IIR

Internet
Infrastructure
Review

Dec.2023
Vol.61

定期観測レポート

IIJインフラから見た インターネットの傾向〜2023年

フォーカス・リサーチ(1)

SIMの最新動向〜ハードウェアプロファイルからソフトウェアプロファイルへの進化〜

フォーカス・リサーチ(2)

IIJとセキュリティの変遷 〜この30年を振り返って

IIJ
Internet Initiative Japan

Internet Infrastructure Review

December 2023 Vol.61

© Internet Initiative Japan Inc.

エグゼクティブサマリ

2023年最後の「IIR Vol.61」では、この1年を振り返ってみたいと思います。

今年、インターネットあるいはIT全般で大きな話題になったのは、間違いなく生成AIの台頭でしょう。生成AIの進化と社会への浸透は非常に速く、大きな可能性を感じると同時に、ある種の恐怖を覚えることも多々あります。AIという技術を正しく利活用する上での倫理やガバナンスが今後、ますます重要になることは間違いありません。

ガバナンスという点では、18回目のIGFが日本で開催されました。ここでもAIが取り上げられましたが、マルチステークホルダーとして178カ国から約1万人が参加し、インターネットの分断、サイバーセキュリティなど幅広いテーマに関して議論が行われました。

社会インフラとなったインターネットは、経済安全保障とも無縁ではいられません。我が国でも2024年に経済安全保障推進法が制定され、施行に向けた準備が進められています。電気通信分野は安全保障上、重要な基幹インフラ役務として位置付けられています。

「IIR」は、IIJで研究・開発している幅広い技術を紹介しており、日々のサービス運用から得られる各種データをまとめた「定期観測レポート」と、特定テーマを掘り下げた「フォーカス・リサーチ」から構成されます。

1章の「定期観測レポート」は、「IIJインフラから見たインターネットの傾向」について説明します。ここでは、BGP・経路数、DNSクエリ解析、IPv6トラフィックに関して、IIJの設備で観測できる統計を毎年取得し、傾向を分析していますが、いずれの統計においても、IPv6の普及が順調に進んでいることが数字に表れています。IPv6の推進力の一因となっているスマートデバイスのIPv6対応については、米国メーカのIPv6有効化率が高いことが非常に印象的です。

2章の「フォーカス・リサーチ」では、「SIMの最新動向〜ハードウェアプロファイルからソフトウェアプロファイルへの進化〜」と題して、あらためて携帯電話で使われるSIM（Subscriber Identity Module）を取り上げました。GSM規格とともにSIMカードが誕生した背景、SIMカードの小型化の歴史、物理的なSIMカードがeSIMのように仮想的に取り扱えるようになった経緯などを振り返っています。それを受けて、IIJが開発したソリューションや今後の規格の展望についても紹介しています。

3章の「フォーカス・リサーチ」では、IIJの30周年特別コンテンツとして、セキュリティを取り上げました。IIJは、インターネットを利用するにあたり、攻撃に対する備えを重要視し、インターネット接続サービスを開始した直後からファイアウォールによる防御をサービスとして提供しています。IIJのセキュリティ事業は、セキュリティ専業ではなく、インターネットを運用している事業者によるセキュリティ事業という点が、他のセキュリティ事業者と大きく異なります。そのようなIIJがこの30年間、インターネットのセキュリティに対してどのように考え、どのように取り組んできたかを紹介します。

IIJは、このような活動を通してインターネットの安定性を維持しながら、日々、改善・発展させていく努力を行っています。今後も企業活動のインフラとして最大限にご活用いただけるよう、様々なサービスやソリューションを提供し続けてまいります。

島上 純一（しまがみ じゅんいち）

IIJ 常務取締役 CTO。インターネットに魅かれて、1996年9月にIIJ入社。IIJが主導したアジア域内ネットワークA-BoneやIIJのバックボーンネットワークの設計、構築に従事した後、IIJのネットワークサービスを統括。2015年よりCTOとしてネットワーク、クラウド、セキュリティなど技術全般を統括。2017年4月にテレコムサービス協会MVNO委員会の委員長に就任し、2023年5月に退任。2021年6月より同協会の副会長に就任。

© Internet Initiative Japan Inc.

IIJインフラから見たインターネットの傾向 ～2023年

インターネットサービスを提供するIIJは、国内でも有数規模のネットワーク・サーバインフラを運用しています。ここでは、その運用によって得られた情報から、この1年間のインターネットの動向について報告します。特に、BGP経路、DNSクエリ解析、IPv6、モバイルの各視点から変化の傾向を分析しました。

Theme 01

BGP・経路数

最初に、IIJ網から他組織に広報している「IPv4フルルート」の情報（表-1）及び「IPv4フルルート」に含まれるunique IPv4アドレス数の情報（表-3）を確認します。

経路総数の年間増加はわずか1.4万に留まり本定期観測開始以来の最低値となりました。2018年をピークとする減少傾向が継続しており（図-1参照）、総数が節目の100万経路に到達しないこともあり得そうな状況です。なお今回初めて/20及び/21経路数の減少が観測されました。加えて/13 ～/18の経路数も軒並み減少している一方で/22 ～/24の経路数の増加は昨年の1/3程度しかなく、その結果unique IPv4アドレス数は1300万弱（0.4%）の減少となっています。

次に「IPv6フルルート」の情報（表-2）及び「IPv6フルルート」に含まれるunique IPv6 /64ブロック数の情報（表-3）を確認します。

経路総数は昨年と同程度の伸びで約18万に達しました。プレフィクス長の短い経路の増加は少なかったものの、その他も含めた増加経路の60%がuniqueブロック数の加算に寄与する、より短いプレフィクス長の情報がない経路であったこともあ

表-1「IPv4フルルート」に含まれるプレフィクス長ごとの経路数の推移

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

表-2「IPv6フルルート」に含まれるプレフィクス長ごとの経路数の推移

年月	/16-/28	/29	/30-/31	/32	/33-/39	/40	/41-/43	/44	/45-/47	/48	total
2014年9月	134	481	133	6025	1447	825	248	709	592	7949	18543
2015年9月	142	771	168	6846	1808	1150	386	990	648	10570	23479
2016年9月	153	1294	216	8110	3092	1445	371	1492	1006	14291	31470
2017年9月	158	1757	256	9089	3588	2117	580	1999	1983	18347	39874
2018年9月	168	2279	328	10897	4828	2940	906	4015	2270	24616	53247
2019年9月	192	2671	606	12664	6914	3870	1566	4590	4165	34224	71462
2020年9月	205	3164	641	14520	9063	4815	2663	5501	4562	45160	90294
2021年9月	223	3628	705	20650	13050	10233	4170	11545	5204	61024	130432
2022年9月	298	4247	895	21926	15147	12509	4108	13840	6994	73244	153208
2023年9月	316	4357	923	23228	17427	14828	5518	16453	9579	86881	179510

© Internet Initiative Japan Inc.

りunique /64ブロック数は大きく増加した昨年から更に30%増となりました。IPv6の導入、IPv6ネットワークの拡大が順調に進んでいることが窺えます。

最後に「IPv4/IPv6フルルート」広報元AS（Origin AS）数を確認します（表-4）。なおこの1年の間に、APNICに2048、RIPE NCCに3072の32-bit onlyAS番号が追加割り振りされています。

16-bit AS番号Origin ASの減少数は昨年より更に減少しました。今回は32-bit only AS番号Origin AS数も大きく減少しましたが、これは一昨年にAPNIC地域で大量増加した「IPv6のみ」ASの多くが経路情報に現れなくなったことが影響しています。なお当該ASから広報されていた経路は現在、同組織と思われる他ASから概ね広報されており、一時的に別ASからとしたIPv6経路広報の整理が行われたものと推測されます。

また今回は「IPv4+IPv6」32-bit only AS数が初めて同16-bit AS数を上回りました。「IPv4のみ」32-bit only AS数の減少も初めて観測されており、少なくとも新興のASではデュアルスタック構成が今後の主流となるのか、来年も注目したいと思います。

表-3「IPv4フルルート」に含まれる unique IPv4アドレス総数及び「IPv6フルルート」に含まれる unique IPv6 /64ブロック総数の推移

年月	IPv4 アドレス数	IPv6 /64ブロック数
2014年9月	2,705,751,040	62,266,023,358
2015年9月	2,791,345,920	31,850,122,325
2016年9月	2,824,538,880	26,432,856,889
2017年9月	2,852,547,328	64,637,990,711
2018年9月	2,855,087,616	258,467,083,995
2019年9月	2,834,175,488	343,997,218,383
2020年9月	2,850,284,544	439,850,692,844
2021年9月	3,036,707,072	461,117,856,035
2022年9月	3,068,374,784	532,578,391,219
2023年9月	3,055,604,992	700,359,397,494

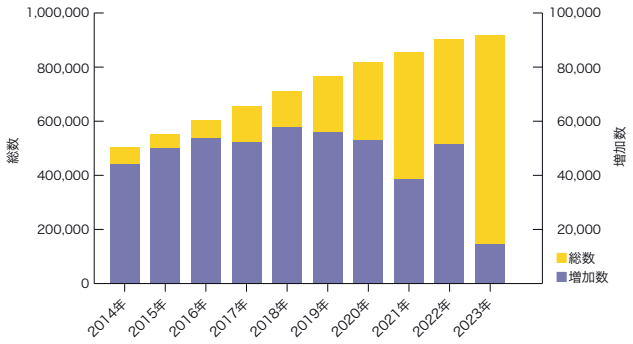


図-1「IPv4フルルート」経路の総数及び年間増加数の推移

表-4「IPv4/IPv6フルルート」の広報元AS数の推移

AS番号	16-bit（1～64495）					32-bit only（131072～4199999999）				
広報経路	IPv4+IPv6	IPv4のみ	IPv6のみ	total	(IPv6 -enabled)	IPv4+IPv6	IPv4のみ	IPv6のみ	total	(IPv6 -enabled)
2014年9月	7405	34555	128	42088	(17.9%)	868	4749	55	5672	(16.3%)
2015年9月	8228	34544	137	42909	(19.5%)	1424	6801	78	8303	(18.1%)
2016年9月	9116	33555	158	42829	(21.7%)	2406	9391	146	11943	(21.4%)
2017年9月	9603	32731	181	42515	(23.0%)	3214	12379	207	15800	(21.7%)
2018年9月	10199	31960	176	42335	(24.5%)	4379	14874	308	19561	(24.0%)
2019年9月	10642	31164	206	42012	(25.8%)	5790	17409	432	23631	(26.3%)
2020年9月	11107	30374	229	41710	(27.2%)	7653	19668	574	27895	(29.5%)
2021年9月	11465	29219	302	40986	(28.7%)	9514	21108	5242	35864	(41.1%)
2022年9月	11613	28398	369	40380	(29.7%)	10816	22211	5764	38791	(42.7%)
2023年9月	11770	27617	460	39847	(30.7%)	12640	22128	2067	36835	(39.9%)

© Internet Initiative Japan Inc.

Theme 02

DNSクエリ解析

IIJでは利用者がDNSの名前解決を利用できるようフルリゾルバを提供しています。この項目では名前解決の情況を解説し、IIJで2023年10月18日に行ったフルリゾルバの1日分の観測データのうち、主にコンシューマサービス向けに提供しているサーバのデータに基づいて分析と考察を行います。

フルリゾルバは利用者端末からのDNS問い合わせに応じて名前解決機能を提供します。具体的には、名前を解決するためrootと呼ばれる最上位のゾーン情報を提供する権威ネームサーバのIPアドレスを手がかりとして、問い合わせを行い、適宜権威ネームサーバをたどって必要なレコードを探します。フルリゾルバで毎回反復問い合わせを行っていると負荷や遅延の影響が問題となるため、得られた情報はしばらくキャッシュしておいて再び同じ問い合わせを受けた場合にはそのキャッシュから応答しています。最近はこの他にも家庭用ルータやファイアウォールなど、通信経路上の機器にもDNS関連の機能が実装されており、DNS問い合わせの中継や制御ポリシーの適用に関わっている場合があります。また、Webブラウザなど一部のアプリケーションでは独自の名前解決機能を実装している場合があり、OSの設定とは異なるポリシーで名前解決を行っている場合もあります。

ISPは接続種別に応じたPPPやDHCP、RA、PCOなどの通知手段を利用してフルリゾルバのIPアドレスを利用者に伝え、利用者端末が名前解決用のフルリゾルバを自動設定できるようにしています。ISPは複数のフルリゾルバを利用者に伝えられるほか、利用者は自身でOSやWebブラウザなどの設定を変更して利用するフルリゾルバを指定することもできます。端末に複数のフルリゾルバが設定されている場合、どれを利用するかは端末の実装やアプリケーションに依存するため、フルリゾルバ側では利用者が総量としてどの程度の問い合わせを行っているか分かりません。このため、利用者側の挙動や状態が変わると、突然あるフルリゾルバ向けの問い合わせが増えることも考えられるため、フルリゾルバでは問い合わせ動向を注視しながら、常に処理能力に余裕を持たせた運用を心がける必要があります。

IIJが提供するフルリゾルバの観測データを見てみると、利用者の利用傾向を示すように時間帯によって問い合わせ量が変動し、朝3時10分頃に問い合わせ元のIPアドレス当たり最小の0.15query/sec、夜22時5分頃にピークを迎えて0.36query/sec程度になっています。昨年に比べると、全般に+0.02ポイント程度伸びています。ピーク時の伸び率は多少鈍化したように見られますが、引き続き増加傾向が続いています。問い合わせ傾向を通信に使われたIPv4とIPv6のIPプロトコル別に見てみると、昨年とほぼ同様の傾向が見られ、IPv4を通信に使った問い合わせが全体の約60%、IPv6が約40%となっています。

近年の特徴的な傾向として、朝方の毎正時などキリの良い時刻に一時的に問い合わせが増加しています。問い合わせ元数も同時に増えていますし、特に朝6時朝7時に顕著に傾向が見られるため、利用者の端末でタスクをスケジュールしたり、目覚まし機能などで端末が起動することに伴う機械的なアクセスが原因ではないかと推測しています。その他、毎正時の14秒前と9秒前の問い合わせも増加しています。これは近年見られている傾向で、毎正時に増加する問い合わせ量では急な増加後、緩やかに問い合わせ量が減っていくのに比べて、毎正時前の増加では急な増加の直後にそれまでの問い合わせ量程度に戻って

© Internet Initiative Japan Inc.

