IPv6 routes advertisements that were temporarily coming from a different AS.

The number of IPv4＋IPv6 32-bit-only ASes exceeded the number of 16-bit ASes for the first time. We also observed the first decrease in 32-bit-only ASes, and we will be watching the data next year closely to see whether a dual-stack configuration is to become the mainstream going forward, at least for new ASes.

Table 3: Total Number of Unique IPv4 Addresses in Full IPv4 Routes and Total Number of Unique IPv6 /64 Blocks in Full IPv6 Routes

Date	No. of IPv4 addresses	No. of IPv6 /64 blocks
Sep. 2014	2,705,751,040	62,266,023,358
Sep. 2015	2,791,345,920	31,850,122,325
Sep. 2016	2,824,538,880	26,432,856,889
Sep. 2017	2,852,547,328	64,637,990,711
Sep. 2018	2,855,087,616	258,467,083,995
Sep. 2019	2,834,175,488	343,997,218,383
Sep. 2020	2,850,284,544	439,850,692,844
Sep. 2021	3,036,707,072	461,117,856,035
Sep. 2022	3,068,374,784	532,578,391,219
Sep. 2023	3,055,604,992	700,359,397,494

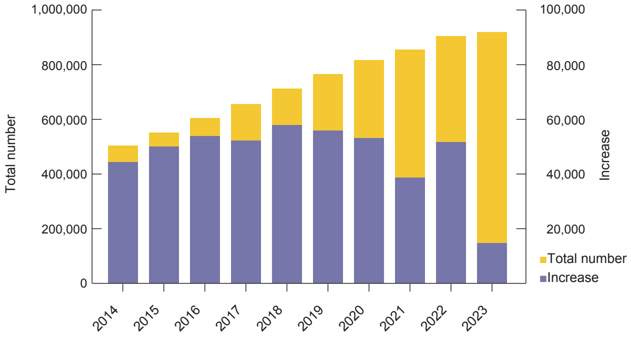


Figure 1: Total Number of Full IPv4 Routes and Annual Increases

Table 4: IPv4/IPv6 Full-Route Origin AS Numbers

ASN	16-bit(1-64495)					32-bit only(131072-4199999999)				
Advertised route	IPv4+IPv6	IPv4 only	IPv6 only	total	(IPv6 -enabled)	IPv4+IPv6	IPv4 only	IPv6 only	total	(IPv6 -enabled)
Sep. 2014	7405	34555	128	42088	(17.9%)	868	4749	55	5672	(16.3%)
Sep. 2015	8228	34544	137	42909	(19.5%)	1424	6801	78	8303	(18.1%)
Sep. 2016	9116	33555	158	42829	(21.7%)	2406	9391	146	11943	(21.4%)
Sep. 2017	9603	32731	181	42515	(23.0%)	3214	12379	207	15800	(21.7%)
Sep. 2018	10199	31960	176	42335	(24.5%)	4379	14874	308	19561	(24.0%)
Sep. 2019	10642	31164	206	42012	(25.8%)	5790	17409	432	23631	(26.3%)
Sep. 2020	11107	30374	229	41710	(27.2%)	7653	19668	574	27895	(29.5%)
Sep. 2021	11465	29219	302	40986	(28.7%)	9514	21108	5242	35864	(41.1%)
Sep. 2022	11613	28398	369	40380	(29.7%)	10816	22211	5764	38791	(42.7%)
Sep. 2023	11770	27617	460	39847	(30.7%)	12640	22128	2067	36835	(39.9%)

Topic 2

DNS Query Analysis

IIJ provides a full resolver to enable DNS name resolution for its users. Here, we discuss the state of name resolution, and analyze and reflect upon data from servers provided mainly for consumer services, based on a day's worth of full resolver observational data obtained on October 18, 2023.

The full resolver provides a name resolution function that replies to DNS queries from user devices. Specifically, to resolve a name, it starts by looking at the IP address of an authoritative name server for the root zone (the highest level zone), which it queries, and then goes through other authoritative nameservers to find the records it needs. Queries repeatedly sent to the full resolver can result in increased load and delays, so the information obtained is cached, and when the same query is received again, the response is sent from the cache. Recently, DNS-related functions are implemented on devices that lie on route paths, such as consumer-level routers and firewalls, and these devices are sometimes also involved in relaying DNS queries and applying control policies. Some applications, such as Web browsers, also have their own implementations of name resolver functionality and in some cases resolve names based on a policy that differs from the OS settings.

ISPs notify users of the IP address of full resolvers via various protocols, including PPP, DHCP, RA, and PCO, depending on the connection type, and they enable automatic configuration of which full resolver to use for name resolution on user devices. ISPs can notify users of multiple full resolvers, and users can specify which full resolver to use by altering settings in their OS, browser, or elsewhere. When more than one full resolver is configured on a device, which one ends up being used depends on the device's implementation or the application, so any given full resolver is not aware of how many queries a user is sending in total. When running full resolvers, therefore, this means that you need to keep track of query trends and always try to keep some processing power in reserve because changes in behavior or status on the user end can conceivably result in a sudden increase in queries to a given resolver.

Observational data on the full resolver provided by IIJ show fluctuations in user query volume throughout the day, with volume hitting a daily trough of about 0.15 queries/sec per source IP address at around 3:10 a.m., and a peak of about 0.36 queries/sec per source IP address at around 10:05 p.m. Overall volume was up 0.02pt vs. the previous year. The peak growth rate looks to have slowed a bit vs. 2022, but the uptrend is ongoing. The breakdown shows that IPv4 accounted for around 60% of queries and IPv6 for around 40%, pretty much the same pattern as in 2022.

Recent years have seen a tendency for queries to rise briefly at certain round-number times, such as on the hour marks in the morning. The number of query sources also increases, with a particularly noticeable pattern around 6 a.m. and 7 a.m., which is possibly due to tasks scheduled on user devices and increases in automated network access that occur when devices are activated by, for example, an alarm clock function. There are also increases in query volume at 14 and 9 seconds before each hour mark. Mirroring the pattern seen in recent years, query volume rises sharply at the hour mark and then tapers off gradually, but with the sudden spikes that occur ahead of the hour mark, query volume quickly returns to roughly where it had been. Hence, because a large number of devices are sending queries in almost perfect sync, we surmise that lightweight, quickly completed tasks of some sort are being executed. For example, there are mechanisms for completing basic tasks, such as connectivity tests or time synchronization, before bringing a device fully out of sleep mode, and we posit that the queries used for these tasks are behind the spikes.

Turning to protocols, UDP accounted for almost all (98.581%) of the queries. That said, TCP queries have been rising over the last few years, from 0.189% of total in 2021 to 0.812% in 2022 and 1.419% in 2023. Possibly the main driver of this is an increase in queries using DNS over TLS (DoT). DoT basically uses TCP port 853 to send queries, so an increase in the use of DoT results in an increase in TCP queries.

Looking at the query record types, A records that query the IPv4 address corresponding to the host name, AAAA records that query IPv6 addresses, and HTTPS records used to resolve Web services account for 96% of the total. The trends in A and AAAA queries differ by IP protocol, with more AAAA record queries being seen for IPv6-based queries. Of IPv4- based queries, around 57% are A record queries and 17% AAAA record queries (Figure 2). With IPv6-based queries, meanwhile, AAAA record queries account for a higher share of the total, with around 38% being A record and 35% being AAAA record queries (Figure 3). Compared with the previous year, we observe 3-percentage-point drops in A record queries for both IPv4 and IPv6. HTTPS records, which we started to see in 2020, accounted for some 20% of IPv4 and 24% of IPv6 queries, marking steady increases of 5 percentage points for IPv4 and 3 percentage points for IPv6. In the IPv4 space in particular, HTTPS records are being queried more often than AAAA records, from which we can infer that there are more implementations that support HTTPS records. SVCB records, which we started to see last year, accounted for 0.26% for IPv4 and 0.60% for IPv6 queries, and while still only a small fraction of the total, those queries are increasing steadily. This may be attributable to the progressing implementation of Discovery of Designated Resolvers (DDR), a newly proposed protocol designed to allow clients to detect encryption-capable full resolvers.

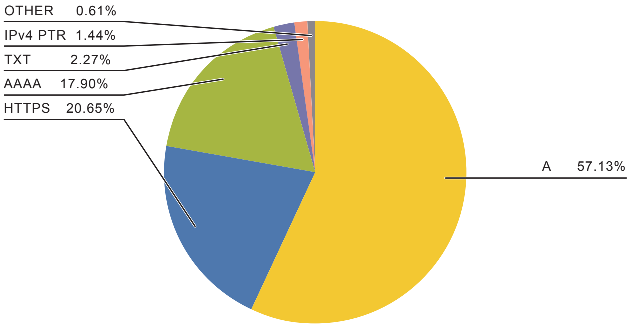


Figure 2: IPv4-based Queries from Clients

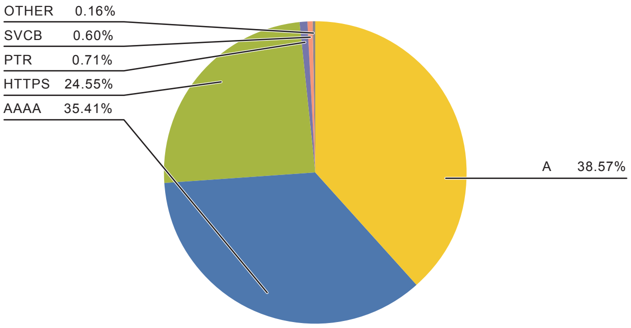


Figure 3: IPv6-based Queries from Clients

Topic 3

IPv6

In this section, we again report on the volume of IPv6 traffic on the IIJ backbone, source ASNs, and the main protocols used. Also in this edition, we go over the state of IPv6 connections on mobile services by device OS, which we also covered last year and back in 2019.

■ Traffic

Figure 4 shows traffic measured using IIJ backbone routers at core POPs (points of presence—3 in Tokyo, 2 in Osaka, 2 in Nagoya). The data cover the eight months from February 2 to September 30, 2023. In 2023, Covid-19 was downgraded to a Class 5 infectious disease in Japan, and social and economic activity is starting to resemble what it was pre-pandemic, but the data on Internet traffic volumes during the period show IPv6 remaining flat and IPv4 increasing only slightly. Yet both IPv6 and IPv4 traffic appear to be increasing to an extent when viewed alongside figures for the same day of the previous year (lighter lines on the graph).

Figure 5 graphs traffic indexed to 100 as of February 1, 2023. As noted, traffic volumes remained mostly flat from the start of the year with no major changes throughout.

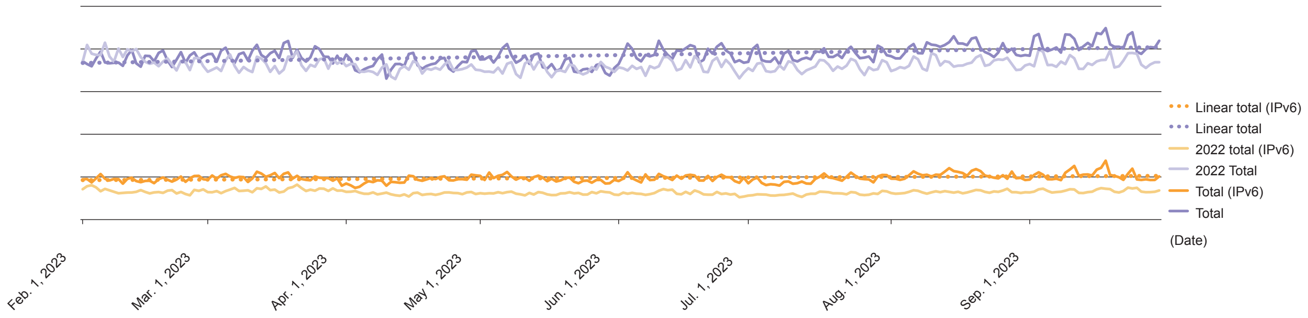


Figure 4: Traffic Measured on Backbone Routes at IIJ's Core POPs

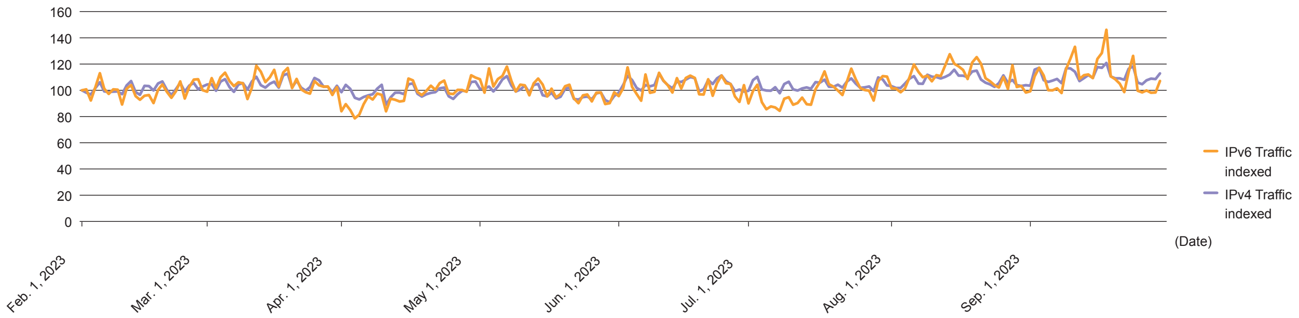


Figure 5: Traffic Indexed to 100 as of February 1

Next, Figure 6 shows IPv6 as a proportion of total traffic. This moves between a minimum of 17% and a maximum of 23%. White no major trends are discernible, the figures are roughly 5 points above the year-earlier level, indicating that IPv6 traffic is growing.