います。つまり多くの端末が綺麗に同期して問い合わせを行っていることから、何かすぐに完了する軽量なタスクが実行されているのではないかと推測しています。例えば接続確認や時刻同期など基本的なタスクを本格的なスリープ解除前に終わらせるような機構があり、これに利用されている問い合わせが影響していると予想しています。

問い合わせプロトコルに注目すると、UDPが98.581%でほとんどがUDPでの問い合わせになっています。ただ、TCPでの問い合わせは2021年が0.189%、2022年が0.812%、2023年が1.419%であり、ここ数年TCPでの問い合わせ割合が増加してきています。主な増加要因として、DNS over TLS (DoT) での問い合わせが増えてきていることが挙げられます。DoTでは基本的にTCPの853番ポートを使って問い合わせするため、DoTの利用が増えるとTCPの問い合わせが増えることになります。

問い合わせレコードタイプに注目すると、ホスト名に対応するIPv4アドレスを問い合わせるAレコードとIPv6アドレスを問い合わせるAAAAレコード、そしてWebサービスの解決に用いられるHTTPSレコードが全体の96%を占めています。AとAAAAの問い合わせ傾向は通信に利用されるIPプロトコルで違いが見られ、IPv6での問い合わせではより多くのAAAAレコード問い合わせが見られます。IPv4での問い合わせでは、全体の57%程度がAレコード問い合わせ、17%程度がAAAAレコード問い合わせです(図-2)。一方IPv6での問い合わせでは、全体の38%程度がAレコード問い合わせ、35%程度がAAAAレコード問い合わせとAAAAレコード問い合わせの比率が高まっています(図-3)。昨年と比べるとIPv4、IPv6共に3ポイント程度Aレコードの問い合わせが減少しています。2020年から観測され始めたHTTPSレコードのDNS問い合わせがIPv4で20%、IPv6で24%程度を占めており、昨年と比べるとIPv4で+5ポイント、IPv6では+3ポイントと順調な伸びを示しています。特にIPv4ではAAAAレコードよりもHTTPSレコードの方が多く問い合わせられるようになっており、HTTPSレコードに対応した実装が多くなっていることが推測できます。昨年から観測され始めたSVCBレコードは、IPv4で0.26%、IPv6では0.60%とまだ全体に対する比率は少ないながらも順調に問い合わせが増えてきています。これは、Discovery of Designated Resolvers (DDR)という、クライアントが暗号化に対応したフルリゾルバを検出するための新しいプロトコル提案の実装が進んでいるためと推測しています。

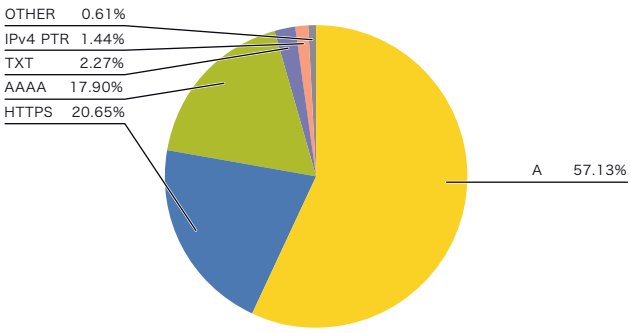


図-2 クライアントからのIPv4による問い合わせ

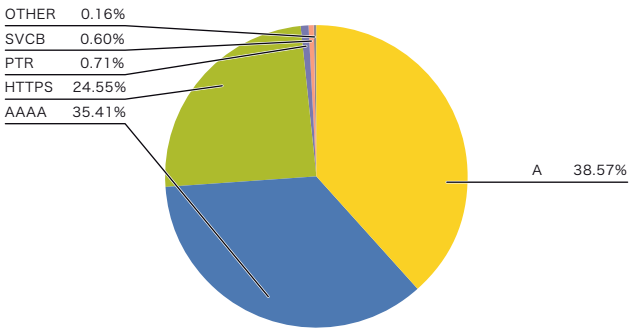


図-3 クライアントからのIPv6による問い合わせ

© Internet Initiative Japan Inc.

Theme 03

IPv6

今回もIIJバックボーンのIPv6トラフィック量、送信元AS、主なプロトコルについて見ていきます。また、2019年と昨年にも紹介した、モバイルサービスの端末OS別のIPv6接続状況などについて、調査したいと思います。

■ トラフィック

IIJのコアPOP（東京3ヵ所、大阪2ヵ所、名古屋2ヵ所）のバックボーンルータで計測したトラフィックを図-4に示します。集計期間は2023年2月1日から9月30日までの8ヵ月間です。2023年は新型コロナウイルス感染症が5類感染症に移行し、社会経済活動もコロナ禍以前に近い形に戻りつつありますが、インターネットトラフィック量の期中の推移としては、IPv6は横ばい、IPv4は微増となっています。ただ、昨年同日（グラフの薄い色の線）と重ねて比較すると、IPv6、IPv4共にそれなりに増加していることが分かります。

図-5に、2023年2月1日を100として指数化したグラフを示します。先ほど紹介したとおり、年初からのトラフィック量の推移としては大きな変化はなく、概ね横ばいとなっています。

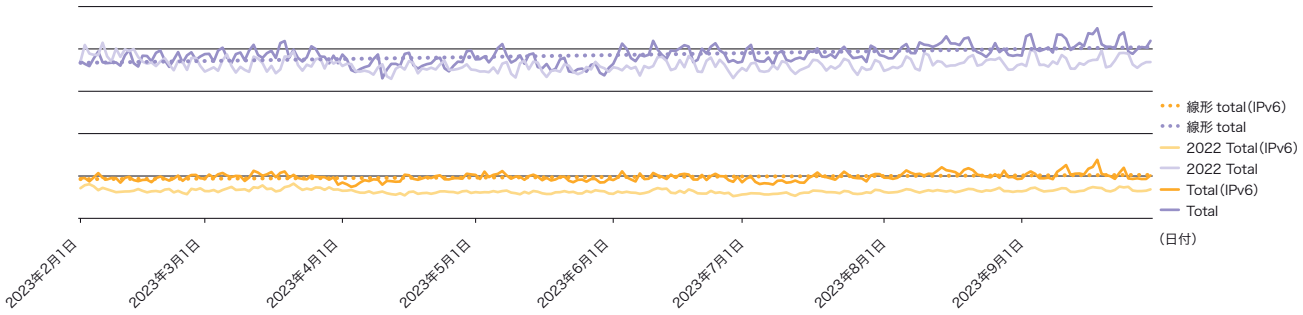


図-4 IIJコアPOPのバックボーンルータで計測したトラフィック

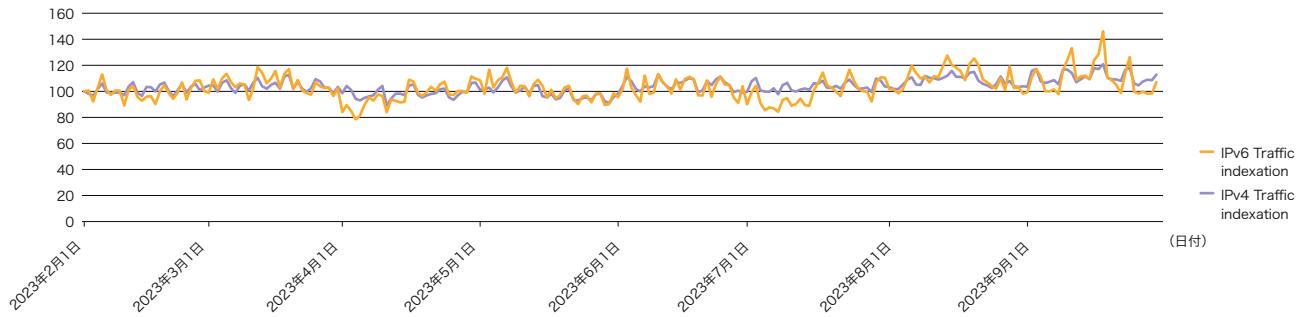


図-5 2月1日のトラフィックを100としたときの変動状況

© Internet Initiative Japan Inc.

次に、トラフィック全体に占めるIPv6の比率を図-6に示します。最小17%から最大23%ほどで推移しています。こちらも大きなトレンドは見て取れませんが、昨年同期と比較すると、5ポイントほど増加しており、IPv6トラフィックが伸びていることが分かります。

表-5に6年前からのIPv6比率の推移を表にします。昨年までも同様に年ごとのIPv6比率を紹介していましたが、2021年と2022年の比率計算が誤っていたことが分かりましたので、お詫びして訂正いたします。

■ 送信元組織(BGP AS)

次に2023年2月1日から2023年9月30日までの、IPv6とIPv4の平均トラフィック送信元組織(BGP AS番号)の上位を図-7と図-8に示します。

IIJ内の配信などが約6割を占めますが、それを除くと前回の本レポートVol.57(https://www.iij.ad.jp/dev/report/iir/057.html)同様に日本の大手コンテンツ事業者であるA社がIPv6トラフィック量1位になっています。2位はほぼ同量で米検索大手のB社、3位はランキング初登場のC社となりました。また、

表-5 過去6年のIPv6比率の推移

	2017年 IIR Vol.37	2018年 IIR Vol.41	2019年 IIR Vol.45	2020年 IIR Vol.49	2021年 IIR Vol.53	2022年 IIR Vol.57	2023年 IIR Vol.61
IPv6比率	4%	6%	10%	10%	~~16%~~ **11.2%**	~~17.8%~~ **15.1%**	20.1%

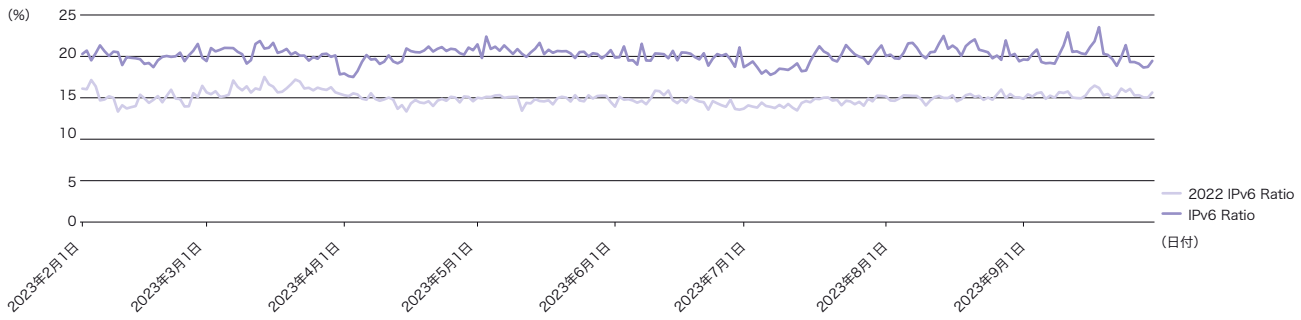


図-6 トラフィック全体に占めるIPv6の比率

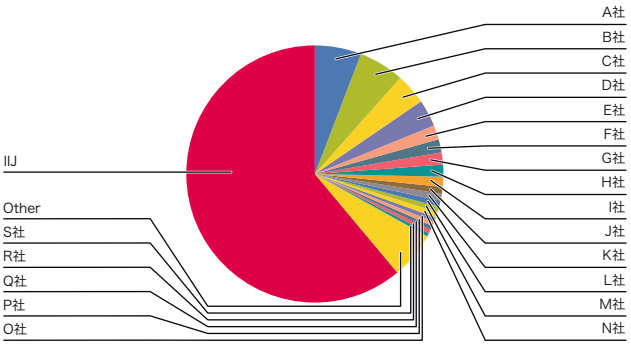


図-7 IPv6の平均トラフィック送信元組織(BGP AS番号)

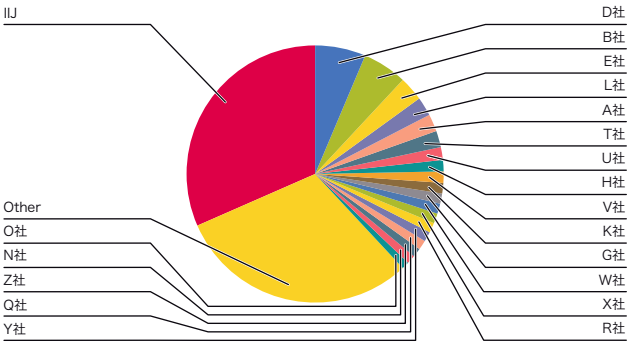


図-8 IPv4の平均トラフィック送信元組織(BGP AS番号)

© Internet Initiative Japan Inc.

大きな順位変動としては、米クラウド事業者のH社が16位から8位に、米CDNのM社が5位から13位に変わっています。M社は昨年買収がありましたので、ネットワーク再編をしているのでしょうか。

■ 利用プロトコル

IPv6トラフィックのProtocol番号（Next-Header）と送信元ポート番号で解析したグラフを図-9に、IPv4トラフィックのProtocol番号と送信元ポート番号のグラフを図-10に示します。期間は2023年10月2日（月）から10月8日（日）までの1週間です。

IPv6では、昨年4位のTCP80（HTTP）が昨年5位のESP（IPSec）と逆転しています。HTTPSやQUICへの移行が進んでいる現れでしょうか。6位以下はトラフィック量が少なく、切り取る期間によって順位変動が大きいものと思われます。

1つこのグラフで興味深いところは、10月8日の夜19時頃から22時頃までのトラフィック量の変化で、図-9の一番右側の山の部分になります。TCP443（HTTPS）がかなり増加しているのが分かりますが、この時間帯に何があったか調べてみると、ラグビーワールドカップ2023フランス大会の日本代表対アルゼンチン代表の試合、そしてパリ五輪予選を兼ねたワールドカップバレー2023の日本対アメリカの試合でした。どちらの試合の影響が大きかったのか分かりませんが、IPv6での中継も一般的になってきていることを感じます。

■ モバイルのIPv6接続状況

昨年の本レポートVol.57（https://www.iij.ad.jp/dev/report/iir/057.html）に引き続き、今回も個人向けモバイルサービス（IIJmioモバイルサービス）の接続における、IPv6有効化率を調査します。今回は端末OS種別による違いに加え、端末メーカによる違いの有無も見てみることにします。

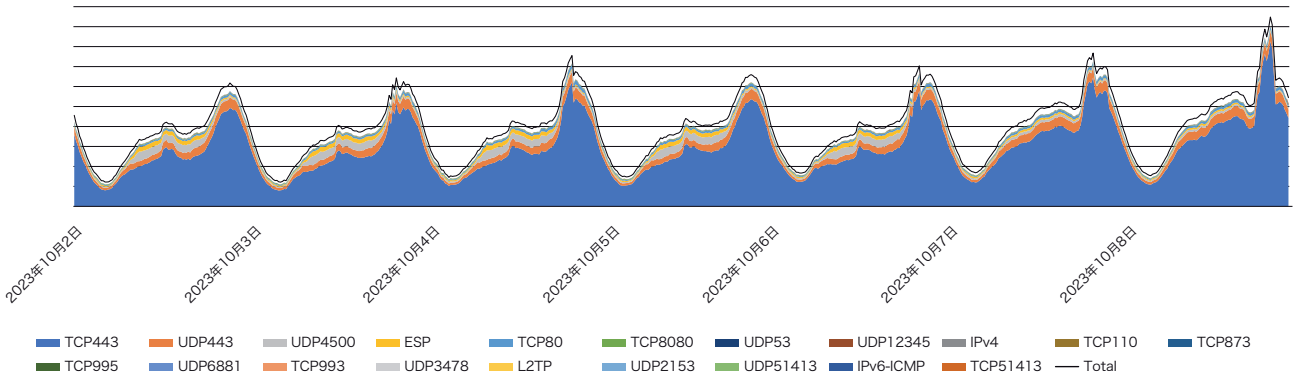


図-9 IPv6トラフィックの送信元ポート解析

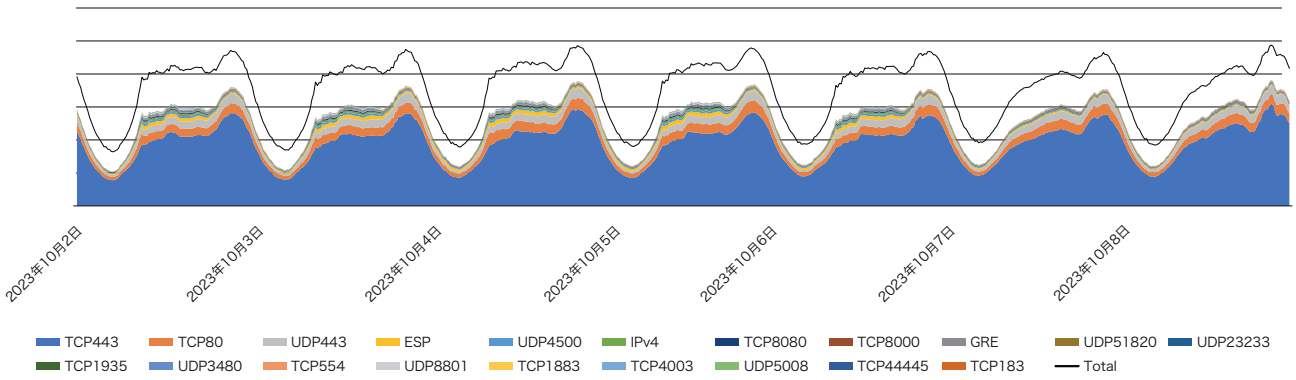


図-10 IPv4トラフィックの送信元ポート解析

© Internet Initiative Japan Inc.