Table 5 tracks the IPv6 ratio over the past six years. We showed this dataset last year as well, but we have discovered that the 2021 and 2022 figures we presented were in error. We offer our apologies and correct them in this edition.

Traffic Source Organization (BGP AS)

Next, Figures 7 and 8 show the top annual average IPv6 and IPv4 traffic source organizations (BGP AS Number) for February 1 – September 30, 2023.

Traffic within IIJ accounts for around 60% of the total. Excluding that, Company A, a major Japanese content provider came in at No. 1, as was the case in IIR Vol. 57 (https://www.iij.ad.jp/en/dev/iir/057.html). At No. 2 with about the same share was Company B, a major US search provider, while at No. 3, Company C made its first

Table 5: IPv6 as a Proportion of Total Traffic Over the Past 6 Years

	2017年 IIR Vol.37	IIR Vol. 41, 2019	IIR Vol. 45, 2020	IIR Vol. 49, 2021	IIR Vol. 53, 2022	IIR Vol. 57, 2023	IIR Vol. 61, 2024
IPv6 ratio	4%	6&	10%	10%	~~16%~~ **11.2%**	~~17.8%~~ **15.1%**	20.1%

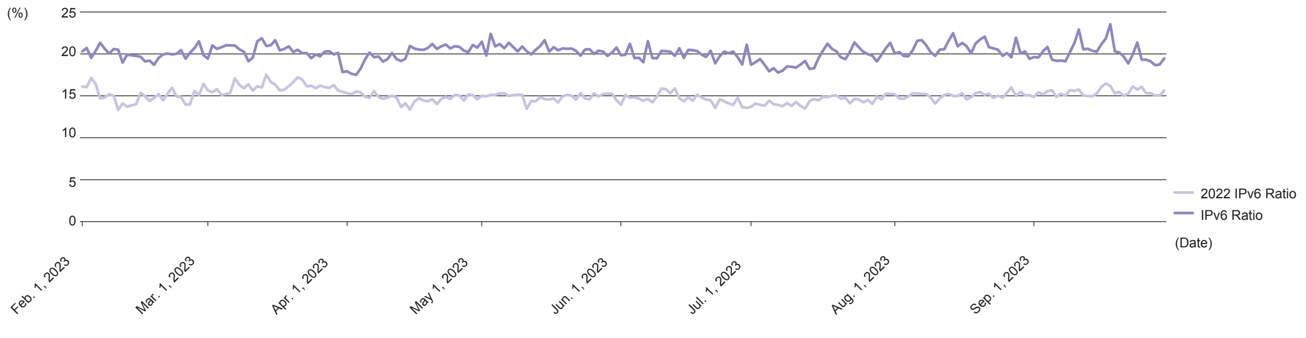


Figure 6: IPv6 as a Proportion of Total Traffic

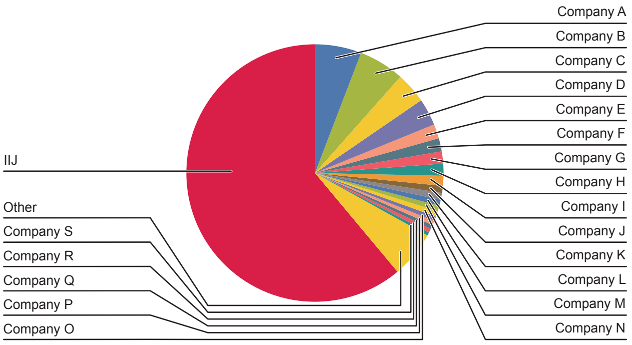


Figure 7: Annual Average IPv6 Traffic by Source Organization (BGP AS Number)

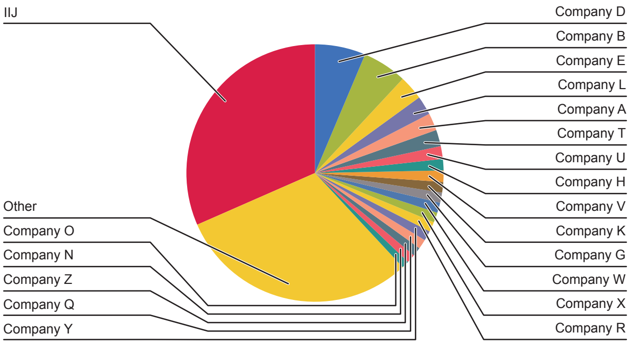


Figure 8: Annual Average IPv4 Traffic by Source Organization (BGP AS Number)

appearance in the rankings. The biggest movers were Company H, a US cloud operator, which went from No. 16 to No. 8 and Company M, a US CDN, which went from No. 5 to No. 13. Company M had an acquisition last year and so may be reorganizing its network.

Protocols Used

Figure 9 plots IPv6 traffic according to protocol number (Next Header) and source port number, and Figure 10 plots IPv4 traffic according to protocol number and source port number (for the week of Monday, October 2 – Sunday, October 8, 2023).

In the IPv6 space, TCP80 (HTTP) moved from 4th last year into 5th this time around, switching places with ESP (IPSec), possibly a sign of progressing migration to HTTPS and QUIC. Traffic volumes for 6th place and below are small, and the rankings can be expected to shift around a lot depending on the time period chosen.

An interesting point to note on the graph is the change in traffic volume from around 7:00 p.m. to around 10:00 p.m. on October 8, corresponding to the peak at the far right of Figure 9. A considerable increase for TCP443 (HTTPS) is evident. A quick investigation reveals that this coincides with a match between Japan and Argentina in the 2023 Rugby World Cup in France, and a Volleyball World Cup match between Japan and the US, which also served as a qualifier for the Paris Olympics. We don't know which match had the biggest impact, but it does feel like streaming over IPv6 is becoming commonplace.

IPv6 on Mobile Devices

Following on from IIR Vol. 57 (https://www.iij.ad.jp/en/dev/iir/057.html), we again look at IPv6-enabled rates on personal mobile service (IIJmio Mobile Service) connections. In addition to differences by device OS, in this edition we also look at whether there are differences depending on device manufacturer.

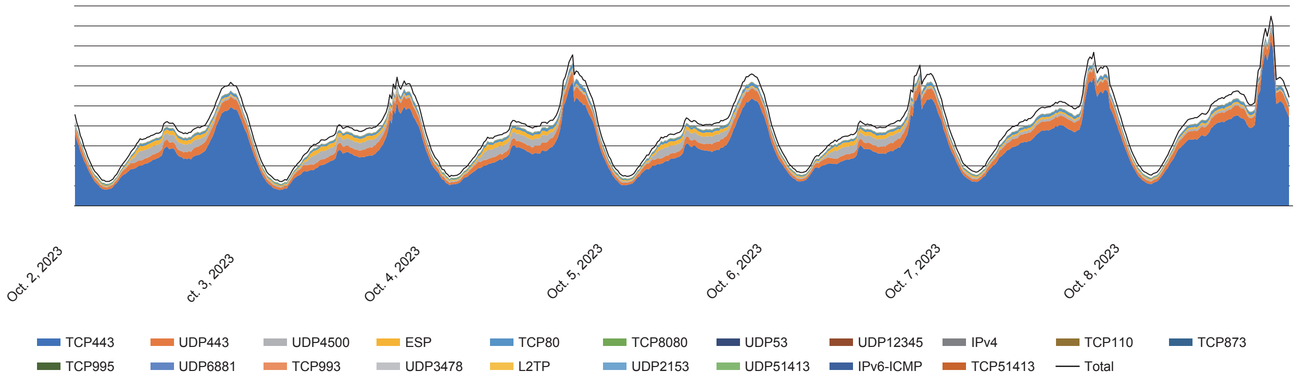


Figure 9: Breakdown of IPv6 Traffic by Source Port Number

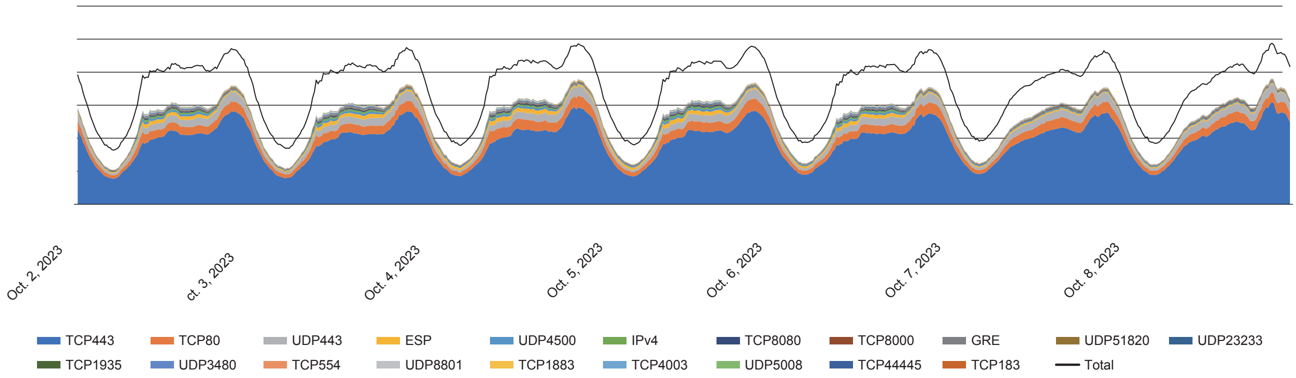


Figure 10: Breakdown of IPv4 Traffic by Source Port Number

In last year's survey, IPv6-enabled connections accounted for the majority at 56.3% of total. As of 3:30 p.m. on Friday, October 20, 2023, that figure was up slightly (2.43 points) to 58.73%. Comparing Apple iOS and Android, IPv6 was enabled on 86.37% of Apple iOS connections, a slight increase of 0.67 points vs. last year, while IPv6 was enabled on 25.82% of Android connections, a 4.12-point increase vs. last year.

Next, we look at IPv6-enabled rates by manufacturer for the top 20 devices connected to the IIJmio Mobile Service. Figure 11 graphs the top 20 spots, but because the top-ranked Apple is so far ahead of the pack in terms of connection count, the lower-ranked bar-graph entries are, unfortunately, difficult to make out. We cannot provide specific numbers, but Apple devices account for 54.3% of IIJmio connections and thus single-handedly take an absolute majority. The IPv6-enabled rate for Apple devices was up slightly vs. the previous survey (85.7%) to 86.35%.

In 2nd place, trailing 1st by a large margin, is a Sharp device. Unfortunately, only 2.73% of these devices had IPv6 enabled, suggesting that IPv6 is not enabled by default in the device's APN profile. On Android devices, the PDP-Type in the APN configuration can be set to IPv4, IPv6, or IPv4v6, but most users probably stick with the default setting or use automatic APN configuration, so we imagine that the IPv6-enabled rates vary greatly depending on the factory default settings.

For 3rd place and below, we only look at manufacturers with high IPv6-enabled rates. Google, in 3rd place, has an extremely high IPv6-enabled rate (89.63%), higher even than Apple's. Motorola, in 7th, also exceeds Apple in this regard with a reading of 89.12%.

Sony and Sony Mobile appear in 10th, 11th, 12th, and 17th place. If these were combined, Sony would leapfrog Huawei to come in at 5th place. Sony's overall IPv6-enabled rate would be 14.7% in this case, which, while not all that high, would be at the high end among Japanese manufacturers.

From an overall perspective, the US manufacturers have high IPv6-enabled rates, while manufacturers from Japan, China, and so forth tend to have low IPv6-enabled rates.

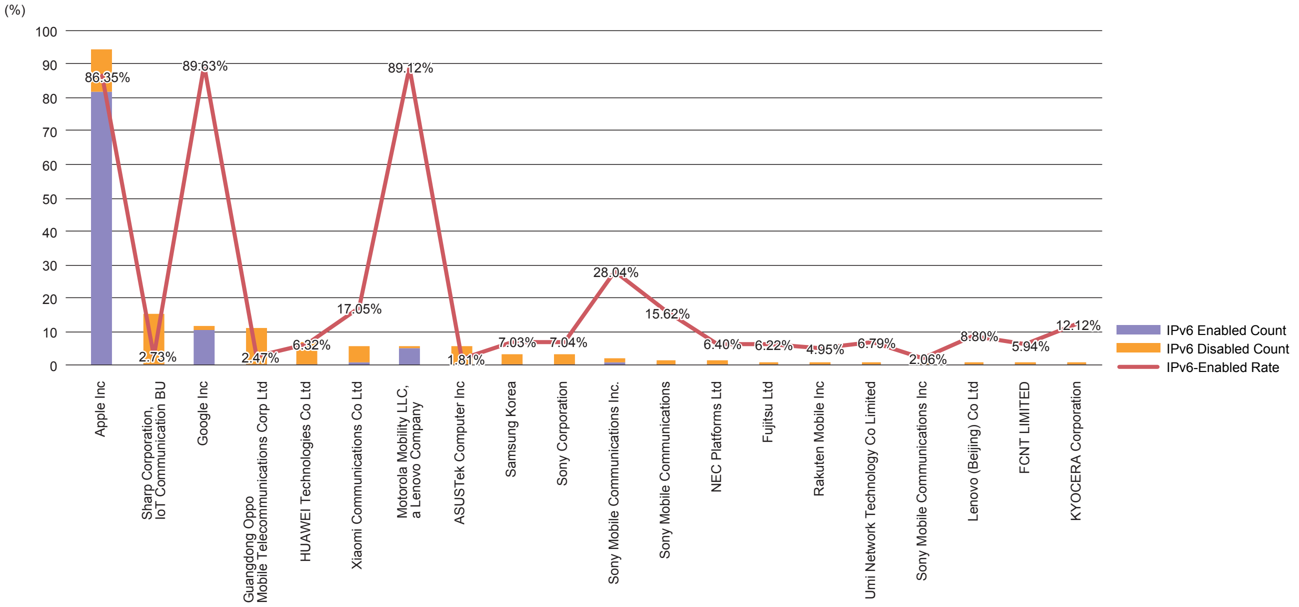


Figure 11: IPv6 Support by Manufacturer (Top 20)

Summary

We have examined traffic on the IIJ backbone core, source ASNs, and main protocols used. Although traffic volumes were range-bound throughout the year, they were up vs. the previous year, and IPv6 usage rates increased over year-earlier levels, reaching their highest point in the past seven years. While it may not be clear because we do not provide names for the origin ASes, we observed growth for some surprising countries. With major CDN operators seemingly having made decent progress on IPv6 support, we appear to be entering an era in which IPv6 is used/enabled pretty much as a matter of course.

Over the past few years (more than a decade?), a lot of services around the world have come to use HTTP(S), including APIs, making it impossible to tell what the app or use case is by looking at the TCP/UDP ports alone. Even so, it seems evident that there is relatively more usage of HTTPS/QUIC over IPv6. One can imagine that with relatively recently built systems, companies are increasingly adopting HTTPS/QUIC and enabling IPv6 along with this too.

In the mobile space, we are seeing IPv6-enabled rates rising on devices running Android OS, but manufacturers in Japan and Asia appear to be lagging those in the US. No doubt there are various reasons for this, but we ask you to consider setting PDP Type to IPv4v6 in your default APN settings so that even more users can get onto IPv6 without any fuss.

We will continue to watch the IPv6 situation from a range of angles and provide updates as new developments come to light.

Topic 4

Mobile 3G, LTE (Including 5G NSA)

Mobile traffic patterns have been affected by the Covid pandemic over the past few years. A key development for Japan in the last year was the May 8, 2023 downgrade of Covid-19 from the “Novel Influenza and Other Diseases” category (or a Class 2 disease) to a Class 5 infectious disease. Here we take a look at traffic over the past year in light of that, based on observations covering October 1, 2022 – September 30, 2023.

Firstly, NTT Docomo will terminate 3G communication services at the end of March 2026, and here we report on the current 3G traffic situation.

3G traffic as a percent of total (Figure 12) is as follows. On consumer services, 3G is virtually nonexistent, accounting for only around 0.033% of all traffic on average. In business services, it averages 4.25% of total. 3G’s share of business

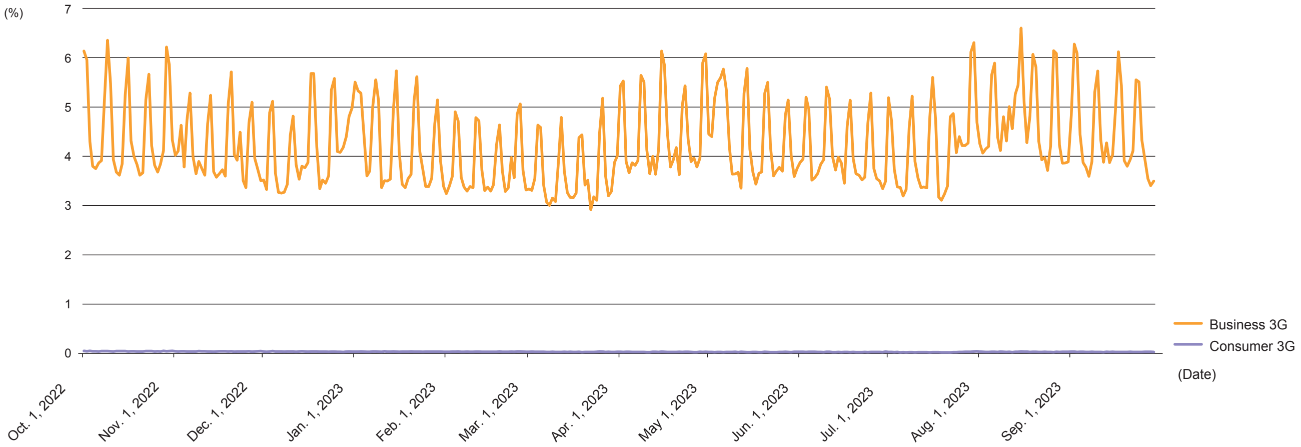


Figure 12:3G Communications as a Proportion of Total Traffic

services traffic remains pretty much range bound, so the degree to which 3G traffic on business services declines over the remaining two years will certainly bear watching.

Next, we look at traffic and session counts on business services. Here, we graph traffic volume (Figure 13) and session counts (Figure 14) for business services indexed to October 1, 2022.

First we look at traffic volumes. LTE traffic volume remained in a gradual uptrend throughout the year, with that uptrend going through slight acceleration spurts from April 2023 and July 2023. This likely reflects the consolidation of contact points with carriers facilitating better traffic flows outside of peak periods and thus leading to more streamlined usage. When we reported on 3G traffic last year, it was in decline, but it has been in a gradual uptrend over

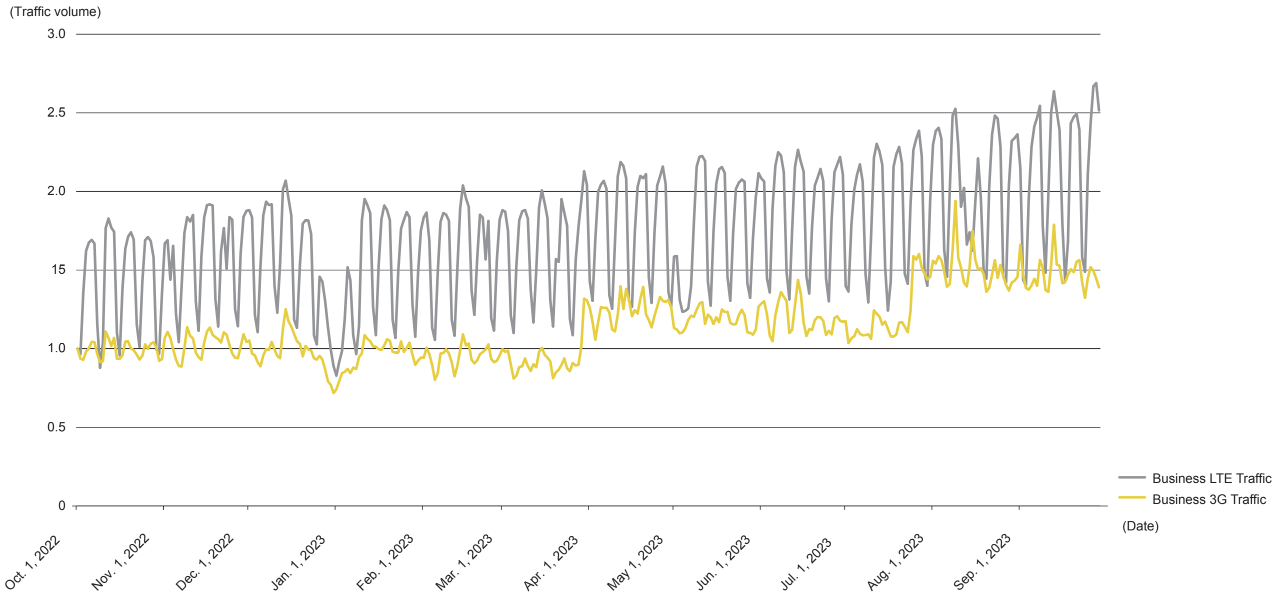


Figure 13:Traffic Volume on Business Services

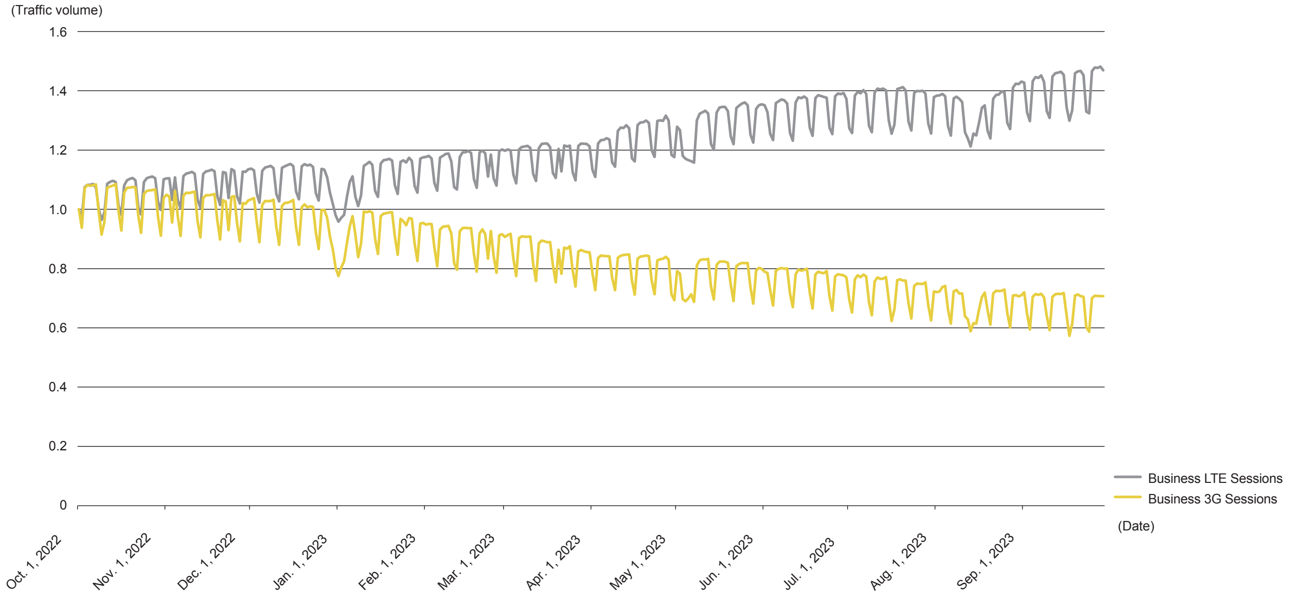


Figure 14:Session Counts on Business Services

the past year. Like LTE traffic volume, 3G traffic also saw spurts of acceleration from April 2023 and July 2023. This also likely reflects the effects of consolidating carrier contact points.