昨年の調査では、IPv6有効な接続が全体の56.3%で過半数となっていました。今回は2023年10月20日（金）15時30分頃の時点で、IPv6有効化率58.73%となっており、若干（2.43ポイント）増加していました。また、Apple iOSとAndroidで比較すると、Apple iOSのIPv6有効化率は86.37%で昨年比0.67ポイントの微増、AndroidのIPv6有効化率は25.82%で昨年比4.12ポイントの増加となっています。

次に、IIJmioモバイルサービスに接続している端末の上位20位までのメーカ別IPv6有効化率を見てみます。図-11に上位20社のグラフを示しますが、1位のAppleが接続数としては飛び抜けているため、下位の棒グラフは見づらいものとなってしまいました。具体的な数は示せませんが、IIJmioにおけるApple端末の接続数シェアとしては、54.3%となっており、1社で過半数となっています。そして、Apple端末のIPv6有効化率は、前回の調査（85.7%）から若干伸びて86.35%となりました。

2位は1位と大きな開きがありますが、シャープ製端末となっています。こちらはIPv6の観点では残念ながら、2.73%しか有効となっておらず、端末のAPNプロファイルのデフォルト設定がIPv6有効になっていないものと思われます。Android端末はAPN設定でPDP-TypeをIPv4、IPv6、IPv4v6の3種の設定から選択できますが、ほとんどのユーザはデフォルト設定のまま使う、もしくはAPN自動設定で使っていると想定され、出荷時のデフォルト設定がどのようになっているかでIPv6有効化率は大きく変わるものと想像しています。

3位以下はIPv6有効化率の高いメーカについてのみ触れます。3位Googleは非常に高いIPv6有効化率（89.63%）となっており、Apple以上のIPv6率となっています。また、7位のMotorolaも89.12%と、率ではAppleより多くなっています。

10、11、12及び17位にSonyやSony Mobileが並んでいますが、こちらをすべてSony1社として合算すると全体の5位になり、Huaweiの上に躍り出ます。なお、その場合SonyのIPv6有効化率は14.7%となり、あまり有効化率は高くありませんが、日本メーカの中では高い方となっています。

メーカ別に全体的に見ると、米国のメーカはIPv6有効化率が高く、日本や中国などのメーカでは、IPv6有効化率が低い傾向にあるようです。

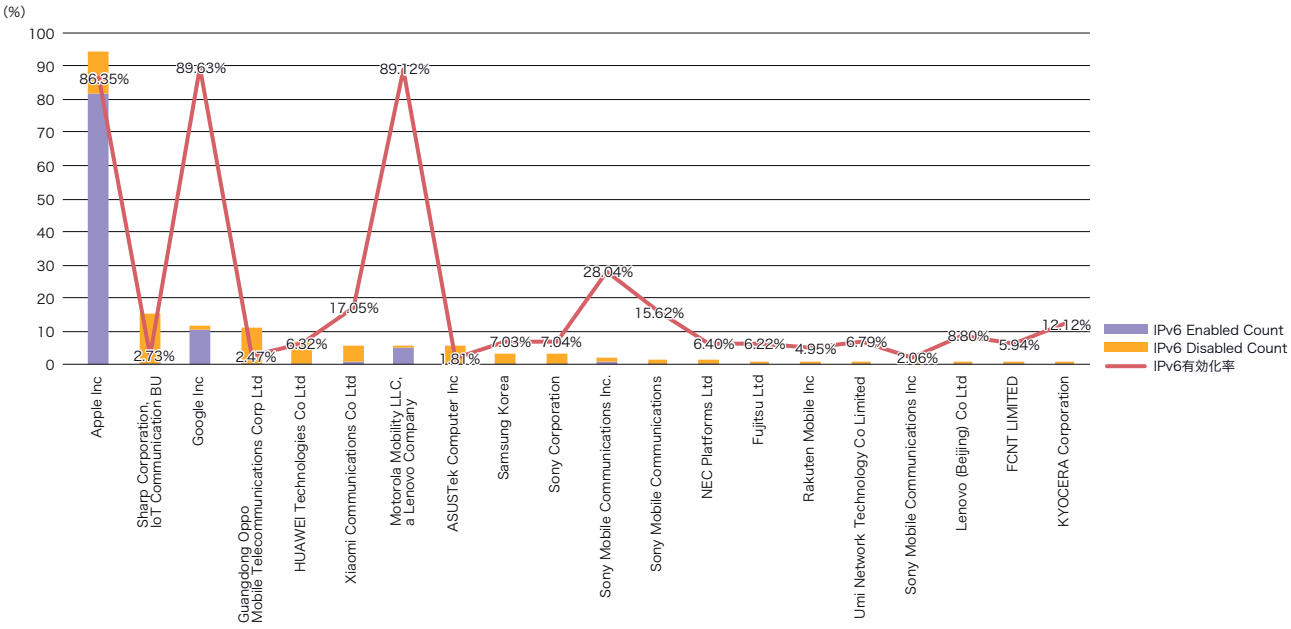


図-11 UEメーカIPv6有効化状況（上位20社）

© Internet Initiative Japan Inc.

■ まとめ

今回もIIJバックボーンコアのトラフィック、送信元AS、プロトコルについて紹介しました。トラフィック量は期中横ばいですが昨年比では増加、IPv6の利用率も1年前より増加し、過去7年で最高となりました。送信元ASは具体的な名前を書いていないので分かりにくいと思いますが、意外な国が伸びていることが分かりました。大手CDN事業者も一通りIPv6対応が進んでいるようで、あまり意識せずIPv6を利用・有効化する時代になってきたようにも思います。

利用プロトコルについては、ここ数年（10年以上？）世の中の多くのサービスがAPI含めてHTTP（S）を利用するようになり、TCP/UDPのポートだけ見てもアプリや利用用途は分かりません。ですが、IPv6の方が相対的にHTTPS/QUICの利用が多いことは見て取れます。比較的新しく構築されたシステムでは、HTTPS/QUICを導入すると共にIPv6も一緒に有効化が進んでいるのだろうと想像しています。

モバイルについては、Android系OSの端末でIPv6有効化率が上がっているのが確認されましたが、日本・アジアのメーカは米国メーカに遅れを取っているように見受けられます。いろいろな事情があるところかとは思いますが、より多くのユーザが自然にIPv6を利用できるよう、APNのデフォルト設定をPDP-Type IPv4v6にすることを検討いただきたいと思います。

引き続き様々な角度からIPv6の状況を観察しつつ、何か新しい発見がありましたら紹介したいと思います。

Theme 04

モバイル3G、LTE（5G NSA含む）の状況

ここ数年間、モバイルのトラフィック傾向はコロナ禍の影響を受けた状況となっていました。ここ1年での世の中の動きとしては、2023年5月8日に新型コロナウイルス感染症の位置づけが「新型インフルエンザ等感染症（いわゆる2類相当）」から「5類感染症」に変更されました。それを踏まえて、ここ1年間のトラフィック状況をまとめます。対象期間は、2022年10月1日から2023年9月30日です。

まずは、NTTドコモが2026年3月末で3G通信サービスを終了することになっています。現状の3Gトラフィックはどのようになっているかを報告します。

全体トラフィックにおける3G（図-12）の割合は下記のとおりになっています。コンシューマ向けサービスにおいては平均で全体トラフィックの0.033%程度しか3G通信はなく、ほぼゼロに等しい状況になっています。法人向けサービスにおいては平均で全体トラフィックの4.25%が3G通信として使われている状況です。法人向けサービスのトラフィック傾向の3G通信に関する割合はほぼ横ばいという状況になっていますので、残り約2年半の間でどれだけ法人向けサービスの3G通信が減っていくかを見守る必要があります。

次は法人向けサービスにおけるトラフィック状況とセッション数状況を見てみます。2022年10月1日を基準日とし

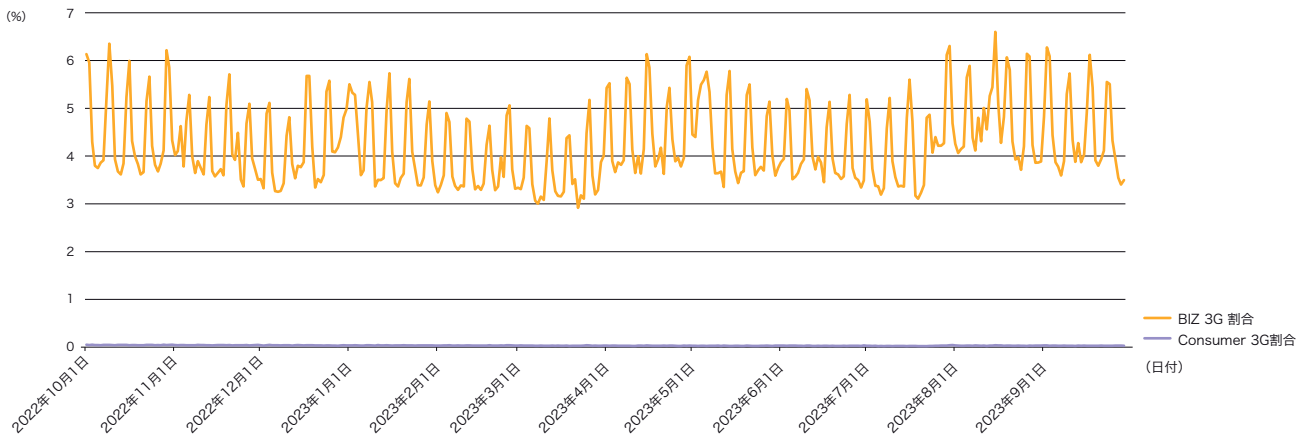


図-12 全体トラフィックにおける3G通信の割合

© Internet Initiative Japan Inc.

たときの法人向けサービスのトラフィック量(図-13)とセッション数(図-14)に関する傾向をグラフにしました。

まずトラフィック量についてです。LTEのトラフィック量に関しては徐々に増加傾向は年間通じて続いていますが、2023年4月以降と2023年7月以降は増加傾向が少しだけ加速しているように見えます。こちらに関してはキャリアとの相接点の集約を行ったことによりピーク時間帯以外の通信がより流れやすい状態になったことで効率的な活用につながったことが要因と考えられます。3Gのトラフィック量に関しては昨年報告した際には減少傾向という状況でしたが、ここ1年に関しては徐々に増加する傾向になっています。LTEのトラフィック