Looking at session counts, we see that, similar to traffic volume, LTE session count remained in a gradual uptrend throughout the year, with somewhat larger increases in both April 2023 and May 2023. This period is prone to

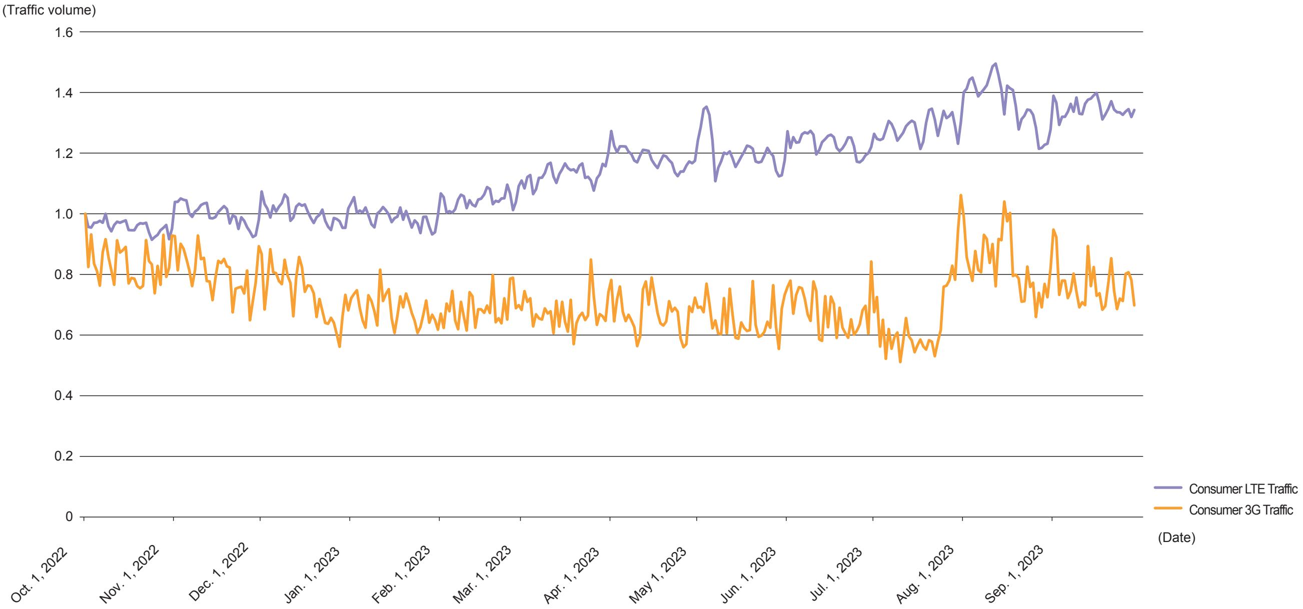


Figure 15: Traffic Volume on Consumer Services

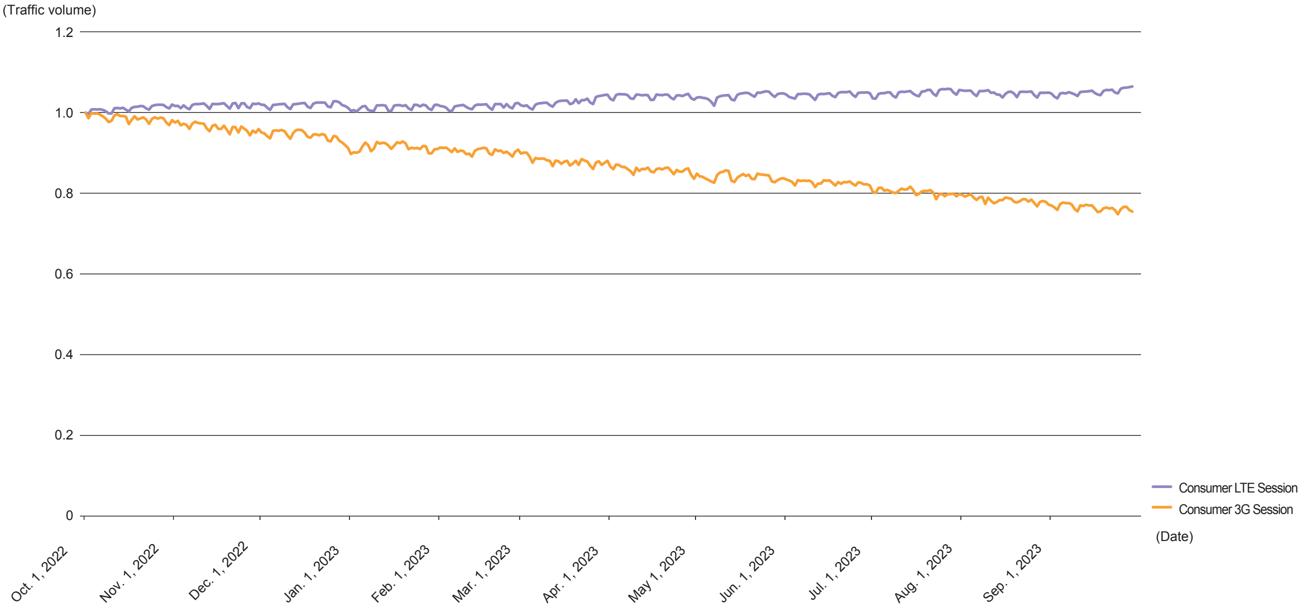


Figure 16: Session Counts on Consumer Services

change as it coincides with the start of the fiscal year for many Japanese companies, but in 2023, it is possible that a change in corporate workstyles due to the reclassification of Covid-19 may have driven increased use of mobile services. The 3G session count, in contrast to 3G traffic volume, remains in an intermittent decline and fell by around 30%. The decline in session count suggests that the 3G exodus is progressing, but we will continue striving to ensure service stability while keeping tabs on these data.

Next, we look at traffic and session counts on consumer services. Here, we graph traffic volume (Figure 15) and session counts (Figure 16) for consumer services indexed to October 1, 2022.

As mentioned, LTE accounts for almost all traffic related to consumer services, and as such, we focus on trends in LTE traffic here. We note no standout changes in consumer services traffic through February 2023, with traffic volumes remaining at around the same level since October 2022. Owing to the timing of consumer service coupon handouts, traffic volumes were high at the beginning of the month and then tended to decline toward the end of the month, rising again at the start of the following month. This monthly trend continued to repeat itself and was prominent up to around February 2023. The trend subsequently changed, with traffic volume then moving into an ongoing uptrend. This is likely due to the effects of the consolidation of carrier contact points, as mentioned earlier. Traffic volume also increased briefly during Japan’s Golden Week holiday period, around the time of May 1, 2023, which is consistent with the usual annual pattern. And traffic volume increased substantially from the end of July 2023 onward, which, again, we think is likely due to the consolidation of carrier contact points. There was, similarly, a considerable effect on 3G communications as well.

The session count data indicate a moderate rise in LTE throughout the year. Meanwhile, 3G has seen an intermittent decline, over the year falling to 80% of its October 1, 2022 level. While we do not disclose specific data here, the absolute numbers indicate that we are on track for the discontinuation of 3G.

1.BGP and Routes
Tomohiko Kurahashi
Technology Development Section, Operation Technology Department, Infrastructure Engineering Division, IIJ

2.DNS Query Analysis
Yoshinobu Matsuzaki
Technology Development Section, Operation Technology Department, Infrastructure Engineering Division, IIJ

3.IPv6
Taisuke Sasaki
Mobile Technology Department, Infrastructure Engineering Division, IIJ

4.Mobile 3G, LTE (Including 5G NSA)
Tsuyoshi Saito
General Manager, Mobile Technology Department, Infrastructure Engineering Division, IIJ

The Latest SIM Developments —Evolving from Hardware to Software Profiles

2.1 SIM

2.1.1 The Advent of SIM Cards in Mobile Phone Systems

These days, we're all familiar with the concept of using SIM (Subscriber Identity Module) cards in our now quite affordable mobile phones. Anyone can swap or replace a SIM card with ease. We take them for granted now, yet they were not born at the same time as the mobile phone. Early mobile phones only supported "embedded" communications standards whereby the subscription parameters were hard-coded into device memory. The earliest analog standards like NMT-450 had no security features, which meant you could clone a mobile phone by copying the subscription parameters to another device. A well-known example of this in the wild from Japan is that of cloned pagers, which made it possible to broadcast messages to dozens of pagers using a single-device contract.

The first means of security came just a little bit later in the form of the SIS (Subscriber Identity Security) code, an 18-digit number unique to each device and hard-coded into the device's application processor. To prevent the same SIS code from being used on multiple devices, it was distributed evenly to carriers. The processor also stored a seven-digit RID code that subscribers send to the base station when registering with a mobile phone network. The SIS codes were distributed evenly among carriers so that no two devices could share the same SIS code. The processor also stored a 7-digit RID code which was transmitted to a base station when a subscriber registered to a mobile network.

The SIS processor would use a random number generated by the base station paired with a unique SIS response to generate the authorization key. Both the keys and numbers were relatively short but quite adequate by 1994 standards, but, as you can probably imagine, this system was later cracked. Three years later came the GSM (Global System for Mobile Communications) standard. This was quite similar to SIS, but it was more secure because it used a cryptographically stronger authorization system. Under communications standards from this point on, subscriber management on the device end thus became "detached." "Detached" meant that subscriber authorization all happened on an external processor integrated into a tiny computer completely separate from the mobile device. The resulting solution was the smart card-based SIM.

The arrival of SIM cards meant that (in theory) subscriptions were no longer device-dependent. This opened the door for device manufacturers to make mobile devices that would work on any carrier's system, facilitating mass production-driven cost reductions. It also meant that mobile users could change devices whenever and as often as they liked while keeping the same mobile identity.

SIM cards are basically based on ISO 7816 smart cards and are virtually the same as other contact IC (integrated circuit) cards like credit cards and cash cards. Indeed, the first SIM cards were the same size as credit cards, but as mobile phones became more advanced and the internal parts and components were increasingly miniaturized, SIM cards also became more compact.

The original full-size 1FF (1st Form Factor) SIM cards would no longer fit into mobile phones of the day, so a simple method of removing the unnecessary part of the card while retaining compatibility was developed. This was the mini-SIM, or 2FF (2nd Form Factor) SIM. Around the time these smaller SIM cards appeared, affordable mobile carriers in the form of MVNOs (Mobile Virtual Network Operators) were also starting to appear in Japan, thus leading to the roll out and widespread use of SIM cards.

SIM cards have continued to shrink with the arrival of the micro-SIM (3FF) and then the nano-SIM (4FF), yet their shape, the electrical contact configuration (pinout), and the features of the embedded IC chips has remained unchanged for around 30 years. To accommodate users who still cherish their old-school mobile phones, plastic SIM adapters are also now available. Even so, a lot of those old devices will not work with modern-day SIM cards even if the device will physically accept the SIM via such an adapter. This is because the earliest SIM cards operated on 5V, whereas the latest SIM cards run on

3V. That is, the processor voltage protection on 3V-only cards prevents them from working on older phones that can only accommodate 5V cards. Dual voltage SIM cards compatible with both 3V and 1.8V are also now becoming commonplace as the need for 1.8V cards rises amid the trend toward lower power consumption in mobile devices.

2.1.2 The Role and Real-world Status of SIM Cards

A SIM card is a small, highly secure, independent computer system detached from (independent of) the device on the mobile phone network system. It stores a dataset called the communications profile represented by an IMSI (International Mobile Subscriber Identity) and a 128-bit key called a Ki (key identifier). The SIM card connects to the mobile phone network system via base stations and is what enables safe and secure encrypted communications. The IMSI contains a Mobile Country Code (MCC) and a Mobile Network Code (MNC). MNCs are allocated to MNOs and full MVNOs.

IIJ Mobile obtained the MNC of 03 in 2018 when it became a full MVNO using the NTT Docomo network. It also obtained issuer number 03 at the same time. Physical cards, as defined by ISO 7816, basically have eight external contacts (pins). The pinout is shown below. The cards usually connect to the mobile device via six contacts: pins 1, 2, 3, 5, 6, and 7 (Figure 1).

An IC called a secure microcontroller is physically embedded within the SIM card's plastic. The IC consists of an MPU, ROM, RAM, and EEPROM—a fairly amazing and capable little system.

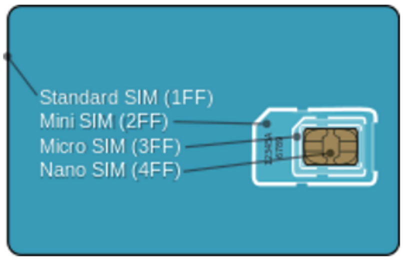
As they are computers, SIMs also have an OS. Many SIMs use an OS based on GlobalPlatform, the OS used in credit cards, which gives them an encrypted file system, the ability to run Java Applets, and both OS- and hardware-based tamper resistance. In terms of software, they have an encryption/decryption engine, as well as a communications profile—the dataset required to function as a SIM. Incidentally, credit card chips store a dataset called the financial profile, necessary for securing credit transactions.

All smart cards, including credit cards, have a unique 19-digit ID called the ICCID. The sequence of digits includes an industry identifier, country code, issuer number, and check digit. IIJ Mobile is able to issue SIM cards because it has obtained an issuer number.

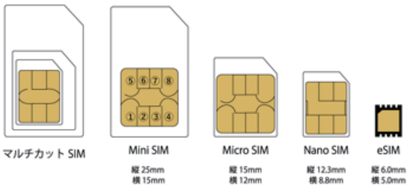
2.2 Toward a World Without Physical SIMs

Until a few years ago, users wishing to subscribe to IIJ's MVNO services online would first have to apply for a service contract, after which we would deliver a physical SIM card to their address, and then their service would only go live once they had inserted that SIM card into their device. The existence of the physical delivery step meant that users had to wait roughly a week before they could start using the service. SIM cards were, in effect, the physical keys used to gain access to mobile services.

A shift is rapidly underway, however, with the rise of eSIM services, which allow virtual SIM data to be downloaded to a device via the Internet, enabling instant access to mobile services. A similar trend is underway in the IoT world, too, whereby SIM data is embedded into cellular communication



Four example SIM card sizes that use the ISO/IEC 7816 interface.



ISO/IEC 7816-2 pinout

Pin #	Name	Description
1	VCC	+5 V or 3.3 V DC
2	Reset	Card Reset (Optional)
3	CLOCK	Card Clock
4	AS	Application Specific
5	GND	Ground
6	VPP	+21 V DC [Programming], or NC
7	I/O	In/Out [Data]
8	AS	Application Specific

Figure 1: The 8-pin Configuration of a SIM Card

modules at the factory before the modules are shipped to the device manufacturer, making it possible to use IoT services without a physical SIM card.

Throughout the evolution of wireless communications from 2G to 3G, 4G, and now 5G, the mobile industry has continued to use physical SIM cards, albeit with SIM card form factors growing ever smaller. Yet we are now approaching a turning point that will mark the end of an era and, with it, the end of the need for physical SIM cards to access mobile services. That era has spanned nearly 30 years and dates all the way back to the time of 2G (GSM) wireless communications. Let's go over the key changes below.

2.2.1 eSIM Support in PCs, Smartphones, Tablets, and Other Consumer Devices

In this article, eSIM refers to the mechanism set out in the Remote SIM Provisioning specification described in SGP.22, a standard put out by the GSMA (GSM Association), an industry association of mobile communications carriers, manufacturers, and the like. The adoption of eSIM makes it possible for users to gain instant access to mobile communications services by subscribing and then immediately downloading SIM data for that service to their mobile device.

Microsoft's Surface Pro LTE Advanced, released in 2017, was the first notebook PC to support eSIM, and all cellular-capable Surface models since then have been equipped with eSIM functionality. This has since fueled the uptake of eSIM functionality in cellular-capable Windows-based PCs from other manufacturers as well.

Support for eSIM has also become standard on many smartphones and tablets, including Apple iPhones and iPads since the 2018 release of the iPhone XS. Support for eSIM has also been available on Android devices since Google's 2018 release of its international-model Pixel 3, and the number of non-Google Android devices supporting eSIM has been increasing since then too. Hence, support for eSIM is becoming the norm in the world of consumer devices, with Apple leading the way.

In a further step in this direction, Apple released an eSIM-only (no physical SIM card slot) version of the iPhone 14 for the North American market in 2022, sending shockwaves around the industry. This is something we are likely to see more of in newly launched devices globally. We are moving headlong into a physical SIM card-free world for consumer devices.

With an eye on this trend, IIJ moved quickly to launch the SGP.22-compliant IIJmio Mobile Service Lite Start Plan (eSIM beta) on July 18, 2019, and has been progressively rolling out eSIM support on its services ever since.

2.2.2 SIMs on Cellular-capable IoT Devices

Unlike consumer handsets, cellular-capable IoT devices typically have a communication module and SIM capable of handling 4G (or the like) built in. IoT device end users often end up using the communication services provided by the IoT device manufacturer without realizing it, and thus do not necessarily enter into separate communications services contracts for their devices. In this scenario, the IoT device manufacturers procure physical SIMs from a mobile operator under contract in advance, and install them into the devices on the production line before shipping them.

Two types of requirements are increasingly coming to the fore in the world of IoT devices.

(1) The need for a physical alternative to SIM cards because either (i) the miniaturization of an IoT device has made it difficult to set aside space for a physical card or (ii) the device use environment is too harsh for an ordinary physical SIM card to withstand

(2) The desire to either (i) decide on which carrier to contract with after the device leaves the factory or (ii) change carriers depending on signal strength available at the device's eventual installed location

To address (1), MFF2, an IC chip form factor standard for smaller physical SIM cards developed by ETSI, a European standards organization, is already in use. In a further step forward, proprietary implementations that embed the SIM functionality into the communication module as software, such as SoftSIM, iSIM, and iUICC, are also coming into use.

Turning to (2), the GSMA released its SGP.02 standard for eSIMs for M2M (machine-to-machine) connections around 2013, before the release of SGP.22, but it has not gained a whole lot of traction in mass-market IoT devices because of the need to use services provided by specific carriers. This has led to people considering proprietary implementations that utilize the SGP.22-based eSIM framework, which is not tied to any specific carrier, and the new SGP.32 standard (which reuses aspects of SGP.22) for IoT released in 2023.

Where (1) is concerned, IIJ began providing MFF2 SIMs in 2019 as well as SoftSIMs combined with a specific communication module. In the case of (2), IIJ is engaged in a number of initiatives and studies, which we will discuss below.

2.2.3 Working Toward a World Without Physical SIMs

We are on the cusp of a physical SIM-free world, and the mobile services business based on the delivery of physical SIMs is approaching a major turning point. I think most people are aware that, from an end-user perspective, the spread of eSIM and other such technologies will make mobile services more convenient. For communications carriers, however, the impending disappearance of important elements like physical SIMs as the key to mobile services could be the writing on the wall if the carriers fail to adopt new technologies and allow themselves to fall behind the times. And as such, we at IIJ continue to carry out technical surveys, research, and development with a view to a physical SIM-free future. The next section focuses on our initiatives for IoT devices, which are a crucial area in particular.

2.3 IIJ Mobile's SIM Cards Applied solutions

Here, we go over a number of IIJ Mobile solutions made possible by rethinking the SIM computer system.

2.3.1 Multi-profile SIM

This solution makes it possible to selectively use multiple SIM cards without imposing a load on the device. Several logical SIM cards are set up on a single physical SIM card, and external instructions (APDU) are used to activate specific internal SIM cards. When multiple SIM sockets are available, this can be achieved by electronically switching access to the SIM socket. This is of course a DSSS (Dual SIM Single Standby) setup. The idea is that, say, two half-thickness SIM cards are stacked and mounted into a SIM socket, and an external command is sent to switch access between the two SIM cards. Functionally, DSSS can work with even a single SIM socket (Figure 2).

2.3.2 SoftSIM

The required elements of a SIM include the MPU, ROM, RAM, I/O, OS, communications profile, encryption/decryption engine, and SIM communication protocol (APDU) implementation. IIJ Mobile's applied solution is SoftSIM.

This solution employs an eSIM-like approach. In simple terms, it uses computer virtualization technology to implement a virtual SIM (computer) in a secure area of the communication module, to which the separately managed communications profile is written OTA (over the air).

2.3.3 LPA-Bridge

It's a bit much to expect IoT devices to have rich UIs and multiple network interfaces like a smartphone, but devices equipped with the sort of sensors, LTE modems, and eSIM chips present in some smartphones can be considered IoT devices. The LPA (Local Profile Assistant, app used to manage eSIM profiles) on a smartphone is normally used to acquire, delete, and select profiles on its own internal eSIM chip. LPA-Bridge can be used to link with such IoT devices and switch the target of the LPA's operations from the phone's internal eSIM chip to the eSIM chip in the IoT device, so that the LPA can manage profiles on the IoT device's eSIM chip as if it were acting on the phone's internal eSIM chip.

This solution makes it possible to use consumer model eSIMs on IoT devices, something that was previously difficult to achieve via software without modifying the standard architecture.

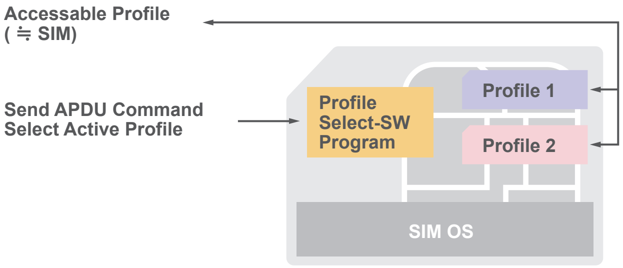


Figure 2: Selectively Using Multiple SIMs

2.4 Changes in eSIM technology Standards and IoT eSIMs

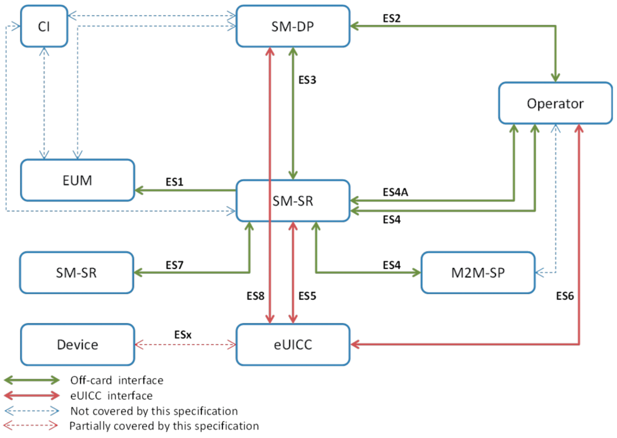
On May 26, 2023, the GSMA released SGP.32, a technical specification for eSIM for IoT devices. SGP.31/32 is the third eSIM specification, following the previously released SGP.01/02, which is for M2M devices, and SGP.21/22, which is for consumer devices. Below, we walk through the changes in eSIM standards leading up to SGP.32 and discuss some key features of the standard.

2.4.1 Road to IoT eSIM Standardization

As the name suggests (eSIM is short for embedded SIM), eSIM is intended to be an implementation of SIM that is embedded directly into a device’s circuit board. Unlike physical SIM cards, eSIMs are difficult to replace once the device is manufactured, so the data that defines the SIM—the profile—is separated out from the hardware, and switching this profile effectively constitutes a SIM replacement. The mechanism for performing operations on the profile remotely is called RSP (Remote SIM Provisioning).