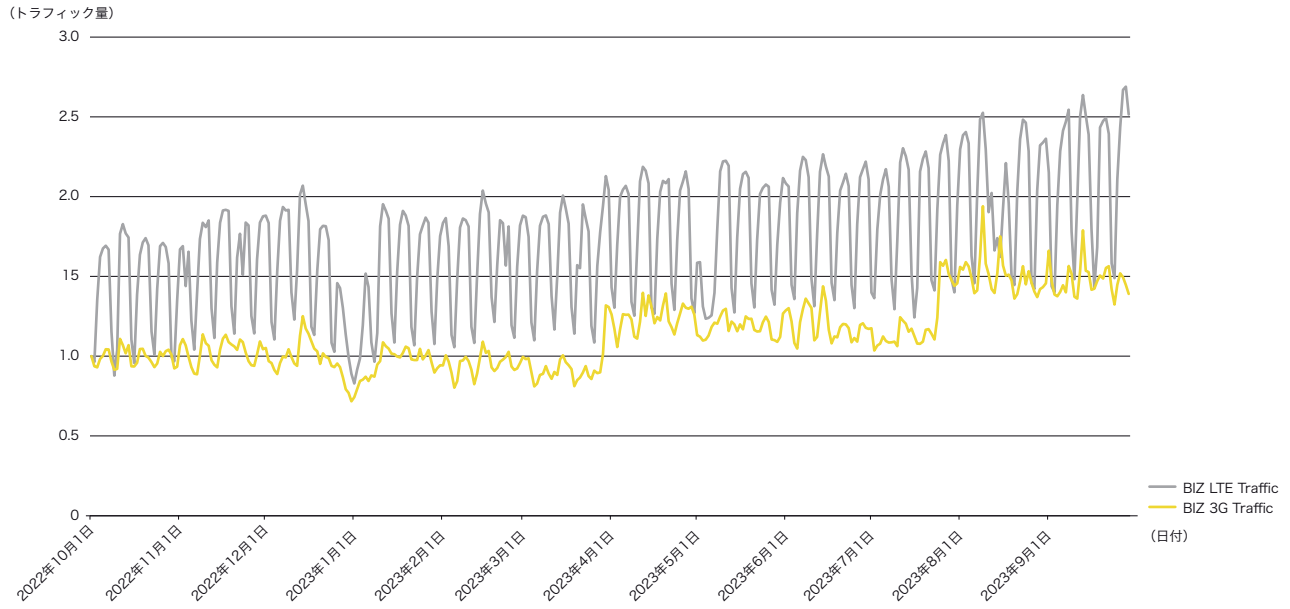


図-13 法人向けサービストラフィック量傾向

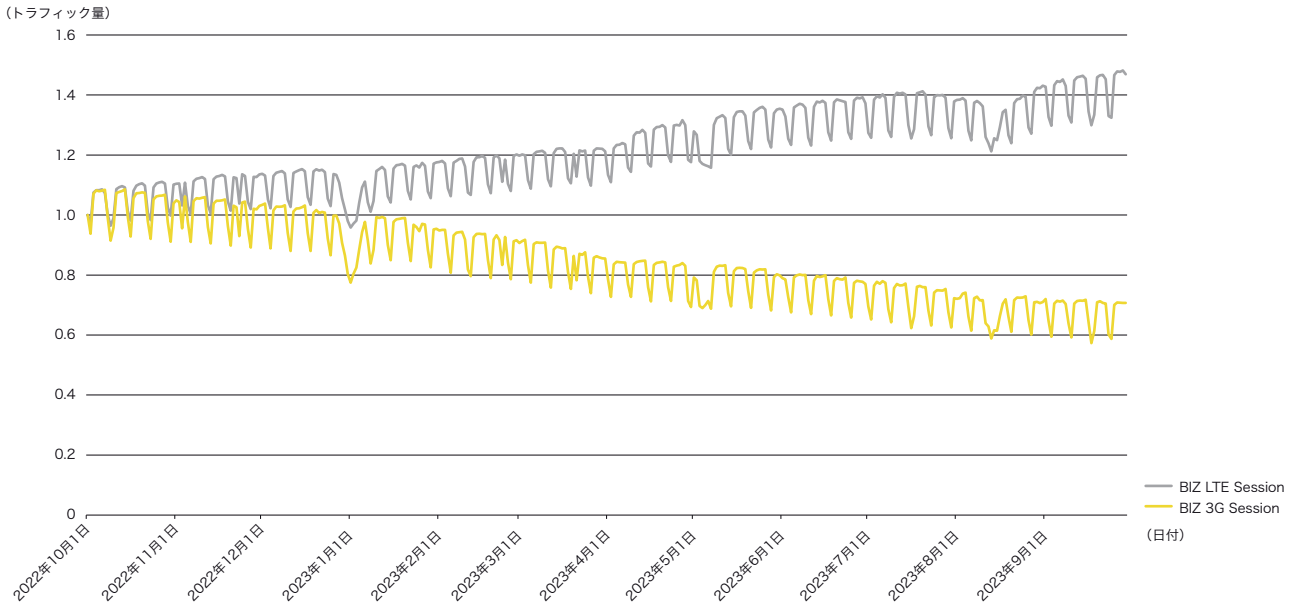


図-14 法人向けサービスセッション数傾向

© Internet Initiative Japan Inc.

量と同様に、3Gのトラフィックに関しても2023年4月以降と2023年7月以降で増加傾向が加速している状況になっています。こちらも前述の通りにキャリアとの相接点の集約による効果と考えられます。

また、セッション数に関してですが、LTEのセッション数はトラフィック量と同様に徐々に増加している傾向が年間を通じて続いている中、2023年4月と2023年5月それぞれで一段と多く増えているように見えます。多くの日本企業の会計年度の始まりという時期であるため傾向が変わりやすい時期ではありますが、今年に関しては新型コロナウイルス感染症の位置づけが変更されることにより企業の働き方が変更されたことによってモバイルの利用状況が増えた可能性があると考えられます。3Gのセッション数に関しては、トラフィック量に反し

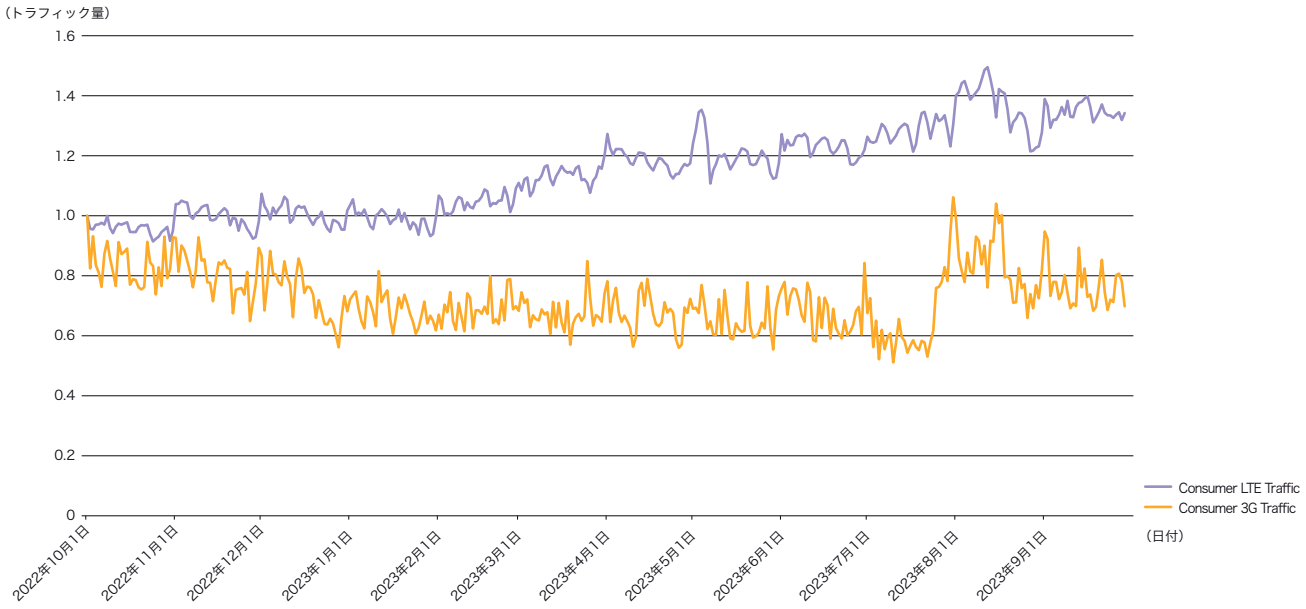


図-15 コンシューマ向けサービストラフィック量傾向

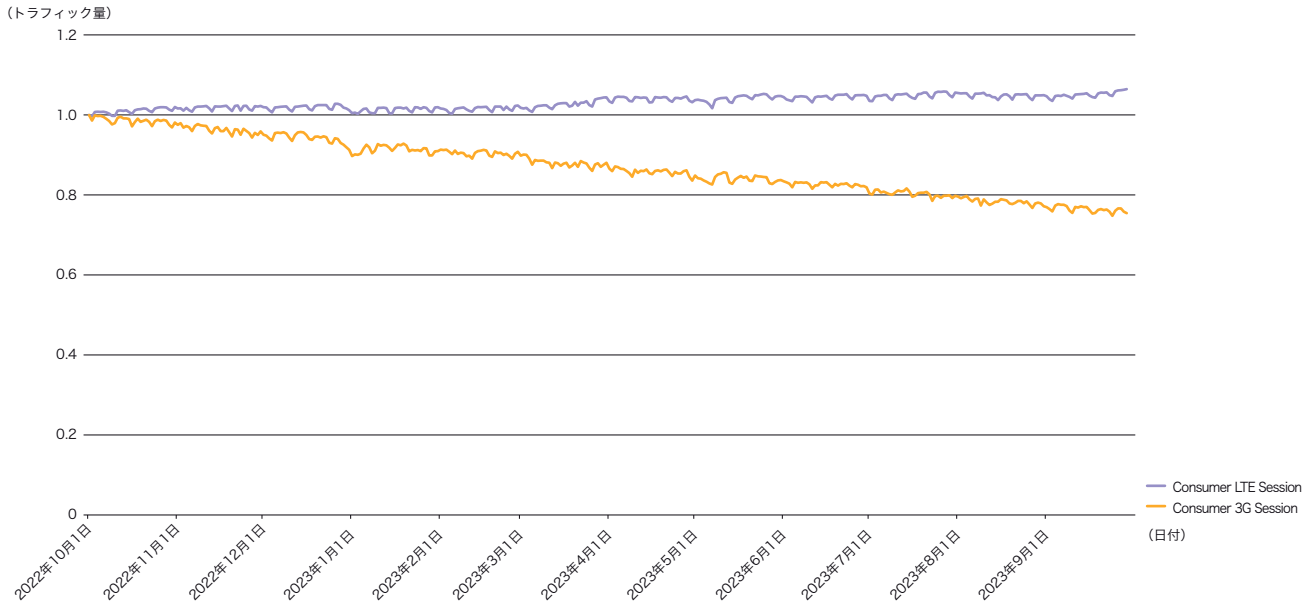


図-16 コンシューマ向けサービスセッション数傾向

© Internet Initiative Japan Inc.

て断続的に減少する傾向が続いており、約30%程度の減少となっています。セッション数が減っていることで3Gからの撤退が進んでいることが伺えますが、引き続き安定的なサービス提供を心がけながら見守りたいと思っています。

次は、コンシューマ向けサービスにおけるトラフィック状況とセッション数状況を見てみます。2022年10月1日を基準日としたときのコンシューマ向けサービスのトラフィック量(図-15)とセッション数(図-16)に関する傾向をグラフにしました。

コンシューマ向けサービスに関するトラフィック量に関しては先述のとおりほぼすべてLTE通信と言っても過言ではない状況です。ですので、ここではLTE通信の傾向を中心に説明していきます。コンシューマ向けサービスに関するトラフィック量は2023年2月頃まで特に目立った増減がなく、2022年10月頃から同等レベルのトラフィック量で推移しています。コンシューマ向けサービスのクーポン付与時期の関係で、1ヵ月間のトラフィック量の傾向は「月頭はトラフィック量が多く月末に向けて減る傾向になり、また翌月の月頭にトラフィック量が増える」ということを繰り返します。2023年2月頃まではこの傾向が顕著に出ています。2023年2月頃以降は傾向が変わり、右肩上がりの傾向となっています。これには前述の通りにキャリアとの相接点の集約による効果と考えられます。更に2023年5月1日前後のゴールデンウィーク期間中は通信量が一時的に増加しています。これは例年どおりの動きです。また2023年7月末以降は大きくトラフィック量が増加していますが、こちらも前述の通りにキャリアとの相接点の集約による効果と考えられます。同様に3G通信に関しても大きく効果が出ています。

また、セッション数を見てみると、LTE通信に関しては1年を通じて微増で推移しています。3G通信に関しては断続的に減少しています。2022年10月1日を基準日として年間で80%まで減少したという状況です。ここでは詳細な数値は控えますが、絶対数は3G停波までの道筋が見えたと思えるような数字になっています。

執筆者:

1.BGP・経路数
倉橋 智彦(くらはし ともひこ)
IIJ 基盤エンジニアリング本部 運用技術部 技術開発課

2.DNSクエリ解析
松崎 吉伸(まつざき よしのぶ)
IIJ 基盤エンジニアリング本部 運用技術部 技術開発課

3.IPv6
佐々木 泰介(ささき たいすけ)
IIJ 基盤エンジニアリング本部 モバイル技術部

4.モバイル3G、LTE(5G NSA含む)の状況
齋藤 毅(さいとう つよし)
IIJ 基盤エンジニアリング本部 モバイル技術部 部長

© Internet Initiative Japan Inc.

SIMの最新動向
～ハードウェアプロファイルからソフトウェアプロファイルへの進化～

2.1 SIM

2.1.1 携帯電話システムにおけるSIMカードの誕生

格安携帯電話で身近になったSIM(Subscriber Identity Module)カード。誰でも簡単に差し替えや交換ができ、当たり前のように利用していますが、それは携帯電話と同時に誕生したわけではありません。初期の携帯電話では「一体式」の通信規格だけがサポートされており、加入者情報は携帯端末内のメモリにハードコーディングされていました。NMT-450のような最古のアナログ規格には、セキュリティの対策が一切施されていない状態でした。要するに加入者情報を別の携帯電話にコピーすることで、クローン携帯電話を作成することができたのです。日本での応用例は、クローン ポケベルが有名で、1台分の契約で数十台のポケベルへメッセージをブロードキャスト的に送信することができました。

その後少し遅れて、初のセキュリティ手段となるSIS (Subscriber Identity Security)コード(端末ごとに異なるユニークな18桁の数値)が開発され、携帯端末内のアプリケーションプロセッサにハードコーディングされていました。また、複数の端末で同じSISコードが使われないよう、通信事業者へ均等に割り振られました。更に、プロセッサには、加入者が携帯電話ネットワークに登録する際に基地局へ送信する7桁のRIDコードも格納されていました。

SISプロセッサは、基地局が生成したランダムな数値と固有のSIS応答のペアを使って、認証鍵を作成しました。当初利用されていた鍵と数値は比較的短いもので、1994年の時点では十分妥当な長さとなりましたが、ご想像のとおりその後このシステムはクラッキングされることとなりました。それから3年後にGSM (Global System for Mobile Communications) 規格が登場します。このGSM規格はSISによく似ていましたが、暗号強度の高い認証システムを使用した、セキュリティの強化された仕様でした。この時点から通信規格における端末側の加入者管理は「分離式」になりました。

分離方式での認証とは、携帯電話機とはまったく別の超小型コンピュータに内蔵された外部プロセッサですべてを実行するということです。その結果、生まれたソリューションがスマートカードをベースにしたSIMカードです。

SIMカードの導入に伴い、加入契約と端末との間に依存関係が(論理的には)なくなったため、端末メーカは通信事業者を横断した端末を作ることが可能となり、大量生産によるコストダウンというメリットが生まれ、携帯電話の利用者は同じモバイルIDを使いながら、いつでも何度でも好きな端末へ変更できるようになりました。

SIMカードとは基本的に、ISO 7816規格のスマートカードがベースで、クレジットカードやキャッシュカードのような接触型ICカードとほぼ同じものです。最初のSIMカードはクレジットカードと同じサイズでしたが、携帯電話機の高度化に伴い各種部品の小型化の流れに従って、このSIMカードもコンパクトになりました。

登場当初のフルサイズ1FF(1st Form Factor)SIMカードは携帯電話のサイズに合わなくなってきたため、不要な部分をカットするという互換性を維持したシンプルな手段が開発されました。それがミニSIM 2FF(2nd Form Factor)と言われるもので、このサイズのSIMカードが登場した頃から日本でも格安携帯電話事業者MVNO(Mobile Virtual Network Operators)が登場し、SIMカードが流通し利用されるようになりました。

以降SIMカード小型化の傾向は、マイクロSIM(3FF)、ナノSIM(4FF)と続いていますが、全体的な形状、端子構成、組込まれているICチップの機能は約30年間変わらず、そのままです。昔ながらの携帯電話を今でも大切に使っている利用者のニーズに対応するため、プラスチック製のSIMアダプターといわれるものも存在します。とはいえ、旧式の端末の多くは、たとえアダプターを使ってSIMカードを装着できたとしても現在のSIMカードで動作するとは限りません。というのも、初期のSIMカードの動作電圧が5Vであるのに対し、最新のSIMカードは3Vだからです。このため、旧式の5Vのみに対応した携帯電話では、3Vのみに対応したSIMカードはプロセッサの電圧保護という理由から動作しません。更に端末の低少消費電力化に合わせ1.8Vで動作する事が求められ、3Vと1.8Vのデュアル電源電圧サポートのものが主流となっています。

© Internet Initiative Japan Inc.