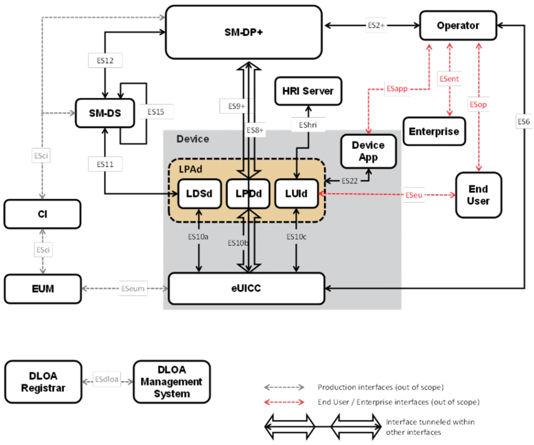
The first specification released was SGP.01/02 for M2M (machine-to-machine) devices (which we’ll call M2M eSIM) (Figure 3). Perhaps because it was assumed that IoT devices would not have much complex functionality, most of the functions are implemented on the SIM, and the device interface is the same as with existing SIM standards. It is, however, a bulky system setup since the server (called the SM-SR) that communicates with the eSIM must be connected to the profile-providing server (called the SM-DP) provided by the carrier. And because SMS is used to trigger remote control, all of the profiles used need to have SMS functionality. SMS requires cellular communications capabilities, so a bootstrap profile is needed to ensure the device can connect to a cellular network in the location it will be deployed. Because the standard necessitates considerable cost outlays to build and operate the system overall, its use seems to be limited to high-priced automobiles and, in particular, the European auto industry, where the eCall system is popular and vehicles often travel across national borders. Speakers at international conferences have presented examples of independent carriers using the specification on smart meters in their country, but our impression is that they have really only used it to distribute their own company’s profiles in the field and that they haven’t been able to take full advantage of M2M eSIM.

The next specification released was SGP.21/22 for consumer devices directly operated by humans (which we’ll call Consumer eSIM) (Figure 4). Because it is designed for devices intended to be directly operated by humans, an app (LPA) for facilitating this was introduced into the specification. Operations are performed via an LPA implemented on the device itself, so SMS (which was needed for remote operations) is no longer required under this standard, and IP is used uniformly for the data transfers used to acquire profiles. The standard also does away with the SM-SR, through which data transfers were relayed under M2M



Source: GSMA SGP.43 v4.3

Figure 3: The M2M eSIM Architecture



Source: GSMA SGP.22 v3.0

Figure 4: The Consumer eSIM Architecture

eSIM. Instead, the device communicates directly with the SM-DP (called the SM-DP+ in Consumer eSIM) provided by the carrier. This allowed for an open market not tied to any particular carriers, which would fuel widespread uptake of the standard. Indeed, once the Apple iPhone XS, for which there is a huge market, added official support for Consumer eSIM in 2018, use of the standard spread rapidly. Beyond Apple's iOS, Microsoft's Windows 10 and Google's Android 10 also came with LPA implementations. This meant that all the major OSes used on notebook PCs, smartphones, and tablets now had eSIM support, and this fostered an ecosystem in which the standard is available on many consumer devices. IIJ launched eSIM services on its full-MVNO platform ahead of its domestic peers in 2019.

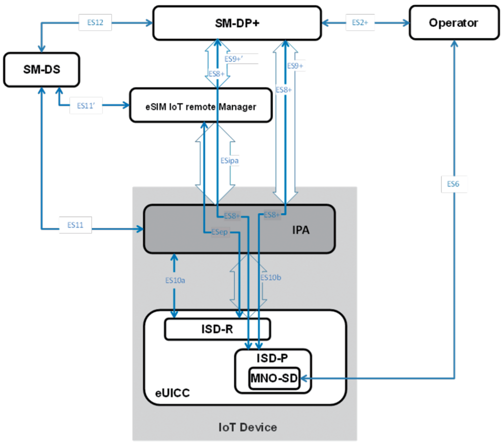
Consumer eSIM is designed for notebook PCs, smartphones, and tablets, but it also defines a mechanism for installing eSIMs on other devices via a smartphone or the like. This mechanism makes it possible to deploy Consumer eSIM on IoT devices that are not directly operated by humans. The GSMA standards, however, only lay out the architecture and do not define inter-device protocols, so at present, vendors implement their own protocols for this. The need to be linked to a smartphone or similar device has also meant that its deployment is limited to wearables like smart watches. It has not really gained much traction in the wider IoT device space. Against that backdrop and with the smartphone market becoming saturated, attention turned to IoT devices as the next target market. Ideally, M2M eSIM should have covered this area, but as discussed, the costs of deploying it can be prohibitive, and Consumer eSIM, meanwhile, requires proprietary protocol implementations to support the remote control features available in M2M eSIM. Hence, there was a need for an eSIM standard for IoT devices (which we'll call IoT eSIM). Development of GSMA standards is not open, and so vendor-hosted seminars and the like are the only way to keep track of what's happening, but from what we have heard, the GSMA began making some progress on the IoT eSIM front from around 2020. Ultimately, the architecture and system requirements (SGP.31) were released in April 2022, and the technical specification (SGP.32) was released in May 2023, thus standardizing the protocol (Figure 5). IoT devices based on this standard are expected to roll into the market ahead, paving the way for eSIM in the IoT device market, where the number of service connections is likely to far outstrip that in the market for consumer operated devices.

2.4.2 Features of the Standard

The IoT eSIM standard is designed to take advantage of the already expansive Consumer eSIM market. It uses the SM-DP+ from Consumer eSIM as the profile-providing server, and it follows Consumer eSIM with respect to the interface for communicating with the eSIM chip. It also adds the functionality necessary to enable remote operations. Because it reuses SM-DP+ from Consumer eSIM, no additional work to support it is required from the perspective of the carrier that provides the profiles.

It differs from Consumer eSIM in that the LPA functionality is divided between a server (called the eIM) and a device app (called the IPA), instead of being implemented entirely on the device. By providing an interface for the user (person operating the eSIM) on the eIM and having the eIM and IPA communicate with each other, it facilitates the remote operation of eSIMs on the device. Since IPA itself does not have a user interface, it has a smaller program footprint than LPA, making it easy to implement even on IoT devices with limited system resources.

The separation of functionality between the eIM and IPA appears to be a pretty flexible design for the purposes of supporting the vast variety of IoT devices out there. One major point is support for functionality called Indirect Profile Download, which makes it possible to communicate with the SM-DP+ via the eIM. The GSMA standard specifications define two methods for communicating between the IPA



Source: GSMA SGP.31 v1.1

Figure 5: The IoT eSIM Architecture

and the SM-DP+: Direct Profile Download (Figure 6) and Indirect Profile Download (Figure 7). With Direct Profile Download, the IPA communicates with the SM-DP+, so there is no need for SM-DP+ address resolution or HTTPS communications. With Indirect Profile Download, meanwhile, the eIM communicates with the SM-DP+, so the IPA itself does not need to perform address resolution or HTTPS communications. The IPA only needs to talk to the eIM.

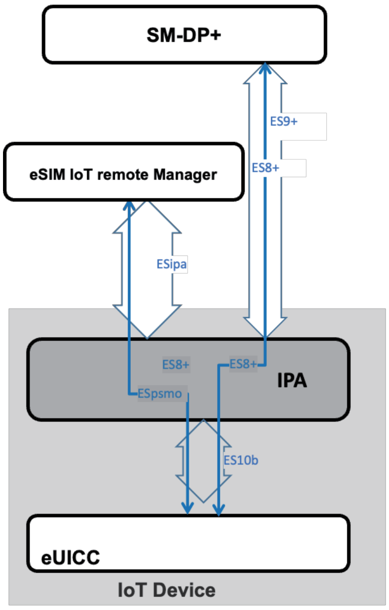
The GSMA standard specifications also define HTTPS and CoAP as the protocols for communication between the IPA and eIM, but any protocol is actually allowed (the appendix describes how to support LwM2M and MQTT), and support for non-IP communications is also considered. Indirect Profile Download makes it possible to use Consumer eSIM, which was designed for IP communications, on non-IP devices without any changes being needed to equipment on the carrier's end. It is possibly set up this way to also be consistent with the M2M eSIM architecture, which allows everything to be done via SMS.

2.4.3 Market Rollout

With Consumer eSIM now widespread, there has been talk in the past few years about IoT devices, particularly wearables, being the next target for eSIMs. While it may spur carriers to seek to increase service connection volumes, the fact that it obviates the need for physical SIM cards means that eSIM holds a lot of promise in the area of wearable devices, where physical space is scarce.

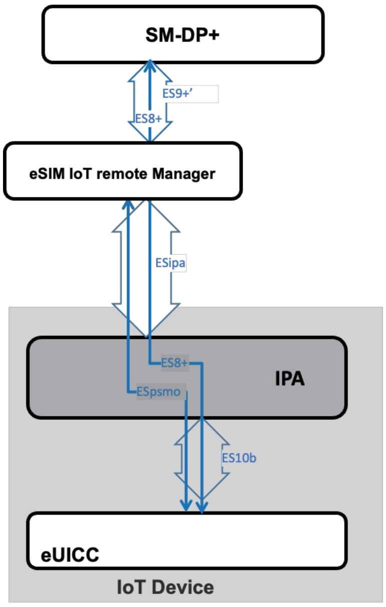
With Consumer eSIM, unlike M2M eSIM, you can simply select any communications carrier that offers Consumer eSIM, and this makes it relatively easy to use such devices even for small-scale rollouts. For manufacturers creating global models of their devices, it also has the benefit of allowing them to add local carrier profiles to the devices post manufacturing.

Challenges to widespread adoption remain, however. While you can use the same profiles as the Consumer eSIM, the issue of what to do about the bootstrap profile remains. The sort of devices that Consumer eSIM targets—laptops, smartphones, tablets, and the like—have non-cellular communications capabilities as well (e.g., Wi-Fi), so it was possible to ignore the bootstrap profile issue. Plus, smart watches and other such devices can communicate via smartphones, which also provides an avenue for installing profiles without a bootstrap profile. On IoT devices, meanwhile, things need to be implemented within resource constraints, so it may not be possible to include non-cellular communications capabilities, in which case a bootstrap



Source: GSMA SGP.31

Figure 6: Direct Profile Download



Source: GSMA SGP.31

Figure 7: Indirect Profile Download

profile is absolutely necessary in order to install the initial profile. Unlike with M2M eSIM, there is no clear bootstrap profile, so using a throwaway profile is fine, but unless the eSIM chip vendor or the IoT eSIM platform provider (not the communications carrier) provides an initial profile, IoT devices vendors may find it difficult to install one.

The implementation of IPA itself may also be a hindrance for IoT device vendors. It necessitates direct SIM access, so it is likely to be commonly implemented within a communication module rather than in a device app, but only a limited range of communication modules would be suitable for this. However, there is a method called IPAe, whereby the IPA functionality is implemented in the SIM, so if SIM card vendors provide IoT eSIM OSes that support this method, that may resolve the issue.

Competition with other systems is also an issue. Before IoT eSIM was released, Consumer eSIM also gained support for remote profile management (via the Remote Profile Manager, RPM) in version 3. According to the current specifications, the RPM functionality only supports the switching of installed profiles and not the adding of new ones. The GSMA is the standardization body in this case as well, so while all-out competition with IoT eSIM seems unlikely, developments in this area will bear close watching.

The IoT eSIM technical specification has only just been released, and test specifications required to validate interconnectivity (which we can assume will be released as SGP.33) are still in development, so a market rollout is still a little way ahead.

2.5 Conclusion

With a physical SIM-free world just around the corner, this article has looked at the current situation in this regard around smartphones, tablets, and the like as well as the situation around IoT devices. In particular, we discussed technical challenges that remain, along with the need for more testing and development, before IoT devices can go physical SIM-free, and we went over IIJ's efforts in this area.

Even in a physical SIM-free world, IIJ will continue to provide an environment for convenient mobile services while driving innovation that takes advantage of Internet technologies as it contributes toward the development of an increasingly networked society.

Daisuke Maruyama
Senior Engineer, MVNO Project Promotion Section, Technology Development Department, MVNO Division, IIJ
Mr. Maruyama had his start in the development of voice switches and later worked on the development of voice equipment for mobile phones before getting into mobile networks. He is primarily engaged in the study of technologies and development of services related to SIMs.

Munenori Ouchi
Senior Engineer, Mobile Platform Development Section, Technology Development Department, MVNO Division, IIJ
Mr. Ouchi investigates and engages in research on cutting-edge mobile technology, and develops services utilizing such technology.

Shigeyoshi Miura
Business Development Department, MVNO Division, IIJ
Mr. Miura has devoted 40 years to his work as an engineer. His career has spanned embedded hardware and software through to the design and development of DBMS applications and the design of system architectures. In recent years, his knowledge as an embedded systems engineer has proved quite useful, and he currently supports the development of mobile IoT devices and the application and use of SIMs.

IIJ and the Evolution of Security —Commemorating 30 Years

3.1 Introduction

All sorts of incidents and accidents have occurred since we started our security business. Looking back on the past 30 years, the Internet has established itself as a platform for one-to-many and many-to-many communications in a communication services world that had primarily been a one-to-one affair. And those communications are always changing, both in form and composition. It started out as a network that only some people used, but those times have changed with the advent of commercial services for business customers and the like, consumer services, always-on connections for the home, mobile phone-based access, the cloud, smartphones, and IoT technologies.