2.1.2 SIMカードの役割と実態

SIMカードとは、携帯電話ネットワークシステムにおいて端末に対して「分離・独立」した非常にセキュアで小さな独立したコンピュータシステムで、そこに加入者契約証明のための認証情報である、IMSI(国際携帯機器加入者識別情報)と128ビットの鍵であるKi(鍵識別子)を代表とした「通信プロファイル」と呼ぶデータセットを保持し、基地局とのやり取りを経て携帯電話ネットワークシステムと接続しセキュアで安全な暗号化通信を実現します。IMSIには、MCC(Mobile Country Code)と呼ばれる国番号とMNC(Mobile Network Code)と呼ばれるモバイル通信事業者コードが存在し、MNCはMNOやフルMVNOに与えられます。

IIJモバイルは、2018年にNTTドコモのネットワークを利用したフルMVNOとなったことで、03というMNCを取得しました。同時に03というイッシュア番号も取得しました。物理的には、ISO 7816で定義され、基本として8つの外部接触端子があります。各端子は、以下のようになっており、通常携帯電話端末とはpin-1、2、3、5、6、7の6つの接点で接続されます(図-1)。

SIMカードの樹脂の中にはセキュアマイコンと呼ばれるICが封入されており、そのICはMPU、ROM、RAM、EEPROMで構成されています。そう、立派なコンピュータシステムです。

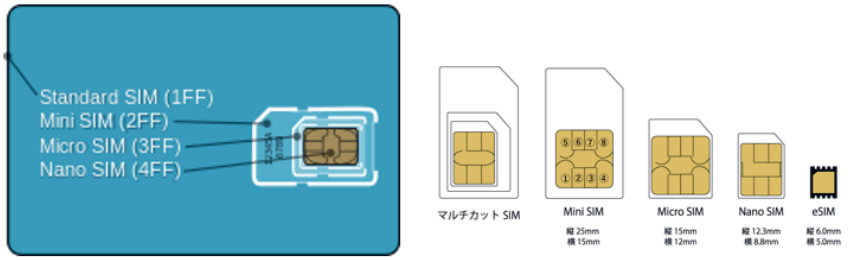
コンピュータであるが故にOSが存在します。多くのSIMはクレジットカードと同じGlobalPlatformをベースにしたOSを採用することで、暗号化File Systemを構成し、Java Appletが動作し、H/W側のみならずOS側でも耐タンパー性を有しています。S/Wとしては、暗号化/復号化エンジンが代表的なものであり、SIMとして利用するために必要なデータセット「通信プロファイル」を有します。余談ですが、クレジットカードにはクレジット決済を担保するために必要なデータセット「金融プロファイル」を有しています。

もう1つのルールとして、クレジットカードを含むスマートカードには、個体を識別する19桁のICCIDと呼ぶユニークなIDが必ずあり、その番号は業界識別子、国番号、イシュア番号とチェックデジットを含みます。IIJモバイルはイシュア番号を取得しているため、SIMカードを発行することが可能になります。

2.2 物理SIMなき世界に向けて

数年前までは、IIJが提供しているMVNOサービスを利用してもらうためには、Web経由の契約の場合、まずサービス契約申し込みをしてもらい、その後ユーザに物理SIMカードを配送し、端末にSIMカードを入れて初めてサービスが利用可能になるという流れでした。そのため物理的な配送を伴い、利用開始までに1週間前後かかる状況でした。SIMカードはモバイルサービスを利用するための物理的な鍵の役割を担っていました。

しかし、この物理SIMカードを利用する形態から、eSIMと呼ばれる仮想的なSIMのデータをインターネット経由で端末にダウンロードし、即座にモバイルサービスが利用できる仕組みが急速に普及しつつあります。更に、IoT分野ではセルラー対応通信モジュールの製造工場などでSIMデータを内蔵して、端末メーカに出荷し、物理SIMカードなしでもサービスが利用できるような仕組みが普及しつつあります。



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

図-1 SIMカードの8つの外部接触端子

© Internet Initiative Japan Inc.

無線通信の世代が2G → 3G → 4G → 5Gと進化する中、物理SIMカード形状が小型化するという変化はありましたが、物理SIMは利用され続けてきました。しかし、2G（GSM）の無線通信時代から約30年近く続いた、モバイルサービスの利用の鍵としての物理SIMが必要な時代が終わりを迎える転換点が迫ってきました。具体的にどのような動きがあるか、以下で紹介します。

2.2.1 PC、スマートフォン、タブレットなどのコンシューマ端末のeSIM対応

ここでのeSIMとはGSMA（GSM Association）と呼ばれるモバイル通信事業者やメーカなどの業界団体で標準化されたSGP.22で規定されるRemote SIM Provisioning仕様に基づく仕組みを指しています。eSIMの仕組みを使うことで、ユーザが持つ端末に自分の契約したいモバイル通信事業のSIMデータをダウンロードして、即座にサービスを利用することが可能になりました。

ノートPCでは、2017年に発売開始されたMicrosoft社Surface Pro LTE AdvancedでeSIM機能が初めて搭載され、それ以降世代のSurfaceのセルラー対応機種で標準的にeSIM機能が搭載されるようになりました。これを契機にMicrosoft社以外のWindows搭載PCのセルラー対応機種でeSIM機能の搭載が普及するようになりました。

また、スマートフォン、タブレットでは、Apple社の2018年発売開始されたiPhone XS世代以降のiPadを含む端末ではeSIM対応が標準となりました。また、Android搭載端末でも2018年発売のGoogle社の海外版Pixel 3からeSIM対応となり、それ以降、Google社以外のAndroid端末でもeSIMに対応した端末が増加しています。コンシューマ向け端末の世界では、Apple社の端末を中心にeSIM対応端末が標準的になりつつある状況です。

更にこの状況が進んで、北米で2022年に発売されたiPhone 14世代で"物理SIMカードスロットがないeSIM対応のみ端末"が出現し、業界に衝撃を与えました。この流れは世界中で発売される端末でも進む可能性が高く、コンシューマ向け端末の世界では、物理SIMなき世界の到来が待ったなしの状況になりつつあります。

この流れに対して、IIJは2019年7月18日に国内でいち早く、SGP.22規格に対応した「IIJmioモバイルサービス ライトスタートプラン（eSIMベータ版）」の提供を開始し、それ以降、順次様々なサービスでeSIM対応を推進してきました。

2.2.2 セルラー通信対応IoT端末のSIMについて

コンシューマ向け端末と異なり、セルラー通信対応IoT端末は4Gなどに対応した通信モジュールとSIMを内蔵しているのが一般的です。IoT端末を利用するエンドユーザは自身で通信サービスを契約するとは限らず、IoT端末メーカのサービスとして意識せずに利用することが多いです。この場合、IoT端末メーカは事前に通信事業者と契約し、物理SIMを調達し、製造ラインで組み込み、端末を出荷するということを行ってきました。

このようなIoT端末の世界では次の2点の要望が高まっています。

(1) IoT端末の小型化で物理SIMカードのスペースの確保が困難な場合や利用環境が過酷な条件では通常の物理SIMカードだと耐えられないのでカード型に代わる物理SIMが欲しい
(2) 契約する通信事業者を工場出荷時点で決めずに後から決定したい、また、端末設置場所の位置の電波状況で通信事業者を変更したい

(1)に関しては、物理SIMカードをより小型化したICチップ形態のMFF2規格の物理SIMがヨーロッパの標準化団体ETSIで策定されており、既に利用されています。更にこれを進めて、SIM機能を通信モジュール内にソフトウェアとして内蔵してしまう独自実装方式のSoftSIM、iSIMまたはiUICCと呼ばれる方式も利用されつつあります。

© Internet Initiative Japan Inc.

また(2)に関しては、IoTを含むM2M用eSIMの GSMA SGP.02規格が、SGP.22よりも前の2013年頃に策定されましたが、特定の通信事業者が提供するサービスを利用する必要があり、一般的なIoT用途では普及しませんでした。そのため、特定通信事業者に縛られないSGP.22ベースのeSIMの仕組みを流用し、独自実装をしてIoT端末で利用できるようにする方法や、SGP.22を流用する形で、2023年にIoT向けの新たな規格SGP.32が策定され、これを利用することが検討されています。

この流れに対して、(1)に関しては、IIJでは2019年からMFF2形態のSIM提供と、また、特定通信モジュールと組み合わせたSoftSIMでの提供を開始してきました。また(2)に関しては、IIJとしていくつかの取り組みや調査を行っていますので、後述します。

2.2.3 物理SIMなき世界に向けての取り組み

物理SIMなき世界が近い将来に迫ってきており、物理SIMを流通させることで行っていたモバイルビジネスが大きな転換期を迎えています。エンドユーザ観点では、eSIMなどの普及によってモバイルサービスが便利に使えるようになる程度の認識の方が多いかと思います。一方で、モバイルサービスの鍵となる物理SIMのような重要なパーツがなくなる際に、新たな技術を取り入れずにその流れに乗り遅れると通信事業者としては死活問題となります。このような流れで物理SIMなき世界に向けて、IIJでは技術的な調査、研究、開発を継続しています。次節では、特に課題となっているIoT端末向けの取り組みを中心に紹介します。

2.3 IIJモバイルが実現しているSIMカード応用ソリューション

IIJモバイルにおいて、SIMというコンピュータシステムを見つめ直すことで可能としたいくつかのソリューションを紹介します。

2.3.1 Multi Profile SIM

端末側に負担を掛けず、複数枚のSIMカードを選択的に利用可能にしたソリューションとして、物理的には1枚のSIMカードに論理的には複数枚のSIMカードを構成し、外部からの指示(APDU)で内蔵している特定のSIMカードを活性化するというものです。SIMソケットが複数ある場合は、電気的にアクセスするSIMソケットを切替えることで実現できます。DSSS(Dual SIM Single Standby)ですね。

イメージとしては、例えば1/2の厚さにした薄い2枚のSIMカードを重ねてSIMソケットへ実装し、外部からのコマンドによる指示で重ねた順番を入れ替えるというものです。SIMソケットが1つでも、機能的にはDSSSが実現できます(図-2)。

2.3.2 SoftSIM

SIMに必要な要素としては、MPU、ROM、RAM、I/O、OS、通信プロファイル、暗号化/複合化エンジン、SIM通信プロトコル(APDU)の実装、etc.となり、IIJモバイルが応用ソリューションとして提供しているのが「SoftSIM」です。

簡単に言えば、コンピュータの仮想化技術を持ち込み、通信モジュールのセキュアな領域に仮想SIM(コンピュータ)を実装し、通信プロファイルを別管理しOTAで書き込むというeSIMの考え方を取り込んだソリューションです。

2.3.3 LPA-Bridge

IoT端末には、スマートフォンのようなリッチなUIや複数のNetwork I/Fを望むことは非常に困難ですが、スマートフォンの一部にも存在するセンサーとLTEモデムとeSIMチップを別端末として切り出したものがIoT端末と捉えることもできます。スマートフォン側のLPA(Local Profile Assistant ≒ eSIMプロファイルの制御アプリ)は自身に内蔵されたeSIMチップへプロファイルを取得/削除/選択 操作するがごとく振る舞わせますが、LPA-Bridgeと連携させることで、LPAの操作ターゲットがスマートフォン自身のeSIMチップからIoT端末内のeSIMチップへ変更します。

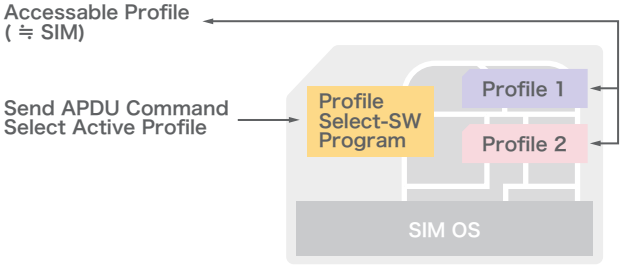


図-2 複数SIMの選択的利用

© Internet Initiative Japan Inc.

標準化されたアーキテクチャに手を入れることなく、ソフトウェアの介在でこれまで導入が困難だったIoT端末へコンシューマモデルのeSIMを導入することを可能にしたソリューションです。

2.4 eSIM技術の規格変遷とIoT eSIM

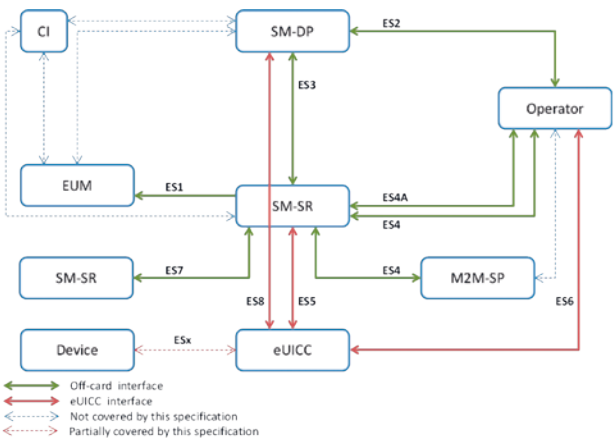
2023年5月26日にGSMAよりIoT端末向けのeSIMの技術仕様であるSGP.32が公開されました。eSIMの技術仕様としては、既にM2M端末向けのSGP.01/02、コンシューマ端末向けのSGP.21/22が公開されており、このIoT端末向けのSGP.31/32が3番目の方式となります。ここでは、本仕様にいたるまでのeSIMの規格の変遷と、特徴について解説します。

2.4.1 IoT eSIMの標準策定まで

eSIMという略称はもともとEmbedded SIMのことであり、端末の基盤上に実装されたSIMを想定しています。物理SIMカードと異なり製造後に交換することが困難なため、プロファイルと呼ばれるSIMを定義するデータをハードウェアから切り離し、このプロファイルを入れ替えることでSIMの交換を実現しています。このプロファイルの操作を遠隔から実現する仕組みをRSP(Remote SIM Provisioning)と呼びます。

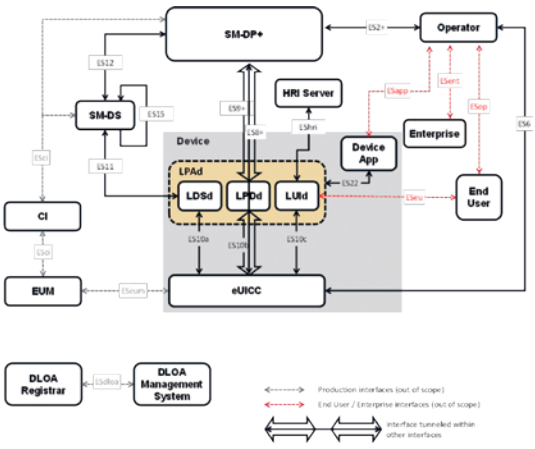
最初に公開された仕様はM2M (Machine-to-Machine)端末向けに定義されたSGP.01/02です(以降M2M eSIMと記載)(図-3)。複雑な機能を持てないIoT端末を想定したのか、ほとんどの機能をSIM上に実装し、端末とのインタフェースもそれまでのSIMの規格内に留める仕様となっています。一方で、eSIMと通信するサーバ(SM-SRと呼びます)を中心に、通信事業者が提供するプロファイル提供サーバ(SM-DPと呼びます)を繋ぐ必要があり、大掛かりなシステム構成となります。また、遠隔操作のためのトリガとしてSMSを利用しており、導入するプロファイルはいずれもSMS機能が要求されていました。SMS利用のためセルラー通信を前提とすることから、Bootstrap Profileと呼ばれる、端末が利用される場所において通信を担保するプロファイルを必要とします。全体的にシステムの構築・運用に多大なコストがかかる規格のため、単価が高い自動車、特にeCallが要求され、国を跨ぐことが多い欧州での自動車業界に留まっている印象です。海外のカンファレンスなどでは単独通信事業者が自国のスマートメータなどへ導入するような事例を紹介されることはありましたが、フィールドでの自社プロファイルの配布に留まり、M2M eSIM本来のスペックを活かしきれていない印象を受けました。

続いて公開された仕様は、ヒトが直接操作するコンシューマ端末向けに定義されたSGP.21/22です(以降Consumer eSIMと記載)(図-4)。ヒトが直接操作することを想定していたため、そのためのアプリ(LPA)を導入した仕組みとなっています。端末上に実装されたLPAを介して操作を行うため、遠隔操作で要求されていたSMSは不要となり、プロファイルを取得するための通信はIPに統一されました。また、M2M



引用元：GSMA SGP.43 v4.3

図-3 M2M eSIMのアーキテクチャ



引用元：GSMA SGP.22 v3.0

図-4 Consumer eSIMのアーキテクチャ

© Internet Initiative Japan Inc.

eSIMで端末との通信を中継していたSM-SRを廃し、通信事業者が提供するSM-DP(Consumer eSIMではSM-DP+と呼びます)と直接通信する方式としました。特定の通信事業者に縛られないオープンなマーケットが構成されることとなり、広く普及していくことになります。実際、2018年に大きな市場を持つApple社のiPhone XSが正式に対応したことで、Consumer eSIMは急激に広まっていきました。Apple社のiOS以外にも、Microsoft社のWindows 10やGoogle社のAndroid 10にもLPAが実装され、ノートPCやスマートフォン、タブレットの主要OS全てがeSIMに対応することとなり、多くのコンシューマ端末で利用可能なエコシステムが構築されることとなりました。IIJでも、2019年にフルMVNOの基盤上にeSIMのサービスを国内の他事業者に先駆けて開始しています。

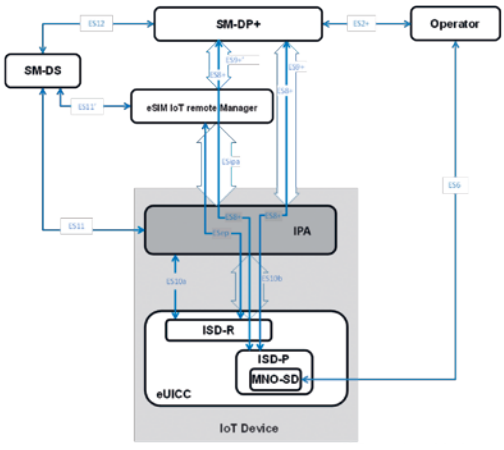
ノートPCやスマートフォン、タブレットが対象となっているConsumer eSIMですが、スマートフォンなどを経由して別の端末にeSIMを導入する仕組みも定義されています。この仕組みによりヒトが直接操作しないIoT端末にもConsumer eSIMが導入可能となりました。しかし、GSMAの標準ではアーキテクチャのみの提示で、端末間のプロトコルの仕様は定義されておらず、個々のベンダーが独自に実装しているのが現状です。また、スマートフォンなどとの連携が必要なため、結果的にスマートウォッチといったウェアラブル端末に限られることとなり、広くIoT端末に普及したとは言い難いものでした。そのような中で、主要なスマートフォンの市場の飽和も見え、次の市場としてIoT端末がターゲットとして考えられるようになりました。本来であればM2M eSIMがこの領域をカバーするべきでしたが、前述のとおりコスト面から導入が難しく、Consumer eSIMではM2M eSIMでサポートしていた遠隔操作の具備に独自実装が必要となるため、IoT端末向けのeSIMの方式(以降IoT eSIMと記載)が必要とされることとなりました。GSMAの標準策定はオープンではないこともあり、状況はベンダーなどが開催するセミナーなどでしか伺えませんが、筆者が聞いている範囲では2020年頃からIoT eSIMに関する動きがありました。最終的に、2022年の4月にアーキテクチャとシステム要件(SGP.31)、そして2023年の5月に技術仕様(SGP.32)が公開され、プロトコルの仕様が標準化されました(図-5)。今後はこの規格に基づいたIoT端末が市場に投入されていくと考えられ、ヒト向けとは比べものにならない回線数が見込まれるIoT端末の市場がeSIMにも開かれると期待されます。

2.4.2 規格の特徴

既に広まっているConsumer eSIMの市場を利用可能となるようIoT eSIMの規格は策定されています。プロファイルを提供するサーバとしてはConsumer eSIMで使用されているSM-DP+を用い、eSIMのチップとのインタフェースについてはConsumer eSIMを踏襲しつつ、遠隔操作を行う上で必要となる機能を追加しています。Consumer eSIMのSM-DP+をそのまま用いることが可能なため、プロファイルを提供する通信事業者の視点では追加対応は不要です。

Consumer eSIMとの違いとして、端末に実装されていたLPAの機能を、サーバ(eIMと呼びます)と端末アプリ(IPAと呼びます)に分離している点が挙げられます。eIMに利用者(eSIMを操作する者)へのインタフェースを実装し、eIMとIPAが通信することで、端末に実装されているeSIMをリモートから操作することが可能となっています。IPA自体はユーザインタフェースを持たないため、LPAと比較してプログラムのフットプリントが軽く、リソースが限られたIoT端末でも実装が容易となっています。

多様なIoT端末に対応するため、eIMとIPA間の機能配分はかなり柔軟な設計が可能なように見受けられます。大きな点と



引用元:GSMA SGP.31 v1.1

図-5 IoT eSIMのアーキテクチャ

© Internet Initiative Japan Inc.

しては、Indirect Profile Downloadと呼ばれるeIM経由でSM-DP+と通信する機能をサポートした点が挙げられます。GSMAの標準仕様では、IPAとSM-DP+との通信方式に関して、直接通信するDirect Profile Download（図-6）と、eIMを介して通信するIndirect Profile Download（図-7）の2つの方式を定義しています。前者のDirect Profile Downloadでは、IPAがSM-DP+との通信を行うため、SM-DP+のアドレス解決やHTTPS通信を行う必要があります。一方、後者のIndirect Profile Downloadでは、eIMがSM-DP+と通信するため、IPA自身がアドレス解決やHTTPS通信を行うことが不要となり、IPAはeIMとの通信のみを考慮すれば十分となります。

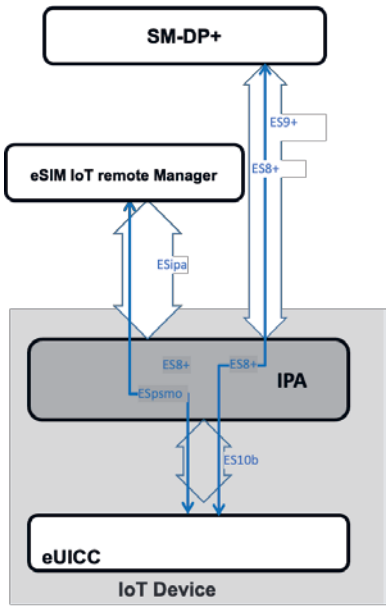
また、IPAとeIM間の通信プロトコルとしてGSMAの標準仕様ではHTTPSとCoAPを定義していますが、任意のプロコトルを許容しており（付録としてLwM2MやMQTTへのサポート方法が記載されている）、非IP通信への対応も考慮されています。Indirect Profile Downloadを採用することで、IP通信を前提としていたConsumer eSIMを通信事業者側の設備変更なしに、非IP通信端末でも利用できることになります。この辺りは、SMSで完結可能なM2M eSIMのアーキテクチャも踏襲して定義されたのではないかと考えられます。

2.4.3 市場への展開

Consumer eSIMが普及し、次のeSIMのターゲットはIoT端末、特にウェアラブルとされる端末という話が数年前より上がっていました。回線数を増やしたい通信事業者の思惑もあるでしょうが、物理的なスペースが限られるウェアラブル端末では、物理SIMカードが不要となるeSIMは非常に魅力的な仕組みです。

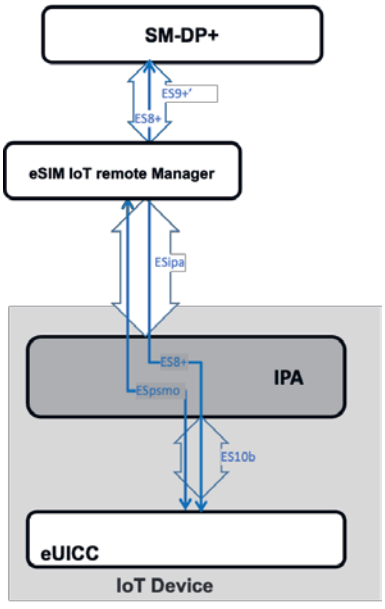
M2M eSIMと異なり、通信を提供する通信事業者を、Consumer eSIMを提供する通信事業者から任意に選択可能なため、小ロットの端末でも比較的導入しやすいと言えます。また、グローバルモデルの端末を作成する場合において、現地の通信事業者のプロファイルを後から導入可能なため、製品を共通化できるメリットがあります。

一方で、普及にはまだ課題があります。プロファイル自体はConsumer eSIMと同じものが使える一方、Bootstrap Profileをどうするかという課題が残っています。Consumer eSIMでは、対象となるノートPCやスマートフォン、タブレットといった端末は、セルラー以外の通信手段（Wi-Fi接続など）を持っており、Bootstrap Profileについては無視できる状



引用元：GSMA SGP.31

図-6 Direct Profile Download



引用元：GSMA SGP.31

図-7 Indirect Profile Download

© Internet Initiative Japan Inc.

況でした。また、スマートウォッチなどにおいてもスマートフォン経由での通信が可能であり、Bootstrap Profileなしでプロファイルの導入が可能でした。一方で、限られたリソースの中で実装が必要なIoT端末では、セルラー以外の通信方式を採用できない可能性があり、初期のプロファイルをインストールするためのBootstrap Profileがどうしても必要となってきます。M2M eSIMと異なり、明確なBootstrap Profileは存在しないため使い捨てのプロファイルでも問題はありませんが、eSIMのチップを提供するベンダー、もしくはIoT eSIMのプラットフォームを提供する事業者(通信事業者ではない)が初期プロファイルを提供しない限り、IoT端末ベンダーが導入するのは難しいのではないかと考えられます。

また、IPA自体の実装もIoT端末ベンダーからは足枷になる可能性があります。SIMへ直接アクセスが必要となるため、端末アプリではなく通信モジュール内で実装されることが多いと考えられますが、その場合、利用可能な通信モジュールが限られてしまうこととなります。ただ、こちらについては、SIM内にIPA機能を実装するIPAeという実装方式も存在するため、SIMカードベンダーがこの方式に対応したIoT eSIM OSを提供するようになれば解決するのではないかと考えられます。

その他、他の方式との競合の問題もあります。IoT eSIMに先立ち、Consumer eSIMもバージョン3においてプロファイルの遠隔操作(Remote Profile Manager:RPMと呼ばれます)をサポートしました。現段階での仕様では、RPM機能がサポートするのはインストール済のプロファイルを切り替えるのみで、新しくプロファイルを追加する機能はサポートされていないようです。標準化自体、同じGSMAが進めていることもありますので、完全に競合する方式とすることはないと考えられますが、このあたりの動向は注意が必要と考えます。

なお、IoT eSIMは技術仕様が公開されたばかりであり相互接続検証に必要となる試験仕様(SGP.33となる想定)が策定中の段階のため、市場への導入はもう少し先になると思われます。

2.5 結び

本稿では、物理SIMなき世界がすぐそこまで迫っており、スマートフォン、タブレットなどの端末向けの状況とIoT端末向けの状況について解説しました。特に、IoT端末では物理SIMなき世界を迎えるあたり、まだ技術的な課題や、検証、開発が必要な状況があり、IIJの取り組みについて紹介しました。

IIJでは物理SIMなき世界においても、モバイルサービスを便利に使える環境を提供し、インターネットによるイノベーションを促進してネットワーク社会の発展に貢献してまいります。

執筆者:

圓山 大介(まるやま だいすけ)
IIJ MVNO事業部技術開発部MVNOプロジェクト推進課 シニアエンジニア
音声交換機の開発から始まり、携帯電話の音声設備開発を経てモバイルネットワークの分野に進出。主にSIMに関する技術の調査やサービスの開発に従事。

大内 宗徳(おおうち むねのり)
IIJ MVNO事業部技術開発部モバイルプラットフォーム開発課 シニアエンジニア
モバイルに関する先端技術の調査、研究とそれを活用したサービス開発に従事。

三浦 重好(みうら しげよし)
IIJ MVNO事業部 ビジネス開発部
組込系のH/W、S/WからDBMS系アプリケーションの設計開発、システムアーキテクチャ設計まで、社会に出て40年技術屋を生業にしている。ここ数年は何周か廻って組込屋の知識が重宝され、モバイル系IoTデバイスの開発支援やSIMの応用利用に取り組んでいる。

© Internet Initiative Japan Inc.