The way we use it has also changed, and this has changed our everyday lives. In particular, with browser-based encrypted communications having become standard, electronic commerce has thrived, and the addition of personal authentication and other such features means we are now able to exchange vital, financially valuable information on a routine basis. Making credit card purchases and logging into online banking via your smartphone is the norm these days.

Yet this situation works in a similar vein for malicious actors too, who are able to exploit the nature of Internet communications to send data out over large distances to many recipients at low cost. Because the transmission of these communications takes place between computer systems, malicious actors are also able to exploit vulnerabilities to wreak havoc before users even realize what is happening. And the spectrum of malicious activities is broad, ranging from simply hijacking and using systems without permission to the theft of valuable information and services, the theft of intellectual property, ransom demands, and more.

In this article, a number of people who have worked on the front lines of IIJ's security business share their experiences and give their own unique perspectives on the past 30 years.

The Changing Face of Network Threats

Hirohide Tsuchiya
Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Divisionn

Commercial Internet arrived in Japan in 1993, and worms, viruses, and other such threats have also been with us since. Attempts to log in to open ports and other such behaviors were also part of the landscape. Given that companies need to guard against such attacks when using the Internet for business purposes, IIJ launched Japan's first firewall service back in 1994.

Initially, the Internet was generally used simply to pass information around; people were mostly browsing homepages or sending emails and messages. Once the year 2000 rolled around, the Internet started to transcend this and serve as a form of social infrastructure for business and other economic activities, including financial services and online shopping, leading to a rapid rise in prominence. This also prompted more awareness of the importance of security, and a recognition of the importance of security defense measures and the need to address vulnerabilities. Individuals were encouraged to use antivirus software, and companies also deployed security products such as firewalls and IDS/IPS on top of this.

Security incidents also became more diverse, with cases of website tampering, website DDoS attacks, and network worm infections via the Internet occuring quite frequently and being reported in the press. The typical network worm infections included CodeRed and Nimda, which reared their heads in 2001, and SQL Slammer, which popped up in 2003. Once these worms gained a foothold, the infections spread around the globe blindingly fast, in some cases resulting in network latency and other impacts. While Internet usage was growing rapidly, communications lines and other equipment were not as abundant back then as they are now, and our means of responding to large-scale attacks like this were limited. Today, our communications infrastructure and attack countermeasures are more fully developed, but with the spread of IoT devices and the like, the volume of data traffic associated with attacks is now several hundred times what it was back then.

As time passed, attack methods became increasingly complex and sophisticated, evolving to include botnets, which exploit vulnerabilities to infect and take control of large numbers of devices, like PCs and routers, to carry out DDoS attacks; malware (malicious computer programs) that steals user information and other data; and ransomware, which encrypts data on infected devices, effectively taking it hostage, so that the attacker can demand a ransom. Systems for carrying out these attacks were developed like any other software and made available on underground markets, such as the dark web, making it possible for anyone with a little money to obtain the tools to launch an attack in pursuit of ill-gotten gains.

As security countermeasures advanced and made it difficult to attack networks directly, the attack methods again morphed in clever ways, instead seeking to infect systems via email or by directing users to malicious links, and so forth.

Even today, infection campaigns that attack networks indiscriminately are still carried out, but attacks in general have become more advanced and include those directed at a narrow range of targets to make the infection campaign more efficient as well as targeted attacks and APT attacks, which seek to fly under the radar so as to evade detection and avoid triggering a security response.

With the Internet having come to serve as a form of social infrastructure, changes in the value of computing resources and information have elicited changes in the purpose of attacks as well. There was a time when some unknown number of faceless individuals out there were carrying out attacks partly for the fun of it, but attacks now serve a range of different agendas. Hacktivist groups like Anonymous, for instance, have carried out protests designed to publicize certain ideologies or claims, we now see financially motivated attacks being carried out by individuals and groups, and certain organizations and countries now engage in efforts to steal information.

These sorts of activities have also now gained the ability to impact on the real world when used in conjunction with methods outside of direct network attacks, such as the spread of false information, “fake” news, and the like on social media and, in some cases, public demonstrations or even terrorist acts.

This increasing sophistication and changing nature of attacks means that it is no longer enough to monitor what’s happening within and on the boundaries of a network to protect information in the hopes of preventing an attack. And as such, new security frameworks are being implemented in the form of zero trust models and the like to provide constant access control and monitoring of people, assets, and data.

If we consider the situation in terms of attackers and defenders, the attackers do seem to have a persistent advantage in many cases. If we are to break this paradigm, we need not only technological solutions but financial and legal countermeasures that diminish the advantage to attackers as well. As the Internet evolves, Japan has been updating its legal system where necessary, establishing the Act on Prohibition of Unauthorized Computer Access, for instance, and adding provisions to its penal code to explicitly criminalize the use of “electronic or magnetic records containing unauthorized commands” (in other words, computer viruses). Yet the Internet is truly borderless, and as such, many issues need to be considered in a multinational or even a global context. Many initiatives and cooperative international efforts have been mounted in all sorts of areas to address these issues we face, but we will need to join forces to an even greater extent going forward.

The range of communication modes available also continues to diversify to serve individual use cases—the reciprocal use of microcells and mobile networks, for example, and satellite-based connectivity services. And as connectivity continues to permeate our everyday conveniences, cars being a key example here, and if such aspects of our lives do become increasingly interconnected through real-time communications, then I think we have an even more convenient and comfortable future ahead of us. At the same time, this will also make our communications infrastructure ever more important.

To deal with these changes, we will no doubt need new mechanisms and forms of security that involve not only government and communications carriers but also the companies and individuals that use communications services. We do not yet have the right answer to all of this, but what is certain is that we will need to remain consistent in our efforts to deal with the ongoing arrival of new threats.

DDoS Attacks

Hiroshi Tamaru
Security Business Development, Advanced Security Division

The term "DDoS attack" began popping up in Internet-related news around 2000, and IIJ has observed many DDoS attacks over the years. Here, I would like to look back at the past 20 years or so as it relates to this and then explore what the future may hold.

We launched our first DDoS protection service in 2005. The trigger for this was a DDoS attack on a customer web server that overloaded the firewall protecting it, rendering it impossible to control. The high load on the firewall was due to an abnormally high volume of requests and a massive amount of half-open TCP connections, which caused the connection management tables to overflow and forced the system to generate and process a huge volume of access logs.

The day before we experienced this DDoS attack, we did have some warning signs, including a large number of port scans being performed, and so we were on alert and had taken precautions. In the end, however, we were unable to fully protect the customer's network from the DDoS attack. This experience prompted us to think hard about what countermeasures we might be able to implement on IIJ's equipment, and I still remember us talking and talking about it—at our desks, during meals, in the break room, everywhere.

■ Background to DDoS attacks

Attacks like these come with background context, and there have been changes over time in this regard. A past attack with historical underpinnings was one that originated in China and was associated with the date of the Manchurian Incident. We observed this pretty much every year from around 2005, but this activity seems to have subsided over the past 10 years. Given the propensity for attacks to occur on historically significant dates like this, IIJ continues to be alert to such attacks. Meanwhile, DDoS attacks carried out by Anonymous as a form of protest are on the rise. Japan has seen such DDoS attacks carried out in opposition to whaling and dolphin fishing, to protest against the discharge of treated water from the Fukushima nuclear power plant into the ocean, and to express opposition to Japan's position on the situation in the Middle East.

When the background involves history, politics, animal welfare activities, or environmental or human rights advocacy, the attacks are often organized ones. Recently, however, we have started to see attacks on service providers in the gaming and entertainment industries for what are apparently personal reasons. You may have heard the phrase DDoS as a Service. The fact that anyone can now easily and cheaply purchase a service that will perform a DDoS attack is a key factor behind this recent trend. Something as trivial as a personal grievance in an online game or an employee's offhanded posts on social media or a message board can trigger an attack on a company.

■ DDoS attack and defense

DDoS attacks, as is well known, can be broadly categorized into resource consumption attacks and volumetric attacks. From a defense perspective, another way to think about it is whether the attack is one in which the source addresses can be spoofed or not.

In attacks like TCP Connection Flood, HTTP Slow, and HTTP Request Flood, for example, a TCP connection must be established, making it relatively difficult to spoof source addresses. With these types of attacks, you can expect to mitigate the impact to an extent by tightening connection criteria when the attack is taking place. Effective steps may, for example, include shortening the timeout for idle TCP connections, putting priority on allowing connections from specific regions, and restricting access based on country/regional IP address allocations.

TCP SYN Flood, on the other hand, is an example of an attack in which source addresses can be spoofed. It has been around for quite some time. With TCP connections, methods based on the TCP protocol can be used to determine whether the sender actually exists or not. Depending on the confirmation method implemented in the DDoS mitigation device, however, the sender may need to retransmit packets (a browser reload in the case of HTTP/HTTPS), or the firewall may deem confirmation packets sent by the DDoS mitigation device as invalid and discard them, thus making an incorrect determination, and so the impact of these factors needs to be taken into account.

Reflection attacks, which exploit responses sent by devices connected to the network, use many protocols not normally used on the Internet, like Memcached, SSDP, MSSQL, ARD, and SNMP. These attacks can easily be mitigated by setting up filters. In the case of DNS and NTP, the ability to restrict source addresses, if this is possible, can make it easier to guard against attacks. The steps we are taking as an ISP to prevent source-address-spoofing attacks include implementing SAV (Source Address Validation) methods such as uRPF.

■ Choosing DDoS countermeasures

Methods of protecting services and infrastructure from DDoS attacks include building a dedicated on-premises DDoS mitigation appliance and using services offered by CDN providers, cloud services, or ISPs such as IIJ.

Attacks that exceed 100Gbps are not uncommon these days, and this can easily exhaust available bandwidth with on-premises solutions, so you may need to consider using another service entirely or in combination with your on-premises solution.

The services offered by CDN providers tend to use anycast and the like to make it possible to disperse attacks by having a broad network of receiving nodes across the globe. They also commonly provide streaming and WAF services in combination with this, making these services well suited to Web systems.

The services provided by ISPs like IIJ, on the other hand, make it possible to protect not only publicly exposed systems but also office Internet connections used for business purposes. If your ISP does not provide DDoS mitigation services, you can protect your network using a cloud-based service, but it must be noted that such services may come with certain restrictions to facilitate route control.

■ Outlook

Increasing PC and server performance means that services with 1Gbps or 10Gbps bandwidths are now available to ordinary household customers. A whole range of services is available via the Internet now that all sorts of devices like surveillance cameras and home appliances have online capabilities. But we also continue to see cases of the OSes and firmware on home routers, surveillance cameras, NAS devices, and the like being infected by malware that turns them into bots for use as DDoS attack sources. In the hopes of mitigating the damage caused by DDoS attacks, we at IIJ will continue to highlight the importance of properly updating software not only on PCs but also on these sorts of devices, and the importance of installing software updates and addressing vulnerabilities on public servers.

We will continue to look at how we can upgrade and configure our environment to detect and block attack traffic in both directions so that we can not only protect our customers from incoming attacks but also ensure they are not implicated in outgoing DDoS attacks, our ongoing aim being to build a safe and secure Internet that people can use with peace of mind.

The Greatest of Frustrations

Mamoru Saito
Director, Advanced Security Division

We respond to cyberattacks directed at our customers on a daily basis, and in many cases we treat the associated problems experienced by our customers as if they were, in a sense, natural disasters. As a private-sector security provider, we are not in a position to attempt to catch the perpetrators even if a cybercrime has been committed. We focus on investigating the technical causes, minimizing the impact, and working to restore systems. We do not seek to identify the perpetrators or confirm their location in the way a judicial entity would. Instead, we simply track down and trace information relevant to our being prepared for the perpetrators' next action.

Even so, as someone who has worked in security for many years, there was just one case in which I really felt the desire to catch and punish the perpetrator. This was the case of Antinny, which caused a whole slew of serious information breaches.