IIJとセキュリティの変遷〜この30年を振り返って

3.1 はじめに

私たちがセキュリティ事業を開始してから現在までの間、様々な事件や事故が発生しています。この30年を振り返ると、インターネットは一対一が主であった通信サービスの世界に、一対多の通信や多対多の通信を実現するプラットフォームとして定着してきました。また、その通信の在り方や構成要素は常に変化しており、一部の人だけが利用するネットワークであった頃から、企業などで使える、商用サービス、個人向けサービス、家庭の常時接続、携帯電話からのアクセス、クラウド、スマートフォン、IoTと変化してきています。

それに合わせて、利用のされ方も変化し、私たちの生活を変えてきました。特に、ブラウザを使った暗号通信の一般化から電子商取引が盛んになり、本人認証の拡張などと合わさって、日々より重要な、金銭的に価値のある情報を交換できるようになっており、今日ではスマートフォンを使ってクレジットカードでの買い物やオンラインバンキングの利用が普通のこととなっています。

一方で、このような状況は悪事を働く者にも同様に作用し、特に長距離や多数の相手に通信を実施してもコストが低く抑えられる通信特性を悪用されたりしています。またコンピュータシステム同士の通信であることから、脆弱性を悪用してユーザの気づかないうちに悪影響を与えるような場合も発生します。その悪事も、単にシステムを乗っ取って勝手に利用することから、金銭価値の高い情報やサービスの盗用、知財などの窃取、身代金の強奪などと、多岐にわたってきています。

本稿では、IIJのセキュリティ事業の第一線で活躍してきた人たちの経験を共有し、それぞれの目線でこの30年を振り返りたいと思います。

ネットワークの脅威の変化

セキュリティ本部セキュリティ情報統括室
土屋 博英

1993年には日本でも商用インターネットが開始されましたが、当時からワームやウイルスといった脅威は存在していました。また、開いているポートに対するログインを試みる通信なども行われていました。企業等が業務でインターネットを利用するにあたっては、こういった攻撃への備えが必要なことからIIJでも1994年には国内初となるファイアウォールサービスの提供を開始しています。

2000年に入ると、インターネットはホームページの閲覧やメールやメッセージのやりとりなど、単純な情報のやりとりといったものを超えて、金融やオンラインショッピングなど、ビジネスを含めた経済活動の社会基盤として使われるようになり、急速に普及していきました。これに伴い、セキュリティの重要性も認識され、防御の重要性や脆弱性への対応の必要性が認識されるようになりました。個人でもアンチウイルスソフトの利用が推奨され、企業であればそれに加えてファイアウォールやIDS/IPSなどのセキュリティ製品が導入されるようになっていきました。

セキュリティインシデントも多様化し、Webの改ざんやDDoS攻撃によるホームページの閲覧障害、インターネットを経由したネットワークワームの感染がたびたび発生し、新聞などで報道されるようになりました。ネットワークワームの感染事例で代表的なものには、2001年に発生したCodeRedやNimda、2003年に発生したSQL Slammerなどがあります。これらのネットワークワームは、感染活動が始まると瞬く間に感染が世界中に拡がり、一部では通信の遅延が発生するなど

© Internet Initiative Japan Inc.

の影響が発生しました。当時は、急速に利用が拡がる中で、今ほど回線や機器などのリソースが潤沢でなかったこともあり、こういった大規模な攻撃に対して対応手段が限られていました。現在では、通信インフラの整備や攻撃への対抗手段の整備がなされていますが、IoT機器などの普及により、攻撃にともなう通信量も当時に比べて数百倍の規模となっています。

時が経つにつれ、攻撃は更に複雑巧妙に変貌を遂げてきました。脆弱性を悪用して感染させたPCやルータなどの機器を多数コントロールし、DDoS攻撃などを行うボットネットや、悪意あるプログラムによりユーザの情報などを盗取するマルウェア、感染した端末上の情報を暗号化して人質にとり、身代金を要求するランサムウェアといった攻撃に進化していきました。これらの攻撃においては、攻撃用のシステムが整備されたことで、ダークウェブなどのアンダーグラウンドマーケットでお金さえ払えば、だれもが安易に不正な利益を求めて攻撃を実施できる事態となっています。

セキュリティ対策が進むにつれ、ネットワークから直接攻撃することがしにくくなると、メールなどを介して感染活動を行ったり、悪意あるリンク先に誘導することで感染させるなど、より巧妙な手法へと変わってきました。

今日でも、ネットワーク上を無差別に攻撃するような感染活動も見受けられますが、より対象を絞って効率的に感染活動を行うものや、標的型攻撃やAPTなど、攻撃活動を捕捉しにくくすることで発覚や対応をさせないようにする、より高度な攻撃へと変化していきました。

インターネットが社会基盤のインフラとして使われていく中で、コンピュータリソースや情報の価値が変化したことにより、攻撃の目的も変化してきています。不特定多数の個人が、ある意味おもしろ半分で攻撃を行っていたような時期もありましたが、Anonymousに代表されるようなハクティビストによる特定の主義や主張を広く知らせるための抗議活動、個人やグループなどによる金銭目的での攻撃活動、情報窃取を目的とした組織や国による活動などが確認されるようになりました。

これらの活動は、SNSによる偽の情報やフェイクニュースの拡散など、直接的なネットワーク上の攻撃以外の手段と併せて用いられることで、場合によっては、現実世界においてデモやテロなどを伴うような、実社会での影響を誘発させるだけの力を持つまでになりました。

このような攻撃の高度化と脅威の変化に伴い、ネットワークの内部や境界を監視し、情報を防御するだけでは、攻撃を防ぐことができなくなってきたことから、ゼロトラストモデルなどのように人・モノ・データなどへのアクセス制御を常に行い、かつモニタリングを実施する新たなセキュリティの枠組みなども実装されてきています。

攻撃と防御で考えると、多くの場合で攻撃側に有利な状況が続いています。この状況を打開するためには技術的な対策だけでなく、攻撃の優位性を削ぐ経済的、法的な対策も併せて必要です。インターネットの発展に伴い、日本でも不正アクセス行為の禁止などに関する法律(不正アクセス禁止法)や、刑法に不正指令電磁的記録に関する罪(いわゆるコンピュータ・ウイルスに関する罪)が設けられるなど、必要に応じて法制度の整備が行われてきました。他方でインターネットは国を超えた通信ができることから、複数の国々の間や、世界規模で考えなければならない問題も多数あります。これまでも様々な分野で多く

© Internet Initiative Japan Inc.

の対処や国際協力といった取り組みが行われていますが、今後さらに協調した取り組みが求められています。

マイクロセルと携帯網の相互利用や、衛星通信による接続サービスなど、個々の需要に応じて、使われる通信も多様化してきています。今後、更に自動車に代表される身近な物の接続や、それらのリアルタイム通信による相互連携などがさらに利用されるようになれば、我々の生活はより便利で快適なものとなっていくでしょう。それは同時に通信インフラの重要性を増すことに繋がります。

このような変化に対応するためには、国や通信事業者だけでなく、利用する企業や個人も含めた、新しい仕組みやセキュリティの形が必要になると考えられます。これが正解というものはまだありませんが、今後も続く新たな脅威に継続的に対応していく必要があるでしょう。

DDoS攻撃について

セキュリティ本部セキュリティビジネス開発部
田丸 浩

2000年頃から「DDoS攻撃」という言葉がインターネット関連のニュースに登場するようになり、IIJでもこれまで多くのDDoS攻撃を観測してきました。ここでは、今日に至るまでの約20年間を振り返ると共に、今後の展望について触れてみたいと思います。

私たちが最初のDDoS対策サービスの提供を開始したのは2005年でした。そのきっかけとなったのは、顧客のWebサーバへのDDoS攻撃によって、それを保護していたファイアウォールが過負荷となり、コントロールできない状態となってしまったことでした。ファイアウォールは、通常ではあり得ない数のアクセスや大量のハーフオープンのTCPコネクション発生により、コネクション管理テーブルが溢れたり、膨大なアクセスログを処理するために高負荷な状態となっていました。この私たちが経験した攻撃では、DDoS攻撃の前日あたりに大量のポートスキャンが行われるなど、予兆のようなものがあったために警戒体制をしくことはできたのですが、結果としてDDoS攻撃からお客様のネットワークを守り切ることはできませんでした。この経験から、IIJの設備側で何か対策ができないか、デスクでも、食事をしながらでも、喫煙しながらでも、あれこれ話し合ったことは今でも覚えています。

■ DDoS攻撃の背景

攻撃には何らかの背景がありますが、この背景にも変化が見られます。歴史的な背景を持つ攻撃として、満州事変に関わる中国からの攻撃がありました。2005年あたりから毎年のように観測されていましたが、ここ10年ほどは沈静化しているように見えます。こういった歴史的特異日は攻撃が発生する可能性が高いため、現在もIIJでは攻撃への警戒を続けています。一方で、Anonymousによる抗議活動としてのDDoS攻撃は多くなってきています。日本においても、捕鯨やイルカ漁に対する反対活動や、福島原発の処理水海洋放出に対する抗議活動、中東情勢に応じた日本の立場への反対表明としてのDDoS攻撃がありました。

歴史や政治、動物の愛護活動や環境・人権に関する主義主張といった背景を持つ攻撃では、組織的な攻撃が行われることが多いのですが、最近ではゲームやエンターテイメント産業といったサービス提供者へ個人的な理由によると思われる攻撃が散見されるようになりました。DDoS as a Serviceという言葉を聞いたことがあると思いますが、誰でも簡単に安価にDDoS攻撃を行えるサービスを買うことができるようになったことが影響しています。オンラインゲームにおける個人的な恨みや、社員の何気ないSNS、掲示板への書き込みなど、ちょっとしたことが企業への攻撃の原因となり得ます。

■ DDoS攻撃と防御

DDoS攻撃には、大きく分けてリソース消費型、ボリューム型の2種類があることは既によく知られています。防御を考える場合、別の見方として送信元アドレスを詐称できる攻撃なのかそうでない攻撃なのかという観点があります。

© Internet Initiative Japan Inc.

例えば、TCP Connection Floodや、HTTP Slow、HTTP Request Floodなどは、TCPの接続を確立させる必要があるため送信元アドレスの詐称は比較的困難です。こういった種類の攻撃については、攻撃を受けている状況下においては接続条件を厳しくすることで攻撃をある程度軽減することが期待できます。例えば、TCP接続における無通信状態のタイムアウトを短くしたり、特定の地域からの接続を救うことを優先し、国・地域別IPアドレス割り振り情報を利用したアクセス制限なども、効果が出る可能性があります。

一方、送信元を詐称できる攻撃には、例えば古くから使われてきているTCP SYN Floodがあります。TCPの場合には、送信元が本当に存在するかどうかをTCPの仕様を用いて判定する方法が用いられますが、そのDDoS対策装置などに実装されている確認方法によっては、送信元での再送(HTTP/HTTPSであればブラウザでのリロード)が必要であったり、ファイアウォールがDDoS対策装置が送信する確認用パケットを不正なパケットとして破棄してしまい、誤判定をしてしまうなどの影響を考慮する必要があります。

また、ネットワークに接続された機器の応答を攻撃に悪用するリフレクション型の攻撃については、MemcachedやSSDP、MSSQL、ARD、SNMPなど、通常インターネット上では利用しないプロトコルも多く用いられます。これらはあらかじめフィルタを用意しておくことで容易に攻撃を緩和することができます。DNSやNTPについても、送信元を限定することが可能であれば対策はしやすくなります。送信元詐称を使った攻撃については、私たちISPでもuRPFなどのSAV(Source Address Validation)を導入することで、攻撃発生の防止につなげる努力をしています。

■ DDoS対策の選択

DDoS攻撃からサービスやインフラを保護するためには、DDoS対策専用のアプライアンスをオンプレミスで構築する方法やCDN事業者やクラウドサービス、IIJのようなISPが提供するサービスの利用といった方法があります。

オンプレミスでの対応は、100Gbps超の攻撃が珍しくない昨今では、接続回線の帯域を埋められてしまう可能性が高いため、他のサービスを利用するか組み合わせて利用することが必要となってきます。

CDN事業者の提供するサービスでは、anycastなどを利用する構成で受け口を全世界に広く持つことで攻撃を分散させることができるという特徴があります。また、配信サービスやWAFを合わせて提供していることが多いため、Webシステムとの相性は良いようです。

一方で、IIJのようなISPが提供するサービスでは、公開システム以外にも業務で利用するオフィスのインターネット接続を保護することも可能です。接続サービスを利用しているISPがDDoS対策サービスを提供していない場合には、クラウド型のサービスを利用することでネットワークの保護が可能ですが、経路制御のための制約が付いていることがありますので注意が必要です。

■ 今後の展望

パソコンやサーバの性能が上がり、一般家庭でも1Gbpsや10Gbpsといった帯域でのサービスが提供されるようになりました。監視カメラや家電などいろいろなものがインターネットにつながり、様々なサービスがインターネットを使って利用できるようになっています。一方で、ホームルータや監視カメラ、NASなどのOSやファームウェアがマルウェアに感染してボット化してしまい、これらがDDoS攻撃の発信元になるケースは今も続いています。パソコンだけではなく、こういったデバイスのソフトウェア更新を正しく実施することや、公開サーバにおいてはソフトウェアの更新や脆弱性への対応を速やかに実施することの重要性を私たちIIJが発信し続けることで、DDoS攻撃の被害軽減につながればと思っています。

IIJでは、お客様宛の攻撃防御だけでなく、お客様がDDoS攻撃の加害者とならないよう、通信の方向に関係なく攻撃トラフィックを検知・破棄ができる環境を継続して検討し、安心して安全に利用できるインターネットの構築を引き続き目指します。

© Internet Initiative Japan Inc.

最も悔しいこと

セキュリティ本部長
齋藤 衛

私たちは日々お客様が受けるサイバー攻撃への対応を行ってきていますが、顧客が困っている事案についてある意味自然災害のように扱うことが多くなります。たとえそれが犯罪者によって引き起こされたサイバー犯罪であったとしても、民間のセキュリティ事業者という立場では犯人を捕まえようとはしません。技術的原因を追究し、影響を最小限にとどめ、復旧に向けた努力を重ねますが、その行為者については、司法機関で行うような人物の特定や所在の確認などはせず、単に次の行為に備えるための関連情報の追跡を行う程度にとどまります。

こうした状況の中で、長年にわたってセキュリティに関わってきた者として、犯人を捕まえて懲らしめたいと思った事案が1つだけあります。それは数々の深刻な情報漏えい事故を引き起こしたAntinnyの事案です。

Antinnyとは、P2Pファイル共有ソフトウェアの1つであるWinnyがインストールされたWindows PCの上で動作するマルウェアで、そのPC上のファイルを利用者の意図しない形で外部に送信してしまう機能がありました。Winnyというシステム単体での是非についての議論は別の場に譲りたいと思いますが[*1]、Antinnyの登場によって、Winnyをインストールして利用することが、極端にリスクの高い行為となりました。

このAntinnyというマルウェアは、ファイル名を詐称して動画ファイルなどとユーザに勘違いさせて実行を促します。実際の悪さとしてはPC内の画像やオフィスファイルを検索し、Winnyの送信フォルダに勝手にコピーすることで外部に送信していました。これにより私的な写真が漏えいしてしまう場合や、家に持ち帰った仕事に関係するファイルが漏えいしてしまい、企業などの情報漏えい事故に発展してしまう場合が多数見受けられました。また、月に1回、画面のスナップショットやPC上のファイルを1つの圧縮ファイルにまとめ、コンピュータ著作権協会のWebにある、著作権侵害の相談窓口にアップロードするという動きもしていました。このアップロードによりDDoS攻撃状の大量通信が協会のWebサーバに集中し、閲覧不能となる事態にまで至っていました。

Antinnyのそれぞれの機能は、脆弱性も使わず、特権も利用せず、Winny共有フォルダへのコピーという通常権限のユーザが可能な行為だけで構成されています。Winny利用者を困らせたり、その利用者の情報を著作権管理団体に送付することなどから、Antinnyを作った作者の意図としては、ある程度メッセージ性を持った冗談のようなソフトウェアだったのかもしれません。しかしながらその流行は、人の人生を狂わせたり、企業や組織活動に影響を及ぼしたり、深刻な社会的影響を与える結果になりました。

また、Antinnyについては、各方面で対応が後手に回ってしまい、数年の間猛威を振るっていました。2004年にはISPのセキュリティ団体であったTelecomISAC Japan（現ICT-ISAC Japan）が、コンピュータ著作権協会と共同でDDoS攻撃状の通信の制御を試みて成功していますが、継続的に制御するためには莫大なコストがかかることも示されました。アンチウイルスの世界では、日本固有の現象と捉えられたためか、Winnyという特殊な環境のためか、多くの海外系のアンチウイルス製品によって駆除できるようになるまでには数年の月日が必要でした[*2]。最終的には著作権保護法の改正などにより、Winnyの利用者が激減して、Antinnyもその影響が小さくなり、事案として収束しました。

＊1　Winnyには通信を最適化する機能がなかったため、ネットワーク上に遠距離間の通信を常時発生させ、不必要にネットワークの容量を圧迫し、多くのISP間の接続において輻輳による通信品質の低下を起こしており、通信事業の観点からも副作用の大きいアプリケーションであった。

＊2　トレンドマイクロなど一部のベンダーでしか駆除ができなかったAntinnyについて、マイクロソフトが対応し非常に多くの駆除実績を公開したことで、多くのアンチウイルスベンダーもそれに追従することになった。マイクロソフトには本件の功績に対し、総務省より総務大臣表彰が、コンピュータ著作権協会より感謝状が贈られている。

© Internet Initiative Japan Inc.