Antinny is malware that runs on Windows PCs on which the P2P file-sharing program Winny is installed and has the ability to send files on the PC to external parties without the PC user's consent. Leaving aside the pros and cons of Winny as a system[*1], the advent of Antinny made installing and using Winny an extremely risky proposition. Antinny tricks users into running it by adopting a deceptive file name that makes users think it is a video file or the like. Its actual malicious behavior is to search for images and office files on the PC and copy them to Winny's upload folder, causing them to be shared externally. This resulted in many information breaches, including the leaking of people's personal photos, and the leaking of work-related files that people had brought home from the office, which then escalated into corporate data breaches and the like. Once a month, it would also bundle screenshots and files stored on the PC into a compressed archive and upload it to the copyright infringement query section of the Association of Copyright for Computer Software's website. These uploads drove DDoS attack-levels of traffic to the association's web server, at times making the website inaccessible.

None of Antinny's functions take advantage of vulnerabilities or privileges. They simply perform actions that a user with normal privileges is permitted to perform, such as copying files to Winny's file-sharing folder. Because Antinny compromises Winny users and sends their information to a copyright management organization, it is conceivable that Antinny's creator intended it as a type of joke or prank program designed to send somewhat of a message. Its proliferation, however, had profound social implications. It disrupted people's lives and impacted on the activities of many businesses and other organizations.

Efforts to combat Antinny also lagged across the board such that the malware was able to rage on for many years. In 2004, the ISP security organization Telecom-ISAC Japan (currently ICT-ISAC Japan), working with the Association of Copyright for Computer Software, made a successful attempt to control the DDoS attack-levels of traffic generated, but it also showed that exercising that control on an ongoing basis would be highly costly. On the antivirus front, perhaps because Antinny was seen as a uniquely Japanese phenomenon or perhaps because of Winny's unique environment, it was several years before many of the antivirus products on the market gained the

[*1] Winny was not equipped with communications optimization features, so it would constantly send data over long distances across the network, putting unnecessary strain on network capacity and causing poor communications quality due to congestion between many ISPs. So it was an application that had considerable side effects from a communications business perspective as well.

ability to remove Antinny[*2]. Eventually, owing to revisions to Japan's Copyright Act, the number of Winny users declined dramatically, and the impact of Antinny also diminished as the issue faded away.

So it is that Antinny is no longer something we need to worry about, but its creator remains at large, and it is extremely frustrating to think that he or she may still be living a normal life in Japan to this day. I think we need to have a proper discussion about whether Antinny constitutes a virus and whether we can consider its effects to be criminal. At this point, with so much time having passed since it was brought under control, it would be a tough ask to dig back into the Antinny issue and discover the real culprit. That said, when the next Antinny rears its head, it is my hope that we in Japan will be able to mount an appropriate response.

The Impact of Snowden

Masafumi Negishi
Head of the Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division

It is impossible not to mention Edward Snowden's revelation of US state secrets when discussing events that impacted heavily on our society during the 2010s and 2020s. In June 2013, Snowden, then working for the US National Security Agency (NSA), appropriated a huge number of classified documents, which included top secret information, and disclosed them through multiple media outlets. A particularly shocking revelation from the information leaked was that of the comprehensive surveillance of the Internet and telephone lines, predominantly carried out by the Five Eyes intelligence alliance, which includes the United States. In the wake of the September 11 terrorist attacks of 2001, the US enacted legislation to strengthen wiretapping and the interception of communications for the purpose of monitoring terrorist activity. This resulted in an immensely vast and comprehensive surveillance network being established and operated, with implications not only for hostile actors but for US citizens and other countries as well. It was also revealed that major US telecommunications carriers and major tech companies, including Microsoft, Google, and Apple, were cooperating in the building of surveillance systems and collection of information in accord with law enforcement agency requests and court orders.

These leaks sparked criticism not only in the US but around the world as people raised concerns about privacy and other human rights violations due to excessive surveillance, and efforts were subsequently made to counter these surveillance networks. The practice of encrypting communication routes became widespread, led in particular by the aforementioned tech companies, and we saw a rapid rise in the encryption of inter-datacenter communications, the use of encryption by default on service-providing sites, and so forth. As a result, encrypted HTTPS communications as a proportion of all traffic from browsers rose to 70% in 2018 and to over 80% in 2020[*3]. IIJ's observations for 2023 also show that over 70% of broadband communications are encrypted[*4].

The TLS 1.3 standardization work that began in 2014 also incorporated encryption methods requiring handshake encryption and forward secrecy to protect against network monitoring. The standardization of the DNS over TLS (DoT) and DNS over HTTPS (DoH) protocols for encrypting DNS communications has also moved ahead, and these protocols are now in the process of widespread uptake. Hence, Snowden's revelations have had a major impact on the formulation and widespread adoption of technical standards.

This has an impact not only on communications but also on devices like smartphones. Major messaging services like Apple, WhatsApp, and LINE, for instance, support end-to-end encryption (E2EE), a strong encryption system that prevents anyone on the communications route, and

[*2] Initially, only a handful of vendors like Trend Micro were able to get rid of Antinny. After Microsoft addressed the issue and revealed that it had removed Antinny from many systems, a lot of other antivirus vendors followed suit. For its service in this case, Microsoft received a Minister's Commendation from Japan's Ministry of Internal Affairs and Communications and a letter of appreciation from the Association of Copyright for Computer Software.

[*3] Based on Firefox telemetry data (https://letsencrypt.org/stats/).

[*4] See "1. Periodic Observation Report" in IIR Vol. 61 (https://www.iij.ad.jp/en/dev/iir/061.html).

even the service provider, from reading the contents of your messages. Apple, Google, and others have been enhancing their smartphone encryption features since 2014, using encryption to protect user data stored on such devices and cloud services. While these efforts protect the security and privacy of users, they also benefit criminals. Since the late 2010s, there have frequently been reports of these mechanisms hindering criminal investigations by making it impossible for law enforcement agencies to extract data from devices seized from suspects. In an attempt to improve this situation, government agencies in the US and Europe are moving to regulate the cryptographic features that the technology industry provides.

Snowden's revelations also illuminated cyberattack activity against other countries by intelligence agencies in the US and elsewhere. The NSA, in particular, has some of the world's most advanced cyberattack capabilities. It engages in a range of espionage, including vulnerability research, the development of attack code and malware, and the use of this to infiltrate organizations in other countries. The large-scale WannaCry outbreak of May 2017 is an example of how the NSA's activities directly affect us. To infect Windows machines, WannaCry used attack code and a backdoor program that had been leaked by a group called The Shadow Brokers. The Shadow Brokers had stolen the leaked data from an attack group called the Equation Group, and it was later revealed that the Equation Group was actually an NSA cyberwarfare unit. While the truth remains unclear, the Shadow Brokers are suspected of having ties to Russia, and the US has issued an official statement claiming that the WannaCry attack was the work of North Korea. And so it is that the Internet, an essential part of the infrastructure of our daily lives, is also a theater not just for cybercriminal activity but also for constant battles among multiple attack groups with connections to nation states. The multiple layers of such activity all have an impact and make for a complex Internet environment, and this presents a huge challenge for us that we must solve if we are to provide safe, secure networks that everyone can use with peace of mind.

The Changing Face of Security Operations Centers

Tsutomu Nakajima
Manager, Data Analytics Section, Security Operations, Advanced Security Division

■ From black to white

Security operations centers (SOCs) started rising to prominence in Japan as security monitoring groups or facilities around 2000. Initially, they were housed in dim, windowless rooms lined with displays, and only security analysts—engineers with a deep knowledge of network security—were given access to the monitoring systems. This picture began to change around 2015, with SOC equipment being reimagined to adopt bright colors, and IIJ's SOC, which we renovated in 2017, also turned into a more welcoming, comfortable space for engineers (Figure 1, Figure 2).

In conjunction with this, to ensure we could respond to increasingly sophisticated threats, we also reimagined the way our SOC and its operations are organized. In the past, the SOC essentially referred to real-time security monitoring, but we now have many security engineers stationed within

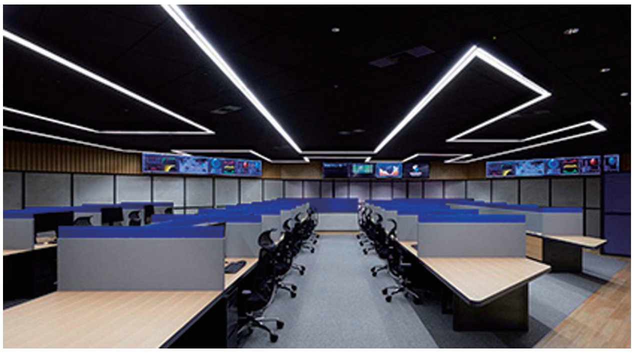


Figure 1: Operations Room

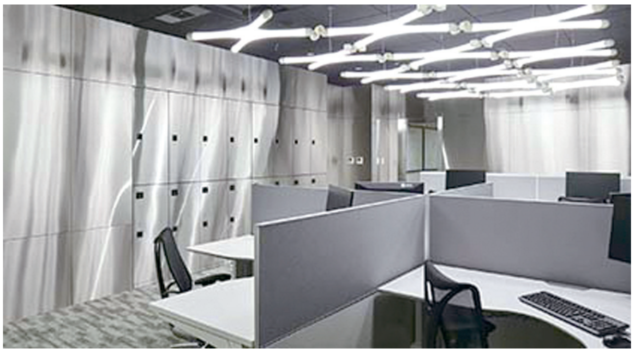


Figure 2: Security Lab

or close to the SOC to ensure that the right people are able to come together and collaborate on incident responses when needed. With diversity also becoming an increasingly important social theme, IIJ's SOC has also adopted a value system that welcomes a diverse range of engineers to the team, united under the single purpose of dealing with security incidents.

■ From networks to devices

The SOC monitors a variety of devices. In the past, firewalls, IPSs, and the like in the form of security appliance boxes located at network boundaries to monitor traffic along communications routes were the mainstream. A lot of the significant security incidents in the 2000s were attacks on servers, and so the SOC's main role was to protect servers necessary for ensuring business continuity.

As a security analyst, I sensed change in the air when email-driven attacks, particularly targeted attacks, began rising to prominence, and it was around this time that I realized, intuitively, that monitoring server segments alone would be insufficient to safeguard the systems we sought to protect. In recent years, the SOC has also had occasion to monitor wide-ranging attacks from indiscriminate malware such as Emotet as well as internal misconduct at some organizations. Attacks on public servers remain, as always, a feature of the landscape, but with attack targets having been expanded to include client devices, we now also need to monitor internal-to-external and internal-to-internal communications. Firewalls are one of the main monitoring tools, and the evolution of firewalls to incorporate multi-featured unified threat management (UTM) technology, and then next-generation firewall (NGFW) technology facilitating application-layer analysis, has improved communications traffic visibility.

Meanwhile, with communications routes and communications themselves increasingly being encrypted, more than a few SOCs now monitor not just the network but also device processes and logs via technologies like endpoint detection and response (EDR). Alongside attacks exploiting vulnerabilities, cases of personal credentials (used in authentication) stolen through whatever means being used in initial attacks are also on the rise of late, and so the management of such credentials has also become an issue.

■ The role of SOC engineers

The role of the SOC is not to maintain normal operating conditions but to discover abnormalities. Even if a monitoring system does not raise a security alert, any signs of suspicious activity still require investigation. Back when the SOC focused primarily on network monitoring, our skilled security analysts, guided by their knowledge and experience, would uncover security incidents by looking through seemingly ordinary event logs to spot anything that just didn't look right. But as such logs grow in variety, there arise limits to what can be achieved through manual monitoring of the complex, intertwined data generated. And in addition to monitoring data in real time, we also now need to recursively investigate past data, and time considerations here also make manual investigations difficult.

These days, the knowhow to detect anomalies comes built in as security sensor detection rules and security information and event management (SIEM) rules, and this has reduced the associated engineer workload and served to make such technology more common. AI is used to perform data-based analysis to reveal anomalies that humans would otherwise not notice, and to mitigate the limits of human memory. Yet attackers can similarly benefit from AI and thus continue to discover new security holes.

People have always been at the heart of the SOC, and even with all of the automation and systemization available today, the knowledge and experience of engineers continues to have a major influence on the SOC's analytical capabilities. "Updating" ourselves as SOC engineers every day can help us to respond to new attacks as well.

3.2 Conclusion

This article has presented the personal reflections on the past 30 years of a number of our security professionals. The Internet's evolution has by no means reached an end. In just the past few years it has redefined our daily lives through the development of telework environments, the proliferation of AI, and the like. The Internet landscape will no doubt continue to change ahead, with new incidents and challenges arising along the way. To protect our modern way of life and keep everyone safe, we will continue to stay ahead of these changes and strive to address the new challenges that arise.

February 2024 Vol.61

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.

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/