以上のようにAntinnyの影響を心配する必要はなくなりましたが、依然としてその作者は捕まっておらず、今日もこの日本において普通に生活していると思うと、非常に悔しい思いが湧いてきます。Antinnyがウイルスに相当するのか、その影響まで罪にできるのかなど、きちんとした議論をしなければならないと思いますし、収束からかなり時間が経っていますので、いまからAntinnyのことを掘り起こして真犯人を捕まえることは難しい状況にあるとは思います。しかしながら、次のAntinnyが現れた時には、適切に対処できる日本という国であってほしいと願っています。

スノーデン事件が与えた影響

セキュリティ本部セキュリティ情報統括室長
根岸 征史

2010年代から2020年代にかけて、社会に大きな影響を及ぼした事件として、エドワード・スノーデン氏による米国家機密の暴露について触れないわけにはいきません。2013年6月、当時米国の国家安全保障局(NSA)に勤務していたスノーデン氏が、トップシークレットを含む大量の機密情報を外部に持ち出し、複数のメディアを通じてこれを暴露するという事件が発生しました。リークされた内容の中でも特に衝撃が大きかったのは、米国を含むFive Eyesと呼ばれる同盟諸国を中心とした、インターネット及び電話回線の包括的な監視の実態が明らかになったことです。2001年に発生したアメリカ同時多発テロ事件を契機とし、米国内ではテロリストの監視を目的とした盗聴や通信の傍受などを強化するための法整備が進められた結果、敵対的な勢力だけでなく米国民や他国にも影響するような遥かに広範囲に及ぶ包括的な監視網が構築され、運用されていたのです。また監視システムの構築や情報収集などにおいて、米国内の主要な通信事業者や、Microsoft、Google、Appleなどの大手Tech企業が、法執行機関からの要請や裁判所命令に基づいて協力していることも分かりました。

こうしたリーク報道を受け、米国だけでなく世界中から行き過ぎた監視によるプライバシーなどの人権侵害を懸念する批判が起こり、その後こうした監視網に対抗するための取り組みが進められました。特に前述のTech企業を中心として通信経路の暗号化の普及が図られ、事業者によるデータセンター間の通信の暗号化や、様々なサービスを提供するサイト側でのデフォルト暗号化などが急速に進みました。その結果、ブラウザからの通信の中で暗号化されたHTTPSの占める割合は2018年には70%、2020年には80%を越えるまでになっています[*3]。2023年のIIJの観測においても、ブロードバンド通信の70%以上を暗号化通信が占めています[*4]。

また2014年から始まったTLS 1.3の標準化作業においては、ネットワーク監視に対抗するために、ハンドシェイクの暗号化や、Forward Secrecyを必須とする暗号方式が採用されました。DNSの通信を暗号化するDNS over TLS(DoT)やDNS over HTTPS(DoH)の標準化も相次いで進められ、現在普及途上にあります。このように、スノーデン氏による暴露は技術標準の仕様策定や普及にも大きな影響を及ぼしています。

通信だけでなくスマートフォンなどの端末への影響もあります。例えばApple、WhatsApp、LINEなどの主要なメッセージングサービスでは、エンドツーエンドの暗号化(E2EE)を採用し、経路上だけでなくサービス提供者でさえもメッセージの内容を知ることができない、強力な暗号化の仕組みをサポートしています。またAppleやGoogleなどは2014年以降スマートフォンの暗号化機能を強化しており、端末上やクラウドサービスに保存される利用者のデータを暗号化して保護しています。このような取り組みにより、利用者のセキュリティやプライバシーは保護されますが、一方で同時に犯罪者もその恩恵を受けることになります。そのため法執行機関が差し押さえた容疑者の端末からデータを取得できず、犯罪捜査の妨げとなる事例が2010年代後半からたびたび報告されています。こうした状況を改善するため、テクノロジー業界が

*3　Firefox Telemetryのデータによる(https://letsencrypt.org/stats/)。
*4　IIR Vol.61「1. 定期観測レポート」を参照(https://www.iij.ad.jp/dev/report/iir/061/01.html)。

© Internet Initiative Japan Inc.

提供する暗号機能に規制をかけようとする動きが、欧米の政府機関によって行われています。

スノーデン氏の暴露により、米国などの情報機関による各国へのサイバー攻撃の活動実態も明るみに出ました。特にNSAは世界有数のサイバー攻撃能力を保持しており、脆弱性の調査、攻撃コードやマルウェアの開発、これらを利用した各国の組織への侵入などのスパイ活動を行っていました。NSAによるこうした活動が、その後私たちにも直接影響を及ぼした事例として、2017年5月に発生したWannaCryの大規模感染があります。WannaCryがWindowsマシンへの感染に利用した攻撃コードやバックドアのプログラムは、The Shadow Brokers というグループが事前にリークしたものを再利用していました。そしてこのリークされたデータはEquation Groupという攻撃グループから盗まれたものであり、この Equation Group は実はNSAによる攻撃活動だったことがその後判明しています。また真偽ははっきりしませんが、リークを行ったThe Shadow Brokersはロシアとの関連が疑われており、米国はWannaCryの攻撃が北朝鮮による仕業であるとして公式に声明を発表しています。このように、私たちの日々の生活に欠かせないインフラであるインターネットにおいて、サイバー犯罪者による活動に加えて、国家を背景とする多数の攻撃者グループによる争いも日常的に行われているのが現状です。こうした様々な活動が何層にも重なってそれぞれが影響を及ぼす複雑なインターネット環境において、誰もが安心して使える安全なネットワークを提供するために何をすればいいのか、非常に大きな課題を私たちは解決していかなければならないと言えます。

セキュリティオペレーションセンターの変遷

セキュリティ本部セキュリティオペレーション部
データ分析課長
中嶋 功

■ 黒から白へ

日本国内のセキュリティオペレーションセンター（以下、SOC）は、2000年ごろからセキュリティ監視の組織あるいは設備として目立つようになりました。当初は多数のディスプレイが並べられた薄暗く窓がない部屋で、セキュリティアナリストと呼ばれるネットワークセキュリティを熟知したエンジニアのみが監視システムへのアクセスを許可されていました。イメージが変化してきたのは2015年頃、一転して明るい色調でSOC設備がリニューアルされるようになり、2017年に刷新されたIIJのSOCもエンジニアが過ごしやすいように作られました（図-1、図-2）。

併せて、高度化する脅威に対応するためにSOCという組織の在り方も大きく変わりました。以前はSOCといえばリアルタイムのセキュリティ監視でしたが、インシデントレスポンスに必要なエンジニアが集まって協調できるよう、SOC内もしくはSOCに近いところに関連するセキュリティエンジニアが置かれることが多くなりました。また、社会における多様性が重視されるようになっていますが、IIJのSOCでもセキュリティインシデントに対応するという1つの目的のもと、多種多様なエンジニアが「そこにいても良い」という価値観が形成されています。

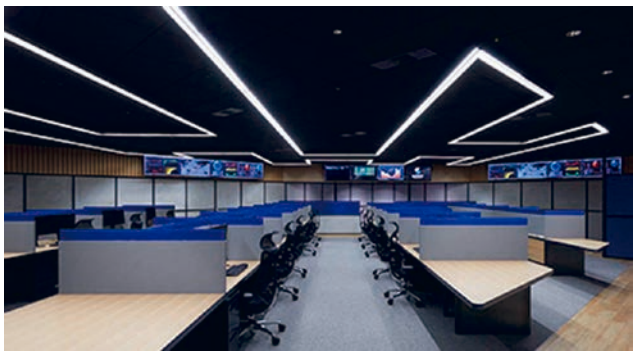


図-1 オペレーションルーム

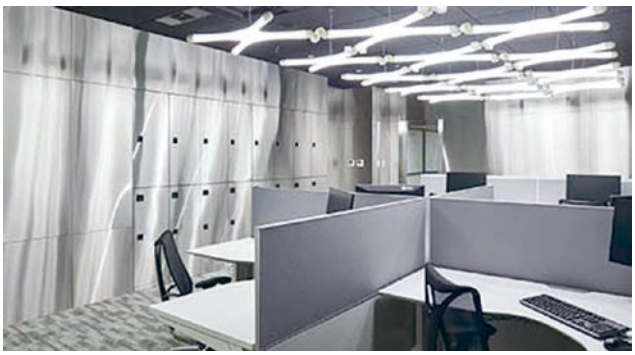


図-2 セキュリティラボ

© Internet Initiative Japan Inc.

■ ネットワークから端末へ

SOCでは様々な機器が監視対象として扱われています。以前はFirewallやIPSなどのネットワーク境界に置かれる箱モノのセキュリティアプライアンスが主流であり、経路上の通信の監視を行っていました。2000年代に発生した重大なセキュリティインシデントの多くはサーバを対象とした攻撃で、事業継続に必要なサーバを保護することがSOCの主な役割でした。

セキュリティアナリストとして変化を感じたのは標的型攻撃に代表されるようなメールを経由した攻撃が流行し始めた頃で、サーバセグメントを監視しているだけでは守りきれないということが直感的に分かりました。近年ではEmotetをはじめとした無差別とも言えるマルウェアによる幅広い対象への攻撃や、組織内部の不正もSOCで監視を行う場合があります。公開サーバへの攻撃は以前と変わらず継続していますが、攻撃対象がクライアント端末へも拡大したことによって、内部から外部への通信、もしくは内部から内部への通信監視も必要となりました。主な監視機器の1つであるFirewallも多機能なUnified Threat Management(UTM)、そしてアプリケーションレイヤーを分析可能なNext Generation Firewall(NGFW)へと進化していったことで通信の可視化が進みました。

一方で、通信自体や通信経路の暗号化も進んでおり、ネットワークではなくEndpoint Detection and Response(EDR)をはじめとした端末のプロセスやログを監視対象とするSOCも少なくありません。直近では脆弱性を悪用した攻撃と並行して、何らかの方法で窃取された個人の認証情報が初期攻撃に利用される事例も増えており、認証情報の管理も課題となっています。

■ SOCエンジニアの役割

SOCの役割は正常状態を維持するのではなく、異常を発見することです。監視システムがセキュリティアラートを発しなくても、疑わしい兆候が見られた場合は調査が必要となります。ネットワーク監視が中心だった頃のSOCでは、熟練のセキュリティアナリストがその知識と経験を持って何の変哲もないログに疑問を抱き、セキュリティインシデントを発見していました。しかし、ログの種類は増え続け、複雑に絡み合ったデータを人手で監視することには限度があります。そして、リアルタイムだけでなく過去のデータを再帰的に調査する必要も出てきており、時間軸の考慮も人手による調査を難しくしています。

現在では、検出のノウハウが監視対象となるセキュリティセンサーの検知ルールとしてあらかじめ組み込まれていたり、Security Information and Event Management(SIEM)のルールに組み込まれたりすることで、エンジニアの負荷低減や技術の一般化がなされるようになりました。AI技術の活用で、データに基づいた分析は人が気づけないことを気づかせ、人が覚えきれないことを補完してくれます。しかしながら、攻撃者も同じようにAI技術の恩恵を受け、新たなセキュリティホールを発見し続けています。

SOCの中心は昔も今も人であり、自動化やシステム化が進んだ現在でもエンジニアの知識と経験がSOCの分析能力に大きな影響を与えます。私たちSOCエンジニアが日々自分自身をアップデートすることで新たな攻撃への対処も可能となるのです。

3.2 最後に

本稿では、セキュリティ関係者にこの30年を振り返ってもらいました。インターネットの進歩はこれで止まっているわけではなく、この数年だけでもテレワーク環境の整備やAI技術の浸透など、私たちの生活を新しいものに変えてきています。今後も変化していくでしょうし、またそれに合わせて事件も起こっていくでしょう。私たちは皆様の生活の安全を守るために、今後も新しい状況の変化に追従し、新たに発生する事案に適切に対応していきたいと考えています。

© Internet Initiative Japan Inc.

December 2023 Vol.61

IIJ
Internet Initiative Japan

株式会社インターネットイニシアティブ(IIJ)について

IIJは、1992年、インターネットの研究開発活動に関わっていた技術者が中心となり、日本でインターネットを本格的に普及させようという構想を持って設立されました。
現在は、国内最大級のインターネットバックボーンを運用し、インターネットの基盤を担うと共に、官公庁や金融機関をはじめとしたハイエンドのビジネスユーザに、インターネット接続やシステムインテグレーション、アウトソーシングサービスなど、高品質なシステム環境をトータルに提供しています。
また、サービス開発やインターネットバックボーンの運用を通して蓄積した知見を積極的に発信し、社会基盤としてのインターネットの発展に尽力しています。

本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されています。本書の一部あるいは全部について、著作権者からの許諾を得ずに、いかなる方法においても無断で複製、翻案、公衆送信等することは禁じられています。当社は、本書の内容につき細心の注意を払っていますが、本書に記載されている情報の正確性、有用性につき保証するものではありません。

本冊子の情報は2023年12月時点のものです。

©Internet Initiative Japan Inc. All rights reserved.
IIJ-MKTG019-0061

株式会社インターネットイニシアティブ
〒102−0071 東京都千代田区富士見2-10-2　飯田橋グラン・ブルーム
E-mail：info@iij.ad.jp　URL：https://www.iij.ad.jp